

QWVTP PZQKZUP

QWVTP PEQKEUP

QWVTS SEQREUS

QWVIS SECRETS

CWVIS SECRETS

CODIS SECRETS

## ABSTRACT

*In this project we will deal with Cryptography.  
First of all, we will expose some mathematical knowledges necessary to understand the calculus of the investigation, including some theorems and their demonstrations. Some of them have been developed specially for this project.*

*Then the two different types of Cryptography will be tackled and some cryptographic algorithms used to encrypt and decrypt information will be revised.  
We will also expose different theoretical attacks to those algorithms.  
We are going to present an implementation of a factorization method that will be used to make one of the theoretical attacks more efficient.*

*Finally, cryptographic protocols will be exposed and a modification of one of them and a new one will be presented, created specially for that project.*

## AGRAÏMENTS

Redactar l'apartat d'agraïments resulta complicat, ja que normalment s'hi ha d'incloure a tantes persones que no se sap per on començar. Així doncs, el redactat d'aquest apartat es farà mantenint un ordre cronològic dels esdeveniments, començant pels més antics i finalitzant pels actuals.

Primer de tot m'agradaria donar les gràcies a l'*Obra Social de Caixa Catalunya* i al programa *Joves i Ciència* per haver confiat en mi d'una forma absolutament professional i anònima; per haver-me donat l'oportunitat de formar part en aquest projecte que va començar l'any 2008 i també per haver-me acceptat com a participant en el Programa de Continuïtat de l'any 2009. Per part meua crec que s'han complert totes les meves expectatives quan vaig decidir apuntar-me a la proposta que em va arribar d'aquest programa per part del professor de Ciències *Aniset Cosialls Manonelles* de l'Institut Guindàvols de Lleida. Ell em va parlar de les *Estades d'Estiu de Ciència de Caixa Catalunya* (E2C3) com una experiència que fomentava la vocació científica i em va animar a participar.

Quan paro a pensar en el passat, em costa arribar a imaginar el que he viscut, les persones que he conegut i els nous coneixements que he adquirit, els quals m'han dut a reafirmar amb més convicció la idea de continuar els meus estudis dins del món de la Ciència.

A efectes pràctics he de dir que si no hagués estat per les E2C3, molt probablement no hauria fet un treball relacionat amb la Criptografia. Però afortunadament aquelles estades d'estiu em van fer redescobrir l'apassionant món dels codis secrets, i des d'aleshores vaig tenir molt clar que el projecte de recerca de Batxillerat tractaria d'això.

Agraeixo al Director de l'Obra Social de Caixa Catalunya, el senyor *Miquel Perdiguer* per la seva col·laboració en el Programa, a *María Calsamiglia*, la Directora del Programa Joves i Ciència de l'Obra Social de Caixa Catalunya pel seu esforç i entusiasme en relació amb aquest Programa i a *Eva Calvés Parcerisas* per la seva col·laboració activa en el Projecte. També he de donar les gràcies a tot l'equip de Professors del Projecte de Matemàtiques de les E2C3, *Angélica*, *Carlos*, *Pablo*, *Mari Luz* i *Ana* pel seu suport i dedicació i per haver contribuït a ampliar els meus coneixements matemàtics i poder gaudir una vegada més d'aquesta disciplina.

Per últim, però no menys important, he de donar les gràcies al meu tutor del treball de recerca i professor de Matemàtiques, *Jordi Sorolla Bardají*, per haver-me donat suport en la realització d'aquest projecte i haver fet possible que s'hagi tirat endavant fins al final. És ben cert que sense la seva ajuda i col·laboració aquesta investigació no hauria estat possible, degut a la complexitat d'alguns dels aspectes que s'han tractat relatius al camp de les Matemàtiques.

De segur que m'he deixat molts noms en aquesta llista, noms de persones que han jugat un paper important en molts dels aspectes de la meua vida. Per aquest motiu demano disculpes a totes aquelles els noms de les quals no he mencionat en aquest escrit.

# ÍNDEX

1. Introducció.....	Pàg. 004
2. Coneixements previs.....	Pàg. 006
2.1. Els nombres primers.....	Pàg. 007
2.2. Calculant equivalències: aritmètica modular.....	Pàg. 012
2.3. Petit Teorema de Fermat.....	Pàg. 022
3. Criptografia Clàssica.....	Pàg. 024
3.1. Introducció.....	Pàg. 024
3.2. Retrospecció: mètodes de xifrat clàssics.....	Pàg. 027
3.2.1. Escítala espartana.....	Pàg. 027
3.2.2. Mètode de xifrat de <i>Polybius</i> .....	Pàg. 030
3.2.3. Mètode de xifrat de <i>Juli Cèsar</i> .....	Pàg. 035
3.3. Criptoanàlisi clàssic: anàlisi de freqüències.....	Pàg. 044
3.3.1. Descripció i procediment.....	Pàg. 044
3.3.2. Taules de freqüències.....	Pàg. 046
3.3.2.1. Taules de freqüències del català.....	Pàg. 046
3.3.2.2. Taules de freqüències del castellà.....	Pàg. 047
3.3.2.3. Taules de freqüències de l'anglès.....	Pàg. 048
3.3.3. Tutorial del software <i>WordCreator</i> .....	Pàg. 049
3.3.4. De la teoria a la pràctica: anàlisi freqüencial.....	Pàg. 055
4. Criptografia Moderna.....	Pàg. 061
4.1. Introducció.....	Pàg. 061
4.2. Deixant el passat enrere: mètodes de xifrat moderns.....	Pàg. 062
4.2.1. Intercanvi de claus de <i>Diffie i Hellman</i> .....	Pàg. 062
4.2.2. Sistema de xifrat <i>ElGamal</i> .....	Pàg. 066
4.2.3. El mètode RSA ( <i>Rivest, Shamir i Adleman</i> ).....	Pàg. 068
4.2.4. L'última frontera: les corbes el·líptiques.....	Pàg. 072
4.2.4.1. Coneixements previs sobre corbes el·líptiques.....	Pàg. 073
4.2.4.2. Intercanvi de claus secretes en canals públics utilitzant CE.....	Pàg. 081
4.2.4.3. Sistema de xifrat <i>ElGamal</i> amb CE.....	Pàg. 084
4.3. Desvetllant els secrets: atacs a DH, RSA i CE.....	Pàg. 086
4.3.1. Atac a l'algoritme bàsic de DH.....	Pàg. 086
4.3.2. Atac al mètode RSA.....	Pàg. 090
4.3.2.1. Atac cíclic.....	Pàg. 090
4.3.2.2. Implementació pròpia de l'atac per força bruta.....	Pàg. 092
4.3.2.2.1. Exposició del programa informàtic propi <i>CleanForce</i> .....	Pàg. 093
4.3.2.2.2. Treballant amb el programa informàtic propi <i>CleanForce</i> .....	Pàg. 100
4.3.3. Atac al mètode d'intercanvi de claus basat en CE.....	Pàg. 101
5. Protocols criptogràfics.....	Pàg. 104
5.1. Introducció.....	Pàg. 104
5.2. Protocols criptogràfics de secrets compartits.....	Pàg. 106
5.2.1. Esquema de <i>Shamir</i> per compartir secrets.....	Pàg. 107
5.2.2. Modificació de l'esquema de <i>Shamir</i> : hiperplans i punts.....	Pàg. 109
5.2.3. Proposta: esquema basat en hiperplans i coeficients.....	Pàg. 111
6. Valoració personal.....	Pàg. 113
7. Referències.....	Pàg. 115

# 1. INTRODUCCIÓ

En l'època en la que estem, l'era de les comunicacions digitals, l'era d'Internet, un individu pot realitzar pràcticament qualsevol cosa que desitgi, ja sigui mantenir una conversació en temps real amb altres individus situats a l'altra punta del món, comprar productes procedents de qualsevol punt del planeta simplement clicant un botó o aconseguir una quantitat inimaginable d'informació referent a qualsevol tema del coneixement humà.

Certament resulta innegable que actualment la tecnologia de comunicacions digitals ofereix grans avantatges. Bàsicament podríem dir que redueix el temps per les comunicacions de veu, dades i imatges; a més, la transmissió de documents es du a terme en temps real, aspecte que juga un paper important en l'augment de la productivitat i la competitivitat de les empreses.

Malauradament, la tecnologia digital, amb tots els seus avantatges, també té un punt dèbil: la vulnerabilitat de la informació que es transmet.

El contingut de les comunicacions digitals sense mesures de seguretat es pot alterar, ja sigui per les deficiències dels canals de comunicació o com a conseqüència de la manipulació de la informació per part dels emissors i receptors d'aquesta.

Resulta evident que es necessita un sistema per protegir les comunicacions i la informació que es transmet, i aquí és on entra en joc la Criptografia.

És molt possible que aquesta paraula sigui desconeguda per la gran majoria de la gent, per tant seria convenient mencionar què és.

A efectes pràctics, la Criptografia consisteix simplement en escriure en clau. És possible que aquesta simple definició no sigui suficient per acabar d'entendre el concepte, per tant, al pensar-ne una de més completa podríem dir que la Criptografia és l'art o ciència de xifrar i desxifrar informació utilitzant tècniques que facin possible l'intercanvi de missatges de manera segura, de tal forma que només puguin ser llegits per les persones a qui van dirigits. Aquest va ser el principal objectiu de la Criptografia: obtenir la confidencialitat dels missatges.

Cal dir que la Criptografia ja es va començar a utilitzar en l'antiguitat, en l'època dels espartans, i també va ser molt utilitzada durant la Segona Guerra Mundial. És més, gràcies a la necessitat dels anglesos per desxifrar les comunicacions secretes dels alemanys va aparèixer el primer ordinador electrònic del món, el *Colossus*, amb el qual es van desxifrar missatges codificats amb dispositius electromecànics com l'*Enigma* o la *Lorenz*, que posteriorment revisarem.

És a dir, que gràcies a la Criptografia existeix l'era informàtica, i aquest és un aspecte que la gran majoria d'individus que utilitzen o han utilitzat un ordinador desconeixen.

Com hem comentat abans, la Criptografia és una ciència, i com a tal disposa d'alguns termes específics. Alguns dels més importants són *text en clar*, informació original que ha de protegir-se; *algoritme de xifrat*, conjunt de passos que s'han de seguir per convertir un text qualsevol en un conjunt de símbols que a primera vista resulten intel·ligibles; *criptograma*, text intel·ligible obtingut a partir d'un procés de xifrat; *clau*, element que ens permetrà recuperar un text en clar a partir d'un criptograma.

Ara que ja hem entrat en matèria, estem en condicions de començar a explorar el món desconegut dels codis secrets i de la Criptografia, i per fer-ho, revisarem els diferents aspectes en els que ens centrarem en aquest projecte.

Començarem exposant tots els coneixements matemàtics que seran indispensables per poder realitzar aquesta investigació. Revisarem alguns teoremes que són fonamentals en l'estudi dels mètodes criptogràfics, tals com el Petit Teorema de Fermat, i aportarem demostracions pròpies per alguns d'ells.

Parlarem dels dos tipus de Criptografia existents, la *Criptografia Clàssica* i la *Criptografia Moderna*, i revisarem alguns dels algorismes de xifrat més coneguts. Fins i tot ens endinsarem en el camp de la Criptografia avançada i estudiarem les corbes el·líptiques.

Exposarem de forma teòrica i pràctica un seguit d'atacs a diversos dels mètodes criptogràfics exposats. Estudiarem de forma detallada i amb exemples un mètode de Criptoanàlisi clàssic, que ens permetrà recuperar un text en clar a partir d'un criptograma sense tenir la clau de xifrat.

Es presentarà una implementació pròpia d'un algorisme de factorització de nombres enters que ens permetrà augmentar l'eficiència d'un dels atacs a un dels mètodes de xifrat moderns. A més, s'escriurà un programa informàtic en llenguatge **Fortran** per tal de dur a terme l'atac de forma ràpida. Tots els fitxers relacionats amb aquest programa informàtic propi es podran descarregar de forma gratuïta de la pàgina web següent:

<http://www.iesguindavols.cat/~eroure>

Finalment es revisaran els *Protocols criptogràfics* i s'aportarà una variació d'un dels sistemes de distribució de secrets que s'estudiaran i també se'n proposarà un de nou, creat específicament per ser presentat en aquest projecte.

Ara ja sabem que farem, per tant estem en condicions de començar a treballar. Ha arribat l'hora aportar un raig de llum al món de la Criptografia per intentar desvetllar alguns dels seus secrets més ben guardats. Així doncs, donem per acabat aquest apartat introductori i comencem a revisar els coneixements previs que ens permetran tirar endavant questa investigació.

## 2. CONEIXEMENTS PREVIS

Ara que ja hem vist quins aspectes de la Criptografia tractarem en aquest treball, necessitarem certs coneixements per poder entendre correctament els diversos procediments que s'exposaran, així com per poder realitzar tots els càlculs sense cap tipus de problema i sense cometre errors.

Per aquest motiu, en aquest bloc aportarem la informació bàsica que necessitem per tirar endavant el treball. Cal remarcar que per alguns procediments que es descriuran en apartats posteriors faran falta alguns coneixements més avançats que els que proporcionarem a continuació, per tant tota la informació que sigui específica per un procediment en concret s'aportarà en l'apartat referent a aquest, per tal d'aconseguir una estructura més clara i entenedora.

Bàsicament podem dividir aquest capítol en tres grans parts. En la primera parlarem de nombres primers i comentarem algunes qüestions relacionades amb aquests, i que seran de gran importància per poder comprendre alguns apartats del treball.

En la segona part ens centrarem en l'aritmètica modular, que serà crucial per poder realitzar tots els càlculs d'aquest projecte, ja que sempre estarem treballant amb aquest tipus d'aritmètica.

Tot i això, cal remarcar que no veurem tots els aspectes relacionats amb aritmètica modular, ja que la complexitat d'alguns d'ells és considerable. Per tant només tractarem aquells que siguin necessaris per realitzar els càlculs del treball.

En la tercera part exposarem el Petit Teorema de Fermat, que serà indispensable per comprendre el funcionament d'alguns dels procediments de xifrat que s'exposaran en apartats posteriors. Aquesta part requerirà d'una comprensió total de les dues parts anteriors, per tal de poder entendre-la, ja que el Petit Teorema de Fermat està basat en nombres primers i aritmètica modular.

## 2.1. Els nombres primers

Els nombres primers són un subconjunt dels nombres naturals  $\mathbb{N}$ , i aquests nombres són, a la vegada, un subconjunt dels nombres enters  $\mathbb{Z}$ .

Els nombres enters són una generalització del conjunt de nombres naturals, que inclou aquells nombres que expressen quantitats senceres, inclosos negatius i zero.

Abans d'entrar de ple en el món dels nombres primers per revelar-ne els secrets hem de saber què és exactament un nombre primer, ja que sinó no podrem comprendre els diferents aspectes relacionats amb aquest tipus de nombres.

**Definició 2.1.1.** En matemàtiques, es coneix com a *nombre primer* tot nombre natural diferent de zero i de 1 que únicament té dos divisors naturals diferents, que són el número 1 i ell mateix. Aquests nombres es contraposen amb els *nombres compostos*, que són aquells que tenen altres divisors naturals a part d'ells mateixos, que anomenem *factors*.

Cal remarcar que el número 1 és un cas especial. La qüestió de si el número 1 s'ha de considerar un nombre primer o no està basada en una convenció.

Ambdues postures tenen els seus avantatges i els seus inconvenients. De fet, fins al segle XIX, la majoria de matemàtics el consideraven un nombre primer.

Actualment, la comunitat matemàtica s'inclina per no considerar-lo en la llista dels nombres primers. Aquesta convenció fa que no hi hagi exemples pràctics que contradiguin el Teorema Fonamental de l'Aritmètica.

**Teorema Fonamental de l'Aritmètica.** *Tot nombre natural té una representació única com a producte de factors primers, sense tenir en compte l'ordre d'aquests factors.*

A continuació s'exposen alguns exemples de nombres primers, més concretament, el conjunt de tots els nombres primers menors que 100:

2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47, 53, 59, 61, 67, 71, 73, 79, 83, 89, 97

La propietat de ser primer es denomina primalitat. De vegades es parla de nombre primer imparell per a referir-se a qualsevol nombre primer major que 2, ja que aquest és l'únic nombre primer parell.

L'estudi dels nombres primers és una part important de la teoria de nombres, la branca de les matemàtiques que comprèn l'estudi dels nombres naturals. Els nombres primers estan presents en algunes conjectures centenàries tals com la Conjectura de Goldbach.

**Conjectura de Goldbach.** *Tot nombre natural parell major que 2 pot ser escrit com a suma de dos nombres primers.*

La distribució dels nombres primers és un tema recurrent d'investigació en la teoria de nombres: si es consideren nombres individuals, els nombres primers semblen estar distribuïts aleatòriament, és a dir, que no es coneix una fórmula que permeti generar tots els nombres primers.

Un es pot plantejar la qüestió de si aquest conjunt de nombres és infinit. És més, hi ha un teorema que recull aquesta qüestió, el Teorema d'Euclides, que tot seguit s'enuncia, juntament amb una de les diverses demostracions que existeixen. [12.1]

**Teorema d'Euclides.** *El conjunt format pels nombres primers és infinit.*

***Demostració:***

Considerem el conjunt format per tots els nombres primers i suposem que és un conjunt finit, en el qual el nombre primer més gran és  $p_n$ , així doncs tenim que  $P = \{p_1, p_2, \dots, p_n\}$ .

Considerem un nombre  $q$  que sigui el producte de tots els nombres primers del conjunt més 1, és a dir, que  $q = (p_1 p_2 \dots p_n) + 1$ . Aquest nombre pot ser primer o compost.

Si és un nombre primer, no pertany al conjunt  $P$  de tots els nombres primers, per tant  $q$  no pot ser un nombre primer, ja que havíem suposat que tot nombre primer existent formaria part del conjunt  $P$ . Així doncs,  $q$  ha de ser un nombre compost.

Si  $q$  és un nombre compost, pel Teorema fonamental de l'aritmètica, ha d'existir com a mínim un nombre primer  $p$  que divideixi a  $q$ . I com que havíem suposat que tots els nombres primers que existeixen pertanyen al conjunt  $P$ ,  $p$  ha de ser algun nombre primer  $p \in P$ .

Per tant, si  $p|q$ ,  $p|[(p_1 p_2 \dots p_n) + 1]$ . Com que havíem suposat que  $p \in P$ ,  $p|(p_1 p_2 \dots p_n)$ , però  $p$  no divideix a 1, per tant  $p$  tampoc dividirà a  $q$ . Així doncs, trobem que no hi haurà cap nombre primer  $p \in P$  que divideixi a  $q$ , per tant  $p$  ha de ser un nombre primer que no pertany al conjunt  $P$ . **Q.E.D.**

D'aquesta forma es demostra que no pot existir un conjunt que contingui tots els nombres primers i que sigui finit, per tant també queda demostrat que el conjunt de nombres primers és infinit.

Passem a comentar alguns dels diferents tipus de nombres primers que podem trobar, i com identificar-los.

## Nombres primers de Fermat

Primer de tot començarem exposant els nombres primers de Fermat. Un nombre primer es considerarà primer de Fermat si es pot escriure de la forma següent:

$$F_n = 2^{2^n} + 1, n \in \mathbb{N}.$$

En cas que un nombre es pugui expressar de la forma anterior però no sigui un nombre primer, es considerarà nombre de Fermat.

Cal remarcar que actualment només es coneixen 5 nombres primers de Fermat, que són 3, 5, 17, 257 i 65537, obtinguts amb els valors de  $n = 0, 1, 2, 3, 4$ , respectivament.

## Nombres primers de Mersenne

Seguidament exposarem els nombres primers de Mersenne. Un nombre primer es considerarà primer de Mersenne si es pot escriure de la forma següent:

$$M_n = 2^n - 1, n \in \mathbb{N}.$$

En cas que un nombre es pugui expressar de la forma anterior però no sigui un nombre primer, es considerarà nombre de Mersenne.

Si comparem l'expressió anterior amb la dels nombres de Fermat veiem que hi ha una gran semblança entre elles.

Cal remarcar que actualment només es coneixen 47 nombres primers de Mersenne, sent el més gran de tots ells  $M_{43112609} = 2^{43112609} - 1$ . Altres exemples de nombres primers de Mersenne són 3, 7, 31, 127, 8191, 131071, 524287, 2147483647 i 2305843009213693951, generats a partir dels valors  $n = 2, 3, 5, 7, 13, 17, 19, 31, 61$ , respectivament.

Com a curiositat cal afegit que els nombres de Mersenne tenen representacions binàries formades per successions de números 1. Aquests nombres es coneixen amb el nom de nombres *repunits* (de l'anglès *repeated unit*, unitat repetida).

El nombre de números 1 de la representació binària de cadascun dels nombres de Mersenne correspon al valor de  $n$  amb què es generen aquests nombres.

Per exemple el nombre  $M_3 = 2^3 - 1 = 7$  serà equivalent a 111 en binari, ja que s'ha generat amb el valor  $n = 3$ :

$$1 \cdot 2^2 + 1 \cdot 2^1 + 1 \cdot 2^0 = 7$$

## Nombres primers de Wagstaff

Un nombre primer serà considerat primer de Wagstaff si es pot escriure de la forma següent:

$$p_q = \frac{2^q + 1}{3},$$

on  $q$  també ha de ser un nombre primer.

Aquests nombres primers estan estrictament relacionats amb els nombres de Mersenne, no necessàriament primers. La relació entre els uns i els altres s'expressa de la següent forma:

$$p_q = \frac{M_q + 2}{3}.$$

Alguns exemples de nombres primers de Wagstaff són 3, 11, 43, 683, 2731, 43691, 174763, 2796203, 715827883 i 2932031007403, generats a partir dels valors  $q = 3, 5, 7, 11, 13, 17, 19, 23, 31, 43$ , respectivament.

Actualment s'ha aconseguit demostrar la primalitat dels nombres de Wagstaff generats amb valors de  $q$  menors o iguals que 42737.

A dia d'avui el major nombre de Wagstaff probablement primer és  $p_{986191} = \frac{2^{986191} + 1}{3}$ , i va ser descobert al 2008.

## Nombres primers de Sophie Germain

Un nombre primer  $p$  serà considerat primer de Sophie Germain si  $2p + 1$  també és un nombre primer.

Es creu que existeixen infinits nombres primers de Sophie Germain, tot i que encara no s'ha pogut demostrar.

A continuació es mostren els 190 nombres primers de Sophie Germain que hi ha entre els 10000 primers nombres naturals:

2, 3, 5, 11, 23, 29, 41, 53, 83, 113, 131, 173, 179, 191, 233, 239, 251, 281, 293, 359, 419, 431, 443, 491, 509, 593, 641, 653, 659, 683, 719, 743, 761, 809, 911, 953, 1013, 1019, 1031, 1049, 1103, 1223, 1229, 1289, 1409, 1439, 1451, 1481, 1499, 1511, 1559, 1583, 1601, 1733, 1811, 1889, 1901, 1931, 1973, 2003, 2039, 2063, 2069, 2129, 2141, 2273, 2339, 2351, 2393, 2399, 2459, 2543, 2549, 2693, 2699, 2741, 2753, 2819, 2903, 2939, 2963, 2969, 3023, 3299, 3329, 3359, 3389, 3413, 3449, 3491, 3539, 3593, 3623, 3761, 3779, 3803, 3821, 3851, 3863, 3911, 4019, 4073, 4211, 4271, 4349, 4373, 4391, 4409, 4481, 4733, 4793, 4871, 4919, 4943, 5003, 5039, 5051, 5081, 5171, 5231, 5279, 5303, 5333, 5399, 5441, 5501, 5639, 5711, 5741, 5849, 5903, 6053, 6101, 6113, 6131, 6173, 6263, 6269, 6323, 6329, 6449, 6491, 6521, 6551, 6563, 6581, 6761, 6899, 6983, 7043, 7079, 7103, 7121, 7151, 7193, 7211, 7349, 7433, 7541, 7643, 7649, 7691, 7823, 7841, 7883, 7901, 8069, 8093, 8111, 8243, 8273, 8513, 8663, 8693, 8741, 8951, 8969, 9029, 9059, 9221, 9293, 9371, 9419, 9473, 9479, 9539, 9629, 9689 i 9791.

Actualment el nombre primer de Sophie Germain més gran que es coneix és el número  $48047305725 \cdot 2^{172403} - 1$ , que té 51910 dígits i va ser descobert al 2007.

### Nombres primers pitagòrics

El conjunt dels nombres pitagòrics és el conjunt de nombres que poden ser la longitud de la hipotenusa d'un triangle rectangle de costats enters. Per explicar això hem de tenir en compte el Teorema de Pitàgores.

**Teorema de Pitàgores.** *En un triangle rectangle, el quadrat de la hipotenusa (costat de major longitud del triangle) és igual a la suma dels quadrats dels catets (els altres dos costats del triangle). És a dir, que  $h^2 = a^2 + b^2$ .*

A partir d'aquest teorema s'introdueix el concepte de terna pitagòrica entera, que consisteix en tres nombres enters positius  $a$ ,  $b$  i  $h$  de la forma  $(a, b, h) = (s^2 - t^2, 2st, s^2 + t^2)$ ,  $\forall s, t \in \mathbb{Z}$  que verifiquen l'expressió  $h^2 = a^2 + b^2$ .

Quan  $h$  sigui un nombre primer de la forma  $4n+1$  ( $s^2 = 4n$ ;  $t^2 = 1$ ) per algun  $n \in \mathbb{Z}$  direm que  $h$  és un nombre primer pitagòric.

Els primers nombres primers pitagòrics són 5, 13, 17, 29, 37, 41, 53, 61, 73, 89, 97, 101, 109 i 113, generats a partir dels valors  $n = 1, 3, 4, 7, 9, 10, 13, 15, 18, 22, 24, 25, 27, 28$ , respectivament.

Com a curiositat afegir que els nombres primers pitagòrics són els únics nombres primers que admeten una representació única com a suma de dos quadrats, a excepció del número 2.

### Nombres primers de Wieferich

Un nombre primer  $p$  serà considerat primer de Wieferich si  $p^2 \mid (2^{p-1} - 1)$ . Actualment els únics nombres primers de Wieferich que es coneixen són 1093 i 3511. Si n'hi ha més, hauran de ser superiors a  $1.25 \cdot 10^{15}$ .

S'ha conjeturat que només existeix un nombre finit de nombres primers de Wieferich, tot i que actualment no s'ha pogut demostrar. Per últim, cal comentar el motiu de la utilització de nombres primers en els procediments criptogràfics.

Bàsicament podem afirmar que el motiu principal és la dificultat que presenta la tasca de factoritzar un nombre gran. Així, coneguts els factors és fàcil aconseguir el nombre, però no a l'inrevés.

Actualment amb els ordenadors dels que disposem podem calcular nombres primers grans de forma relativament fàcil i els podem multiplicar entre ells sense cap tipus de problema, però a l'intentar factoritzar aquests productes la cosa canvia, de tal forma que fins i tot els ordenadors més potents del món poden necessitar mesos i en alguns casos anys per arribar a factoritzar-los.

## 2.2. Calculant equivalències: aritmètica modular

Considerem el conjunt de nombres enters  $\mathbb{Z}$ :

$$\{\dots, -5, -4, -3, -2, -1, 0, 1, 2, 3, 4, 5, \dots\}.$$

Dins de  $\mathbb{Z}$  podem considerar subconjunts del tipus  $N\mathbb{Z} = \{\text{múltiples de } N\}$ .  
Per exemple  $3\mathbb{Z} = \{\text{múltiples de } 3\}$  és el subconjunt de  $\mathbb{Z}$  format pels nombres en claudàtors:

$$\{\dots, [-6], -5, -4, [-3], -2, -1, [0], 1, 2, [3], 4, 5, [6], \dots\}.$$

Es diu que  $N\mathbb{Z}$  és un ideal de  $\mathbb{Z}$  en tant que es compleix la següent propietat:

- Si  $a \in \mathbb{Z}$  i  $k \in N\mathbb{Z} \Rightarrow ak \in N\mathbb{Z}$ .

És clar que entre dos nombres consecutius de  $N\mathbb{Z}$  hi ha sempre la mateixa quantitat d'elements de  $\mathbb{Z}$ , i es caracteritzen perquè els residus  $r$  de la divisió entera d'un nombre  $a \in \mathbb{Z}$  entre  $N$  van repetint els seus valors de forma periòdica.

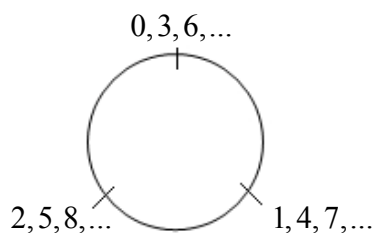
Per exemple,  $\frac{0}{3} = 0, r = 0$ ;  $\frac{1}{3} = 0, r = 1$ ;  $\frac{2}{3} = 0, r = 2$ ;

$$\frac{3}{3} = 1, r = 0; \frac{4}{3} = 1, r = 1; \frac{5}{3} = 1, r = 2;$$

$$\frac{6}{3} = 2, r = 0; \frac{7}{3} = 2, r = 1; \frac{8}{3} = 2, r = 2;$$

$$\{\dots, [-6], -\underline{5}, -\underline{\underline{4}}, [-3], -\underline{2}, -\underline{\underline{1}}, [0], \underline{1}, \underline{\underline{2}}, [3], \underline{4}, \underline{\underline{5}}, [6], \dots\}$$

En realitat podríem pensar que estem classificant els nombres enters segons el residu de la divisió  $a \div 3$  i per tant més que una representació en línia recta els podríem representar en una circumferència:



Els possibles residus són  $\{0, 1, 2\}$ .

En general, els possibles residus de dividir  $x \div N$  són  $\{0, 1, 2, \dots, N-1\}$ .

**Definició 2.2.1.** Es defineix el conjunt  $\mathbb{Z}/N\mathbb{Z}$  com el conjunt de residus que resulten de dividir un nombre enter  $a$  entre  $N$ . Es llegeix “z mòdul N”.

$$\mathbb{Z}/N\mathbb{Z} = \{0, 1, \dots, N-1\}.$$

Es diu que dos nombres  $a$  i  $b$  són congruents mòdul  $N$  si els residus de les divisions  $a \div N$  i  $b \div N$  són iguals. Equivalentment,  $a - b$  és múltiple de  $N$ .

S’expressa  $a \equiv b \pmod{N}$ , i es llegeix “a és congruent amb b mòdul N”.

La congruència mòdul  $N$  de nombres enters és una relació d’equivalència en el sentit que es compleixen les següents propietats:

- **Reflexivitat:**  $a \equiv a \pmod{N}$
- **Simetria:** si  $a \equiv b \pmod{N}$ , aleshores  $b \equiv a \pmod{N}$
- **Transitivitat:** si  $a \equiv b \pmod{N}$  i  $b \equiv c \pmod{N}$ , aleshores  $a \equiv c \pmod{N}$

A part, també es compleix la propietat de cancel·lació:

- Si  $(k, a, b) \in \mathbb{Z}$ ,  $k$  no és divisible per un nombre primer  $p$  i  $ka \equiv kb \pmod{p}$ , aleshores  $a \equiv b \pmod{p}$ .

Cada nombre enter és congruent amb una quantitat infinita de nombres  $\pmod{N}$ . Tots aquests nombres formen el que s’anomena una classe d’equivalència mòdul  $N$ . Com a representant de cada classe d’equivalència es pren aquell element de la classe que està entre 0 i  $N-1$ .

Així es pot interpretar  $\mathbb{Z}/N\mathbb{Z} = \{0, 1, \dots, N-1\}$  com el conjunt de totes les classes d’equivalència de nombres enters mòdul  $N$ .

A simple vista pot semblar que el concepte d'aritmètica modular no té cap aplicació en la vida quotidiana, però això no és així. És més, fins i tot podem afirmar que tothom l'utilitza diàriament i de forma rutinària, tot i que ignoren que l'estan fent servir.

L'exemple d'aplicació més comú de l'aritmètica modular en una situació de la vida quotidiana és el càlcul de les equivalències entre les hores d'un rellotge digital i les hores d'un rellotge analògic.

Un rellotge digital marca des de les 0 hores fins a les 23 hores (les 24 hores vindrien a ser les 0 hores, ja que  $24 \equiv 0(\text{mod } 12)$ ), mentre que un rellotge analògic només marca des de les 0 hores fins a les 11 hores (les 12 hores vindrien a ser les 0 hores, ja que  $12 \equiv 0(\text{mod } 12)$ ).

Així doncs cal desenvolupar un procediment que ens permeti conèixer la correspondència de les hores dels dos rellotges. El que la gent acostuma a fer és restar 12 a les hores del rellotge digital que siguin majors que 12, i així obtenen el valor de les hores del rellotge analògic.

Un pot pensar que tot es redueix a una simple resta, però en realitat s'estan calculant congruències en mòdul 12. El que realment s'està fent és aplicar l'equació modular següent:

$$h_d \equiv h_a(\text{mod } 12)$$

Així doncs, per saber quina hora analògica  $h_a$  li correspon a una hora digital  $h_d$ , agafem aquesta última (sense la part dels minuts, que no varia al passar de digital a analògic) i mirem quin residu  $r$  deixa en mòdul 12, de tal forma que  $r = h_a$ .

Per exemple, suposem que ens hem descuidat el rellotge a casa i necessitem saber quina hora és. Al passar per davant d'una farmàcia veiem que són les 17:23 hores. Agafem la part de les hores, que és 17 i apliquem l'equació modular anterior, de tal forma que obtenim el següent:

$$17 \equiv 5(\text{mod } 12)$$

Per tant arribem a la conclusió que les 17:23 hores corresponen a les 5:23 hores de la tarda.

Com a curiositat cal mencionar que a vegades a l'aritmètica modular se la sol anomenar *aritmètica del rellotge*, ja que els valors congruents dels nombres es repeteixen un cop sobrepassen el valor del mòdul de treball, de la mateixa manera que les hores es tornen a repetir un cop se superen les 12 o les 24 hores, depenent del rellotge que s'utilitzi.

Les operacions a  $\mathbb{Z}/N\mathbb{Z}$  venen induïdes per les operacions a  $\mathbb{Z}$ .

## Operació suma a $\mathbb{Z}/N\mathbb{Z}$

Per sumar  $n$  nombres treballant en mòdul  $N$  es poden seguir dos procediments:

1. **Sumar els  $n$  nombres de forma habitual i posteriorment calcular la congruència en mòdul  $N$  del resultat.**
2. **Calcular les congruències en mòdul  $N$  dels nombres que siguin majors que  $N$ , sumar la nova successió de nombres i finalment tornar a calcular la congruència en mòdul  $N$  del resultat.**

Vegem un exemple pràctic per tal de posar en pràctica aquests dos procediments.

Suposem que tenim l'expressió següent:  $x \equiv 2 + 5 + 7 + 11 \pmod{3}$ .

Volem calcular el valor de  $x$ , i per fer-ho, hem de calcular les sumes i passar el resultat a mòdul 3.

Aplicant el primer procediment descrit anteriorment obtenim el següent:

$$x \equiv 2 + 5 + 7 + 11 \equiv 25 \equiv 1 \pmod{3}.$$

D'aquesta forma obtenim que  $x \equiv 1 \pmod{3}$ .

A continuació calcularem el valor de  $x$  aplicant el segon procediment, és a dir, que abans de sumar calcularem les congruències dels elements de la successió que siguin majors que el mòdul de treball. D'aquesta forma obtenim el següent:

$$x \equiv 2 + 5 + 7 + 11 \equiv 2 + 2 + 1 + 2 \equiv 7 \equiv 1 \pmod{3}.$$

Com podem observar, obtenim el mateix resultat amb els dos procediments. Cal dir que aquest segon procediment requereix un major nombre d'operacions per poder calcular el resultat desitjat, i no resulta pràctic quan els nombres que es volen sumar tenen pocs dígit.

No obstant això, aquest procediment ens serà extremadament útil quan vulguem sumar nombres més grans, i aleshores ens convindrà calcular les congruències en mòdul  $N$  abans de començar a sumar, per tal de facilitar la tasca d'arribar al resultat desitjat.

Passem a descriure els procediments que s'han de seguir per poder restar elements treballant en mòdul  $N$ . Cal dir que són procediments molt semblants als de la suma, tot i que s'hi introdueix una petita variació.

## Operació resta a $\mathbb{Z}/N\mathbb{Z}$

Per poder operar les restes en mòdul  $N$  primer cal aclarir un petit aspecte que ens permetrà comprendre els procediments.

Hem de tenir clar que  $a - b = a + (-b)$ , és a dir, que restar un nombre  $b$  a un nombre  $a$  és sumar l'oposat del nombre  $b$  al nombre  $a$ .

Per tenir clara l'afirmació anterior, cal tenir en compte la definició d'element oposat.

**Definició 2.2.2.** L'element oposat  $(-b)$  d'un nombre  $b$  és aquell que verifica l'expressió  $b + (-b) = 0$ . En aritmètica modular, l'element oposat  $(-b)$  d'un nombre  $b$  és aquell que verifica l'expressió  $b + (-b) \equiv 0 \pmod{N}$ ,  $(-b) \in \{0, 1, 2, \dots, N-1\}$ .

Vegem un exemple pràctic per tal de comprendre el concepte d'element oposat en aritmètica modular.

Suposem que tenim la següent expressió:  $x \equiv -1 \pmod{3}$ . Tal i com podem observar,  $(-1) \notin \{0, 1, 2, \dots, N-1\}$ , per tant haurem de calcular el valor congruent de  $(-1)$  que pertanyi al conjunt mencionat.

Així doncs, estem buscant un nombre que pertanyi al conjunt  $\{0, 1, 2\}$  i que al ser sumat a 1 ens doni un resultat congruent amb 0 en mòdul 3. En aquest cas resulta bastant fàcil trobar aquest valor. Podem observar que és 2, ja que  $1 + 2 \equiv 3 \equiv 0 \pmod{3}$ . De forma general podem escriure el següent:

$$b + (-b) \equiv b + (N - b) \pmod{N}.$$

Podem observar que la petita variació introduïda no invalida la congruència, ja que  $N \equiv 0 \pmod{N}$ , i a més ens soluciona el problema del càlcul de l'element oposat, ja que el podem calcular operant  $N - b$ , a més  $(N - b) \in \{0, 1, 2, \dots, N-1\}$ .

Així doncs, per calcular una resta primer calcularem l'element oposat del nombre negatiu i posteriorment sumarem els termes aplicant els procediments de la suma.

Vegem un exemple pràctic per tal d'aclarir els conceptes.

Suposem que tenim la següent expressió:  $x \equiv -2 - 5 - 7 + 11 \pmod{3}$ . Calculem els elements oposats dels termes negatius, de tal forma que obtenim el següent:

$$x \equiv -2 - 5 - 7 + 11 \equiv (3 - 2) + (3 - 5) + (3 - 7) + 11 \equiv 1 - 2 - 4 + 11 \pmod{3}.$$

Tal i com podem veure, a l'aplicar el procediment de càlcul de l'element oposat no hem pogut eliminar tots els signes negatius de l'expressió, per tant tornem a aplicar el procediment fins que no quedin signes negatius a l'expressió i calculem les congruències, de tal forma que obtenim el següent:

$$x \equiv -2 - 5 - 7 + 11 \equiv 1 - 2 - 4 + 11 \equiv 1 + 1 + 2 + 2 \equiv 0 \pmod{3}.$$

Una altra forma d'arribar al resultat final és calcular inicialment totes les operacions de forma normal, com si no estiguéssim treballant en mòdul, i finalment calcular la congruència del resultat, de tal forma que obtindríem el següent:

$$x \equiv -2 - 5 - 7 + 11 \equiv -3 \equiv 3 - 3 \equiv 0 \pmod{3}.$$

El conjunt  $\mathbb{Z}/N\mathbb{Z}$  té una estructura de grup abelià amb l'operació suma (+), en el sentit que es compleixen les següents propietats:

1. **Associativa:**  $(a+b)+c = a+(b+c)$ .
2. **Commutativa:**  $a+b = b+a$ .
3. **Element neutre:** (0) tal que  $a+0 = 0+a = a$ .
4. **Element oposat:**  $(-b)$  tal que  $b+(-b) = (-b)+b = 0$ .

Per exemple, a  $\mathbb{Z}/3\mathbb{Z} = \{0,1,2\}$ ,  $-1 \equiv 2 \pmod{3}$  i  $-2 \equiv 1 \pmod{3}$ . A  $\mathbb{Z}/4\mathbb{Z} = \{0,1,2,3\}$ ,  $-1 \equiv 3 \pmod{4}$ ,  $-2 \equiv 2 \pmod{4}$  i  $-3 \equiv 1 \pmod{4}$ .

### **Multiplicació a $\mathbb{Z}/N\mathbb{Z}$**

Multiplicar nombres en mòdul  $N$  és molt simple, i per fer-ho es poden seguir uns procediments molt semblants als de la suma:

1. **Multiplicar els  $n$  nombres de forma habitual i posteriorment calcular la congruència en mòdul  $N$  del resultat.**
2. **Calcular les congruències en mòdul  $N$  dels nombres que siguin majors que  $N$ , multiplicar els nous termes de la successió i finalment tornar a calcular la congruència en mòdul  $N$  del resultat.**

Vegem un exemple pràctic per tal de posar en pràctica aquests dos procediments.

Suposem que tenim l'expressió següent:  $x \equiv 2 \cdot 5 \cdot 7 \cdot 11 \pmod{3}$ .

Volem calcular el valor de  $x$ , i per fer-ho, hem de calcular productes i passar el resultat a mòdul 3.

Aplicant el primer procediment descrit anteriorment obtenim el següent:

$$x \equiv 2 \cdot 5 \cdot 7 \cdot 11 \equiv 770 \equiv 2 \pmod{3}.$$

D'aquesta forma obtenim que  $x \equiv 2 \pmod{3}$ .

A continuació calcularem el valor de  $x$  aplicant el segon procediment, és a dir, que abans de multiplicar calcularem les congruències dels elements de la successió que siguin majors que el mòdul de treball. D'aquesta forma obtenim el següent:

$$x \equiv 2 \cdot 5 \cdot 7 \cdot 11 \equiv 2 \cdot 2 \cdot 1 \cdot 2 \equiv 8 \equiv 2 \pmod{3}.$$

Com podem observar, obtenim el mateix resultat amb els dos procediments. Cal dir que aquest segon procediment requereix un major nombre d'operacions per poder calcular el resultat desitjat, i no resulta pràctic quan els nombres que es volen multiplicar tenen pocs dígitos.

No obstant això, aquest procediment ens serà extremadament útil quan vulguem multiplicar nombres més grans, i aleshores ens convindrà calcular les congruències en mòdul  $N$  abans de començar a calcular els productes, per tal de facilitar la tasca d'arribar al resultat desitjat.

El producte  $(\cdot)$  compleix les següents propietats:

1. **Associativa:**  $(a + b) + c = a + (b + c)$ .
2. **Commutativa:**  $a + b = b + a$ .
3. **Element neutre:** (1) tal que  $a \cdot 1 = 1 \cdot a = a$ .
4. **Element invers:**  $(b^{-1})$  tal que  $bb^{-1} = b^{-1}b = 1$ .

Cal afegir que no tot element té invers. Per exemple a  $\mathbb{Z}/4\mathbb{Z} = \{0, 1, 2, 3\}$ ,  $3^{-1} \equiv 3 \pmod{4}$ , ja que  $3 \cdot 3 = 9 \equiv 1 \pmod{4}$ . Però per altra banda no existeixen valors de  $x$  tals que verifiquin l'expressió  $2x \equiv 1 \pmod{4}$ , per tant  $2^{-1}$  no existeix a  $\mathbb{Z}/4\mathbb{Z}$ .

## Divisió a $\mathbb{Z}/N\mathbb{Z}$

Per poder operar les divisions en mòdul  $N$  primer hem d'aclarir un petit aspecte que ens permetrà comprendre els procediments.

Primer de tot cal tenir clar que  $a \div b = ab^{-1}$ , és a dir, que dividir un nombre  $a$  entre un nombre  $b$  no és res més que multiplicar el nombre  $a$  per l'element invers  $b^{-1}$  del nombre  $b$ .

Per tenir clara l'afirmació anterior, cal tenir en compte la definició d'element invers.

**Definició 2.2.3.** L'element invers  $b^{-1}$  d'un nombre  $b$  és aquell que verifica l'expressió  $bb^{-1} = 1, b \neq 0$ . En aritmètica modular, l'element invers  $b^{-1}$  d'un nombre  $b$  és aquell que verifica l'expressió  $bb^{-1} \equiv 1 \pmod{N}$ . Només existirà  $b^{-1}$  quan  $\text{mcd}(b, N) = 1$ , per tant  $b^{-1}$  sempre existirà si  $b \neq 0$  i si  $N$  és un nombre primer, ja que, en aquest cas,  $\text{mcd}(b_i, N) = 1, \forall b_i \in \{1, 2, \dots, N-1\}$ .

Vegem un exemple pràctic per tal de comprendre el concepte d'element invers en aritmètica modular.

Suposem que tenim la següent expressió:  $5x \equiv 1 \pmod{7}$ . Tal i com podem observar,  $\text{mcd}(5, 7) = 1$ , per tant existirà l'element invers de  $5 \pmod{7}$ . Així doncs haurem de calcular el valor congruent de  $5^{-1}$  que pertanyi al conjunt mencionat.

Així doncs, estem buscant un nombre que pertanyi al conjunt  $\{1, 2, 3, 4, 5, 6\}$  i que al ser multiplicat per 5 ens doni un resultat congruent amb 1 en mòdul 7. En aquest cas resulta bastant fàcil trobar aquest valor. Podem observar que és 3, ja que  $5 \cdot 3 \equiv 15 \equiv 1 \pmod{7}$ .

Per trobar una expressió general que ens permeti calcular inversos modulars sempre que el mòdul ho permeti necessitarem tenir en compte un petit aspecte que s'exposa a continuació.

**Lema 2.2.4.** En tota divisió es compleix que  $D = dq + r$ , és a dir, que el dividend  $D$  és igual al producte del divisor  $d$  pel quocient  $q$  més el residu  $r$ .

Tenint en compte aquesta informació podem escriure el següent:

$$bb^{-1} \equiv 1 \pmod{N} \Rightarrow bb^{-1} = Nq + 1.$$

Així doncs, obtenim una equació que ens permet calcular l'element invers  $b^{-1}$  d'un nombre  $b$  en mòdul  $N$ .

El problema que presenta aquesta equació és que s'han d'anar provant valors de  $q$  fins que obtenim un valor de  $b^{-1} \in \{1, 2, \dots, N-1\}$ , i a vegades pot resultar una tasca pesada. Per aquest motiu, sempre que haguem de calcular inversos modulars ho farem aplicant un procediment que es coneix amb el nom d'algoritme d'Euclides.

**Teorema 2.2.5.: Algoritme d'Euclides.** Donats dos nombres  $a$  i  $b$ ,  $\text{mcd}(a,b)$  es calcula de la següent forma:

1. Dividir el nombre gran entre el petit.
2. Si la divisió és exacta, el divisor és  $\text{mcd}(a,b)$ .
3. Si no ho és, es divideix el divisor entre el residu obtingut i es continua així fins que s'obtingui una divisió exacta, sent l'últim divisor el  $\text{mcd}(a,b)$ .

Per exemple suposem que volem calcular el  $\text{mcd}(3,7)$ . Aleshores calculem  $\frac{7}{3} = 2, r = 1$ . La divisió no és exacta, per tant repetim el procés, però aquesta vegada calculem  $\frac{d}{r} = \frac{3}{1} = 3, r' = 0$ . En aquest cas, la divisió és exacta, per tant  $\text{mcd}(3,7) = \text{mcd}(3,1) = 1$ .

Passem a veure com podem calcular inversos modulars. Per fer-ho hem modificat l'algoritme anterior per obtenir-ne un altre de diferent que ens ho permeti fer.

**Teorema 2.2.6.** Donats dos nombres  $a$  i  $b$ ,  $b^{-1}(\text{mod } a)$  existirà si i només si  $\text{mcd}(a,b) = 1$ , i és calcularà de la següent forma:

1. Calcular el residu  $r$  de  $\frac{a}{b}$ .
2. Si  $r = 1$ , aleshores  $b^{-1} \equiv -q(\text{mod } a)$ , on  $q = \frac{a-r}{b}$ .
3. Si  $r \neq 1$ , aleshores  $b^{-1} \equiv -qr^{-1}(\text{mod } a)$ . Calcular  $r^{-1}(\text{mod } a)$  repetint l'algoritme, tenint en compte que ara  $b = r$ . Si el residu  $r'$  de  $\frac{a}{r}$  és 1, repetir el pas 2; si no ho és, repetir el pas 3 tenint en compte que  $r = r'$ . Finalment calcular  $b^{-1}(\text{mod } a)$  multiplicant tots els inversos dels residus per  $-q$  i reduir el resultat  $(\text{mod } a)$ .

Per exemple suposem que volem calcular  $x \equiv 5^{-1}(\text{mod } 17)$ . Comencem dividint  $\frac{a}{b} = \frac{17}{5} = 3, r = 2$ . Com que  $r = 2 \neq 1$ , calculem  $y \equiv r^{-1} \equiv 2^{-1}(\text{mod } 17)$  tornant a aplicar l'algoritme i tenint en compte que ara  $b = r$ . Comencem dividint  $\frac{a}{r} = \frac{17}{2} = 8, r' = 1$ . Com que  $r' = 1$ ,  $r^{-1} \equiv -q \equiv -(a - r') \cdot r^{-1}(\text{mod } a)$ , per tant  $2^{-1} \equiv -(17 - 1) \cdot 2^{-1} \equiv -8 \equiv 9(\text{mod } 17)$ . Finalment calculem  $x \equiv 5^{-1}(\text{mod } 17)$  multiplicant tots els inversos dels residus per  $-q = \frac{-a + r}{b} = \frac{-17 + 2}{5} = -3$ , tot reduint el resultat  $(\text{mod } 17)$ , de tal forma que  $x \equiv 5^{-1} \equiv 2^{-1} \cdot (-3) \equiv 9 \cdot 14 \equiv 7(\text{mod } 17)$ .

Així doncs, obtenim el valor de  $5^{-1}(\text{mod } 17)$ , que és 7.

Un cop revisats els procediments de suma, resta, multiplicació i divisió a  $\mathbb{Z}/N\mathbb{Z}$ , tancarem aquest apartat comentant que en el cas en què  $N$  sigui un nombre primer, el conjunt  $\mathbb{Z}/N\mathbb{Z}$  serà un grup abelià en respecte de la suma i del producte, i també complirà la propietat distributiva del producte respecte de la suma,  $a(b+c) = ab+ac$ . Direm aleshores que  $\mathbb{Z}/N\mathbb{Z}$  amb  $N$  primer té estructura de cos.

Així docs podem concloure amb el següent:

- Un conjunt  $\mathbb{Z}/N\mathbb{Z}$ ,  $N \in \mathbb{N}$  sempre serà un grup commutatiu o abelià en respecte de la suma.
- Un conjunt  $\mathbb{Z}/N\mathbb{Z}$ ,  $N \in \mathbb{N}$ , amb  $N$  primer serà un grup commutatiu o abelià en respecte de la suma i del producte, per tant estarem parlant d'un cos.
- Cal remarcar que el conjunt de nombres racionals  $\mathbb{Q}$ , el dels nombres reals  $\mathbb{R}$  i el dels nombres complexos  $\mathbb{C}$  són cossos, ja que són grups abelians respecte de la suma i del producte.

I així finalitzem aquest apartat per donar pas al següent, dedicat al Petit Teorema de Fermat, que serà crucial per comprendre alguns procediments moderns de xifrat.

## 2.3. Petit Teorema de Fermat

Ara que ja hem vist tots els aspectes referents a nombres primers i a aritmètica modular que ens feien falta per realitzar el projecte, ja estem en condicions d'exposar un dels teoremes que seran de vital importància per poder comprendre el funcionament d'alguns dels procediments de xifrat moderns que s'exposaran posteriorment.

Primer de tot començarem exposant un resultat tècnic o lema i la seva demostració, i posteriorment parlarem del Petit Teorema de Fermat, juntament amb un corol·lari d'aquest. També aportarem les demostracions pertinents.

**Lema 2.3.1.** *La seqüència  $a, 2a, \dots, (p-1)a$ , amb  $p$  no divisible per  $a$ , al ser reduïda en mòdul  $p$ , es pot tornar a agrupar en la seqüència  $1, 2, \dots, (p-1)$ .*

### **Demostració:**

Definim el subconjunt de nombres naturals  $C = \{1, 2, \dots, (p-1)\}$ . Suposem que  $a \in \{1, 2, \dots, (p-1)\}$ . En cas que  $a > p$ , calculem  $a \equiv a' \pmod{p}$ ,  $a' \in C$ .

Com que  $p$  és un nombre primer,  $\text{mcd}(a, p) = 1$  i  $\text{mcd}(n_i, p) = 1, n_i \in C$ , per tant  $\text{mcd}(an_i, p) = 1$ . Sabem que  $n_i \neq n_j, n_j \in C$ , per tant  $n_i$  no és congruent amb  $n_j$  en mòdul  $p$ , la qual cosa implica que  $an_i$  tampoc és congruent amb  $an_j$  en mòdul  $p$ .

Així doncs, cadascun dels elements de la seqüència  $a, 2a, \dots, (p-1)a$  haurà de tenir un valor congruent en mòdul  $p$  que sigui diferent de la resta. A més sabem que tots aquest valors hauran de pertànyer a  $C$ .

I com que la successió té el mateix nombre d'elements que el conjunt  $C$ , cadascun d'aquests  $p-1$  elements haurà de ser el valor congruent en mòdul  $p$  d'algun dels elements de la seqüència.

Així queda demostrat que cadascun dels elements de la primera seqüència és congruent amb algun dels de la segona en mòdul  $p$ . **Q.E.D.**

**Petit Teorema de Fermat.** *Si  $p$  és un nombre primer, aleshores  $\forall a \in \mathbb{Z}$ :  $a^p \equiv a \pmod{p}$ , i, equivalentment,  $a^{p-1} \equiv 1 \pmod{p}$  si  $\text{mcd}(a, p) = 1$ .*

### **Demostració:**

Partint del resultat anterior, podem escriure la següent expressió:

$$a \cdot 2a \cdot 3a \cdot \dots \cdot (p-1)a \equiv 1 \cdot 2 \cdot 3 \cdot \dots \cdot (p-1) \pmod{p}.$$

Si agrupem els factors i reescrivim l'expressió, obtenim el següent:

$$a^{p-1} (p-1)! \equiv (p-1)! \pmod{p}.$$

Simplificant l'expressió anterior obtenim el següent:

$$a^{p-1} \equiv 1 \pmod{p}.$$

D'aquesta forma queda demostrat el Petit Teorema de Fermat. **Q.E.D.**

**Corol·lari 2.3.2.** Si  $p$  és un nombre primer es verifica que  $\forall a, k \in \mathbb{Z}$ :  
 $a^{k(p-1)} \equiv 1 \pmod{p}$ , i, equivalentment,  $a^{k(p-1)} \equiv 1 \pmod{p}$  si  $\text{mcd}(a, p) = 1$ .

***Demostració:***

Partint de l'expressió  $a^{k(p-1)} \equiv 1 \pmod{p}$  efectuem el canvi de variable  $b = a^k, b \in \mathbb{Z}$  i obtenim que  $b^{p-1} \equiv 1 \pmod{p}$ , que és l'expressió del Petit Teorema de Fermat demostrada anteriorment, per tant queda demostrat el corol·lari. **Q.E.D.**

Finalment cal afegir que algunes de les aplicacions del Petit Teorema de Fermat estan relacionades amb la Criptografia moderna i també amb la comprovació de la primalitat d'un nombre, ja que el Petit Teorema de Fermat estableix una condició indispensable que ha de complir tot nombre primer.

Ara que ja hem vist en què consisteix aquest teorema, podem donar per acabat aquest bloc de coneixements previs per tal de començar un altre bloc, referent a la Criptografia clàssica.

Però abans de fer-ho cal remarcar que les demostracions que s'han mostrat en aquest apartat s'han elaborat específicament per aquest projecte. És cert que existeixen moltes altres demostracions vàlides, però s'ha preferit elaborar-ne de pròpies i s'ha intentat que fossin simples, per tal de facilitar-ne la comprensió.

## 3. CRIPTOGRAFIA CLÀSSICA

### 3.1. Introducció

Tal i com hem vist en el primer apartat, podem classificar els mètodes de xifrat que existeixen en dos grans grups, el de la *Criptografia Clàssica* i el de la *Criptografia Moderna*.

Primer de tot començarem explicant en què consisteix la *Criptografia Clàssica* i posteriorment veurem alguns mètodes de xifrat pertanyents a aquest grup, juntament amb alguns criptogrames obtinguts a partir de l'aplicació dels mètodes descrits, i tancarem el bloc dedicat a la *Criptografia Clàssica* descrivint un dels atacs més antics i utilitzats per desxifrar missatges obtinguts a partir de l'aplicació d'alguns dels mètodes de xifrat més antics.

Què entenem per *Criptografia Clàssica*? Doncs, molt senzill. Entenem que ens estem referint a uns sistemes de xifrar informació que formen part del passat i que a dia d'avui ja no són efectius davant dels avenços en el camp de la informàtica, i que han estat substituïts per altres sistemes més moderns, amb uns nivells de seguretat inimaginables fa escassament cinquanta anys.

La *Criptografia Clàssica* també es coneix com a Criptografia simètrica o de clau privada, ja que l'emissor i el receptor del missatge utilitzen la mateixa clau tant per xifrar com per desxifrar un missatge, per tant aquesta s'ha de mantenir en secret per tal d'evitar que terceres persones puguin accedir a la informació que es transmet. Aquesta és la característica principal de tots els mètodes de xifrat clàssics.

Els algorismes de xifrat simètric es basen principalment en dues tècniques que a simple vista poden semblar molt senzilles, però que al ser combinades van servir per crear mètodes de xifrat que generaven criptogrames aparentment impossibles de descodificar. Aquestes són la *substitució*, que consisteix en canviar els caràcters que formen el missatge per uns altres de diferents, ja siguin lletres, xifres o altres símbols, i la *transposició*, que consisteix en reordenar aquests elements.

A partir d'aquestes dues tècniques i amb el pas del temps es van anar desenvolupant diversos algorismes de xifrat simètric arreu del món. És de suposar que de tots aquests, alguns no van ser publicats, malgrat això el nombre d'algorismes de xifrat simètric que es coneixen és tan gran que necessitaríem un sol treball de recerca per poder estudiar-los tots, i ni així els podríem tractar en profunditat. Per aquest motiu s'han escollit tres algorismes de xifrat simètric que seran estudiats en el següent apartat, per tal de veure com es xifrava la informació en una època en la que els ordenadors i les telecomunicacions s'escapaven de la imaginació dels més somiadors. Cal dir que els algorismes que es descriuran s'han escollit per la seva simplicitat, de tal forma que resulta relativament fàcil entendre'n el funcionament.

Existeixen altres mètodes de xifrat que impliquen la utilització de dispositius electromecànics, tals com l'*Enigma* o la *Lorenz*, però no els tractarem en aquest treball, degut a la complexitat del funcionament d'aquests dispositius.

Tot i això en comentarem alguns aspectes importants. Comencem per l'*Enigma*. [12.3]

*Enigma* era el nom d'una màquina que disposava d'un mecanisme de xifrat rotatori, que permetia utilitzar-la tant per a xifrar com per a desxifrar missatges. Diversos dels seus models van ser utilitzats a Europa des d'inicis dels anys 1920.

La seva fama es deu a haver estat adoptada per les forces militars d'Alemanya des de 1930. La seva facilitat de maneig i suposada inviolabilitat van ser les principals raons per al seu ampli ús.

El seu sistema de xifrat va ser finalment descobert, mitjançant anàlisis freqüencials, i la lectura de la informació que contenien els missatges suposadament protegits, és considerada, de vegades, com la causa d'haver pogut concloure la Segona Guerra Mundial, almenys, dos anys abans del que hagués esdevingut sense el seu desxifrat.



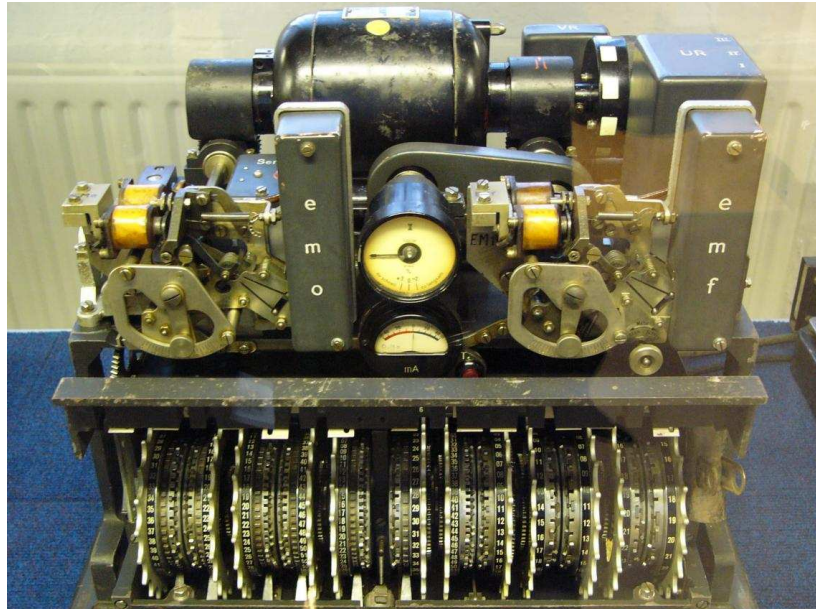
**Figura 1:** Màquina *Enigma*.

Passem a parlar de la *Lorenz*. [12.4]

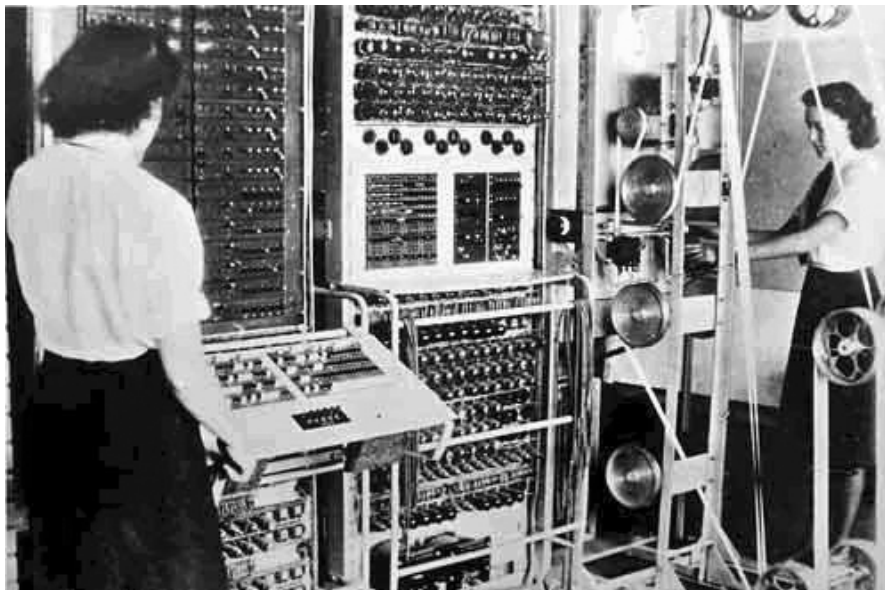
La *Lorenz SZ 40* i la *SZ 42* eren màquines alemanyes de xifrat utilitzades durant la Segona Guerra Mundial en circuits de teletip. Criptògrafs britànics, que es van referir al tràfic alemany de dades de teletip xifrades com *Fish*, van denominar a l'aparell i el seu tràfic com *Tunny*. Mentre la famosa *Enigma* va ser usada generalment per unitats de combat, la Màquina de *Lorenz* va ser usada per a comunicacions d'alt nivell. L'enginy en si tenia unes mesures de 51cm × 46cm × 46cm, i va funcionar com dispositiu adjunt a les màquines de teletip de Lorenz estàndards.

Màquines realment complexes van ser construïdes pels britànics per atacar al sistema *Tunny*. Les primeres van ser una família de màquines conegudes com *Heath Robinsons*, que usaven cintes magnètiques construïdes amb circuits de lògica electrònica, per a poder trencar el sistema *Tunny*.

La següent va ser *Colossus*, el primer computador electrònic digital del món, programat mitjançant panells de cablejat. Era molt més ràpid i fiable que les *Heath Robinsons*; usant-lo, els britànics van ser capaços de llegir una gran proporció de tràfic *Tunny*.



**Figura 2:** Màquina *Lorenz*.

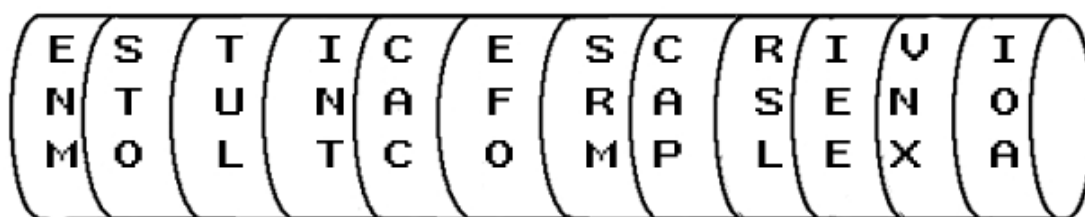


**Figura 3:** Ordenador *Colossus*.

## 3.2. Retrospecció: mètodes de xifrat clàssics

### 3.2.1. Escítala espartana

El primer mètode de xifrat clàssic que veurem és un dels més antics i també un dels primers mètodes de xifrat que es van utilitzar. En aquest cas es tracta d'un mètode de transposició, que data del segle IV aC. Se'l coneix com l'escítala espartana, i està basat en un cilindre d'un diàmetre determinat que serveix com clau, al voltant del qual els espartans enrotllaven una cinta i escrivien el missatge damunt. Al desenrotllar-la, el missatge quedava xifrat, però les lletres no quedaven descol·locades a l'atzar, sinó que seguien un ordre lògic. Com a curiositat cal afegir que normalment els missatges s'escriuien als cinturons, per evitar que els enemics dels espartans els pogessin interceptar. Aquí podeu veure un exemple:



El text del dibuix, al desenrotllar la cinta, es llegiria:  
***ENMSTOTULINTCACEFOSRMCAPRSLIEEVNXIOA***

En la pràctica, això és equivalent a escriure el text en una taula en la qual triem el nombre de columnes,  $c$ . El text xifrat serà el que s'obtingui al llegir les lletres en vertical. Al variar el nombre de columnes de la taula, obtenim criptogrames diferents. Vegem com quedaria el missatge si el nombre de columnes fos  $c=6$ :

E	S	T	I	C	E
S	C	R	I	V	I
N	T	U	N	A	F
R	A	S	E	N	O
M	O	L	T	C	O
M	P	L	E	X	A

Al llegir les columnes en vertical i de dalt cap baix obtenim el següent missatge:  
***ESNRMMSCTAOPTRUSLLIINETECVANCXEIFOOA***

Una observació sobre aquest mètode és que els valors que prengui  $c$  han d'estar compresos entre  $1 \leq c \leq \frac{L}{2}$ , on  $L$  és la longitud del missatge, és a dir, el nombre de caràcters que el formen. Per a valors de  $c$  superiors a  $\frac{L}{2}$  el criptograma es torna més vulnerable, ja que hi apareixen grups de lletres que mantenen la posició inicial, i s'han d'afegir caràcters addicionals per evitar-ho. També cal tenir en compte que quan  $c=1$  i quan  $c=L$ , el criptograma obtingut és el text en clar i que per valors de  $c$  superiors a  $L$  el missatge queda completament sense transposar.

Vegem un exemple per comprovar les vulnerabilitats que presenta el criptograma del missatge a mesura que s'augmenta al valor de  $c$ . Per fer-ho, triarem una paraula curta, com per exemple *XIFRAT*, i generarem tots els criptogrames possibles que permeti aquest mètode, que són  $c=L=6$ .

- **Criptograma per  $c=1$ :**

<b>X</b>
<b>I</b>
<b>F</b>
<b>R</b>
<b>A</b>
<b>T</b>

El criptograma obtingut és el missatge en clar: *XIFRAT*.

- **Criptograma per  $c=2$ :**

<b>X</b>	<b>I</b>
<b>F</b>	<b>R</b>
<b>A</b>	<b>T</b>

El criptograma obtingut és *XFAIRT*. Tal i com podem veure, totes les parts del missatge en clar s'han transposat, excepte la primera lletra i l'última.

- **Criptograma per  $c=\frac{L}{2}=3$ :**

<b>X</b>	<b>I</b>	<b>F</b>
<b>R</b>	<b>A</b>	<b>T</b>

El criptograma obtingut és *XRIAFT*. Tal i com podem veure, totes les parts del missatge en clar s'han transposat, excepte la primera lletra i l'última. Aquest és l'últim criptograma segur que es pot obtenir amb aquest mètode.

- **Criptograma per  $c=4$ :**

<b>X</b>	<b>I</b>	<b>F</b>	<b>R</b>
<b>A</b>	<b>T</b>		

El criptograma obtingut és *XAITFR*. En aquest criptograma podem observar una vulnerabilitat i és que les lletres *F* i *R* continuen unides, degut a la manca de caràcters per acabar d'omplir la taula.

– **Criptograma per  $c=5$ :**

X	I	F	R	A
T				

El criptograma obtingut és ***XTIFRA***. Podem observar una vulnerabilitat major que en el criptograma anterior, ja que en aquest cas són quatre les lletres que continuen juntes en el criptograma.

– **Criptograma per  $c=L=6$ :**

X	I	F	R	A	T
---	---	---	---	---	---

El criptograma obtingut en aquest cas és el missatge en clar: ***XIFRAT***.

Després d'observar els exemples de criptogrames generats amb aquest mètode de xifrat podem concloure que com més llarg sigui un missatge, més difícil resulta la tasca de desxifrar el criptograma obtingut sense disposar del valor de  $c$ , o en cas de treballar amb cilindres, del valor del diàmetre d'aquest.

En cas de voler desxifrar un criptograma generat amb aquest mètode, necessitaríem saber el valor de  $c$  utilitzat en el procés, o el valor del diàmetre si estem treballant amb cilindres.

Suposem que rebem el criptograma ***XRI AFT***, i sabem que s'ha utilitzat un valor de  $c=3$  per xifrar. Per tant, agafaríem el missatge xifrat i el col·locaríem en una taula de tres columnes. El nombre de files  $f$  de la taula el podem obtenir a partir del quocient  $q = \frac{L}{c}$ .

Si la divisió és exacta, aleshores  $f = q$  i si no, el nombre de files serà  $f = q + 1$ , ja que la presència d'un residu diferent de 0 en la divisió ens indica que tenim un nombre  $q$  de files completes i una altra fila incompleta.

En el nostre cas, la divisió és exacta i dona com a resultat 2, per tant,  $f=2$ . Creant una taula de 3 columnes i 2 files, i distribuint les lletres del missatge per columnes obtenim:

X	I	F
R	A	T

Llegint fila per fila recuperem el missatge en clar, ***XIFRAT***.

Actualment, els criptogrames obtinguts a partir de l'aplicació d'aquest mètode de xifrat no són segurs, ja que amb un ordinador es pot desxifrar qualsevol criptograma generat, sense importar la longitud  $L$  del missatge ni el nombre de columnes  $c$  utilitzat en el procés de xifrat.

No obstant, cal dir que aquest mètode va ser utilitzat durant un llarg període de temps, ja que resultava molt simple xifrar informació i era eficaç.

Temps després van aparèixer altres mètodes de xifrat més efectius que van substituir a l'escitala espartana. Un d'aquests mètodes es coneix com el mètode de xifrat de Polybius, i és el mètode de xifrat clàssic que descriurem en el següent apartat.

### 3.2.2. Mètode de xifrat de *Polybius*

El criptosistema que veurem a continuació va ser un dels que va substituir al mètode de l'escítila espartana, ja que permet obtenir missatges xifrats més segurs que el mètode anterior.

Tal i com el seu nom indica, el sistema va ser creat per un historiador grec anomenat *Polybius* (200aC - 118aC). És un sistema de substitució basat en la posició de les lletres en una taula. Aquesta taula també es coneix amb el nom de *Quadrat Grec*. A continuació se n'adjunta un exemple:



	1	2	3	4	5
1	A	B	C	D	E
2	F	G	H	I	J
3	K	L	M	N	O
4	P	Q	R	S	T
5	U	V	W	X/Z	Y

**Figura 4:** *Quadrat Grec*.

El xifrat de missatges és molt simple, cal substituir cada lletra per un valor numèric de dues xifres que s'obté com a resultat de la posició de cada lletra en la taula anterior. El primer que cal fer és localitzar la lletra en la taula i després posar primer el nombre de la columna en la qual es troba i després el nombre de la fila. Es diu que Polybius utilitzava aquest mètode per transmetre missatges a llarga distància utilitzant torxes, de tal forma que amb dos grups de torxes transmetia els dos dígitos corresponents a cada lletra.

A continuació s'adjunten els valors numèrics que s'assignen a cadascuna de les lletres de l'abecedari:

A	B	C	D	E	F	G	H	I	J	K	L	M
11	21	31	41	51	12	22	32	42	52	13	23	33
N	O	P	Q	R	S	T	U	V	W	X	Y	Z
43	53	14	24	34	44	54	15	25	35	45	55	45

Es pot observar que la X i la Z xifren en un mateix valor numèric. Bàsicament un es pot permetre assignar-los el mateix valor ja que aquestes dues lletres són d'ús poc comú, en comparació amb altres lletres com les vocals.

Aquest és potser el mètode de xifrat menys conegut de tots els que s'exposaran en aquest apartat, i encara que sembli simple, pot resultar molt útil en els fòrums o per passar informació entre els amics.

Vegem un exemple pràctic de xifrat d'informació utilitzant aquest mètode, per tal d'acabar de comprendre el funcionament d'aquest algoritme:

- **Missatge en clar:** *XIFRAT*
- **Valors numèrics corresponents a les lletres:**

X	I	F	R	A	T
45	42	12	34	11	54

- **Criptograma:** 454212341154

El *Quadrat Grec* de Polybius posseeix algunes propietats interessants. En particular, redueix el nombre de símbols utilitzats per la codificació, la qual cosa dificulta l'anàlisi dels criptogrames. A més altera la freqüència dels caràcters, a diferència que els xifrats monoalfabètics. És per això que aquest mètode és un precursor dels mètodes moderns.

Cal remarcar que podem omplir la taula de manera diferent de com s'ha fet aquí, per exemple començant posant una paraula clau i després la resta de les lletres en ordre alfabètic i també podem alterar l'ordre de la numeració de les files i les columnes.

Vegem alguns exemples de taules modificades per tal d'examinar de quina forma varia el xifrat d'una mateixa paraula:

- ***Quadrat Grec* amb alteració de les lletres utilitzant una paraula clau (*CODIS*):**

	1	2	3	4	5
1	C	O	D	I	S
2	A	B	E	F	G
3	H	J	K	L	M
4	N	P	Q	R	T
5	U	V	W	X/Z	Y

En aquest cas, els valors numèrics que s'assignen a cadascuna de les lletres de l'abecedari són:

A	B	C	D	E	F	G	H	I	J	K	L	M
12	22	11	31	32	42	52	13	41	23	33	43	53
N	O	P	Q	R	S	T	U	V	W	X	Y	Z
14	21	24	34	44	51	54	15	25	35	45	55	45

Per poder obtenir la taula correcta s'ha de buscar una paraula generadora que no tingui lletres repetides ja que s'ha de tenir en compte que cada lletra només pot aparèixer una vegada a la taula.

Si xifrem la paraula *XIFRAT* utilitzant aquesta nova taula obtenim el criptograma 454142441254, que és completament diferent al criptograma obtingut amb la taula sense modificar.

– **Quadrat Grec amb alteració de la numeració de files i columnes:**

	1	3	5	7	9
0	A	B	C	D	E
2	F	G	H	I	J
4	K	L	M	N	O
6	P	Q	R	S	T
8	U	V	W	X/Z	Y

En aquest cas, els valors numèrics que s'assignen a cadascuna de les lletres de l'abecedari són:

A	B	C	D	E	F	G	H	I	J	K	L	M
10	30	50	70	90	12	32	52	72	92	14	34	54
N	O	P	Q	R	S	T	U	V	W	X	Y	Z
74	94	16	36	56	76	96	18	38	58	78	98	78

Si xifrem la paraula **XIFRAT** utilitzant aquesta nova taula obtenim el criptograma 787212561096, que és completament diferent als criptogrames obtingut amb les taules anteriors.

Cal dir que la numeració de files i columnes és pot alterar de moltes maneres i si a més ho combinem amb l'alteració de les lletres podem obtenir una enorme llista de taules diferents, totes elles igualment útils per xifrar informació.

Aquest criptosistema admet altres tipus de variacions, les alteracions del criptograma. És a dir, que podem agafar una paraula qualsevol, convertir-la en una seqüència numèrica, dividir-la en blocs de lletres i tornar-la a convertir en una seqüència de lletres diferents a les de la paraula inicial. Vegem-ne un exemple, suposant que estem treballant amb la taula sense modificar:

	1	2	3	4	5
1	A	B	C	D	E
2	F	G	H	I	J
3	K	L	M	N	O
4	P	Q	R	S	T
5	U	V	W	X/Z	Y

Cal tenir en compte que el nombre  $n$  de blocs de lletres en què dividirem el criptograma ha de complir que  $2 \leq n < 2L$ , on  $L$  és la longitud del missatge en clar i tenint en compte que  $n$  ha de ser un nombre natural.

Això és així ja que si dividim el criptograma en 1 bloc aquest no varia i si el dividim en  $2L$  blocs i els col·loquem l'un a sota de l'altre obtenim el propi criptograma però en vertical.

Agafem la paraula **XIFRAT** i el seu criptograma corresponent a aquesta taula, que és 454212341154, i l'alterem amb diferents valors de  $n$ :

- **Criptograma per  $n=1$ :** tal i com hem comentat, al dividir 454212341154 en 1 bloc obtenim 454212341154, per tant no hi ha alteració del criptograma, la qual cosa vol dir que al tornar-lo a passar a text obtindríem el missatge en clar, que és **XIFRAT**.
- **Criptograma per  $n=2$ :** al dividir el criptograma en 2 blocs i col·locar-los un a sota de l'altre obtenim:

4	5	4	2	1	2
3	4	1	1	5	4

Si tornem a construir parelles de dígit agafant-los per columnes obtenim el criptograma 435441211524, i si el convertim en text obtenim **NTDBUQ**, que és completament diferent al missatge en clar.

- **Criptograma per  $n=L=6$ :** al dividir el criptograma en 6 blocs i col·locar-los un a sota de l'altre obtenim:

4	5
4	2
1	2
3	4
1	1
5	4

Si tornem a construir parelles de dígit agafant-los per columnes obtenim el criptograma 441315522414, i si el convertim en text obtenim **SKUJQP**, que és completament diferent al missatge en clar i al criptograma textual obtingut amb  $n=2$ .

- **Criptograma per  $n=2L=12$ :** al dividir el criptograma en 12 blocs i col·locar-los un a sota de l'altre obtenim:

4
5
4
2
1
2
3
4
1
1
5
4

Si tornem a construir parelles de dígit agafant-los per columnes obtenim el criptograma 454212341154, per tant no hi ha alteració del criptograma, la qual cosa vol dir que al tornar-lo a passar a text obtindríem el missatge en clar, que és **XIFRAT**.

Per acabar, cal remarcar que aplicant els mètodes d'alteració de taules juntament amb el mètode d'alteració de criptogrames s'obté una gran varietat de possibilitats per xifrar informació.

En cas de voler desxifrar un criptograma generat amb aquest algorisme necessitaríem saber les característiques de la taula emprada en el procés, així com el valor  $n$  utilitzat per alterar el criptograma.

Suposem que rebem el criptograma **SKUXGD**, i sabem que la taula emprada és la taula no modificada i que el criptograma ha estat alterat amb  $n=7$ . Primer de tot cal convertir aquesta seqüència de lletres en una seqüència numèrica, tot utilitzant la mateixa taula emprada en el procés de xifrat. Així obtindríem el criptograma 441315452241.

Posteriorment, cal invertir el procés d'alteració. Per fer-ho, hem de col·locar la seqüència numèrica anterior en una taula de 7 files. Per saber el nombre de columnes  $c$  que ha de tenir aquesta taula només cal calcular el quocient  $q = \frac{2L}{n}$ , de tal forma que si és una divisió exacta, el nombre de columnes correspondrà al quocient  $q$  d'aquesta. En cas de no ser exacta, el nombre de columnes serà  $c = q + 1$ , ja que la presència d'un residu diferent de 0 en la divisió ens indica que tenim un nombre  $q$  de columnes completes i una altra d'incompleta.

En el nostre cas, la divisió no és exacta i dona com a resultat 1 i residu 5, per tant,  $c=2$ . Creant una taula de 2 columnes i 7 files, i distribuint els nombres del criptograma per columnes obtenim:

4	5
4	2
1	2
3	4
1	1
5	
4	

Llegint fila per fila obtenim la seqüència numèrica corresponent al missatge en clar, 454212341154, i si la passem a text obtenim el missatge original, **XIFRAT**.

Un cop més cal afegir que actualment, els criptogrames obtinguts a partir de l'aplicació d'aquest mètode de xifrat, amb o sense alteracions, no són segurs, ja que amb un ordinador es pot desxifrar qualsevol missatge xifrat generat, sense importar la longitud  $L$  del missatge ni les alteracions realitzades.

### 3.2.3. Mètode de xifrat de *Juli Cèsar*

Seguim amb un mètode que té un nom familiar. Ens referim al mètode de xifrat de *Juli Cèsar* (100aC - 44aC), anomenat així ja que *Juli Cèsar* el va utilitzar en les seves campanyes, encara que hi ha alguns autors que afirmen que ell no el feia servir.

Aquest mètode de xifrat consisteix a canviar cada lletra del text per la que estigui  $n$  llocs més endavant en l'abecedari, on  $n$  solament és coneguda per l'emissor i el receptor del missatge. Per exemple, si  $n=1$ , es canviaria cada lletra per la següent de l'abecedari (la A per la B, la B per la C, la C per la D... la Z per la A). Si  $n=7$ , la A es canviaria per la H, la B per la I, etc.

Aquest mètode, amb  $n=3$ , va ser el que va utilitzar *Juli Cèsar* per xifrar els seus missatges. Com a curiositat m'agradaria afegir que hi ha un cas especial, el qual té nom propi. Aquest cas és quan  $n=13$ . Es denomina xifrat *ROT-13*, i és un mètode que s'utilitza actualment en els fòrums d'Internet. La peculiaritat d'aquest cas és que per a desxifrar un text cal fer el mateix que per a xifrar-lo, perquè l'alfabet (l'anglès, sense la ñ) té 26 lletres, per tant, al desplaçar 13 dues vegades, tornem a la posició inicial.

Amb aquest mètode podem moure les lletres  $n$  posicions, on els valors que pot prendre  $n$  són  $0 \leq n \leq 25$ , tenint en compte que  $n=0$  no modifica la posició de les lletres i que per a valors superiors a 25 es torna a començar a contar des del principi (considerant un alfabet de 26 lletres), és a dir, que  $n=26$  genera el mateix resultat que  $n=0$ , i així successivament.

D'aquesta forma, si assignem un valor numèric a cada lletra i considerem un alfabet de  $N$  caràcters, la transformació criptogràfica seria:

$$T_n(x) \equiv x + n \pmod{N}, \forall x, n, N \in \mathbb{Z}.$$

En aquesta equació modular,  $T_n$  és el valor numèric de la lletra ja xifrada,  $x$  és el valor de la lletra sense xifrar,  $n$  és el nombre de posicions que s'ha de desplaçar la lletra i  $N$  és el nombre d'elements del grup finit en què treballem, que en el nostre cas serà 26, ja que treballarem amb un alfabet de 26 lletres. Cal remarcar que a  $\mathbb{Z}/N\mathbb{Z}$ , els valors numèrics que poden prendre les lletres han d'anar des del 0 fins al 25, però nosaltres donem valor 26 a la Z ja que  $26 \equiv 0 \pmod{26}$ .

Aquí s'adjunta la taula amb els valors numèrics de les lletres de l'alfabet que farem servir:

A	B	C	D	E	F	G	H	I	J	K	L	M
01	02	03	04	05	06	07	08	09	10	11	12	13
N	O	P	Q	R	S	T	U	V	W	X	Y	Z
14	15	16	17	18	19	20	21	22	23	24	25	26

Vegem alguns exemples pràctics per tal d'assimilar el funcionament d'aquest mètode i comprovar que l'equació modular exposada és vàlida. Suposem que la paraula que volem xifrar és **XIFRAT**. Si assignem un valor numèric a cadascuna de les lletres a partir de la taula anterior obtenim la seqüència numèrica 240906180120, de tal forma que cada parella de dígit correspon al valor de cadascuna de les lletres de la paraula que volem xifrar. Partint d'aquesta seqüència podem xifrar el missatge per diferents valors de  $n$ , tal i com es mostra a continuació:

- **Criptograma per  $n=3$ :** adaptant l'equació modular anterior a aquest cas obtenim l'expressió  $T_3(x) \equiv x + 3 \pmod{26}$  (treballem a  $\mathbb{Z}/N\mathbb{Z}$  ja que l'alfabet que estem utilitzant té 26 lletres). Partint dels valors numèrics de les lletres passem a xifrar el missatge lletra per lletra:

- Lletra: **X**; valor numèric: 24; xifrat:  $T_3(24) \equiv 24 + 3 \equiv 1 \pmod{26}$
- Lletra: **I**; valor numèric: 09; xifrat:  $T_3(9) \equiv 9 + 3 \equiv 12 \pmod{26}$
- Lletra: **F**; valor numèric: 06; xifrat:  $T_3(6) \equiv 6 + 3 \equiv 9 \pmod{26}$
- Lletra: **R**; valor numèric: 18; xifrat:  $T_3(18) \equiv 18 + 3 \equiv 21 \pmod{26}$
- Lletra: **A**; valor numèric: 01; xifrat:  $T_3(1) \equiv 1 + 3 \equiv 4 \pmod{26}$
- Lletra: **T**; valor numèric: 20; xifrat:  $T_3(20) \equiv 20 + 3 \equiv 23 \pmod{26}$

Un cop tenim calculats els diferents valors numèrics corresponents a les lletres xifrades del missatge, l'únic que hem de fer és escriure les lletres que corresponen a aquests valors, tot observant la taula anterior. D'aquesta forma obtenim el criptograma **ALIUDW**.

Per comprovar que realment aquestes lletres corresponen a les lletres situades tres posicions més cap a la dreta respecte les lletres inicials del missatge, podem observar la taula i contar les posicions de forma manual.

D'aquesta forma veiem que els resultats que ens dona l'equació són correctes, per tant podem afirmar que aquesta equació modular és vàlida per xifrar missatges amb el mètode de xifrat de *Juli Cèsar*.

- **Criptograma per  $n=13$ . Mètode ROT-13:** adaptant l'equació modular anterior a aquest cas obtenim l'expressió  $T_{13}(x) \equiv x + 13 \pmod{26}$ . Partint dels valors numèrics de les lletres passem a xifrar el missatge lletra per lletra:

- Lletra: **X**; valor numèric: 24; xifrat:  $T_{13}(24) \equiv 24 + 13 \equiv 11 \pmod{26}$
- Lletra: **I**; valor numèric: 09; xifrat:  $T_{13}(9) \equiv 9 + 13 \equiv 22 \pmod{26}$
- Lletra: **F**; valor numèric: 06; xifrat:  $T_{13}(6) \equiv 6 + 13 \equiv 19 \pmod{26}$
- Lletra: **R**; valor numèric: 18; xifrat:  $T_{13}(18) \equiv 18 + 13 \equiv 5 \pmod{26}$
- Lletra: **A**; valor numèric: 01; xifrat:  $T_{13}(1) \equiv 1 + 13 \equiv 14 \pmod{26}$
- Lletra: **T**; valor numèric: 20; xifrat:  $T_{13}(20) \equiv 20 + 13 \equiv 7 \pmod{26}$

Un cop tenim calculats els diferents valors numèrics corresponents a les lletres xifrades del missatge, l'únic que hem de fer és escriure les lletres que corresponen a aquests valors, tot observant la taula anterior. D'aquesta forma obtenim el criptograma **KVSENG**.

Per comprovar que realment aquestes lletres corresponen a les lletres situades tretze posicions més cap a la dreta respecte les lletres inicials del missatge, podem observar la taula i sabent que entre les dues lletres d'una mateixa columna de la taula hi ha tretze posicions de diferència, resulta molt senzill verificar els resultats obtinguts.

Cal dir que si tornéssim a aplicar l'equació modular però aquesta vegada treballant amb els valors xifrats calculats anteriorment, obtindríem els valors inicials de les lletres del missatge sense xifrar:

- Lletra: **K**; valor numèric: 11; xifrat:  $T_{13}(11) \equiv 11 + 13 \equiv 24 \pmod{26}$
- Lletra: **V**; valor numèric: 22; xifrat:  $T_{13}(22) \equiv 22 + 13 \equiv 9 \pmod{26}$
- Lletra: **S**; valor numèric: 19; xifrat:  $T_{13}(19) \equiv 19 + 13 \equiv 6 \pmod{26}$
- Lletra: **E**; valor numèric: 05; xifrat:  $T_{13}(5) \equiv 5 + 13 \equiv 18 \pmod{26}$
- Lletra: **N**; valor numèric: 14; xifrat:  $T_{13}(14) \equiv 14 + 13 \equiv 1 \pmod{26}$
- Lletra: **G**; valor numèric: 07; xifrat:  $T_{13}(7) \equiv 7 + 13 \equiv 20 \pmod{26}$

Efectivament, al tornar a aplicar l'equació, obtenim els valors numèrics inicials, corresponents al missatge en clar. És a dir, que  $T_{13}^{-1}(x) = T_{13}(x)$ , o bé  $T_{13}^2(x) = x$ .

Ara que ja hem vist com es xifra amb l'equació modular exposada anteriorment ens falta saber com podem invertir el procés de xifrat per tornar a obtenir el missatge en clar. Hem vist que per a  $n=13$  només cal tornar a aplicar l'equació modular i obtenim els valors inicials, però això no és vàlid si variem el valor de  $n$ .

Així doncs, per desxifrar necessitarem una altra equació modular, que obtindrem modificant l'equació inicial de xifrat. És a dir, que l'equació modular que farem servir per revertir el procés de xifrat serà aquesta (hem utilitzat la relació inversa  $x = T_n^{-1}(y)$ ):

$$T_n^{-1}(y) \equiv y - n \pmod{N}, \forall y, n, N \in \mathbb{Z}.$$

Si volem obtenir resultats positius directament, sense haver de calcular congruències de nombres negatius amb el mòdul de treball podem modificar l'equació anterior, obtenint la següent expressió:

$$T_n^{-1}(y) \equiv y + N - n \pmod{N}, \forall y, n, N \in \mathbb{Z}.$$

Tal i com podem observar, les dues equacions són com la que utilitzàvem per xifrar, amb la diferència que en aquest cas hem aïllat la variable  $x$ . Cal remarcar que les dues equacions són vàlides per desxifrar, però la segona simplifica els càlculs, ja que no apareixeran valors de  $x$  negatius.

Per tal de comprovar que l'equació exposada permet invertir els processos de xifrat adjuntarem un exemple pràctic en el que desxifrarem un criptograma obtingut amb l'equació modular inicial.

Suposem que tenim el criptograma *ALIUDW*, i sabem que s'ha generat amb el valor  $n=3$  i amb  $N=26$ . És a dir, que l'equació de desxifrat que utilitzarem serà la següent:

$$T_3^{-1}(y) \equiv y + 23 \pmod{26}.$$

Per tant, l'únic que hem de fer es substituir cadascuna de les lletres del criptograma pel seu valor numèric corresponent i aplicar l'equació del desxifrat per obtenir el missatge en clar:

- Xifrat: *A*; valor numèric: 01; desxifrat:  $T_3^{-1}(1) \equiv 1 + 23 \equiv 24 \pmod{26}$
- Xifrat: *L*; valor numèric: 12; desxifrat:  $T_3^{-1}(12) \equiv 12 + 23 \equiv 9 \pmod{26}$
- Xifrat: *I*; valor numèric: 09; desxifrat:  $T_3^{-1}(9) \equiv 9 + 23 \equiv 6 \pmod{26}$
- Xifrat: *U*; valor numèric: 21; desxifrat:  $T_3^{-1}(21) \equiv 21 + 23 \equiv 18 \pmod{26}$
- Xifrat: *D*; valor numèric: 04; desxifrat:  $T_3^{-1}(4) \equiv 4 + 23 \equiv 1 \pmod{26}$
- Xifrat: *W*; valor numèric: 23; desxifrat:  $T_3^{-1}(23) \equiv 23 + 23 \equiv 20 \pmod{26}$

Si substituïm els valors numèrics obtinguts per les lletres corresponents obtenim la paraula **XIFRAT**, que és el missatge en clar.

Com hem pogut comprovar, l'equació modular de desxifrat proposada ens serveix per revertir els processos de xifrat, de tal forma que ens permet recuperar el missatge en clar.

Ja hem vist com funciona l'algoritme de xifrat de *Juli Cèsar* i també hem treballat amb les equacions modulares que ens permeten xifrar i desxifrar missatges. Podem afirmar que arribats a aquest punt ja estem en condicions d'exposar una generalització d'aquest algoritme.

És a dir, que introduïrem una modificació en l'equació modular inicial de tal forma que podrem augmentar considerablement el nombre de xifrats diferents que es podran obtenir partint d'un mateix missatge.

Partint de l'equació  $T_n(x) \equiv x + n \pmod{N}$ , hi afegirem un coeficient multiplicador a la variable  $x$ , de tal forma que l'equació modular resultant és la següent:

$$T_{(m,n)}(x) \equiv mx + n \pmod{N}, \forall x, m, n, N \in \mathbb{Z}.$$

En aquest cas, a diferència que en el cas anterior, la clau de desxifrat  $k$  està formada per la parella de nombres  $m$  i  $n$ , de tal forma que  $k = (m, n)$ . Per tant, els valors de  $m$  i  $n$  són els que s'han de mantenir en secret tant per part de l'emissor com del receptor del missatge, de tal forma que terceres persones no puguin accedir a la informació xifrada.

A la pràctica, l'aplicació de l'equació anterior equival a saltar des d'una posició inicial  $x$  fins a una altra posició  $mx$  múltiple d'aquesta i posteriorment desplaçar  $n$  posicions cap a la dreta o cap a l'esquerra de l'abecedari.

Cal afegir que aquesta equació modular comprèn totes les possibilitats de xifrat que ofereix l'algoritme no generalitzat de *Juli Cèsar*, ja que aquest algoritme representa el cas en què  $m=1$ .

Aquest algoritme generalitzat presenta un petit inconvenient, i és que a l'hora de desxifrar s'ha de calcular l'invers modular de  $m$ , que haurà de ser únic, i, tal i com s'ha comentat anteriorment, això només serà possible si  $m$  i  $N$  no tenen factors comuns, és a dir, que  $\text{mcd}(m, N)=1$ . D'aquesta forma evitarem les col·lisions (dues o mes entrades diferents que generen una mateixa sortida, ó, en el nostre cas, dues o més lletres diferents que queden xifrades de la mateixa forma) i podrem revertir el procés de xifrat per recuperar el missatge en clar sense cap tipus de dificultat.

Vegem alguns exemples pràctics per tal d'assimilar el funcionament d'aquest mètode i comprovar que l'equació modular exposada és vàlida. Suposem que la paraula que volem xifrar és **XIFRAT**. Si assignem un valor numèric a cadascuna de les lletres a partir de la taula anterior obtenim la seqüència numèrica 240906180120, de tal forma que cada parella de dígit correspon al valor de cadascuna de les lletres de la paraula que volem xifrar. Partint d'aquesta seqüència podem xifrar el missatge per diferents valors de  $m$  i  $n$ , tal i com es mostra a continuació.

- **Criptograma per  $m=3$  i  $n=3$ :** adaptant l'equació modular anterior a aquest cas obtenim l'expressió  $T_{(3,3)}(x) \equiv 3x + 3 \pmod{26}$  (en aquest cas podem comprovar fàcilment que no hi haurà col·lisions i que podrem invertir el procés de xifrat ja que  $\text{mcd}(3,26)=1$ ). Partint dels valors numèrics de les lletres passem a xifrar el missatge lletra per lletra:

- Lletra: **X**; valor numèric: 24; xifrat:  $T_{(3,3)}(24) \equiv 72 + 3 \equiv 23 \pmod{26}$
- Lletra: **I**; valor numèric: 09; xifrat:  $T_{(3,3)}(9) \equiv 27 + 3 \equiv 4 \pmod{26}$
- Lletra: **F**; valor numèric: 06; xifrat:  $T_{(3,3)}(6) \equiv 18 + 3 \equiv 21 \pmod{26}$
- Lletra: **R**; valor numèric: 18; xifrat:  $T_{(3,3)}(18) \equiv 54 + 3 \equiv 5 \pmod{26}$
- Lletra: **A**; valor numèric: 01; xifrat:  $T_{(3,3)}(1) \equiv 3 + 3 \equiv 6 \pmod{26}$
- Lletra: **T**; valor numèric: 20; xifrat:  $T_{(3,3)}(20) \equiv 60 + 3 \equiv 11 \pmod{26}$

Un cop tenim calculats els diferents valors numèrics corresponents a les lletres xifrades del missatge, l'únic que hem de fer és escriure les lletres que corresponen a aquests valors, tot observant la taula anterior. D'aquesta forma obtenim el criptograma **WDUEFK**.

- **Criptograma per  $m=5$  i  $n=7$ :** adaptant l'equació modular anterior a aquest cas obtenim l'expressió  $T_{(5,7)}(x) \equiv 5x + 7 \pmod{26}$  (en aquest cas podem comprovar fàcilment que no hi haurà col·lisions i que podrem revertir el procés de xifrat ja que  $\text{mcd}(5,26)=1$ ). Partint dels valors numèrics de les lletres passem a xifrar el missatge lletra per lletra:

- Lletra: **X**; valor numèric: 24; xifrat:  $T_{(5,7)}(24) \equiv 120 + 7 \equiv 23 \pmod{26}$
- Lletra: **I**; valor numèric: 09; xifrat:  $T_{(5,7)}(9) \equiv 45 + 7 \equiv 26 \equiv 0 \pmod{26}$
- Lletra: **F**; valor numèric: 06; xifrat:  $T_{(5,7)}(6) \equiv 30 + 7 \equiv 11 \pmod{26}$
- Lletra: **R**; valor numèric: 18; xifrat:  $T_{(5,7)}(18) \equiv 90 + 7 \equiv 19 \pmod{26}$
- Lletra: **A**; valor numèric: 01; xifrat:  $T_{(5,7)}(1) \equiv 5 + 7 \equiv 12 \pmod{26}$
- Lletra: **T**; valor numèric: 20; xifrat:  $T_{(5,7)}(20) \equiv 100 + 7 \equiv 3 \pmod{26}$

Un cop calculats els diferents valors numèrics corresponents a les lletres xifrades del missatge, l'únic que cal fer és escriure les lletres que corresponen a aquests valors, tot observant la taula anterior. D'aquesta forma obtenim el criptograma **WZKSLC**.

Ara que ja hem vist com es xifra amb l'equació modular exposada anteriorment ens falta saber com podem invertir el procés de xifrat per tornar a obtenir el missatge en clar.

Així doncs, per desxifrar necessitarem una altra equació modular, que obtindrem modificant l'equació inicial de xifrat. És a dir, que l'equació modular que farem servir per invertir el procés de xifrat serà aquesta (hem utilitzat la relació inversa  $x = T_{(m,n)}^{-1}(y)$ ):

$$T_{(m,n)}^{-1}(y) \equiv m^{-1}(y - n)(\text{mod } N), \forall y, m, n, N \in \mathbb{Z}.$$

Si volem obtenir resultats positius directament, sense haver de calcular congruències de nombres negatius amb el mòdul de treball podem modificar l'equació anterior, obtenint la següent expressió:

$$T_{(m,n)}^{-1}(y) \equiv m^{-1}(y + N - n)(\text{mod } N), \forall y, m, n, N \in \mathbb{Z}.$$

Tal i com podem observar, les dues equacions són com la que utilitzàvem per xifrar, amb la diferència que en aquest cas hem aïllat la variable  $x$ . Cal remarcar que les dues equacions són vàlides per desxifrar, però la segona simplifica els càlculs, ja que no apareixeran valors de  $x$  negatius.

Per tal de comprovar que l'equació exposada permet revertir els processos de xifrat adjuntarem un exemple pràctic en el que desxifrarem un criptograma obtingut amb l'equació modular inicial.

Suposem que tenim el criptograma **WZKSLC**, i sabem que la clau de xifrat és  $k = (5, 7)$  i amb  $N = 26$  com a mòdul de treball. És a dir, que l'equació de desxifrat que utilitzarem serà la següent:

$$T_{(5,7)}^{-1}(y) \equiv 5^{-1}(y + 19)(\text{mod } 26)$$

Abans de començar a substituir els valors numèrics a l'equació modular per tal de recuperar el missatge en clar calcularem l'invers modular de 5 a  $\mathbb{Z}/_{26}\mathbb{Z}$ , per tal de facilitar els càlculs posteriors. Aplicant l'algoritme d'Euclides modificat per calcular inversos modulars obtenim que  $5^{-1} \equiv 21(\text{mod } 26)$ .

Un cop calculat l'invers modular de 5 a  $\mathbb{Z}/_{26}\mathbb{Z}$ , modifiquem l'equació de desxifrat substituint  $5^{-1}$  pel seu valor congruent, que és 21, i obtenim la següent expressió:

$$T_{(5,7)}^{-1}(y) \equiv 21(y + 19) \equiv 21y + 9(\text{mod } 26)$$

Arribats a aquest punt ja podem passar a desxifrar el missatge tot substituint a l'equació anterior els valors de cadascuna de les lletres que el formen:

- Xifrat: **W**; valor numèric: 23; desxifrat:  $T_{(5,7)}^{-1}(23) \equiv 483 + 9 \equiv 24(\text{mod } 26)$
- Xifrat: **Z**; valor numèric: 00; desxifrat:  $T_{(5,7)}^{-1}(0) \equiv 9(\text{mod } 26)$
- Xifrat: **K**; valor numèric: 11; desxifrat:  $T_{(5,7)}^{-1}(11) \equiv 231 + 9 \equiv 6(\text{mod } 26)$
- Xifrat: **S**; valor numèric: 19; desxifrat:  $T_{(5,7)}^{-1}(19) \equiv 399 + 9 \equiv 18(\text{mod } 26)$
- Xifrat: **L**; valor numèric: 12; desxifrat:  $T_{(5,7)}^{-1}(12) \equiv 252 + 9 \equiv 1(\text{mod } 26)$
- Xifrat: **C**; valor numèric: 03; desxifrat:  $T_{(5,7)}^{-1}(3) \equiv 63 + 9 \equiv 20(\text{mod } 26)$

Si substituïm els valors numèrics obtinguts per les lletres corresponents obtenim la paraula **XIFRAT**, que és el missatge en clar.

Com hem pogut comprovar, l'equació modular de desxifrat proposada ens serveix per revertir els processos de xifrat, de tal forma que ens permet recuperar el missatge en clar.

Ja hem vist com podem xifrar i desxifrar missatges utilitzant l'algoritme generalitzat de *Juli Cèsar*, però encara falta comentar una petita qüestió abans de tancar aquest apartat.

Anteriorment hem parlat de col·lisions, és a dir, quan dues o més lletres diferents xifren d'una mateixa forma. A continuació es mostraran alguns exemples de col·lisions obtingudes a partir d'una clau de xifrat  $k$  i un mòdul de treball  $N$  que ho permetin.

- **Càlcul de col·lisions per  $k=(2,1)$  i  $N=26$ :** podem observar que en aquest cas poden aparèixer col·lisions en el procés de xifrat, ja que  $\text{mcd}(2,26)=2 \neq 1$ . Partint de les dades anteriors obtenim l'equació de xifrat, que en aquest cas és  $T_{(2,1)}(x) \equiv 2x + 1(\text{mod } N)$ :

- Llettra: **A**; valor numèric: 01; xifrat:  $T_{(2,1)}(1) \equiv 2 + 1 \equiv 3(\text{mod } 26)$
- Llettra: **N**; valor numèric: 14; xifrat:  $T_{(2,1)}(14) \equiv 28 + 1 \equiv 3(\text{mod } 26)$
- Llettra: **B**; valor numèric: 02; xifrat:  $T_{(2,1)}(2) \equiv 4 + 1 \equiv 5(\text{mod } 26)$
- Llettra: **O**; valor numèric: 15; xifrat:  $T_{(2,1)}(15) \equiv 30 + 1 \equiv 5(\text{mod } 26)$
- Llettra: **C**; valor numèric: 03; xifrat:  $T_{(2,1)}(3) \equiv 6 + 1 \equiv 7(\text{mod } 26)$
- Llettra: **P**; valor numèric: 16; xifrat:  $T_{(2,1)}(16) \equiv 32 + 1 \equiv 7(\text{mod } 26)$

- Lletra: **D**; valor numèric: 04; xifrat:  $T_{(2,1)}(4) \equiv 8 + 1 \equiv 9(\text{mod } 26)$
- Lletra: **Q**; valor numèric: 17; xifrat:  $T_{(2,1)}(17) \equiv 34 + 1 \equiv 9(\text{mod } 26)$
- Lletra: **E**; valor numèric: 05; xifrat:  $T_{(2,1)}(5) \equiv 10 + 1 \equiv 11(\text{mod } 26)$
- Lletra: **R**; valor numèric: 18; xifrat:  $T_{(2,1)}(18) \equiv 36 + 1 \equiv 11(\text{mod } 26)$
- Lletra: **F**; valor numèric: 06; xifrat:  $T_{(2,1)}(6) \equiv 12 + 1 \equiv 13(\text{mod } 26)$
- Lletra: **S**; valor numèric: 19; xifrat:  $T_{(2,1)}(19) \equiv 38 + 1 \equiv 13(\text{mod } 26)$
- Lletra: **G**; valor numèric: 07; xifrat:  $T_{(2,1)}(7) \equiv 14 + 1 \equiv 15(\text{mod } 26)$
- Lletra: **T**; valor numèric: 20; xifrat:  $T_{(2,1)}(20) \equiv 40 + 1 \equiv 15(\text{mod } 26)$
- Lletra: **H**; valor numèric: 08; xifrat:  $T_{(2,1)}(8) \equiv 16 + 1 \equiv 17(\text{mod } 26)$
- Lletra: **U**; valor numèric: 21; xifrat:  $T_{(2,1)}(21) \equiv 42 + 1 \equiv 17(\text{mod } 26)$
- Lletra: **I**; valor numèric: 09; xifrat:  $T_{(2,1)}(9) \equiv 18 + 1 \equiv 19(\text{mod } 26)$
- Lletra: **V**; valor numèric: 22; xifrat:  $T_{(2,1)}(22) \equiv 44 + 1 \equiv 19(\text{mod } 26)$
- Lletra: **J**; valor numèric: 10; xifrat:  $T_{(2,1)}(10) \equiv 20 + 1 \equiv 21(\text{mod } 26)$
- Lletra: **W**; valor numèric: 23; xifrat:  $T_{(2,1)}(23) \equiv 46 + 1 \equiv 21(\text{mod } 26)$
- Lletra: **K**; valor numèric: 11; xifrat:  $T_{(2,1)}(11) \equiv 22 + 1 \equiv 23(\text{mod } 26)$
- Lletra: **X**; valor numèric: 24; xifrat:  $T_{(2,1)}(24) \equiv 48 + 1 \equiv 23(\text{mod } 26)$
- Lletra: **L**; valor numèric: 12; xifrat:  $T_{(2,1)}(12) \equiv 24 + 1 \equiv 25(\text{mod } 26)$
- Lletra: **Y**; valor numèric: 25; xifrat:  $T_{(2,1)}(25) \equiv 50 + 1 \equiv 25(\text{mod } 26)$
- Lletra: **M**; valor numèric: 13; xifrat:  $T_{(2,1)}(13) \equiv 26 + 1 \equiv 1(\text{mod } 26)$
- Lletra: **Z**; valor numèric: 26; xifrat:  $T_{(2,1)}(26) \equiv 52 + 1 \equiv 1(\text{mod } 26)$

Tal i com podem observar, utilitzant l'equació modular obtinguda per  $k=(2,1)$  i  $N=26$  ha generat 13 col·lisions en el xifrat, la qual cosa vol dir que la combinació de  $k$  i  $N$  utilitzada no és vàlida per xifrar missatges.

### 3.3. Criptoanàlisi clàssic: anàlisi de freqüències

#### 3.3.1. Descripció i procediment

Criptoanàlisi és l'estudi dels mètodes per obtenir un missatge en clar partint del criptograma d'aquest missatge, sense conèixer la informació secreta requerida per desxifrar-lo normalment. És a dir, que estem parlant de trencar o forçar el codi.

Encara que l'objectiu ha estat sempre el mateix, els mètodes i tècniques del Criptoanàlisi han canviat dràsticament a través de la història de la Criptografia, adaptant-se a una creixent complexitat criptogràfica, que abasta des dels mètodes de llapis i paper del passat, passant per màquines com l'*Enigma*, utilitzada durant la Segona Guerra Mundial, fins als sistemes basats en computadores del present.

Els resultats del Criptoanàlisi han canviat també: ja no és possible tenir un èxit il·limitat al trencar un codi. Bàsicament podem distingir dos tipus de Criptoanàlisi, el clàssic, que comprèn els mètodes per desxifrar criptogrames obtinguts amb algorismes de la Criptografia clàssica, i el modern, que comprèn els mètodes de desxifrat de criptogrames generats amb algorismes de xifrat pertanyents a la Criptografia moderna.

Cal afegir que en aquest projecte no es tractarà el Criptoanàlisi de forma exhaustiva, ja que aquest no és un dels objectius del treball.

No obstant això, a continuació mostrarem el funcionament d'un dels mètodes de Criptoanàlisi clàssic més coneguts i més utilitzats per desxifrar criptogrames obtinguts a partir de mètodes clàssics de substitució, tals com el de *Juli Cèsar* o el de *Polybius*.

Com a curiositat cal afegir que partint d'anàlisis freqüencials es van aconseguir desxifrar els jeroglífics egipcis. [12.2]

En Criptoanàlisi, l'anàlisi de freqüències és l'estudi de les freqüències amb que apareixen les lletres o grups de lletres en un text xifrat.

Està basat en el fet que, donat un text, certes lletres o combinacions de lletres apareixen més sovint que unes altres, existint diferents freqüències per a elles. És més, per a cada llenguatge, cada lletra té una freqüència d'aparició concreta, que es manté en la majoria de textos escrits en el mateix llenguatge.

Per exemple, en anglès la lletra I és molt comuna, mentre que la X és molt rara. Igualment, les combinacions ST, NG, TH i QU són parells de lletres comunes, mentre que NZ i QJ són rars. En el castellà i el català, les vocals són molt freqüents, ocupant al voltant del 45% del text.

En els algorismes de xifrat basats en la substitució, cada lletra del text en clar es reemplaça per una altra, i una lletra donada del text en clar sempre tindrà el mateix xifrat. És a dir, que si la lletra E és xifrada com a X, i en el text xifrat n'apareixen moltes, un criptoanalista podria suposar que la X correspon a la E.

En la majoria dels casos per desxifrar un criptograma no n'hi ha prou amb l'anàlisi de les freqüències de les lletres, i s'han d'analitzar altres freqüències, tals com les de les síl·labes o les de combinacions de dues o tres lletres.

Bàsicament el procediment per realitzar un anàlisi de freqüències és el següent:

1. Calcular la freqüència d'aparició de les lletres que formen el text xifrat.
2. Obtenir una taula de freqüències mitjanes d'aparició de les lletres en la llengua en la que estava escrit el text en clar (si no se sap en quina llengua estava escrit el text abans de ser xifrat la tasca per intentar desxifrar el criptograma es complica considerablement).
3. Comparar les freqüències d'aparició de les lletres en el text xifrat amb les freqüències de la taula, i intentar fer associacions per tal de poder desxifrar total o parcialment el missatge.

Les taules de freqüències mitjanes d'aparició de les lletres en cadascuna de les llengües mostren dades que moltes vegades no es correspondran completament amb les dades extretes d'un criptograma. Aquest és un dels motius pels quals resulta complex poder desxifrar completament un missatge amb aquest mètode.

Cal dir que aquestes taules normalment es generen a partir de textos molts llargs i de continguts temàtics molt variats. Això és així per tal que les freqüències mitjanes obtingudes s'ajustin amb més exactitud a qualsevol tipus de missatge que es vulgui desxifrar.

A continuació adjuntarem les taules de freqüències mitjanes de lletres i síl·labes en les llengües més comunes per nosaltres, que són el català, el castellà i l'anglès. [13]  
Cal remarcar que aquestes taules s'han generat a partir de textos de més de 1.500.000 caràcters. No obstant això, les freqüències calculades a partir de qualsevol altre text sempre seran lleugerament diferents.

Aquestes taules s'han obtingut amb l'ajuda d'un software gratuït que s'anomena **WordCreator**. [13]

Per tal que s'entengui el funcionament d'aquest programa informàtic i que qualsevol persona pugui calcular les freqüències d'aparició de les lletres en qualsevol text, s'adjuntarà un petit tutorial on tractarem aquestes i altres qüestions relacionades amb el programa, i en comentarem les funcions principals.

### 3.3.2. Taules de freqüències

#### 3.3.2.1. Taules de freqüències del català

Aquesta és la taula de les freqüències d'aparició de les lletres:

<b>A</b>	13.04%	<b>S</b>	7.94%
<b>B</b>	1.48%	<b>T</b>	6.31%
<b>C</b>	3.24%	<b>U</b>	4.12%
<b>D</b>	3.36%	<b>V</b>	2.17%
<b>E</b>	13.18%	<b>W</b>	0.04%
<b>F</b>	0.82%	<b>X</b>	0.51%
<b>G</b>	1.24%	<b>Y</b>	0.15%
<b>H</b>	0.82%	<b>Z</b>	0.10%
<b>I</b>	6.26%	<b>Ç</b>	0.12%
<b>J</b>	0.39%	<b>À</b>	0.31%
<b>K</b>	0.11%	<b>È</b>	0.32%
<b>L</b>	6.41%	<b>É</b>	0.71%
<b>M</b>	3.49%	<b>Í</b>	0.22%
<b>N</b>	6.20%	<b>Ï</b>	0.02%
<b>O</b>	4.70%	<b>Ò</b>	0.26%
<b>P</b>	2.93%	<b>Ó</b>	0.42%
<b>Q</b>	1.27%	<b>Ú</b>	0.11%
<b>R</b>	7.12%	<b>Û</b>	0.04%

Aquesta és la taula de les freqüències d'aparició d'algunes síl·labes formades per dues lletres (només hi ha les síl·labes que presenten una freqüència d'aparició igual o superior al 0.75%):

<b>AL</b>	1.25%	<b>NA</b>	1.01%
<b>AM</b>	0.88%	<b>NO</b>	0.77%
<b>AN</b>	1.31%	<b>NT</b>	1.64%
<b>AR</b>	1.84%	<b>ON</b>	0.76%
<b>AT</b>	1.04%	<b>OR</b>	0.89%
<b>CA</b>	0.93%	<b>PE</b>	1.31%
<b>CI</b>	0.75%	<b>QU</b>	1.65%
<b>CO</b>	1.08%	<b>RA</b>	1.54%
<b>DE</b>	2.12%	<b>RE</b>	1.84%
<b>EL</b>	2.00%	<b>RI</b>	0.75%
<b>EN</b>	2.79%	<b>SA</b>	0.79%
<b>ER</b>	2.55%	<b>SE</b>	1.52%
<b>ES</b>	2.97%	<b>ST</b>	1.11%
<b>IA</b>	0.78%	<b>TA</b>	1.65%
<b>IN</b>	0.81%	<b>TE</b>	1.02%
<b>LA</b>	1.87%	<b>TI</b>	0.78%
<b>LE</b>	0.91%	<b>UE</b>	1.36%
<b>LL</b>	1.06%	<b>UN</b>	1.12%
<b>ME</b>	1.07%	<b>VA</b>	1.35%

### 3.3.2.2. Taules de freqüències del castellà

Aquesta és la taula de les freqüències d'aparició de les lletres:

<b>A</b>	11.72%	<b>Q</b>	1.11%
<b>B</b>	1.49%	<b>R</b>	6.41%
<b>C</b>	3.87%	<b>S</b>	7.20%
<b>D</b>	4.67%	<b>T</b>	4.60%
<b>E</b>	13.72%	<b>U</b>	4.55%
<b>F</b>	0.69%	<b>V</b>	1.05%
<b>G</b>	1.00%	<b>W</b>	0.04%
<b>H</b>	1.18%	<b>X</b>	0.14%
<b>I</b>	5.28%	<b>Y</b>	1.09%
<b>J</b>	0.52%	<b>Z</b>	0.47%
<b>K</b>	0.11%	<b>Ñ</b>	0.17%
<b>L</b>	5.24%	<b>Á</b>	0.44%
<b>M</b>	3.08%	<b>É</b>	0.36%
<b>N</b>	6.83%	<b>Í</b>	0.70%
<b>O</b>	8.44%	<b>Ó</b>	0.76%
<b>P</b>	2.89%	<b>Ú</b>	0.12%
		<b>Ü</b>	0.02%

Aquesta és la taula de les freqüències d'aparició d'algunes síl·labes formades per dues lletres (només hi ha les síl·labes que presenten una freqüència d'aparició igual o superior al 0.75%):

<b>AD</b>	1.02%	<b>NA</b>	0.88%
<b>AL</b>	0.91%	<b>NO</b>	0.82%
<b>AN</b>	1.15%	<b>NT</b>	1.68%
<b>AR</b>	1.54%	<b>ON</b>	1.15%
<b>AS</b>	1.28%	<b>OR</b>	1.04%
<b>CI</b>	0.98%	<b>OS</b>	1.73%
<b>CO</b>	1.31%	<b>PA</b>	0.88%
<b>DE</b>	2.77%	<b>QU</b>	1.44%
<b>DO</b>	1.35%	<b>RA</b>	1.83%
<b>EL</b>	1.40%	<b>RE</b>	1.29%
<b>EN</b>	3.01%	<b>RO</b>	0.85%
<b>ER</b>	2.25%	<b>SE</b>	0.99%
<b>ES</b>	2.20%	<b>ST</b>	1.09%
<b>IE</b>	1.01%	<b>TA</b>	1.38%
<b>IN</b>	0.77%	<b>TE</b>	1.55%
<b>LA</b>	1.91%	<b>TO</b>	1.11%
<b>LO</b>	1.10%	<b>UE</b>	2.03%
<b>ME</b>	0.80%	<b>UN</b>	1.07%

### 3.3.2.3. Taules de freqüències de l'anglès

Aquesta és la taula de les freqüències d'aparició de les lletres:

<b>A</b>	8.34%	<b>N</b>	6.80%
<b>B</b>	1.54%	<b>O</b>	7.70%
<b>C</b>	2.73%	<b>P</b>	1.66%
<b>D</b>	4.14%	<b>Q</b>	0.09%
<b>E</b>	12.60%	<b>R</b>	5.68%
<b>F</b>	2.03%	<b>S</b>	6.11%
<b>G</b>	1.92%	<b>T</b>	9.37%
<b>H</b>	6.11%	<b>U</b>	2.85%
<b>I</b>	6.71%	<b>V</b>	1.06%
<b>J</b>	0.23%	<b>W</b>	2.34%
<b>K</b>	0.87%	<b>X</b>	0.20%
<b>L</b>	4.24%	<b>Y</b>	2.04%
<b>M</b>	2.53%	<b>Z</b>	0.06%

Aquesta és la taula de les freqüències d'aparició d'algunes síl·labes formades per dues lletres (només hi ha les síl·labes que presenten una freqüència d'aparició igual o superior al 0.75%):

<b>AL</b>	0.93%	<b>ME</b>	0.83%
<b>AN</b>	2.17%	<b>ND</b>	1.62%
<b>AR</b>	1.06%	<b>NE</b>	0.75%
<b>AS</b>	1.09%	<b>NG</b>	0.99%
<b>AT</b>	1.17%	<b>NT</b>	0.77%
<b>EA</b>	0.84%	<b>ON</b>	1.36%
<b>ED</b>	1.29%	<b>OR</b>	1.09%
<b>EN</b>	1.37%	<b>OU</b>	1.41%
<b>ER</b>	2.11%	<b>RE</b>	1.64%
<b>ES</b>	1.00%	<b>SE</b>	0.85%
<b>HA</b>	1.17%	<b>ST</b>	0.96%
<b>HE</b>	3.65%	<b>TE</b>	1.00%
<b>HI</b>	1.07%	<b>TH</b>	3.99%
<b>IN</b>	2.10%	<b>TI</b>	0.92%
<b>IS</b>	0.99%	<b>TO</b>	1.24%
<b>IT</b>	1.24%	<b>VE</b>	1.11%
<b>LE</b>	0.95%	<b>WA</b>	0.84%

### 3.3.3. Tutorial del software *WordCreator*

Les taules de freqüències anteriors s'han generat a partir del programa informàtic *WordCreator*. Per aquest motiu s'ha elaborat aquest tutorial, en el que es descriuen els passos que s'han de seguir per poder obtenir les freqüències d'aparició de lletres i síl·labes en qualsevol text.

El primer que cal fer és obtenir el programa, que al ser gratuït, es pot baixar d'Internet sense haver de pagar una llicència.

Principalment aquest software presenta dos avantatges importants: primerament és un programa que no necessita ser instal·lat, simplement consta d'un únic arxiu executable; el segon avantatge és que aquest arxiu ocupa molt poca memòria, uns 974KB, la qual cosa vol dir que fins i tot pot ser copiat i executat des d'un disquet de 3½, d'aquells que s'utilitzaven abans i que tenien una forma quadrada.

La versió del programa que hem fet servir és la 1.0.0.0, l'aspecte que presenta l'arxiu dins d'una carpeta és aquest:



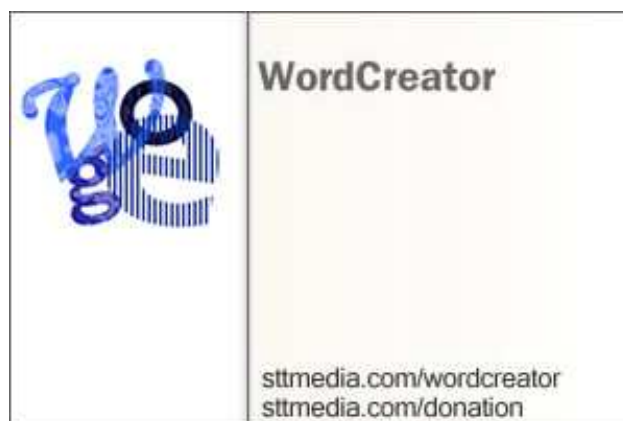
**Figura 5:** Icona del programa *WordCreator*.

El valor del *HASH MD5* de l'arxiu que nosaltres hem fet servir és el següent:

D86868E0929B195E21807636D94AB4DC

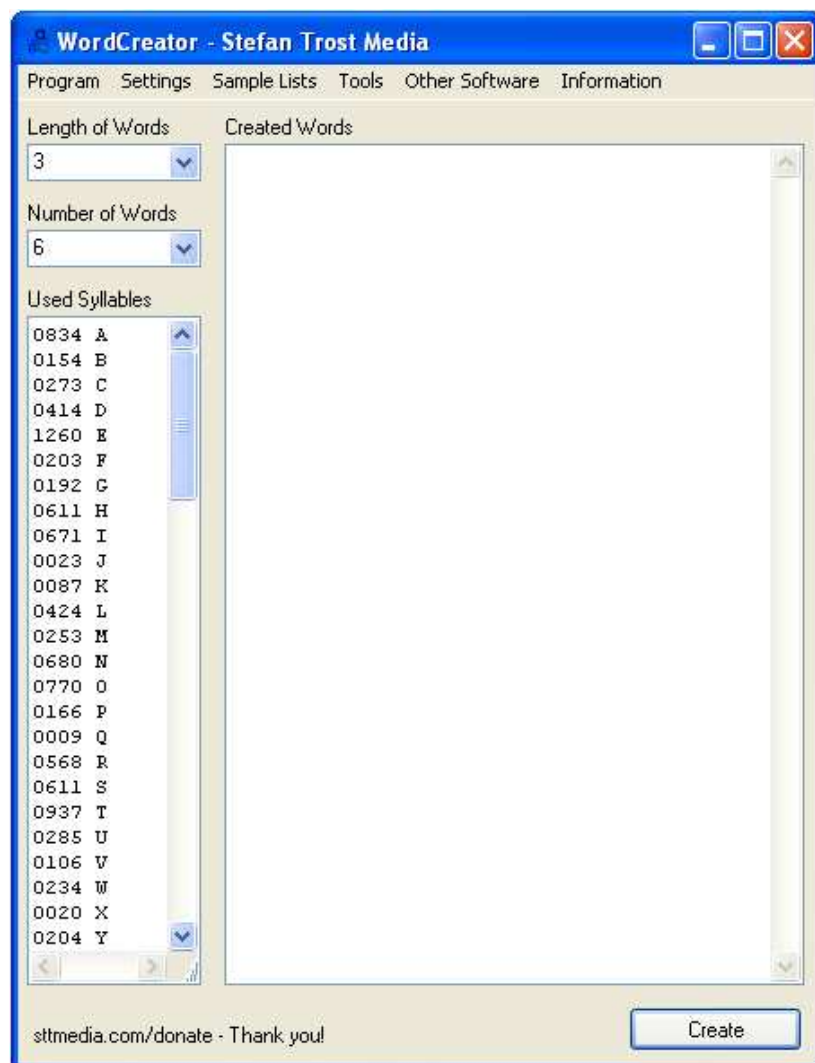
Aquest valor s'adjunta per tal de comprovar que l'arxiu descarregat no ha estat modificat n'hi combinat amb codi maliciós (aquest valor *HASH* només servirà per comprovar la fiabilitat d'un arxiu executable *WordCreator.exe* que sigui exactament igual que el que hem utilitzat, ja que si agafem una altra versió del programa, el *HASH* serà diferent, però no podrem saber si hi ha hagut modificacions de l'arxiu original).

Un cop tenim el programa, l'executem en un ordinador qualsevol, i ens apareixerà la següent pantalla, a mode de presentació del software:



**Figura 6:** Pantalla de presentació del programa *WordCreator*.

Aquest requadre de presentació del programa apareixerà durant uns segons, i posteriorment sortirà la pantalla principal del software, que és la següent:



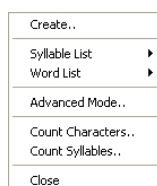
**Figura 7:** Pantalla principal del programa *WordCreator*.

El programa està en anglès, però és molt fàcil d'utilitzar, a més nosaltres només utilitzarem dues de les funcions que ens ofereix, per tant els procediments a seguir resulten molt senzills.

Començarem explicant com calcular les freqüències d'aparició de les lletres en un text qualsevol.

Per aconseguir-ho, el primer que hem de fer és anar a la barra de tasques del programa, situada just a sota de la capçalera d'aquest i clicar a sobre de l'opció **Program**.

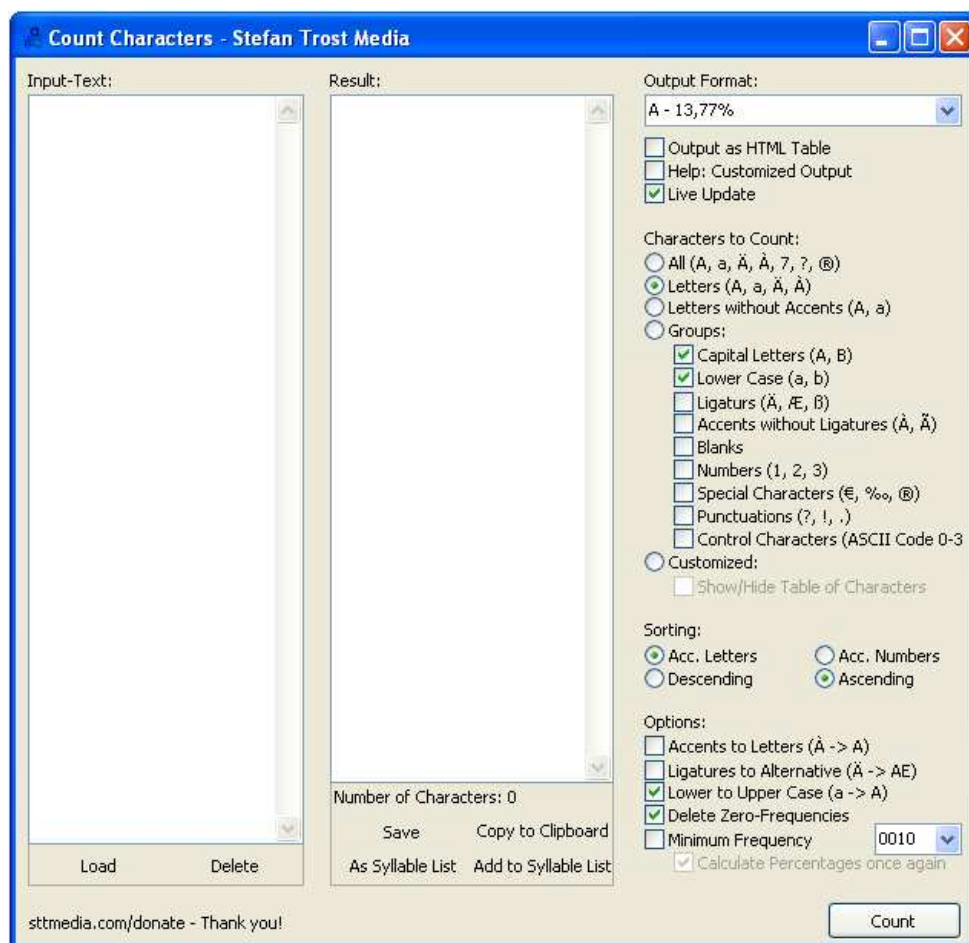
Un cop fet això ens apareixerà un menú desplegable amb diverses funcions, com aquest:



**Figura 8:** Menú desplegable del programa *WordCreator*.

De totes les opcions que ens ofereix aquest menú, seleccionarem l'opció de **Count Characters...**

Un cop seleccionada aquesta opció ens apareixerà una altra pantalla, tal com aquesta:



**Figura 9:** Pantalla d'anàlisi del programa *WordCreator*.

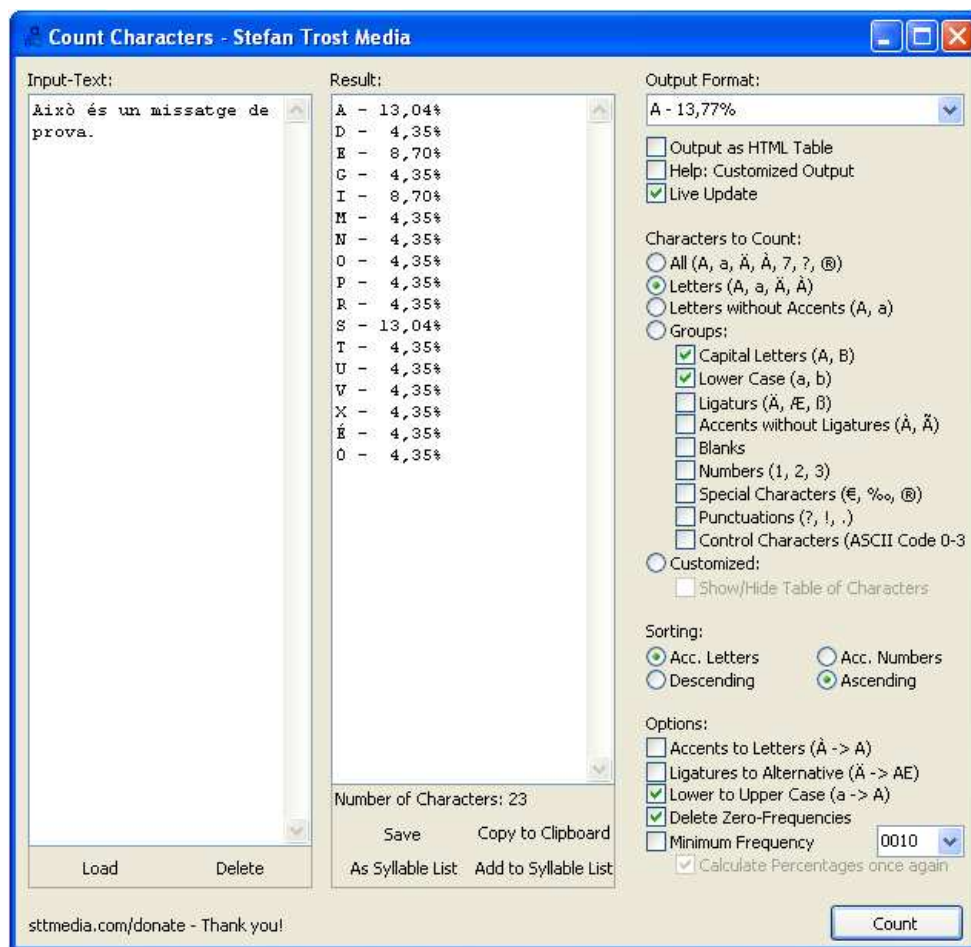
Podem observar dos grans rectangles blancs i a la dreta d'aquests, un seguit d'opcions, algunes de les quals estan activades i altres no. Després de realitzar algunes proves hem arribat a la conclusió que no cal tocar la configuració inicial d'opcions que presenta el programa, és a dir, que el deixarem tal com es pot veure en la imatge anterior.

Un cop tenim aquesta pantalla oberta, només cal introduir el text que es vol analitzar en el rectangle blanc de l'esquerra de tot.

Posteriorment, ja només quedarà clicar sobre la icona **Count**, situada a la part inferior dreta de la pantalla.

Al fer-ho, el programa analitzarà el text introduït i ens mostrarà les freqüències d'aparició de les lletres en el segon rectangle blanc.

Suposem que volem analitzar el text següent: *Això és un missatge de prova.*  
L'introduïm al programa i li donem l'ordre d'anàlisi, i obtenim el següent:

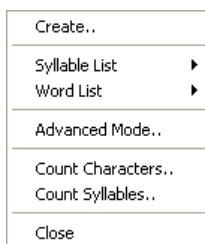


**Figura 10:** Pantalla d'anàlisi del programa *WordCreator*.

I així és com s'obtenen les freqüències d'aparició de les lletres en un text determinat. A continuació passarem a descriure els passos que s'han de seguir per tal de poder calcular les freqüències d'aparició d'algunes síl·labes en un text determinat.

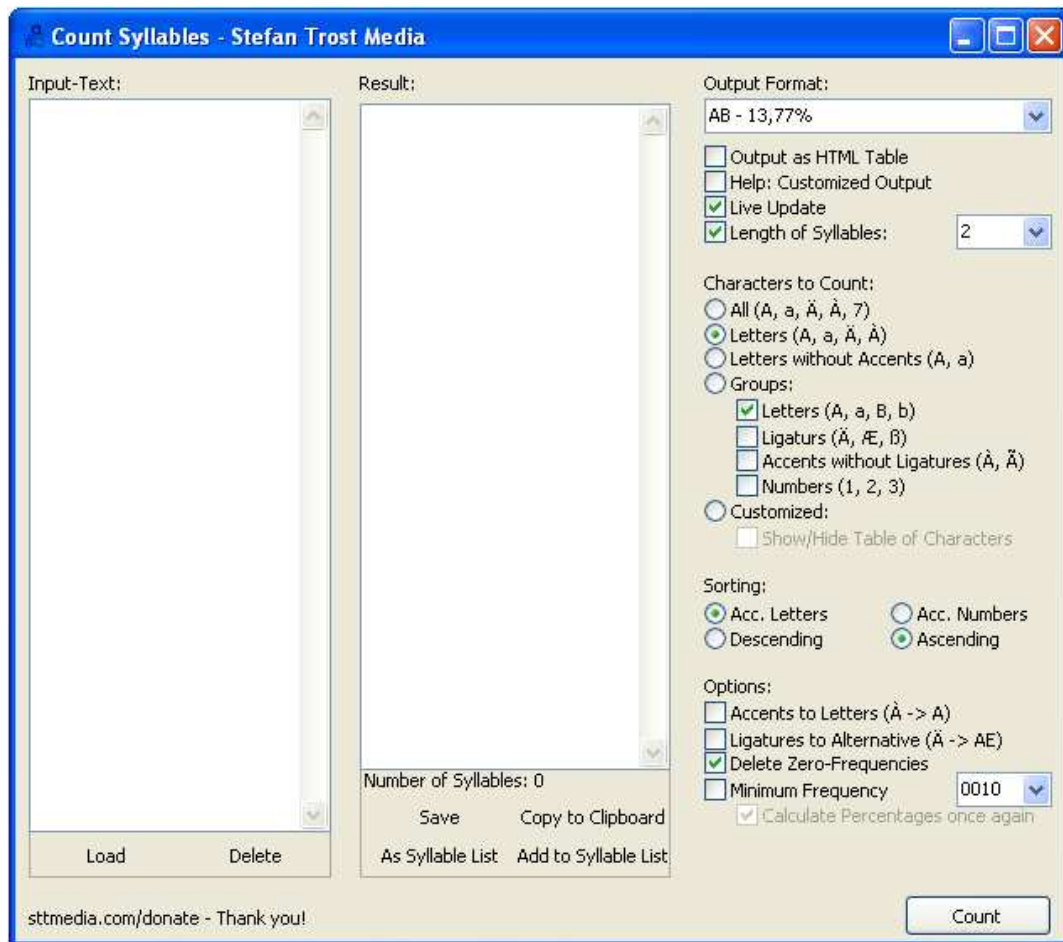
Per aconseguir-ho, el primer que hem de fer és anar a la barra de tasques del programa, situada just a sota de la capçalera d'aquest i clicar a sobre de l'opció **Program**.

Un cop fet això ens apareixerà un menú desplegable amb diverses funcions, com aquest:



**Figura 11:** Menú desplegable del programa *WordCreator*.

En aquest cas seleccionarem l'opció de **Count Syllables...**.  
Un cop seleccionada aquesta opció ens apareixerà una altra pantalla, tal com aquesta:

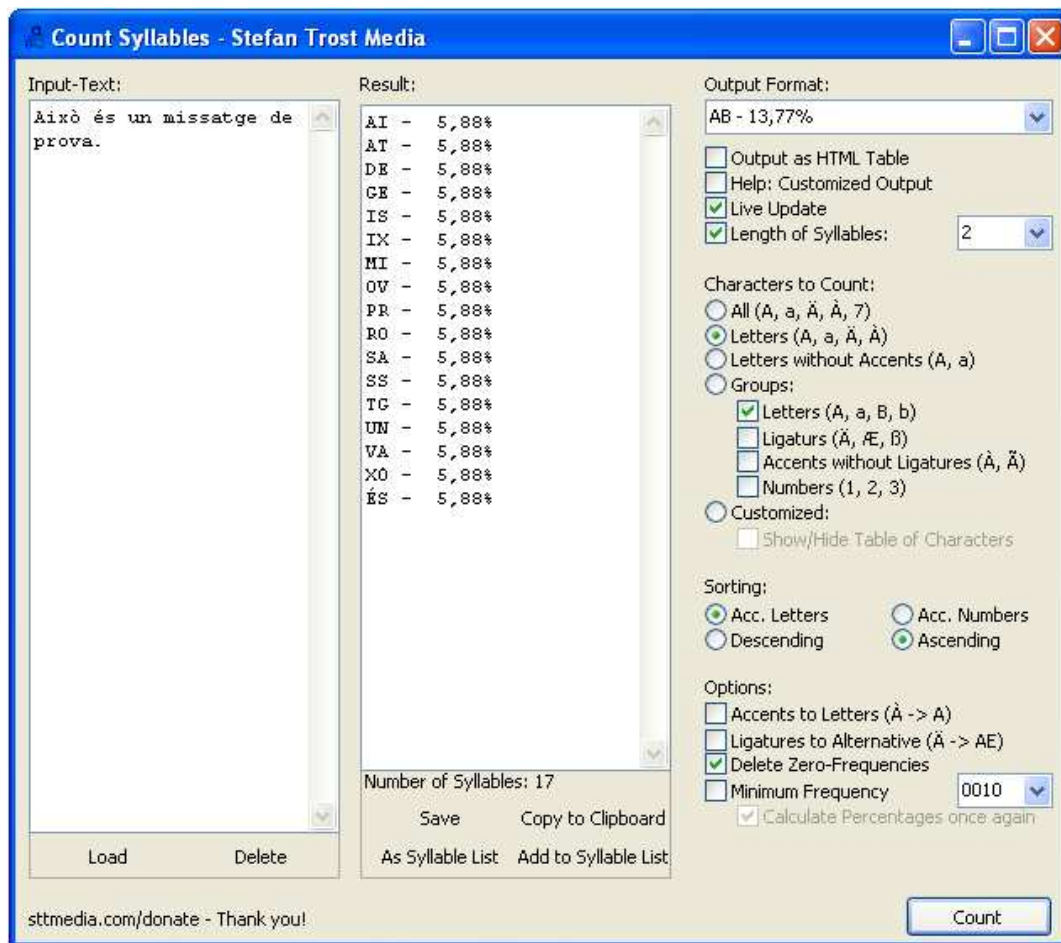


**Figura 12:**Pantalla d'anàlisi del programa *WordCreator*.

El funcionament és el mateix que en el cas anterior. Per que fa a la configuració del programa, també deixarem la que ens ofereix el programa. La configuració que s'observa a la imatge ens permetrà calcular freqüències d'aparició de síl·labes formades per dos caràcters. Si volem calcular freqüències de síl·labes amb un nombre major de caràcters, l'únic que hem de fer és seleccionar la longitud que vulguem en el rectangle situat a la dreta de la pantalla, que presenta un número 2, en la imatge.

Posteriorment introduïm el text i cliquem sobre la icona **Count**, i el programa ens calcularà les freqüències que necessitem.

Suposem que volem analitzar el text següent: *Això és un missatge de prova.*  
L'introduïm al programa i li donem l'ordre d'anàlisi, i obtenim el següent:



**Figura 13:** Pantalla d'anàlisi del programa *WordCreator*.

D'aquesta forma, el programa ens genera totes les síl·labes de dos caràcters presents en el text i també ens indica la freqüència d'aparició de cadascuna d'elles.

Ja hem vist com es calculen les freqüències d'aparició de lletres i síl·labes en un text qualsevol, per tant podem donar per finalitzat aquest petit tutorial del programa informàtic *WordCreator*.

En el següent apartat presentarem un exemple pràctic en el que intentarem desxifrar un criptograma sense disposar de la clau de xifrat, per tal d'aplicar tots els coneixements que s'han exposat anteriorment.

### 3.3.4. De la teoria a la pràctica: anàlisi freqüencial

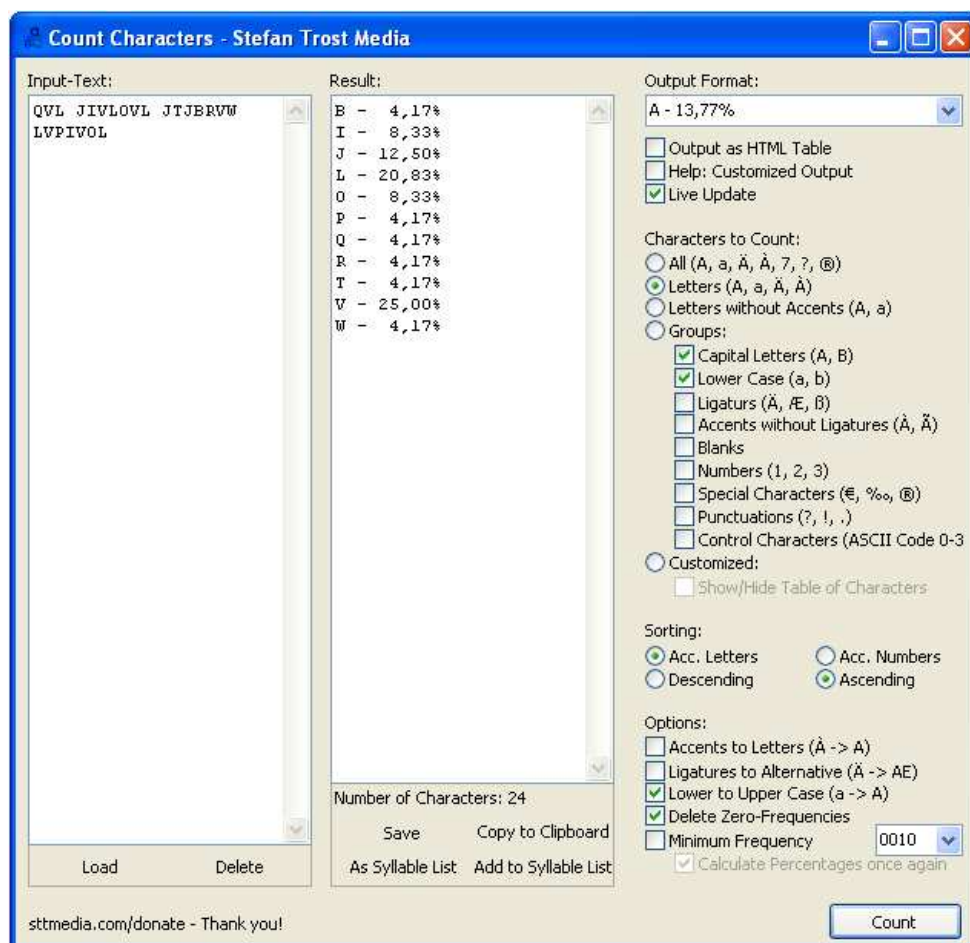
Ara que ja hem vist la part teòrica de l'anàlisi freqüencial podem posar-ho en pràctica per tal d'intentar recuperar el text en clar partint del criptograma d'aquest, generat amb un algoritme basat en la substitució, com per exemple l'algoritme generalitzat de *Juli Cèsar*.

Suposem que som criptoanalistes professionals que treballem pel servei secret i que la nostra feina és desxifrar conversacions confidencials. Ara imaginem que un dia interceptem el següent missatge:

***QVL JIVLOVL JTJBRVW LVPIVOL***

La nostra feina és intentar descobrir quina informació amaga aquest criptosistema, és a dir, que hem de reconstruir el text en clar que forma el missatge partint de la versió xifrada.

Com que no sabem amb seguretat quin mètode s'ha utilitzat per xifrar el missatge, haurem de començar per l'atac més simple que coneixem, que és l'anàlisi freqüencial. Així doncs, amb el programa informàtic ***WordCreator*** calcularem les freqüències d'aparició de cadascuna de les lletres en el text, i obtenim el següent:



**Figura 14:** Pantalla d'anàlisi del programa *WordCreator*.

Partint de la informació que ens proporciona el programa, elaborem la taula de freqüències que haurem d'estudiar per tal de desxifrar el criptograma:

<b>B</b>	4.17%
<b>I</b>	8.33%
<b>J</b>	12.50%
<b>L</b>	20.83%
<b>O</b>	8.33%
<b>P</b>	4.17%
<b>Q</b>	4.17%
<b>R</b>	4.17%
<b>T</b>	4.17%
<b>V</b>	25.00%
<b>W</b>	4.17%

A continuació passem a estudiar les dades de la taula. Bàsicament podem observar que hi ha 5 freqüències diferents, però crida l'atenció el fet que tres d'elles són considerablement majors que les altres dues. Per tant, primer de tot suposarem que el missatge original està escrit en llengua catalana, i posteriorment passarem a comparar la taula anterior amb la taula de freqüències mitjanes de la llengua catalana.

Així doncs, agafem la taula de freqüències de les lletres en la llengua catalana i mirem quines són les tres lletres que tinguin freqüències d'aparició altes.

Tal i com podem observar, les tres lletres que tenen les freqüències d'aparició més altes són la E, la A i la S, amb freqüències de 13.18%, 13.04% i 7.94%, respectivament.

Per tant podem suposar que les lletres V, L i J del missatge xifrat corresponen a les lletres E, A i S del missatge en clar, tot i que no necessàriament en aquest ordre de correspondència. Així doncs, hem de trobar la correspondència correcta entre aquestes lletres.

A partir de la comparació de les freqüències podem suposar que la lletra V del criptograma, que apareix amb una freqüència relativament elevada, correspon a la lletra E del missatge en clar, ja que aquesta lletra és la que té la freqüència d'aparició més alta en llengua catalana.

Per tant substituïm totes les lletres V del criptograma per lletres E, i obtenim el següent:

***QEL JIELOEL JTJBREW LEPIEOL***

A simple vista sembla que les posicions de les lletres E en el text no presenten cap tipus d'incoherència, per tant podem pensar que de moment les suposicions que hem fet són correctes.

Ara que ja hem agrupat dues de les sis lletres proposades anteriorment, intentarem relacionar les altres quatre.

Sabem que en la llengua catalana la segona lletra amb la freqüència d'aparició elevada és la A. Per tant podem pensar que les lletres L del criptograma corresponen a lletres A en el text en clar. Però no en podem estar segurs al 100%, la qual cosa vol dir que podria ser que les lletres J correspongessin a les lletres A en el text en clar.

Com que no podem extreure una conclusió fiable, escriurem les dues possibilitats que se'ns plantegen, i intentarem descartar-ne alguna a partir de les incoherències que puguin aparèixer en el criptograma.

Així doncs obtenim aquestes dues possibles solucions:

***QEA JIEAOEA JTJBREW AEPIEOA***

***QEL AIELLOEL ATABREW LEPIEOL***

A simple vista sembla que la primera possibilitat és incorrecta, ja que apareixen juntes moltes vegades les lletres A i E, la qual cosa no és molt comuna en català, tal i com podem observar en la taula de les freqüències d'aparició de síl·labes de dues lletres en la llengua catalana.

Per tant podem suposar que la primera possibilitat és incorrecta, la qual cosa vol dir que passarem a treballar amb la segona possibilitat, que aparentment no presenta incoherències. Si aquesta suposició no és correcta, sempre podrem reprendre l'anàlisi a partir de la primera possibilitat.

Així doncs, ara tenim el següent criptograma:

***QEL AIELLOEL ATABREW LEPIEOL***

Com que ja hem substituït dues de les tres lletres més freqüents, passarem a canviar l'última d'aquestes lletres, és a dir, que substituïrem totes les lletres L per S, ja que suposem que es corresponen. D'aquesta forma obtenim el següent criptograma:

***QES AIESOES ATABREW SEPIEOS***

Un cop més, tornem a observar el criptograma per intentar identificar alguna incoherència que invalidi les nostres suposicions. Com que a simple vista no se'n detecta cap, tornem a revisar la taula de freqüències mitjanes d'aparició de les lletres en la llengua catalana, per tal de generar noves suposicions.

Tal i com podem observar, les següents lletres amb freqüències d'aparició elevades són la R, la L i la T, amb freqüències de 7.12%, 6.41% i 6.31%, respectivament. En la taula de freqüències generada a partir del criptograma podem observar que les lletres I i O presenten freqüències semblants a les de les lletres R, L i T, per tant, podem suposar que tant la I com la O del criptograma corresponen a una d'aquestes tres lletres.

La qüestió és saber quina lletra és quina, i per tal de poder-ho descobrir, escriurem tots els casos possibles que es puguin generar. Per tal de facilitar la feina, primer treballarem amb la I, i quan l'haguem relacionat amb la lletra corresponent passarem a treballar amb la O.

Abans d'escriure els casos possibles mencionats anteriorment, tornem a revisar el criptograma i intentem deduir la correspondència d'alguna de les lletres pel context. Crida l'atenció el primer bloc de tres lletres del criptograma, de les quals suposem que coneixem la correspondència de dues d'elles.

A simple vista sembla que tot el criptograma sigui una oració simple, amb una estructura de subjecte, verb i complements. D'aquesta forma podem suposar que el bloc de tres lletres que encapçala el criptograma correspon al xifrat d'un article, que podria ser "les", per tant arribem a la conclusió que la lletra Q del criptograma desxifra com a L.

Així doncs, si aquesta suposició és correcta, els possibles desxifrats de I i O es redueixen, ja que no es podrien desxifrar com a L. Reescrivim el criptograma aplicant la nova substitució i obtenim el següent:

LES *A*IES*O*ES AT*A*B*R*E*W* SE*P*IEOS

Ara passem a treballar amb la lletra I. Donem per suposat que els seus possibles desxifrats són R i T, per tant escrivim els dos casos possibles:

LES ARES*O*ES AT*A*B*R*E*W* SE*P*REOS

LES ATES*O*ES AT*A*B*R*E*W* SE*P*TEOS

A simple vista no sembla que puguem descartar cap dels dos casos, per tant passem a treballar amb la lletra O. Havíem suposat que els seus possibles desxifrats eren R i T, per tant escrivim els quatre casos possibles partint dels criptogrames anteriors, on ja havíem substituït la I, per tal d'intentar trobar alguna incoherència en el missatge que ens permeti saber quin dels casos és el correcte, en cas que no ens haguem equivocat en les suposicions anteriors.

Així doncs, obtenim els següents criptogrames:

LES ARESRES AT*A*B*R*E*W* SE*P*RRERS

LES ARESTES AT*A*B*R*E*W* SE*P*RETS

LES ATESRES AT*A*B*R*E*W* SE*P*TERS

LES ATESTES AT*A*B*R*E*W* SE*P*TETS

Tal i com podem observar, en tots els casos la segona paraula del criptograma està desxifrada, per tant l'únic que hem de fer és mirar quina és la paraula que té sentit, i descartar les altres. Sembla ser que l'única paraula que té sentit és "arestes" que pertany al segon criptograma, per tant descartem tots els altres i passem a treballar amb aquest.

Si examinem el criptograma, podem intentar deduir l'última paraula d'aquest pel context. Una de les paraules catalanes que més s'assembla a la del criptograma és "secrets", per tant podem suposar que la lletra P del xifrat correspon a la lletra C del text en clar.

Així doncs, el criptograma que obtenim al realitzar la substitució anterior és el següent:

### LES ARESTES *ATABREW* SECRETS

Ja només ens queda una paraula per desxifrar, i ho intentarem fer a partir del context. Si acceptem que el criptograma és una oració amb subjecte, verb i complements, veiem que la paraula no desxifrada correspon al verb de l'oració.

Aleshores només cal que pensem què es pot fer amb els secrets. Un possible verb podria ser “ocultar”, però no serveix ja que ha de començar per A, per tant busquem un sinònim del verb proposat, i trobem “amagar”, que comença per A.

Així doncs busquem la tercera persona del plural del present d'indicatiu del verb amagar (informació que obtenim a partir del subjecte de l'oració), que és “amaguen” i mirem si hi ha coincidència.

Sembla ser que les lletres de les dues paraules coincideixen, per tant podem suposar que el text en clar a partir del qual s'ha obtingut el criptograma amb el que hem estat treballant és el següent:

### LES ARESTES AMAGUEN SECRETS

Sembla ser que l'oració obtinguda té sentit i no presenta incoherències, per tant podem suposar que el missatge s'ha desxifrat correctament, per tant la nostra feina com a criptoanalistes ja s'ha acabat.

Un cop finalitzat l'exemple pràctic cal remarcar que aquí s'ha intentat buscar un criptograma fàcil de desxifrar, i a més s'han donat les paraules separades. En un cas real, totes les paraules estarien juntes, la qual cosa augmentaria considerablement la complexitat del procés de desxifrat. A més hi podria haver seqüències de lletres que no formessin part del missatge, i que s'haguessin afegit per falsejar l'anàlisi freqüencial.

Un altre avantatge que tenim nosaltres és que coneixem el procediment de xifrat utilitzat i la clau per desxifrar correctament i de forma ràpida el criptograma.

Per tal de comprovar que hem desxifrat correctament el missatge amb l'anàlisi freqüencial, el tornarem a desxifrar, però aquesta vegada utilitzarem la clau de desxifrat, la qual cosa ens permetrà anar més ràpids.

El missatge s'ha xifrat amb l'algoritme generalitzar de Juli Cèsar, amb els paràmetres  $k=(3,7)$  i  $N=26$ , per tant l'equació de xifrat utilitzada és la següent:

$$T_{(3,7)}(x) \equiv 3x + 7 \pmod{26}$$

Partint d'aquesta expressió obtenim l'equació modular del desxifrat, que és la següent:

$$T_{(3,7)}^{-1}(y) \equiv 3^{-1}(y + 19) \pmod{26}$$

Abans de començar a substituir els valors numèrics a l'equació modular per tal de recuperar el missatge en clar calcularem l'invers modular de 3 en mòdul 26, per tal de facilitar els càlculs posteriors. Aplicant l'algoritme d'Euclides modificat per calcular inversos modulars obtenim que  $3^{-1} \equiv 9(\text{mod } 26)$ .

Un cop calculat l'invers modular de 3 en mòdul 26, modifiquem l'equació de desxifrat substituint  $3^{-1}$  pel seu valor congruent, que és 9, i obtenim la següent expressió:

$$T_{(3,7)}^{-1}(y) \equiv 9(y+19) \equiv 9y+15(\text{mod } 26)$$

Arribats a aquest punt ja podem passar a desxifrar el missatge tot substituint a l'equació anterior els valors de cadascuna de les lletres que el formen:

- Xifrat: **Q**; valor numèric: 17; desxifrat:  $T_{(3,7)}^{-1}(17) \equiv 153+15 \equiv 12(\text{mod } 26)$
- Xifrat: **V**; valor numèric: 22; desxifrat:  $T_{(3,7)}^{-1}(22) \equiv 198+15 \equiv 5(\text{mod } 26)$
- Xifrat: **L**; valor numèric: 12; desxifrat:  $T_{(3,7)}^{-1}(12) \equiv 108+15 \equiv 19(\text{mod } 26)$
- Xifrat: **J**; valor numèric: 10; desxifrat:  $T_{(3,7)}^{-1}(10) \equiv 90+15 \equiv 1(\text{mod } 26)$
- Xifrat: **I**; valor numèric: 09; desxifrat:  $T_{(3,7)}^{-1}(9) \equiv 81+15 \equiv 18(\text{mod } 26)$
- Xifrat: **O**; valor numèric: 15; desxifrat:  $T_{(3,7)}^{-1}(15) \equiv 135+15 \equiv 20(\text{mod } 26)$
- Xifrat: **T**; valor numèric: 20; desxifrat:  $T_{(3,7)}^{-1}(20) \equiv 180+15 \equiv 13(\text{mod } 26)$
- Xifrat: **B**; valor numèric: 02; desxifrat:  $T_{(3,7)}^{-1}(2) \equiv 18+15 \equiv 7(\text{mod } 26)$
- Xifrat: **R**; valor numèric: 18; desxifrat:  $T_{(3,7)}^{-1}(18) \equiv 162+15 \equiv 21(\text{mod } 26)$
- Xifrat: **W**; valor numèric: 23; desxifrat:  $T_{(3,7)}^{-1}(23) \equiv 207+15 \equiv 14(\text{mod } 26)$
- Xifrat: **P**; valor numèric: 16; desxifrat:  $T_{(3,7)}^{-1}(16) \equiv 144+15 \equiv 3(\text{mod } 26)$

D'aquesta forma, si substituïm els valors numèrics calculats anteriorment per les seves lletres corresponents, i aquestes lletres les substituïm al criptograma obtenim el mateix text en clar que havíem obtingut a partir de l'anàlisi freqüencial.

## 4. CRIPTOGRAFIA MODERNA

### 4.1. Introducció

En l'apartat anterior hem parlat de *Criptografia Clàssica*, així doncs, ens queda comentar els aspectes relacionats amb l'altre tipus de Criptografia existent, la *Criptografia Moderna*.

Primer de tot començarem explicant en què consisteix la *Criptografia Moderna* i posteriorment veurem alguns mètodes de xifrat pertanyents a aquest grup, juntament amb alguns criptogrames obtinguts a partir de l'aplicació dels mètodes descrits, i tancarem el bloc dedicat a la *Criptografia Moderna* descrivint alguns dels atacs més coneguts a dos dels mètodes de xifrat descrits.

Què entenem per *Criptografia Moderna*? Doncs entenem que ens estem referint a uns sistemes de xifrar informació actuals, i que a dia d'avui s'utilitzen per xifrar tota la informació que es transmet per les xarxes de comunicació i que ofereixen uns nivells de seguretat molt superiors als que oferien els mètodes de xifrat clàssics que hem vist anteriorment.

La *Criptografia Moderna* també es coneix com a Criptografia asimètrica o de clau pública, ja que l'emissor i el receptor del missatge posseeixen dues claus, una de pública amb la qual tota persona pot xifrar un missatge, i una clau privada, amb la qual el receptor desxifra la informació que rep, i que s'ha xifrat amb la seva clau pública.

En aquest cas, a diferència dels mètodes antics, la clau pública d'un receptor és accessible per qualsevol individu, mentre que la clau privada només es coneguda per la persona que rep el missatge i per ningú més, la qual cosa implica que aquest l'ha de mantenir en secret per tal d'evitar que terceres persones puguin accedir a la informació que es transmet. Aquesta és la característica principal de tots els mètodes de xifrat moderns.

Els algoritmes de xifrat asimètric basen la seva seguretat en problemes matemàtics de difícil solució, tals com la factorització de nombres que siguin el producte de dos nombres primers molt grans o també la resolució del problema del logaritme discret aplicat a nombres extremadament grans. Aquests aspectes els comentarem posteriorment en els apartats corresponents.

Cal remarcar que en els algoritmes de xifrat asimètric hi intervenen unes matemàtiques més complexes que ens els seus antecessors, i pot resultar complicat d'entendre'n el funcionament en molts dels casos.

Per aquest motiu hem seleccionat quatre mètodes de xifrat asimètric que seran descrits de forma detallada en aquest projecte. Cal remarcar que la complexitat dels mètodes que descriurem serà ascendent, de tal forma que començarem veient els fàcils i finalment acabarem amb un dels mètodes més recents i moderns, que requerirà uns coneixements especials que es proporcionaran juntament amb la descripció del mètode.

## 4.2. Deixant el passat enrere: mètodes de xifrat moderns

### 4.2.1. Intercanvi de claus de *Diffie* i *Hellman*

Al 1976 *Diffie* i *Hellman* van inventar un mètode per intercanviar claus secretes en canals oberts. El procediment està basat en un sistema de claus asimètric en el que cada comunicant disposa de dos claus, una de secreta i una altra de pública.

Aquest mètode no només va permetre resoldre el problema de l'intercanvi de claus, sinó que a més va ser l'origen de la Criptografia de clau pública, la qual és de gran importància en l'àmbit de la seguretat de les comunicacions digitals.

Per a que dos comunicants  $A$  i  $B$  puguin mantenir una comunicació xifrada és indispensable que cadascun d'ells conegui la clau de xifrat dels missatges transmesos. Això resulta un problema, ja que la clau de xifrat s'ha de transmetre en clar, no pot estar xifrada, la qual cosa vol dir que terceres persones podrien accedir-hi i interceptar els missatges xifrats que intercanvien els comunicants  $A$  i  $B$ . Per aquest motiu resulta indispensable distribuir la clau de forma segura, i això ho permet l'intercanvi de claus proposat per *Diffie* i *Hellman*.

El mètode proposat per *Diffie* i *Hellman* per intercanviar claus secretes a través de canals oberts està basat en l'existència de funcions unidireccionals.

Una funció unidireccional és aquella que té un càlcul directe viable, mentre que el càlcul de la funció inversa té una complexitat tant elevada que resulta impossible.

Per exemple si  $f$  és una funció unidireccional, el càlcul de  $y = f(x)$  és senzill, però el càlcul de  $x = f^{-1}(y)$  és tant complex que no es pot realitzar amb els coneixements matemàtics actuals ni tampoc amb els ordenadors més potents del planeta.

Una funció unidireccional típica és l'exponenciació modular. Un exemple es veu representat en l'equació següent, on  $p$  és un nombre primer gran, d'uns 200 dígit:

$$y \equiv g^x \pmod{p}, \forall x, g \in \mathbb{N}.$$

En aquestes condicions, el càlcul de  $y$  és possible però per contra el càlcul de  $x \equiv \log_g y \pmod{p}$  té una complexitat tan elevada que és totalment inviable.

Cal remarcar que la dificultat per calcular aquesta funció es coneix amb el nom del problema del logaritme discret, i és la base de la seguretat d'aquest mètode d'intercanvi de claus secretes en canals oberts.

Ara que ja hem vist les característiques principals d'aquest mètode podem passar a descriure els passos que s'han de seguir per tal de poder intercanviar claus secretes en canals oberts.

Començarem introduint un nou element que necessitem per poder treballar amb aquest mètode.

**Definició 4.2.1.1.** Anomenem *generador*  $g$  del grup multiplicatiu  $\mathbb{Z}/p\mathbb{Z}$ , amb  $p$  primer, a tot nombre enter  $g \in \mathbb{Z}/p\mathbb{Z}$ , tal que les seves potències mòdul  $p$  generin tots els elements de  $\mathbb{Z}/p\mathbb{Z}$ , excepte el 0.

Per exemple suposem que estem treballant a  $\mathbb{Z}/7\mathbb{Z}$ , i volem trobar un generador  $g$  d'aquest grup. En aquest cas podem afirmar que 3 és un generador d'aquest grup multiplicatiu, i per comprovar-ho, calculem les potències de 3 mòdul 7 fins que els resultats es repeteixin:

$3^0 \equiv 1(\text{mod } 7)$	$3^4 \equiv 4(\text{mod } 7)$
$3^1 \equiv 3(\text{mod } 7)$	$3^5 \equiv 5(\text{mod } 7)$
$3^2 \equiv 2(\text{mod } 7)$	$3^6 \equiv 1(\text{mod } 7)$
$3^3 \equiv 6(\text{mod } 7)$	$3^7 \equiv 3(\text{mod } 7)$

Tal i com podem observar, al calcular les potències anteriors obtenim tots els elements de  $\mathbb{Z}/7\mathbb{Z}$  excepte el 0, per tant podem afirmar que  $g = 3$  és un enter generador de  $\mathbb{Z}/7\mathbb{Z}$ .

Un cop aclarit aquest concepte podem passar a descriure el mètode d'intercanvi de claus.

Considerem un nombre primer  $p$  gran, que tingui 200 dígits o més.

Considerem també un enter  $g$  que sigui generador del grup multiplicatiu  $\mathbb{Z}/p\mathbb{Z}$ . Els valors  $g$  i  $p$  són públics.

Suposem que dos comunicants  $A$  i  $B$  desitgen intercanviar una clau secreta a través d'un canal obert. Per fer-ho,  $A$  tria un enter aleatori  $x_a$  tal que  $1 < x_a < (p-1)$  i envia a  $B$  el valor públic  $y_a$ , calculat amb l'equació següent:

$$y_a \equiv g^{x_a} (\text{mod } p).$$

Paral·lelament  $B$  tria un enter aleatori secret  $x_b$  tal que  $1 < x_b < (p-1)$  i envia a  $A$  el valor públic  $y_b$ , calculat amb l'expressió següent:

$$y_b \equiv g^{x_b} (\text{mod } p).$$

En aquestes condicions,  $B$  calcula el valor secret  $z_{ab}$  amb la següent equació:

$$z_{ab} \equiv y_a^{x_b} \equiv g^{x_a x_b} \pmod{p}.$$

Paral·lelament  $A$  calcula el valor secret  $z_{ba}$  amb la següent equació:

$$z_{ba} \equiv y_b^{x_a} \equiv g^{x_b x_a} \pmod{p}.$$

Òbviament el valor enter  $z_{ab} = z_{ba}$  pot ser utilitzat com a clau secreta compartida entre els comunicants  $A$  i  $B$  per posteriors comunicacions xifrades.

Les claus públiques  $y_a$  i  $y_b$ , així com les claus secretes  $x_a$  i  $x_b$  no s'utilitzen per xifrar i desxifrar missatges sinó que només es fan servir per generar una clau secreta comuna que pugui ser utilitzada posteriorment en qualsevol sistema de xifrat simètric, com els que s'han exposat en el capítol anterior.



**Figura 15:** *Hellman i Diffie.*

Ara que ja hem vist la part teòrica corresponent al mètode d'intercanvi de claus secretes en canals oberts de *Diffie* i *Hellman* passarem a aplicar-ho en un exemple pràctic, per tal d'acabar de comprendre el funcionament d'aquest mètode.

Suposem que tenim un sistema DH per intercanviar claus definit per un nombre primer  $p = 71$  i un generador  $g = 21$  del grup  $\mathbb{Z}/71\mathbb{Z}$ .

Suposem també que els comunicants  $A$  i  $B$  volen intercanviar un valor secret per utilitzar-lo com a clau secreta de xifrat en un sistema de xifrat simètric. Per tant,  $A$  tria un enter aleatori secret  $x_a = 42$  i envia a  $B$  el valor públic  $y_a$ , que calcula de la següent forma:

$$y_a \equiv 21^{42} \equiv 54 \pmod{71}.$$

Paral·lelament,  $B$  tria un enter aleatori secret  $x_b \equiv 62$  i envia a  $A$  el valor públic  $y_b$ , que calcula de la següent forma:

$$y_b \equiv 21^{62} \equiv 36 \pmod{71}.$$

Aleshores  $A$  calcula el valor secret  $z_{ba}$ :

$$z_{ba} \equiv 36^{42} \equiv 5 \pmod{71}.$$

A continuació  $B$  calcula el valor secret  $z_{ab}$ :

$$z_{ab} \equiv 54^{62} \equiv 5 \pmod{71}.$$

En aquestes condicions la clau secreta comuna és  $z_{ab} \equiv z_{ba} \equiv 5 \pmod{71}$ .

En aquestes condicions suposem que  $A$  desitja enviar a  $B$  un missatge secret  $M = 44$  i que el xifrat és el producte  $(\text{mod } 71)$  del missatge i la clau (es podria utilitzar qualsevol altre sistema de xifrat simètric). Aleshores  $A$  envia a  $B$  el xifrat  $C(M)$  amb la clau secreta  $z_{ba}$ :

$$C(M) \equiv 44 \cdot 5 \equiv 7 \pmod{71}.$$

Aleshores  $B$  desxifra  $C(M)$  amb la clau secreta  $z_{ab}$ :

$$M \equiv \frac{7}{5} \equiv 7 \cdot 57 \equiv 44 \pmod{71}.$$

Així doncs,  $B$  recupera el missatge  $M = 44$  enviat per  $A$ .

### 4.2.2. Sistema de xifrat *ElGamal*

A continuació exposarem un mètode de xifrat asimètric en el qual també s'utilitza el problema del logaritme discret per establir la seguretat del sistema. Aquest mètode es coneix com el sistema de xifrat de *ElGamal*.

El mètode va ser proposat per *T. ElGamal*, i els paràmetres del procediment de xifrat són un nombre primer  $p$  gran, d'uns 200 dígits o més, i un valor enter  $g$  generador del grup multiplicatiu  $\mathbb{Z}/p\mathbb{Z}$ , és a dir, un enter  $g \in \mathbb{Z}/p\mathbb{Z}$  tal que les seves potències generin tots els elements del grup. Els valors  $g$  i  $p$  són públics.

En aquestes condicions, la clau secreta del receptor és un enter aleatori  $x$  triat per ell mateix tal que  $1 < x < (p-1)$ , mentre que la clau pública associada  $y$  ve donada per l'equació següent:

$$y \equiv g^x \pmod{p}.$$

El xifrat  $C$  d'un missatge en clar  $M$  tal que  $1 < M < (p-1)$  es porta a terme escollint un enter aleatori  $k$  tal que  $1 < k < (p-1)$  i  $\text{mcd}(k, p-1) = 1$ . En aquestes condicions, el xifrat  $C$  està constituït per la parella de valors enters  $(r, s)$  donats per les congruències següents:

$$\begin{aligned} r &\equiv g^k \pmod{p}, \\ s &\equiv My^k \pmod{p}. \end{aligned}$$

La recuperació del missatge en clar  $M$  a partir del xifrat  $C = (r, s)$  es porta a terme mitjançant el càlcul de la congruència següent:

$$M \equiv \frac{s}{r^x} \pmod{p}.$$

L'expressió anterior es pot verificar de la forma següent:

$$M \equiv \frac{s}{r^x} \equiv \frac{My^k}{g^{kx}} \equiv \frac{My^k}{y^k} \equiv M \pmod{p}.$$

Una de les característiques més destacables d'aquest procediment de xifrat de clau pública és que els xifrats d'un mateix missatge en clar poden ser diferents, ja que només cal computar-los a partir de valors enters aleatoris  $k$  diferents. No obstant això, el sistema de xifrat *ElGamal* presenta alguns inconvenients, sent un dels més seriosos el fet que el xifrat es de longitud doble que el missatge en clar, la qual cosa suposa un augment considerable en les necessitats d'emmagatzematge de dades.

Després de tot el que s'ha comentat anteriorment és fàcil adonar-se que la ruptura d'aquest sistema de xifrat de clau pública és equivalent a la resolució del problema del logaritme discret  $(\text{mod } p)$ . En particular, el càlcul de la clau secreta de desxifrat  $x$  a partir de la clau pública de xifrat  $y$  requereix el càlcul del logaritme discret següent:

$$x \equiv \log_g y (\text{mod } p).$$

Els mètodes que es coneixen actualment per calcular logaritmes discrets són viables per valors de  $p$  de fins a 80 dígit, el problema és que a la pràctica s'utilitzen valors de  $p$  amb un 200 dígit o més, la qual cosa fa que el càlcul del logaritme discret sigui inviable, cosa que constitueix la base de la seguretat d'aquest mètode.

Ara que ja hem vist la part teòrica referent al mètode de xifrat asimètric *ElGamal* podem passar a aplicar-ho en un exemple pràctic, per tal de comprendre el funcionament d'aquest sistema de xifrat de clau pública.

Suposem que tenim un sistema de xifrat asimètric de clau pública *ElGamal* definit pels paràmetres  $(p, g) = (107, 32)$ .

Suposem que la clau secreta d'un receptor  $B$  d'un sistema de comunicació segur basat en aquest mètode és  $x = 95$ .

En aquestes condicions, la clau pública del receptor  $B$  ve donada per la congruència següent:

$$y \equiv 32^{95} \equiv 80 (\text{mod } p).$$

Suposem que un emissor  $A$  desitja enviar a  $B$  de forma confidencial el missatge  $M = 75$ . Per fer-ho,  $A$  tria un valor enter  $k = 51$ , i comprova que  $\text{mcd}(51, 106) = 1$ .

En aquestes condicions, el xifrat  $C$  del missatge  $M$  està constituït per la parella de valors enters  $C = (r, s)$ , donats per les congruències següents:

$$\begin{aligned} r &\equiv 32^{51} \equiv 7 (\text{mod } 107), \\ s &\equiv 75 \cdot 80^{51} \equiv 84 (\text{mod } 107). \end{aligned}$$

El receptor  $B$  recupera el missatge en clar  $M$  a partir el xifrat  $C = (7, 84)$ , computant la congruència següent:

$$M \equiv \frac{84}{7^{95}} \equiv \frac{84}{91} \equiv 84 \cdot 20 \equiv 75 (\text{mod } 107).$$

Tancarem aquest apartat exposant una fotografia del creador d'aquest mètode de xifrat:



**Figura 16:** *T. ElGamal.*

### 4.2.3. El mètode RSA (*Rivest, Shamir i Adleman*)

RSA és un sistema criptogràfic de clau pública, un algoritme asimètric de xifrat en blocs, que utilitza una clau pública que pot ser coneguda per tothom, i una altra de privada, la qual es guarda en secret, ja que és amb aquesta clau privada amb la qual es desxifren els missatges.

Cal dir que a mesura que augmentem la longitud de les claus obtenim criptogrames més segurs, que ofereixen més dificultat en cas de voler desxifrar-los sense la clau privada.

L'algorisme va ser descrit al 1977 per *Ron Rivest, Adi Shamir i Len Adleman* al MIT i el nom que li van posar prové d'ajuntar les tres inicials dels seus cognoms. Va ser patentat pel MIT al 1983 als Estats Units amb el nombre 4.405.829.

Cal remarcar que el sistema de xifrat asimètric RSA és un dels mètodes més utilitzats en l'actualitat per xifrar informació degut a les seves característiques i prestacions, que es descriuran a continuació.

Siguin  $p$  i  $q$  dos nombres primers grans, d'uns 100 dígits cadascun, i  $N = pq$  el producte d'aquests nombres. Sigui  $\phi(N)$  la funció d'Euler de  $N$ , que indica el nombre de valors enters  $n_i$  menors que  $N$  tals que  $\text{mcd}(n_i, N) = 1$ .

En aquest cas particular, la funció  $\phi(N)$  ve donada pel següent producte:

$$\phi(N) = (p-1)(q-1).$$

Això és així ja que  $p$  i  $q$  són dos nombres primers, per tant existiran  $(p-1)$  enters menors que  $p$  tals que  $\text{mcd}(n_i, p) = 1$  i també existiran  $(q-1)$  enters menors que  $q$  tals que  $\text{mcd}(n_i, q) = 1$ . És a dir, que  $\phi(p) = p-1$  i  $\phi(q) = q-1$ . Per tant,  $\phi(N) = \phi(pq) = (p-1)(q-1)$ .

En aquestes condicions, sigui  $e$  un valor enter tal que  $\text{mcd}(e, \phi(N)) = 1$  i on  $1 < e < N$ , i sigui  $d$  un altre valor enter tal que verifiqui la següent congruència:

$$ed \equiv 1 \pmod{\phi(N)},$$

o de forma equivalent:

$$ed = k\phi(N) + 1, k \in \mathbb{Z}.$$

En aquestes condicions, per qualsevol valor enter  $M$  es verifica que si  $C \equiv M^e \pmod{N}$  aleshores  $M \equiv C^d \pmod{N}$ , és a dir, que es verifica la següent expressió:

$$M^{ed} \equiv M \pmod{N}.$$

Per demostrar aquesta expressió s'utilitza el teorema xinès dels residus congruents.

**Teorema xinès dels residus congruents.** *Siguin  $m_1, \dots, m_n$  nombres enters tals que  $\text{mcd}(m_i, m_j) = 1$  si  $i \neq j$ , i siguin  $b_1, \dots, b_n$  valors enters qualsevol. Aleshores, el sistema de congruències  $x \equiv b_1 \pmod{m_1}, \dots, x \equiv b_n \pmod{m_n}$  té una única solució entera entre  $0$  i  $m_1 m_2 \dots m_n - 1$ , és a dir, una única solució  $\pmod{m_1 m_2 \dots m_n}$ .*

**Demostració:**

Suposem que som capaços de trobar enters  $E_k$  (un per cada  $k$  entre  $1$  i  $n$ ) tals que:

$$E_k \equiv \begin{cases} 0 \pmod{m_j} \\ 1 \pmod{m_k} \end{cases}, j \neq k. \quad (4.1.)$$

Si existeixen aquests  $E_k$ ,  $x = \sum_{k=1}^n E_k b_k$  és solució del nostre problema. Per trobar els  $E_k$ , siguin  $M = m_1 m_2 \dots m_n$  i  $M_k = \frac{M}{m_k}, k = 1, \dots, n$ . Com que  $\text{mcd}(m_i, m_j) = 1$  si  $i \neq j$ , s'obté que  $\text{mcd}(m_k, M_k) = 1$ , i, per tant, que existeixen enters  $t_k$  i  $s_k$  tals que  $s_k M_k + t_k m_k = 1, k = 1, \dots, n$ .

És fàcil comprovar que els enters  $E_k = s_k M_k$  verifiquen l'expressió (4.1.). Clarament  $E_k$  és múltiple de  $m_j$  si  $k \neq j$ , i, per tant, congruent amb  $0$  mòdul  $m_k$ .

Per concloure la demostració falta veure que la solució és única en mòdul  $M$ . Suposem dos solucions  $x$  i  $y$ . Aleshores es té que  $x - y \equiv 0 \pmod{m_i} \forall i \in \{1, 2, \dots, n\}$ , és a dir,  $x - y$  és un múltiple de tots els  $m_i$ , i, en conseqüència, del mínim comú múltiple de  $m_1, m_2, \dots, m_n$ , que és  $M$ , ja que tots els  $m_i$  són primers entre ells. Per tant,  $x \equiv y \pmod{M}$ . **Q.E.D.**

Així doncs, si apliquem el teorema veiem que la congruència anterior es verifica si i només si es verifiquen les congruències següents:

$$\begin{aligned} M^{ed} &\equiv M \pmod{p}, \\ M^{ed} &\equiv M \pmod{q}. \end{aligned}$$

Aquestes dues expressions es poden demostrar utilitzant el Petit Teorema de Fermat, exposat anteriorment:

$$M^{ed} \equiv M^{k\phi(N)+1} \equiv M^{k(p-1)(q-1)+1} \equiv M^{k(q-1)(p-1)} M \equiv M^{k'(p-1)} M \equiv M \pmod{p}, \text{ on } k' = k(q-1), k' \in \mathbb{Z}.$$

$$M^{ed} \equiv M^{k\phi(N)+1} \equiv M^{k(p-1)(q-1)+1} \equiv M^{k(q-1)(p-1)} M \equiv M^{k'(q-1)} M \equiv M \pmod{q}, \text{ on } k' = k(p-1), k' \in \mathbb{Z}.$$

Aquesta demostració és la base del sistema de xifrat asimètric RSA. Aquest sistema està constituït per les claus  $N$ ,  $e$  i  $d$ , que són el mòdul de treball, la clau de xifrat i la clau del desxifrat, respectivament.

El valor de  $N$  és públic, així com el valor de  $e$ , mentre que el valor de  $d$  correspon a la clau secreta.

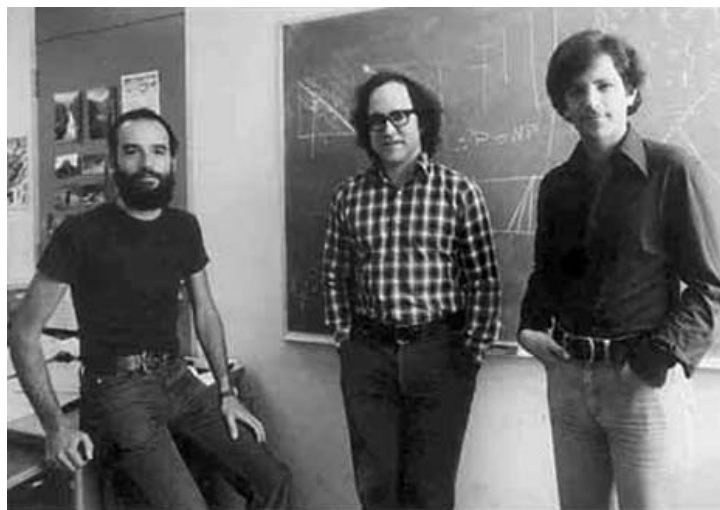
Per realitzar el xifrat  $C$  d'un missatge en clar  $M$  tal que  $1 < M < N$ , el missatge s'eleva a la potència  $e$  i es redueix en mòdul  $N$ . És a dir, que per xifrar un missatge  $M$  es calcula la següent congruència:

$$C \equiv M^e \pmod{N}.$$

La recuperació del missatge en clar  $M$  es porta a terme elevant el missatge xifrat  $C$  a la potència  $d$  i reduint-lo en mòdul  $N$ , és a dir, que es calcula amb la següent congruència:

$$M \equiv C^d \pmod{N}.$$

Per tancar aquest apartat on hem exposat la part teòrica referent al sistema de xifrat asimètric RSA exposarem una fotografia dels seus creadors:



**Figura 17:** Rivest, Shamir i Adleman.

A continuació passarem a exposar un exemple pràctic on xifrarem i desxifrarem un missatge utilitzant el mètode de xifrat de clau pública RSA.

Suposem que tenim un sistema de xifrat RSA definit pels paràmetres següents:

$$\begin{cases} p = 29, \\ q = 37, \\ N = 1073, \\ (p-1)(q-1) = 1008, \\ e = 23. \end{cases}$$

Suposem que un comunicant  $A$  vol enviar a  $B$  un missatge  $M = 347$ . El comunicant  $A$  busca la parella de claus públiques  $(N, e)$  de  $B$  i xifra el missatge  $M$  de la forma següent:

$$C \equiv 347^{23} \equiv 637 \pmod{1073}.$$

D'aquesta forma  $B$  rep el missatge xifrat  $C = 637$ . Aleshores  $B$  calcula el valor de  $d$ , que és el valor de la seva clau privada de desxifrat, de la següent forma:

$$d \equiv \frac{1}{e} \equiv \frac{1}{23} \equiv 263 \pmod{1008}.$$

Aleshores  $B$  recupera el missatge en clar  $M$  calculant la següent congruència:

$$M \equiv C^d \equiv 637^{263} \equiv 347 \pmod{1073}.$$

Per acabar cal remarcar que els nombres  $p$  i  $q$  són secrets, la qual cosa atorga seguretat al sistema, ja que el càlcul de la clau privada  $d$  és molt senzill si es coneixen els valors de  $p$  i  $q$ , mentre que si aquests valors no es coneixen, el càlcul de la clau secreta  $d$  equival a la factorització de la clau pública  $N$ .

Aquí és on veritablement radica la seguretat del mètode RSA, ja que actualment resulta molt complicat calcular els factors primers d'un valor  $N$  extremadament gran. És per aquest motiu que es requereix la utilització de nombres primers molt grans per tal d'assegurar que la factorització de  $N$  sigui impracticable.

Així doncs, en el següent apartat passarem a parlar de corbes el·líptiques.

#### 4.2.4. L'última frontera: les corbes el·líptiques

Tal i com s'ha indicat en l'apartat anterior, la violació del sistema RSA, així com la de la majoria de procediments de xifrat de clau pública, requereix la factorització del mòdul de treball o el càlcul del logaritme discret en cossos finits de nombres enters.

La complexitat d'aquests problemes és molt elevada quan es treballa amb nombres enters suficientment grans, creixent exponencialment amb el tamany dels mateixos.

No obstant això, els avenços en mètodes i prestacions dels ordenadors exigeixen la utilització de nombres enters cada vegada més grans per tal de garantir la seguretat dels mètodes criptogràfics que els utilitzen, la qual cosa representa un inconvenient a l'hora de generar i distribuir les claus secretes utilitzades.

El problema anterior es pot solucionar utilitzant procediments de xifrat de clau pública basats en corbes el·líptiques. Les corbes el·líptiques tenen la propietat de que els seus punts formen un grup additiu abelià amb una operació suma especial. Això permet utilitzar-les per dissenyar nous sistemes de xifrat de clau pública.

La característica més destacable d'aquests sistemes és que ofereixen un nivell de seguretat equivalent al dels mètodes de xifrat de clau pública descrits anteriorment, però utilitzant un menor nombre de dígit, la qual cosa implica que les claus de xifrat són més curtes.

Per aconseguir-ho, els mètodes de xifrat amb corbes el·líptiques requereixen la realització d'un major nombre de càlculs.

Tenint en compte tots aquests aspectes, en aquest apartat descriurem de forma general la Criptografia amb corbes el·líptiques, i aportarem alguns exemples pràctics de xifrat i desxifrat de missatges per tal de comprendre'n el funcionament.

#### 4.2.4.1. Coneixements previs sobre corbes el·líptiques

Primer de tot començarem explicant què és el que entenem per corba el·líptica.

**Definició 4.2.4.1.1.** Una *corba el·líptica* és una corba de gènere 1, on el conjunt de punts  $(x, y)$  que la formen satisfan l'equació de *Weierstrass*:

$$y^2 = x^3 + ax + b.$$

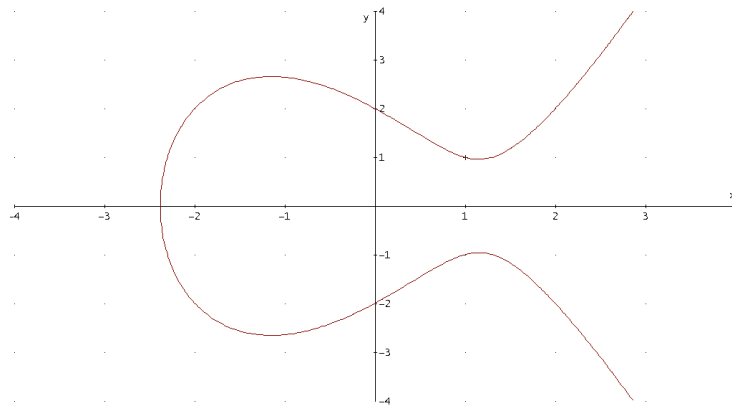
A més s'hi inclou un punt a l'infinit  $O(\infty, \infty)$  que fa d'element neutre en la suma en el conjunt format per tots els punts de la corba. Cal afegir que aquest conjunt forma un grup abelià amb la suma, ja que compleix la propietat associativa, hi ha element neutre, que és  $O$ , hi ha element oposat, i també compleix la propietat commutativa.

Per definició una corba el·líptica ha de ser no singular, és a dir, que no ha de presentar ni autointerseccions ni cúspides. Per aquest motiu a l'hora d'escollir una corba el·líptica per utilitzar-la en procediments criptogràfics haurem de procurar que el determinant  $\Delta$  d'aquesta no sigui 0:

$$\Delta = -16(4a^3 + 27b^2) \neq 0, \forall a, b \in \mathbb{R}.$$

Pot semblar que el factor -16 del determinant és irrellevant, però resulta important quan s'estudien les corbes el·líptiques de forma més detallada.

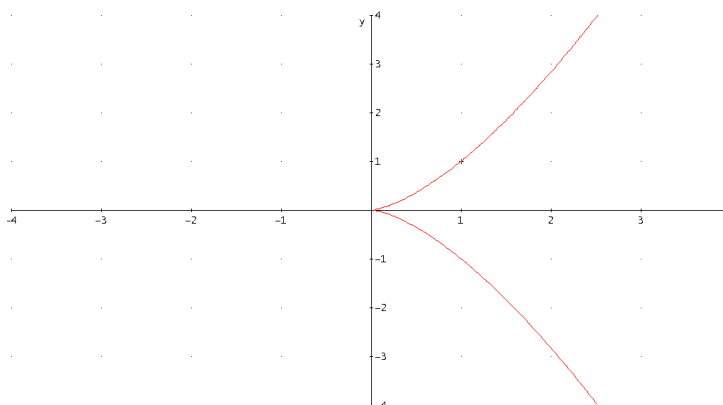
Aquí podem veure un exemple de corba el·líptica definida sobre el cos dels nombres reals  $\mathbb{R}$ :



**Figura 18:** Representació gràfica de la corba  $y^2 = x^3 - 4x + 4$ .

L'equació d'aquesta corba el·líptica és  $y^2 = x^3 - 4x + 4$ . Com podem veure és no singular ja que  $\Delta = -16(4 \cdot (-4)^3 + 27 \cdot 4^2) = -2816 \neq 0$ .

Un exemple de corba singular seria el següent:



**Figura 19:** Representació gràfica de l'equació  $y^2 = x^3$ .

Tal i com podem observar, la corba presenta una cúspide, la qual cosa indica que és singular. A més sabent que l'equació de la representació gràfica és  $y^2 = x^3$  podem calcular el determinant i comprovar que  $\Delta = 0$ , la qual cosa indica que aquesta corba no és el·líptica.

Les corbes el·líptiques poden estar definides en qualsevol conjunt  $K$ , tant de dimensió finita com infinita.

En particular, les corbes el·líptiques utilitzades en Criptografia es defineixen sobre conjunts finits  $K = \mathbb{Z}/q\mathbb{Z}$  de nombres enters, sent  $q = p^m$  on  $p$  és un nombre primer i  $m$  un valor enter. Els coeficients de la corba són valors enters tals que  $a, b \in \{0, 1, 2, \dots, (q-1)\}$ .

En aquest apartat treballarem amb corbes el·líptiques definides sobre el cos finit  $\mathbb{Z}/p\mathbb{Z}$  amb  $p$  primer, de forma que totes les operacions es realitzaran  $(\text{mod } p)$ .

Ara que ja sabem què són les corbes el·líptiques passarem a definir i descriure els procediments que ens permetran sumar, restar i multiplicar els punts que les formen.

Primer de tot cal tenir en compte que tota línia recta talla a una corba el·líptica en tres punts. Pot semblar que en alguns casos això no és així, però cal recordar que existeix el punt a l'infinit  $O$ , i que si una recta només talla en dos punts a una corba el·líptica, el tercer punt és  $O$ .

A més, com que no treballem amb nombres complexos, pot semblar que algunes rectes només tallen a la corba en dos punts, incloent el punt  $O$ , però això no és així quan es treballa amb nombres complexos.

Un cop aclarit aquest petit detall començarem definint el procediment per sumar els punts d'una corba el·líptica. En aquesta suma el punt de l'infinit  $O$  representa l'element neutre, és a dir que  $P + O = P$  per qualsevol punt  $P$  de la corba.

Per definir la suma de punts establim la següent regla, tenint en compte el que hem comentat abans sobre les interseccions d'una recta amb una corba el·líptica:

Si  $P, Q$  i  $R$  són tres punts alineats de la corba, aleshores  $P + Q + R = O$ .

Si  $P = (x, y)$  és un punt de la corba el·líptica, aleshores  $Q = (x, -y)$  és un altre punt de la corba i aquests dos punts estan alineats amb un punt del infinit. Per tant:

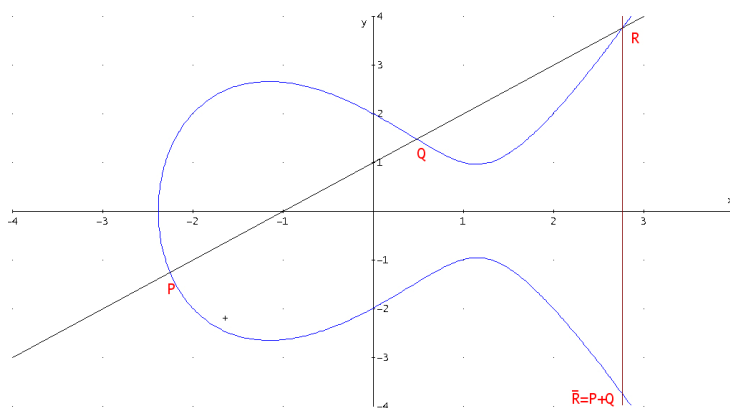
$$O = O + P + Q = P + Q \Rightarrow Q = -P,$$

és a dir, que l'oposat del punt  $(x, y)$  és el punt  $(x, -y)$  i l'oposat del  $O$  és  $O$ .

Per tant si volem sumar  $P$  i  $Q$  primer calculem la recta que passa pels dos punts, tenint en compte que:

- Si  $P = Q$ , la recta és tangent a la corba per  $P$ .
- Si  $P = O$  o  $Q = O$  i  $P \neq Q$ , es tracta de la recta vertical que passa pel punt que no és  $O$ .

Un cop tenim la recta, calculem el tercer punt d'intersecció  $R$  de la corba amb la recta, de tal forma que la suma  $P + Q$  és  $\bar{R}$ .



**Figura 20:** Suma de punts en una corba el·líptica.

La suma de punts en una corba el·líptica és pot realitzar de forma geomètrica, tal i com s'ha mostrat anteriorment, i de forma algebraica. Cal dir que és molt més ràpid sumar punts de forma aritmètica, per tant a continuació mostrarem com fer-ho.

Sigui  $E$  una corba el·líptica de la forma  $y^2 = x^3 + ax + b$ , amb  $\Delta \neq 0$  definida sobre  $\mathbb{R}$ . Siguin  $P = (x_P, y_P)$  i  $Q = (x_Q, y_Q)$  dos punts qualsevol de la corba  $E$ .

En aquestes condicions, suposem que volem sumar  $P$  i  $Q$ . Sabent que aquests punts són de la corba, podem expressar els coeficients  $a$  i  $b$  de  $E$  en funció de les coordenades dels punts  $P$  i  $Q$  resolent el següent sistema d'equacions:

$$\begin{cases} y_P^2 = x_P^3 + ax_P + b, \\ y_Q^2 = x_Q^3 + ax_Q + b. \end{cases}$$

Un cop tinguem els coeficients  $a$  i  $b$  els substituïrem a l'equació de la corba  $E$ . Seguidament buscarem la recta  $r$ , que talla a  $E$  en tres punts, que són  $P$ ,  $Q$  i  $R$ .

Sabent que  $r$  serà de la forma  $y = mx + n$  i que contindrà a  $P$  i  $Q$ , expressarem els coeficients  $m$  i  $n$  en funció de les coordenades de  $P$  i  $Q$ , resolent el següent sistema d'equacions:

$$\begin{cases} y_P = mx_P + n, \\ y_Q = mx_Q + n. \end{cases}$$

Les solucions obtingudes són les següents:

$$\begin{cases} m = \frac{y_P - y_Q}{x_P - x_Q}, \\ n = \frac{x_P y_Q - x_Q y_P}{x_P - x_Q}. \end{cases}$$

Ara que ja tenim els coeficients  $m$  i  $n$  els substituïm a l'equació de  $r$ .

Finalment només caldrà calcular els tres punts d'intersecció de la recta  $r$  amb la corba  $E$ , i per fer-ho s'haurà de resoldre el següent sistema d'equacions, tenint en compte que  $a$ ,  $b$ ,  $m$  i  $n$  estan expressats en funció de les coordenades dels punts  $P$  i  $Q$ :

$$\begin{cases} y^2 = x^3 + ax + b, \\ y = mx + n. \end{cases}$$

El sistema anterior té tres solucions, cadascuna d'elles formada per un valor de  $x$  i un de  $y$ . La primera parella són les coordenades del punt  $P$ ; la segona són les coordenades del punt  $Q$  i la tercera són les coordenades del punt  $R = (x_R, y_R)$ .

Es pot comprovar que les expressions de la tercera parella de valors es poden simplificar, de forma que s'obtenen les següents equacions:

$$\begin{cases} x_R = m^2 - x_P - x_Q, \\ y_R = y_P - m(x_P - x_R). \end{cases}$$

Sabent que  $P + Q = \bar{R}$  i que  $\bar{R} = (x_R, -y_R) = (x_{\bar{R}}, y_{\bar{R}})$  obtenim que les equacions que ens permetran calcular la suma dels punts  $P$  i  $Q$  són les següents:

$$\begin{aligned} m &= \frac{y_P - y_Q}{x_P - x_Q}, \\ x_{\bar{R}} &= m^2 - x_P - x_Q, \\ y_{\bar{R}} &= -y_P + m(x_P - x_{\bar{R}}). \end{aligned}$$

Aquestes equacions són les que utilitzarem a partir d'ara per sumar punts en una corba el·líptica definida sobre  $\mathbb{R}$ .

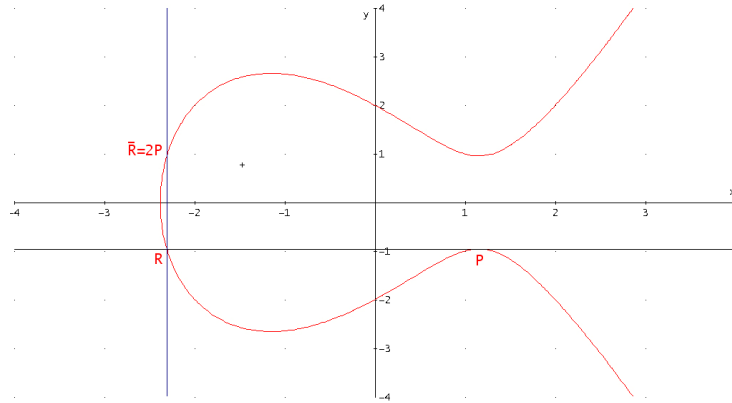
Cal dir que per tal de sumar dos punts  $P$  i  $Q$  en una corba el·líptica definida sobre un cos  $\mathbb{Z}/p\mathbb{Z}$  per tal d'obtenir el punt  $\bar{R}$ , haurem d'introduir una petita modificació a les equacions anteriors, de tal forma que obtindrem les següents:

$$\begin{aligned} m &\equiv \frac{(y_P - y_Q)}{(x_P - x_Q)} \pmod{p}, \\ x_{\bar{R}} &\equiv m^2 - x_P - x_Q \pmod{p}, \\ y_{\bar{R}} &\equiv -y_P + m(x_P - x_{\bar{R}}) \pmod{p}. \end{aligned}$$

Per que fa a la resta de punts cal remarcar que  $P - Q = P + (-Q) = (x_P, y_P) + (x_Q, -y_Q)$ , per tant pot ser calculada amb les equacions del procediment suma, descrites anteriorment.

Ara que ja sabem com se sumen els punts d'una corba el·líptica passarem a descriure com podem calcular productes per escalars, és a dir, descriurem el mètode per tal de calcular  $\bar{R} = kP, k \in \mathbb{Z}$ . Cal remarcar que és un procediment molt semblant al de la suma, ja que multiplicar un punt  $P$  per un escalar  $k$  equival a sumar  $P$  amb ell mateix  $k$  vegades.

En el cas en que  $k=2$ , el procediment que es porta a terme és el de calcular la recta tangent a la corba pel punt  $P$ . Posteriorment es busca l'altre punt d'intersecció  $R$  de la recta amb la corba, i finalment el punt buscat serà l'oposat de  $R$ , de manera que  $\bar{R} = 2P$ :



**Figura 21:** Producte per escalars de punts en una corba el·líptica.

El producte, igual que la suma, és pot realitzar de forma geomètrica, tal i com s'ha mostrat anteriorment, i de forma algebraica. Cal dir que és molt més ràpid multiplicar per 2 un punt  $P$  de forma algebraica, per tant a continuació mostrarem com fer-ho.

Sigui  $E$  una corba el·líptica de la forma  $y^2 = x^3 + ax + b$ , amb  $\Delta \neq 0$  definida sobre  $\mathbb{R}$ . Sigui  $P = (x_P, y_P)$  un punt qualsevol de la corba  $E$ .

En aquestes condicions, suposem que volem calcular  $2P$ . Sabent que aquest és el punt de tangència de la recta  $r$  amb la corba  $E$ , podem calcular  $r$  de la forma següent:

$$r : E_x(x_p, y_p)(x - x_p) + E_y(x_p, y_p)(y - y_p) = 0,$$

tenint en compte que  $E_x(x, y) = \frac{\partial E}{\partial x} = 3x^2 + a$  i  $E_y(x, y) = \frac{\partial E}{\partial y} = -2y$ .

Si realitzem els càlculs obtenim el següent:

$$\begin{aligned} r : (3x_p^2 + a)(x - x_p) - 2y_p(y - y_p) &= 0, \\ \Downarrow \\ r : (y - y_p) &= \left( \frac{3x_p^2 + a}{2y_p} \right) (x - x_p), \text{ on } m = \frac{3x_p^2 + a}{2y_p}. \end{aligned}$$

Veiem que el coeficient  $m$  de la recta està expressat en funció de les coordenades del punt  $P$  i del coeficient  $a$  de  $E$ . Per tant, a continuació hauré de definir la corba  $E$ , i per fer-ho hauré d'expressar el coeficient  $b$  en funció de  $a$  i de les coordenades del punt  $P$ .

El que cal fer és substituir les coordenades del punt  $P$  a l'equació de  $E$  i aïllar  $b$ , de la forma següent:

$$y_p^2 = x_p^3 + ax_p + b \Rightarrow b = y_p^2 - x_p^3 - ax_p.$$

Ara que ja hem expressat  $b$  en funció de les coordenades de  $P$  i del coeficient  $a$ , només falta substituir-lo a l'equació de la corba i calcular els punts d'intersecció de la recta  $r$  amb la corba  $E$ , resolent el següent sistema d'equacions:

$$\begin{cases} (y - y_p) = \left( \frac{3x_p^2 + a}{2y_p} \right) (x - x_p), \\ y^2 = x^3 + ax + y_p^2 - x_p^3 - ax_p. \end{cases}$$

Es pot comprovar que les expressions de la parella de valors corresponent a les coordenades del punt  $R$  es poden simplificar, de forma que s'obtenen les següents equacions:

$$\begin{cases} x_R = m^2 - 2x_p, \\ y_R = y_p - m(x_p - x_R). \end{cases}$$

Sabent que  $2P = \bar{R}$  i que  $\bar{R} = (x_R, -y_R) = (x_{\bar{R}}, y_{\bar{R}})$  obtenim que les equacions que ens permetran calcular  $2P$ :

$$\begin{aligned} m &= \frac{3x_P^2 + a}{2y_P}, \\ x_{\bar{R}} &= m^2 - 2x_P, \\ y_{\bar{R}} &= -y_P + m(x_P - x_{\bar{R}}). \end{aligned}$$

Aquestes equacions són les que utilitzarem a partir d'ara per multiplicar per 2 un punt qualsevol d'una corba el·líptica definida sobre  $\mathbb{R}$ .

Cal dir que per tal de multiplicar per 2 un punt  $P$  d'una corba el·líptica definida sobre un cos  $\mathbb{Z}/p\mathbb{Z}$  per tal d'obtenir el punt  $\bar{R}$ , haurem d'introduir una petita modificació a les equacions anteriors, de tal forma que obtindrem les següents:

$$\begin{aligned} m &\equiv \frac{(3x_P^2 + a)}{2y_P} \pmod{p}, \\ x_{\bar{R}} &\equiv m^2 - 2x_P \pmod{p}, \\ y_{\bar{R}} &\equiv -y_P + m(x_P - x_{\bar{R}}) \pmod{p}. \end{aligned}$$

Finalment cal remarcar que per multiplicar  $P$  per un escalar diferent de 2 es combinarien els procediments de suma i de càlcul del doble d'un punt, fins a obtenir el valor desitjat.

Per exemple, en cas que  $k = 3$ , es calcularia  $\bar{R} = 3P = 2P + P$ , i així successivament per qualsevol valor de  $k$ .

Ara que ja hem definit els procediments per poder sumar, restar i multiplicar punts per un escalar ja estem en condicions de revisar els mètodes de xifrat de clau pública basats en corbes el·líptiques.

No obstant això, comentarem un petit aspecte que ens farà falta per tal de comprendre alguns dels conceptes que tractarem quan exposarem els mètodes de xifrat.

**Definició 4.2.4.1.2.** Definim l'ordre  $N$  d'una corba el·líptica com el nombre de punts que conté sobre el conjunt  $\mathbb{Z}/p\mathbb{Z}$  en el qual està definida.

**Definició 4.2.4.1.3.** Definim l'ordre  $N_P$  d'un punt  $P$  d'una corba el·líptica definida sobre  $\mathbb{Z}/p\mathbb{Z}$  com el mínim valor enter que verifiqui l'expressió  $N_P P = O(\infty, \infty)$ .

Partint d'aquestes dues definicions, introduïm un nou concepte al que anomenarem generador  $G$  d'una corba el·líptica.

**Definició 4.2.4.1.4.** Definim el generador  $G$  d'una corba el·líptica com un punt d'aquesta tal que generi tots els punts de la pròpia corba, és a dir, que qualsevol altre punt  $P$  pertanyent a la corba pugui ser expressat de la forma  $P = \alpha G, \alpha \in \{1, 2, \dots, N\}$ , on  $N$  és l'ordre de la corba el·líptica. Un punt d'una corba el·líptica serà generador d'aquesta si i només si  $N_P = N$ .

Per tal d'exemplificar aquests conceptes, suposem que tenim la corba el·líptica  $y^2 \equiv x^3 + 4x + 4 \pmod{5}$ . Aquesta corba el·líptica definida sobre  $\mathbb{Z}/5\mathbb{Z}$  té 8 punts incloent el punt a l'infinit  $O$ , que es poden calcular substituint les  $x$  per valors entre 0 i 4. Per tant diem que la corba anterior és d'ordre  $N = 8$ .

(0,2)	(2,0)
(0,3)	(4,2)
(1,2)	(4,3)
(1,3)	( $\infty, \infty$ )

Un generador  $G$  d'aquesta corba serà un punt d'ella que tingui un ordre  $N_p = 8$ , és a dir, que  $8P = O(\infty, \infty)$ . En aquest cas, un possible generador és el punt  $P = (0, 2)$ , que té un ordre  $N_p = 8$ . Per comprovar si realment és generador de la corba, només cal comprovar si els múltiples de  $P = (0, 2)$  generen tots els punts de la corba anterior definida sobre  $\mathbb{Z}/5\mathbb{Z}$ :

$1 \cdot (0,2) = (0,2)$	$5 \cdot (0,2) = (4,2)$
$2 \cdot (0,2) = (1,2)$	$6 \cdot (0,2) = (1,3)$
$3 \cdot (0,2) = (4,3)$	$7 \cdot (0,2) = (0,3)$
$4 \cdot (0,2) = (2,0)$	$8 \cdot (0,2) = (\infty, \infty)$

Per tant podem afirmar que  $P = (0, 2)$  és generador de la corba el·líptica  $y^2 \equiv x^3 + 4x + 4 \pmod{5}$ .

Finalment cal afegir que la seguretat dels sistemes de xifrat basats en corbes el·líptiques es basa en el problema del logaritme el·líptic.

Aquest es basa en el fet que donada una corba el·líptica, un punt  $P$  d'aquesta i un escalar  $k$ , resulta senzill calcular  $Q = kP$ . Però si es proporciona el valor de  $P$  i  $Q$  i la corba el·líptica que conté aquests punts, resulta pràcticament impossible recuperar el valor de  $k$ , sempre i quan la corba estigui definida sobre un conjunt  $\mathbb{Z}/p\mathbb{Z}$  amb  $p$  un nombre primer gran, d'uns 80 dígits.

Aquest problema és anàleg al del logaritme discret mencionat anteriorment, tot i que en aquest cas la complexitat del problema és molt superior.

Podem afirmar que al treballar amb valors d'una determinada dimensió, el logaritme el·líptic pot ser una funció criptogràfica molt més segura que el logaritme discret o la factorització. És a dir, que el logaritme el·líptic ofereix la mateixa seguretat que aquestes funcions utilitzant un menor nombre de dígits.

El principal inconvenient és que el càlcul de múltiples de punts d'una corba el·líptica requereix un major nombre de càlculs que no pas els que es requereixen per calcular els paràmetres dels sistemes de xifrat asimètric descrits anteriorment.

Revisats els conceptes bàsics referents a corbes el·líptiques que ens feien falta podem passar a exposar alguns mètodes de xifrat basats en aquestes.

#### 4.2.4.2. Intercanvi de claus secretes en canals públics utilitzant CE

El logaritme el·líptic pot ser utilitzat com a funció unidireccional per intercanviar claus secretes a través de canals oberts, de forma equivalent a com ho era el logaritme discret en el procediment d'intercanvi de claus proposat per *Diffie* i *Hellman*, descrit anteriorment.

Per realitzar l'intercanvi de claus utilitzant les corbes el·líptiques es parteix d'una corba  $E$  definida sobre un cos  $\mathbb{Z}/p\mathbb{Z}$  amb  $p$  primer i d'un punt  $G$  de la mateixa que sigui generador de grup, és a dir, un punt que tingui el mateix ordre que la corba el·líptica. Els paràmetres  $E$  i  $G$  són públics.

En aquestes condicions, suposem que els comunicants  $A$  i  $B$  desitgen intercanviar una clau secreta a través d'un canal obert.

Per fer-ho,  $A$  tria un valor aleatori  $a \in \mathbb{Z}/p\mathbb{Z}$  i envia a  $B$  el punt de la corba  $P_a = aG$ .

Paral·lelament  $B$  tria un valor aleatori  $b \in \mathbb{Z}/p\mathbb{Z}$  i envia a  $A$  el punt de la corba  $P_b = bG$ .

Aleshores  $A$  calcula el punt secret  $P_{ab} = aP_b = abG$ .

Paral·lelament  $B$  calcula el punt secret  $P_{ba} = bP_a = baG$ .

Com que el grup de punts de la corba el·líptica és abelià es verifica que  $P_{ab} = P_{ba}$ , de tal forma que aquest punt pot ser utilitzat com a clau secreta compartida entre els comunicants  $A$  i  $B$  per posteriors comunicacions xifrades.

Així doncs, en aquest procediment d'intercanvi, els punts  $P_{ab}$  i  $P_{ba}$  actuen com claus públiques mentre que els valors enters  $a$  i  $b$  són les seves respectives claus privades.

Un cop vista la part teòrica d'aquest mètode d'intercanvi de claus secretes basat en corbes el·líptiques passarem a exposar un exemple pràctic per tal de comprendre'n el funcionament correctament.

Suposem que tenim un sistema d'intercanvi de claus secretes basat en corbes el·líptiques definit pels següents paràmetres:

$$\begin{cases} E : y^2 \equiv x^3 + 4x + 4 \pmod{5}, \\ G = (0, 2). \end{cases}$$

Suposem també que dos comunicants  $A$  i  $B$  volen intercanviar una clau secreta en un canal obert.

En aquestes condicions,  $A$  tria un valor enter aleatori  $a = 2$ , i calcula la seva clau pública  $P_a$ , que posteriorment envia a  $B$  de la següent forma:

$$P_a = 2G = 2 \cdot (0, 2) = (x_R, y_R),$$

$$m \equiv \frac{(3x_G^2 + a)}{2y_G} \equiv \frac{4}{4} \equiv 1 \pmod{5},$$

$$x_R \equiv m^2 - 2x_G \equiv 1 \pmod{5},$$

$$y_R \equiv -y_G + m(x_G - x_R) \equiv -2 + 1(0 - 1) \equiv -3 \equiv 2 \pmod{5},$$

$$P_a = (x_R, y_R) = (1, 2).$$

Paral·lelament  $B$  tria un valor enter aleatori  $b = 3$ , i calcula la seva clau pública  $P_b$ , que posteriorment envia a  $A$  de la següent forma:

$$P_b = 3G = 2G + G = 2 \cdot (0, 2) + (0, 2) = (x_{R_2}, y_{R_2}),$$

$$m_1 \equiv \frac{(3x_G^2 + a)}{2y_G} \equiv \frac{4}{4} \equiv 1 \pmod{5},$$

$$x_{R_1} \equiv m_1^2 - 2x_G \equiv 1 \pmod{5},$$

$$y_{R_1} \equiv -y_G + m_1(x_G - x_{R_1}) \equiv -2 + 1(0 - 1) \equiv -3 \equiv 2 \pmod{5},$$

$$P_b = (1, 2) + (0, 2) = (x_{R_2}, y_{R_2}),$$

$$m_2 \equiv \frac{(y_{R_1} - y_G)}{(x_{R_1} - x_G)} \equiv \frac{0}{1} \equiv 0 \pmod{5},$$

$$x_{R_2} \equiv m_2^2 - x_{R_1} - x_G \equiv 0 - 1 - 0 \equiv 4 \pmod{5},$$

$$y_{R_2} \equiv -y_{R_1} + m_2(x_{R_1} - x_{R_2}) \equiv -2 + 0 \equiv 3 \pmod{5},$$

$$P_b = (x_{R_2}, y_{R_2}) = (4, 3).$$

Aleshores  $A$  calcula el punt secret  $P_{ab}$  de la forma següent:

$$\begin{aligned}
 P_{ab} &= aP_b = 2 \cdot (4, 3) = (x_R, y_R), \\
 m &\equiv \frac{(3x_P^2 + a)}{2y_P} \equiv \frac{48 + 4}{6} \equiv \frac{52}{1} \equiv 2 \pmod{5}, \\
 x_R &\equiv m^2 - 2x_P \equiv 4 - 8 \equiv -4 \equiv 1 \pmod{5}, \\
 y_R &\equiv -y_P + m(x_P - x_R) \equiv -3 + 2(4 - 1) \equiv -3 + 6 \equiv 3 \pmod{5}, \\
 P_{ab} &= (x_R, y_R) = (1, 3).
 \end{aligned}$$

Paral·lelament  $B$  calcula el punt secret  $P_{ba}$  de la forma següent:

$$\begin{aligned}
 P_{ba} &= bP_a = 3 \cdot (1, 2) = 2 \cdot (1, 2) + (1, 2) = (x_{R_2}, y_{R_2}), \\
 m_1 &\equiv \frac{(3x_P^2 + a)}{2y_P} \equiv \frac{3 + 4}{4} \equiv \frac{7}{4} \equiv 7 \cdot 4 \equiv 3 \pmod{5}, \\
 x_{R_1} &\equiv m_1^2 - 2x_P \equiv 9 - 2 \equiv 7 \equiv 2 \pmod{5}, \\
 y_{R_1} &\equiv -y_P + m_1(x_P - x_{R_1}) \equiv -2 + 3(1 - 2) \equiv -2 - 3 \equiv 0 \pmod{5}, \\
 P_{ba} &= (2, 0) + (1, 2) = (x_{R_2}, y_{R_2}), \\
 m_2 &\equiv \frac{(y_{R_1} - y_P)}{(x_{R_1} - x_P)} \equiv \frac{0 - 2}{2 - 1} \equiv -2 \equiv 3 \pmod{5}, \\
 x_{R_2} &\equiv m_2^2 - x_{R_1} - x_P \equiv 9 - 2 - 1 \equiv 6 \equiv 1 \pmod{5}, \\
 y_{R_2} &\equiv -y_{R_1} + m_2(x_{R_1} - x_{R_2}) \equiv 0 + 3(2 - 1) \equiv 3 \pmod{5}, \\
 P_{ba} &= (x_{R_2}, y_{R_2}) = (1, 3).
 \end{aligned}$$

D'aquesta forma,  $A$  i  $B$  recuperen el valor secret  $P_{ab} = P_{ba} = (1, 3)$ , que pot ser utilitzat com a clau secreta de xifrat per possibles comunicacions confidencials.

En aquestes condicions suposem que  $A$  vol enviar el missatge  $M = (4, 3)$ , i que el xifrat  $C(M)$  és un punt de la corba  $E$  obtingut al sumar  $M$  amb la clau secreta  $(1, 3)$ :

$$C(M) = (4, 3) + (1, 3) = (0, 2)$$

Aleshores  $B$  recuperaria el missatge  $M$  amb la clau compartida  $(1, 3)$ :

$$M = (0, 2) - (1, 3) = (0, 2) + (1, 2) = (4, 3)$$

#### 4.2.4.3. Sistema de xifrat *ElGamal* amb CE

Un altre possible algoritme de xifrat de clau pública basat en corbes el·líptiques és l'equivalent al de *ElGamal* descrit anteriorment. En aquest cas, els paràmetres del procediment són una corba el·líptica  $E$  definida sobre un cos  $\mathbb{Z}/p\mathbb{Z}$  amb  $p$  primer i un punt  $G$  de la mateixa que sigui generador de grup. La corba  $E$  i el punt  $G$  són públics.

En aquestes condicions, suposem que els comunicants  $A$  i  $B$  volen intercanviar un missatge secret representat per un punt  $P$  de la corba. Per fer-ho, cada comunicant posseeix un sistema de clau pública.

El comunicant  $A$  posseeix una parella de claus  $(a, P_a)$ , sent  $a \in \mathbb{Z}/p\mathbb{Z}$  un valor aleatori secret i  $P_a = aG$  un punt públic de la corba  $E$ .

De la mateixa forma,  $B$  posseeix la seva parella de claus  $(b, P_b)$ , sent  $b \in \mathbb{Z}/p\mathbb{Z}$  un valor aleatori secret i  $P_b = bG$  un punt públic de la corba  $E$ .

D'aquesta forma,  $A$  pot transmetre a  $B$  un missatge confidencial  $P$  triant un valor enter aleatori  $k \in \mathbb{Z}/p\mathbb{Z}$  i enviant a  $B$  la parella de punts  $(M, N)$ , calculats a partir de l'expressió següent:

$$(M, N) = (kG, P + kP_b) = (kG, P + kbG).$$

Per la seva part, el comunicant  $B$  recupera el punt  $P$  utilitzant la seva clau secreta  $b$ , amb la qual realitza el càlcul següent:

$$P = N - bM.$$

Aquesta igualtat es pot verificar de la forma següent:

$$P = N - bM = P + kbG - bkG = P.$$

Després de l'anterior és fàcil adonar-se de que si un atacant volgués violar aquest sistema de xifrat de clau pública intentant obtenir la clau secreta de desxifrat  $b$  a partir de la clau pública de xifrat  $P_b$  aleshores hauria de ser capaç de resoldre el problema del logaritme el·líptic, ja que les dues claus estan relacionades mitjançant l'equació següent:

$$P_b = bG.$$

Una de les característiques més destacables d'aquest procediment de xifrat de clau pública és que els xifrats d'un mateix missatge poden ser diferents simplement computant-los a partir de valors enters aleatoris  $k$  diferents. Això també passava amb el procediment de *ElGamal*. No obstant, en aquest cas aquest procediment també té l'inconvenient de que el xifrat format per  $(M, N)$  és de longitud doble que el missatge en clar, la qual cosa suposa un augment considerable en les necessitats d'emmagatzematge de dades.

Ara que ja hem vist la part teòrica d'aquest mètode de xifrat podem passar a exposar un exemple pràctic per tal de comprendre'n el funcionament correctament.

Suposem que tenim un sistema de xifrat asimètric de clau pública *ElGamal* basat en corbes el·líptiques definit pels següents paràmetres:

$$\begin{cases} E : y^2 \equiv x^3 + 4x + 4 \pmod{5}, \\ G = (0, 2). \end{cases}$$

Suposem també els dos comunicants  $A$  i  $B$  volen intercanviar un missatge secret representat pel punt  $P = (1, 3)$  de la corba  $E$ .

Per fer-ho, cada comunicant posseeix un sistema de clau pública.

El comunicant  $A$  posseeix una parella de claus  $(a, P_a) = (2, (1, 2))$ , sent  $a \in \mathbb{Z}/p\mathbb{Z}$  un valor aleatori secret i  $P_a = aG$  un punt públic de la corba  $E$ .

De la mateixa forma,  $B$  posseeix la seva parella de claus  $(b, P_b) = (3, (4, 3))$ , sent  $b \in \mathbb{Z}/p\mathbb{Z}$  un valor aleatori secret i  $P_b = bG$  un punt públic de la corba  $E$ .

D'aquesta forma,  $A$  tria un valor enter aleatori  $k = 2$  i envia a  $B$  la parella de punts  $(M, N)$ , calculats a partir de l'expressió següent:

$$\begin{aligned} (M, N) &= (kG, P + kP_b) = (2 \cdot (0, 2), (1, 3) + 2 \cdot (4, 3)) = ((1, 2), (1, 3) + (1, 3)), \\ &\begin{cases} M = (1, 2), \\ N = (1, 3) + (1, 3) = 2 \cdot (1, 3) = (x_N, y_N), \end{cases} \\ m &\equiv \frac{(3x_P^2 + a)}{2y_P} \equiv \frac{3+4}{6} \equiv \frac{7}{1} \equiv 2 \pmod{5}, \\ x_N &\equiv m^2 - 2x_P \equiv 4 - 2 \equiv 2 \pmod{5}, \\ y_N &\equiv -y_P + m(x_P - x_N) \equiv -3 + 2(1 - 2) \equiv -5 \equiv 0 \pmod{5}, \\ N &= (x_N, y_N) = (2, 0). \end{aligned}$$

Aleshores  $B$  recupera  $P$  a partir del xifrat  $(M, N) = ((1, 2), (2, 0))$  de la forma següent:

$$\begin{aligned} P &= N - bM = (2, 0) - 3(1, 2) = (2, 0) - (1, 3) = (2, 0) + (1, -3) = (x_P, y_P), \\ m &\equiv \frac{(y_N - y_{M'})}{(x_N - x_{M'})} \equiv \frac{0 - (-3)}{2 - 1} \equiv 3 \pmod{5}, \\ x_P &\equiv m^2 - x_N - x_{M'} \equiv 9 - 2 - 1 \equiv 6 \equiv 1 \pmod{5}, \\ y_P &\equiv -y_N + m(x_N - x_P) \equiv 0 + 3(2 - 1) \equiv 3 \pmod{5}, \\ P &= (x_P, y_P) = (1, 3). \end{aligned}$$

D'aquesta forma el comunicant  $B$  recupera el missatge  $P = (1, 3)$ .

### 4.3. Desvetllant els secrets: atacs a DH, RSA i CE

Ara que ja hem vist com funcionen alguns dels procediments de xifrat asimètric més utilitzats en l'actualitat per codificar la informació que es transmet a través de les xarxes de comunicació es hora de fer un pas més enllà i veure com podem rebentar de forma teòrica els criptogrames obtinguts amb alguns dels mètodes de xifrat exposats anteriorment.

Més concretament, mostrarem diversos procediments per desxifrar criptogrames obtinguts a partir de tres mètodes de xifrat asimètric, que són el mètode d'intercanvi de claus de *Diffie* i *Hellman*, el mètode RSA i el mètode d'intercanvi de claus basat en corbes el·líptiques. Cal remarcar que pel mètode RSA s'ha dissenyat un procediment d'atac única i exclusivament per ser mostrat en aquest treball. Aquest atac ha estat programat en *Fortran*.

Així doncs, passem a exposar alguns dels procediments que ens permetran desxifrar criptogrames obtinguts amb mètodes de xifrat asimètric sense tenir la clau privada de desxifrat.

#### 4.3.1. Atac a l'algoritme bàsic de DH

Entre els possibles atacs dels quals pot ser objectiu l'algoritme d'intercanvi de claus de DH es poden considerar dos grans grups: atacs passius i atacs actius. Els atacs corresponents al primer grup es caracteritzen pel fet que l'atacant intenta obtenir informació escoltant la comunicació però sense intervenir-hi, és a dir, sense modificar-la.

En canvi, els atacs del segon grup es caracteritzen pel fet que l'atacant no solament escolta la conversació sinó que a més intenta modificar la informació que es transmet. A continuació es descriurà un dels atacs més representatius, que combina elements dels dos grups d'atacs.

Suposem que l'atacant escolta la comunicació durant un intercanvi de claus mitjançant l'algoritme de DH. En aquest cas, tot i que l'atacant coneix els valors públics  $p$ ,  $g$ ,  $y_a$  i  $y_b$ , és molt poc probable que pugui obtenir la clau secreta comuna  $z_{ab} = z_{ba}$  intercanviada entre  $A$  i  $B$ . Això és degut a que per calcular-la, l'atacant hauria de computar la clau secreta  $x_a$  de  $A$  o la clau secreta  $x_b$  de  $B$ , per tant hauria de resoldre al menys un dels logaritmes discrets següents:

$$x_a \equiv \log_g(y_a)(\text{mod } p),$$

$$x_b \equiv \log_g(y_b)(\text{mod } p).$$

Això resulta inviable per nombres de 200 dígit, que són els que s'acostumen a utilitzar, ja que els algorismes per calcular logaritmes discrets són viables per valors enters de fins a 80 dígit.

No obstant això, existeix la possibilitat que l'atacant violi el sistema sense necessitat de calcular la clau secreta comuna entre  $A$  i  $B$ .

Això es possible si l'atacant pren part en la comunicació. Per descriure aquest tipus d'atac actiu considerem un atacant  $C$  que intercepta la línia de comunicació. En aquestes condicions,  $A$  tria un enter aleatori secret  $x_a$  tal que  $1 < x_a < (p-1)$  i calcula el valor públic  $y_a$ , que posteriorment serà enviat a  $B$ , de la següent forma:

$$y_a \equiv g^{x_a} \pmod{p}.$$

Paral·lelament,  $C$  intercepta el valor de  $y_a$  evitant que  $B$  el rebi. Seguidament tria un enter aleatori secret  $x_c$  tal que  $1 < x_c < (p-1)$  i calcula el valor públic  $y_c$ , que posteriorment serà enviat a  $B$ , de la següent forma:

$$y_c \equiv g^{x_c} \pmod{p}.$$

D'aquesta forma,  $B$  rep el valor  $y_c$  creient que procedeix de  $A$ . Aleshores  $B$  tria un enter aleatori secret  $x_b$  tal que  $1 < x_b < (p-1)$  i calcula el valor públic  $y_b$ , que posteriorment serà enviat a  $A$ , de la forma següent:

$$y_b \equiv g^{x_b} \pmod{p}.$$

Aleshores  $C$  intercepta el valor de  $y_b$  evitant que  $A$  el rebi, i a continuació li envia el valor de  $y_c$ . En aquestes condicions  $A$  rep el valor de  $y_c$  pensant que prové de  $B$  y calcula el valor secret  $z_{ca}$  utilitzant la següent expressió:

$$z_{ca} \equiv y_c^{x_a} \equiv g^{x_c x_a} \pmod{p}.$$

De la mateixa forma,  $B$  calcula el valor secret  $z_{cb}$  utilitzant la següent expressió:

$$z_{cb} \equiv y_c^{x_b} \equiv g^{x_c x_b} \pmod{p}.$$

Aleshores l'atacant  $C$  calcula els valors de les claus secretes  $z_{ac}$  i  $z_{bc}$ , respectivament iguals als valors  $z_{ca}$  i  $z_{cb}$  recuperats per  $A$  i  $B$ . Els valors d'aquestes claus es calculen amb les equacions següents:

$$\begin{aligned} z_{ac} &\equiv y_a^{x_c} \equiv g^{x_a x_c} \pmod{p}, \\ z_{bc} &\equiv y_b^{x_c} \equiv g^{x_b x_c} \pmod{p}. \end{aligned}$$

D'aquesta forma, quan  $A$  envii un missatge xifrat a  $B$  utilitzant la clau  $z_{ca}$ , l'atacant  $C$  podrà interceptar-lo, desxifrar-lo amb la clau  $z_{ac}$ , modificar-lo, tornar-lo a xifrar amb la clau  $z_{bc}$  i enviar-lo a  $B$ , que el desxifrarà amb la seva clau  $z_{cb}$ .

Aquest procediment pot semblar complicat, per tant a continuació s'adjunta un exemple pràctic per tal de facilitar-ne la comprensió.

Suposem que tenim un sistema DH per intercanviar claus definit per un nombre primer  $p = 71$  i un generador  $g = 21$  del grup  $\mathbb{Z}/71\mathbb{Z}$ .

Suposem també que els comunicants  $A$  i  $B$  volen intercanviar un valor secret per utilitzar-lo com a clau secreta de xifrat en un sistema de xifrat simètric. Per tant,  $A$  tria un enter aleatori secret  $x_a = 37$  i envia a  $B$  el valor públic  $y_a$ , que calcula de la següent forma:

$$y_a \equiv 21^{37} \equiv 56 \pmod{71}.$$

Paral·lelament,  $B$  tria un enter aleatori secret  $x_b \equiv 61$  i envia a  $A$  el valor públic  $y_b$ , que calcula de la següent forma:

$$y_b \equiv 21^{61} \equiv 22 \pmod{71}.$$

Aleshores  $A$  calcula el valor secret  $z_{ba}$ :

$$z_{ba} \equiv 22^{37} \equiv 13 \pmod{71}.$$

A continuació  $B$  calcula el valor secret  $z_{ab}$ :

$$z_{ab} \equiv 56^{61} \equiv 13 \pmod{71}.$$

En aquestes condicions la clau secreta comuna és  $z_{ab} \equiv z_{ba} \equiv 13 \pmod{71}$ .

Un atacant  $C$  pot violar el sistema sense haver de calcular la clau secreta  $z_{ab} = z_{ba}$ . Per fer-ho, intercepta els valors  $y_a$  i  $y_b$ , evitant que siguin rebuts per  $B$  i  $A$  respectivament. Seguidament,  $C$  tria un enter aleatori secret  $x_c = 19$  i envia a  $A$  i  $B$  el valor públic  $y_c$ :

$$y_c \equiv 21^{19} \equiv 53 \pmod{71}.$$

Els comunicants  $A$  i  $B$  reben  $y_c$  i calculen respectivament els valors secrets  $z_{ca}$  i  $z_{cb}$ :

$$\begin{aligned} z_{ca} &\equiv 53^{37} \equiv 31 \pmod{71}, \\ z_{cb} &\equiv 53^{61} \equiv 59 \pmod{71}. \end{aligned}$$

Aleshores l'atacant  $C$  calcula les claus secretes  $z_{ac}$  i  $z_{bc}$  per comunicar-se respectivament amb  $A$  i  $B$ :

$$\begin{aligned} z_{ac} &\equiv 56^{19} \equiv 31 \pmod{71}, \\ z_{bc} &\equiv 22^{19} \equiv 59 \pmod{71}. \end{aligned}$$

En aquestes condicions suposem que  $A$  desitja enviar a  $B$  un missatge secret  $M = 44$  i que el xifrat és el producte (mod 71) del missatge i la clau. Aleshores  $A$  envia a  $B$  el xifrat  $C(M)$  amb la clau secreta  $z_{ca}$ :

$$C(M) \equiv 44 \cdot 31 \equiv 15 \pmod{71}.$$

L'atacant  $C$  recupera el missatge  $M$  desxifrant  $C(M)$  amb la clau secreta  $z_{ac}$ , de forma que:

$$M \equiv \frac{15}{31} \equiv 15 \cdot 55 \equiv 44 \pmod{71}.$$

Aleshores  $C$  pot enviar a  $B$  un missatge modificat  $M' = 67$  xifrat amb la clau secreta  $z_{bc}$ . Sigui  $C(M')$  el xifrat donat per:

$$C(M') \equiv 67 \cdot 59 \equiv 48 \pmod{71}.$$

Aleshores  $B$  desxifra  $C(M')$  amb la clau secreta  $z_{cb}$ :

$$M' \equiv \frac{48}{59} \equiv 48 \cdot 65 \equiv 67 \pmod{71}.$$

Així doncs,  $B$  recupera un missatge incorrecte que no correspon amb el que ha enviat  $A$ .

I aquí s'acaba la descripció de l'atac al sistema d'intercanvi de claus de *Diffie* i *Hellman*. A continuació és descriuran dos possibles atacs al mètode RSA.

### 4.3.2. Atac al mètode RSA

Una gran varietat d'atacs criptoanalítics han estats proposats per tal de rebentar el sistema de xifrat RSA. No obstant això, no sembla que cap d'ells hagi aconseguit el seu objectiu de forma efectiva. A continuació en descriurem dos, un dels quals és una implementació dissenyada exclusivament per ser exposada en aquest projecte. Com a material de suport s'ha creat un programa informàtic que posa en pràctica l'algorisme d'atac.

#### 4.3.2.1. Atac cíclic

L'atac cíclic està basat en la idea que tot sistema RSA consisteix en un grup multiplicatiu amb un nombre finit d'elements. Per descriure l'atac, considerem un sistema de xifrat RSA definit per les claus públiques  $e$  i  $N$  i la clau secreta  $d$ . Sigui  $M$  un missatge tal que  $1 < M < N$  i  $C$  el seu xifrat amb la clau pública  $e$  donat per:

$$C \equiv M^e \pmod{N}.$$

En aquestes condicions l'atac cíclic permet desxifrar  $C$  sense necessitat de conèixer la clau privada  $d$ . Per fer-ho només cal realitzar xifrats successius del xifrat inicial  $C$  amb la clau pública  $e$  fins a obtenir novament el xifrat  $C$ . Això és equivalent al càlcul de la successió de congruències  $C_i \equiv C_{i-1}^e \pmod{N}, i \in \mathbb{N}$ , amb la condició inicial  $C_0 = C$  fins que es verifiqui que  $C_i \equiv C \pmod{N}$ .

Arribats a aquest punt es fàcil adonar-se de que a la vegada s'ha de verificar que  $M \equiv C_{i-1} \pmod{N}$ .

És a dir, si després de  $i$  xifrats consecutius s'obté novament el xifrat inicial, aleshores el xifrat  $(i-1)$  correspon al missatge en clar. Una vegada més, aquest atac pot ser evitat si els factors primers  $p$  i  $q$  de la clau pública  $N$  són suficientment grans i de la forma  $p = 2p' + 1$  i  $q = 2q' + 1$ , amb  $p'$  i  $q'$  primers, la qual cosa fa que l'atac sigui inviable degut a la gran quantitat de xifrats consecutius que s'haurien de realitzar.

Passem a exposar un exemple pràctic per tal de comprendre'n el funcionament.

Suposem que tenim un sistema de xifrat RSA definit pels paràmetres següents:

$$\begin{cases} p = 19, \\ q = 23, \\ N = 437, \\ (p-1)(q-1) = 396, \\ e = 17. \end{cases}$$

Sigui  $M = 257$  un missatge i  $C$  el seu xifrat donat per:

$$C \equiv 257^{17} \equiv 2 \pmod{437}.$$

Un atacant pot desxifrar  $C$  sense necessitat de conèixer la clau secreta  $d \equiv \frac{1}{17} \equiv 233 \pmod{396}$ . Per fer-ho utilitza xifrats successius de  $C=2$  amb la clau pública  $e=17$  fins a obtenir novament el valor de  $C=2$ , tal i com es mostra en la taula següent:

$i$	$C_i$
$i = 0$	$C_0 \equiv 2 \pmod{437}$
$i = 1$	$C_1 \equiv 2^{17} \equiv 409 \pmod{437}$
$i = 2$	$C_2 \equiv 409^{17} \equiv 192 \pmod{437}$
$i = 3$	$C_3 \equiv 192^{17} \equiv 105 \pmod{437}$
$i = 4$	$C_4 \equiv 105^{17} \equiv 420 \pmod{437}$
$i = 5$	$C_5 \equiv 420^{17} \equiv 219 \pmod{437}$
$i = 6$	$C_6 \equiv 219^{17} \equiv 78 \pmod{437}$
$i = 7$	$C_7 \equiv 78^{17} \equiv 371 \pmod{437}$
$i = 8$	$C_8 \equiv 371^{17} \equiv 154 \pmod{437}$
$i = 9$	$C_9 \equiv 154^{17} \equiv 257 \pmod{437}$
$i = 10$	$C_{10} \equiv 257^{17} \equiv 2 \pmod{437}$

Com que  $C_{10} \equiv C \equiv 2 \pmod{437}$ , aleshores  $M \equiv C_9 \equiv 257 \pmod{437}$ .

#### 4.3.2.2. Implementació pròpia de l'atac per força bruta

Una forma evident de rebentar el sistema de xifrat RSA és factoritzant la clau pública  $N$ , el problema és que això no resulta fàcil sempre que els factors primers de  $N$  siguin suficientment grans. A més, és precisament aquesta dificultat la que fa que el sistema de xifrat sigui segur.

Un dels algorismes de factorització més utilitzats i més coneguts actualment és el que es coneix amb el nom d'algoritme de factorització per força bruta o *BruteForce*. Bàsicament consisteix en anar dividint el nombre  $n$  que es vulgui factoritzar entre tots els nombres més petits que ell, de forma que prova totes les possibilitats existents i així troba els factors primers de  $n$ .

El problema és que si el nombre  $n$  és extremadament gran, com en el cas de la clau pública  $N$  en el sistema de xifrat RSA, la cosa pot durar mesos o fins i tot anys, per molt potents que siguin els ordenadors que apliquin l'algoritme.

Per aquest motiu s'ha dissenyat una possible implementació que permet reduir considerablement el temps que tardaria un ordinador per trobar els factors primers d'un nombre  $n$ . El que s'ha fet és buscar una forma de reduir el nombre d'operacions a realitzar, i com que el temps de computació és directament proporcional al nombre d'operacions a realitzar, al reduir aquest nombre també es redueix el temps emprat.

El funcionament de l'algoritme implementat és el mateix que el normal però amb una petita variació que el fa més eficaç. Donat un nombre  $n$ , es va dividint únicament pels nombres primers que siguin més petits que ell, d'aquesta forma es redueix el nombre d'operacions a realitzar, ja que no tots els nombres més petits que  $n$  són nombres primers.

És més, tampoc és necessari que els nombres siguin primers, amb nombres probablement primers també serveix, ja que no tots els nombres més petits que  $n$  són nombres probablement primers, a més resulta més fàcil calcular probables primers que nombres primers. Cal constatar que un nombre probablement primer és un nombre considerat primer, tot i que no s'hagi demostrat.

Partint d'aquesta idea s'ha escrit un programa informàtic que divideix un nombre  $n$  donat entre tots els nombres d'una llista guardada en un document de text, i quan troba un nombre d'aquesta llista que divideixi a  $n$  ho indica en pantalla. D'aquesta forma, si a la llista s'hi inclouen tots els nombres primers i probablement primers més petits que  $n$ , el programa trobarà els factors primers de  $n$  d'una forma més ràpida que si calculés totes les divisions de  $n$  entre tots els nombres més petits que aquest.

Per exemple, suposem que volem factoritzar el nombre 1000001. Si ho féssim amb l'algoritme *BruteForce* no implementat s'haurien de calcular  $10^6$  divisions. Però si ho fem amb l'algoritme implementat només s'han de calcular 78498 divisions, nombre corresponent a la quantitat de primers que hi ha entre 1 i 1000000.

Ara que ja coneixem la teoria, passem a descriure el funcionament del programa dissenyat, tot mostrant un exemple pràctic d'aplicació d'aquest.

#### 4.3.2.2.1. Exposició del programa informàtic propi *CleanForce*

Primer de tot cal remarcar que aquest programa s'ha escrit en llenguatge de programació *Fortran* (*Formula Translating System*), que és un llenguatge de programació d'alt nivell desenvolupat per IBM en 1957. Va ser el primer desenvolupat amb aquestes característiques.

Està fortament orientat al càlcul i per tant és un dels de major eficiència en l'execució. S'ha de tenir en compte que la sintaxi de *Fortran* va ser dissenyada per l'ús en treballs numèrics i científics. Cal remarcar que *Fortran* ha estat, clàssicament, una de les millors opcions a escollir per tal d'executar tasques de computació numèrica d'alt rendiment.

Per tal de crear el nostre programa hem utilitzat el compilador ***Force 2.0.8***, programa gratuït que pot ser descarregat d'Internet. Cal dir que hi ha molts altres compiladors de *Fortran*, i tots ells són vàlids, així que no hi ha necessitat en utilitzar el mateix que hem fet servir nosaltres aquí.

L'icona del programa utilitzat és la següent:



**Figura 22:** Icona del programa *Force 2.0*.

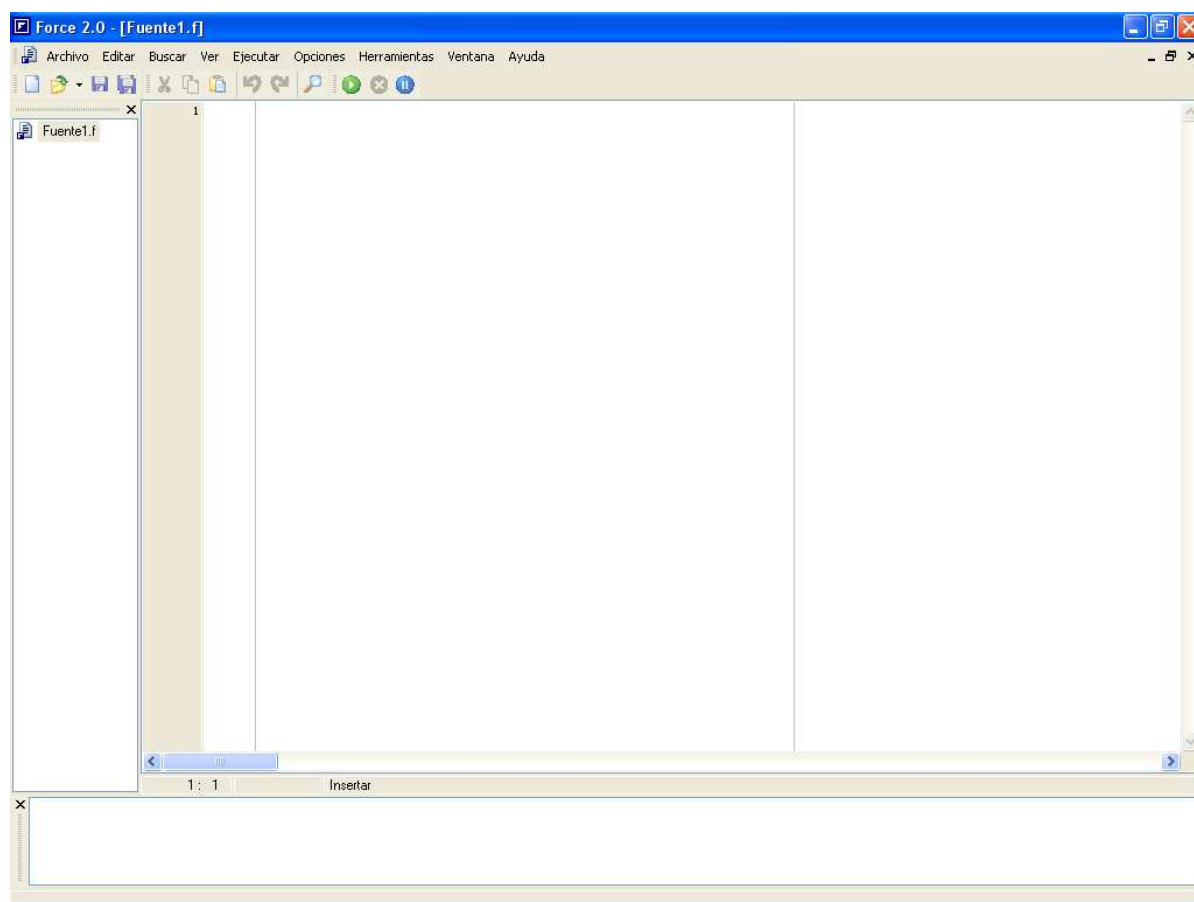
Quan s'executa es mostra una petita pantalla amb el nom i la versió del programa, els autors del mateix i la web del projecte:



**Figura 23:** Pantalla de presentació del programa *Force 2.0*.


A continuació es mostrarà la pantalla principal del programa, que és on escriurem el codi font del mateix.

Aquesta és la pantalla principal:



**Figura 24:** Pantalla principal del programa *Force 2.0*.

El codi font s'ha d'escriure en el rectangle central de color blanc, a partir de la primera línia vertical de color gris.

Un cop acabat, només caldrà pressionar la icona  , situada just a sobre del rectangle on hem escrit el codi. Aleshores el programa ens guardarà el codi font en un arxiu i posteriorment el compilarà, i si no troba cap error greu en el codi, el nostre programa arrancarà.

En cas que el compilador trobi errors, ens els indicarà en el rectangle inferior, i els haurem de corregir si volem que el nostre programa es compili i funcioni correctament.

Ara que ja sabem com funciona el compilador, passem a exposar el programa que hem creat i a comentar el seu funcionament.

Començarem exposant-ne el codi font, el text a partir del qual el compilador crea els arxius executables del nostre programa.

Posteriorment comentarem el significat de les línies de codi que el formen, per tal de poder comprendre millor el funcionament del programa en si.

## Codi font del programa informàtic propi CleanForce

```

1  / Versió 3.0 del programa d'implementació de
2  / l'algoritme de factorització Bruteforce
3  program CleanForce ! Escrit per Eduard Roure Pardides 06/12/2009
4  ! Definim les variables com a enteres en doble precisió
5  integer*8::j,Y,m
6  ! Decidir què ha de fer el programa
7  1 write(*,*) 'Què vols fer? (1 / 2)' ! Introduir 1 o 2
8  write(*,*) '1. Introduir un nombre i factoritzar-lo.' ! Acció 1
9  write(*,*) '2. Factoritzar un nombre guardat en factor.txt.' ! Acció 2
10 ! Assignant el número escrit a una variable
11 read(*,*) x ! Legint el número escrit
12 if (x.eq.1) then ! Si és 1, introduir un nombre
13     write(*,*) 'Introdueix el nombre que vols factoritzar.'
14     read(*,*) y ! Legint el número escrit
15     write(*,*) 'El nombre és', y ! Mostrant el número escrit
16     ! Per llegir nombres d'un fitxer línia a línia
17     open(3,file='primes.txt',status='unknown') ! Obrint l'arxiu primes.txt
18     do i=1,78498 ! 78498 és el nombre de files de l'arxiu primes.txt
19         read(3,*) m ! Llegint els nombres de l'arxiu
20         if (mod(y,m).eq.0) then ! Mirant si y és congruent amb 0 en mod m
21             write(*,*) 'El nombre', y, ' és divisible entre', m ! Mostrant el resultat
22         end if ! Tancant condicional IF
23     end do ! Tancant DO
24     close(3) ! Tancant l'arxiu primes.txt
25     GO TO 2 ! Redirecció a elecció d'accions
26 else if (x.eq.2) then ! Si és 2, carregar nombre des de l'arxiu factor.txt
27     write(*,*) 'Llegint el nombre des de factor.txt ...' ! Mostrant l'acció
28     open(7,file='factor.txt',status='unknown') ! Obrint l'arxiu factor.txt
29     read(7,*) j ! Llegint el nombre de l'arxiu
30     write(*,*) 'El nombre és', j ! Mostrant el nombre llegit
31     open(3,file='primes.txt',status='unknown') ! Obrint l'arxiu primes.txt
32     do i=1,78498 ! 78498 és el nombre de files de l'arxiu primes.txt
33         read(3,*) m ! Llegint els nombres de l'arxiu
34         if (mod(j,m).eq.0) then ! Mirant si n és congruent amb 0 mod m
35             write(*,*) 'El nombre', j, ' és divisible entre', m ! Mostrant el resultat
36         end if ! Tancant condicional IF
37     end do ! Tancant DO
38     close(7) ! Tancant l'arxiu factor.txt
39     close(3) ! Tancant l'arxiu primes.txt
40     GO TO 2 ! redirecció a elecció d'accions
41 else ! Si no és ni 1 ni 2, repetició de confirmació
42     Write(*,*) 'Torna-ho a intentar.' ! Repetició
43     GO TO 1 ! Redirecció a elecció d'accions del programa
44 end if ! Tancant condicional IF
45 2 write(*,*) 'Vols seguir? (S 1 / N 0)' ! Confirmació al finalitzar el procés
46 read(*,*) a ! Legint el nombre escrit
47 if (a.eq.0) then ! Si és 0, tasca cancel·lada i fi del programa
48     write(*,*) 'Tasca cancel·lada.' ! Mostrant elecció
49     GO TO 4 ! Redirecció a END
50 else if (a.eq.1) then ! Si és 1, reinici de procés, salt a GO TO 1
51     write(*,*) 'Reiniciant el procés...' ! Mostrant l'acció
52 else ! Si no és ni 0 ni 1, repetició de confirmació
53     Write(*,*) 'Torna-ho a intentar.' ! Repetició
54     GO TO 2 ! Redirecció a confirmació
55 end if ! Tancant condicional IF
56 GO TO 1 ! Redirecció al principi, torna a començar
57 4 end program ! Final del programa

```

A continuació passarem a comentar significat dels blocs de les línies que formen el codi, tot i que cal remarcar que les lletres en color gris que es veuen són comentaris que indiquen la funció de cadascuna de les línies del codi.

Per tal de poder descriure el funcionament dels blocs de línies del codi utilitzarem els números de les línies per indicar quin bloc estem comentant en cada moment, la qual cosa ens facilitarà la feina.

Comencem per les tres primeres línies del codi. Aquestes presenten el programa, indicant l'autor i la data de creació.

La línia 5 defineix les variables com a nombres enters en doble precisió, és a dir, que el programa treballarà correctament amb nombres de fins a 18 - 19 xifres.

Les línies 7, 8 i 9 fan que a la pantalla hi apareguin les accions que pot realitzar el programa.

Des de la línia 11 fins a la línia 44 hi podem veure el codi que fa possible que el programa dugui a terme les funcions exposades al principi.

Un cop finalitzada l'acció, el programa ofereix la possibilitat de tornar a realitzar una de les accions inicials. Aquesta funció està programada a partir de la línia 45 fins a la línia 56.

La línia 57 permet que el programa finalitzi.

Ara que ja hem comentat breument el funcionament del programa a partir del codi font d'aquest podem passar a comprovar de forma pràctica que el programa fa les accions corresponents a les descrites al codi font.

Comencem exposant els arxius necessaris per a que el programa funcioni sense problemes:



**Figura 25:** Arxius necessaris per a que *CleanForce* funcioni correctament.

El primer arxiu, *CleanForce 3.0.f* conté el codi font del programa. No és un arxiu necessari per fer-lo funcionar però en cas que es vulgui modificar algun aspecte caldrà disposar d'aquest arxiu.

L'arxiu *CleanForce 3.0* és un accés directe a l'arxiu *CleanForce 3.0.exe*, que és el que hem d'obrir per iniciar el programa.

L'arxiu *primes.txt* conté els nombres primers entre els quals el programa dividirà un nombre  $n$  donat per intentar trobar els factors primers d'aquest. Sense aquest arxiu el programa no funcionarà correctament.

L'arxiu *factor.txt* és l'arxiu on escriurem un nombre  $n$  per tal que el programa busqui els seus factors primers, en cas que no vulguem introduir  $n$  de forma manual al programa. Si aquest arxiu no hi és, el programa pot no funcionar correctament depenent de l'acció que es vulgui realitzar.

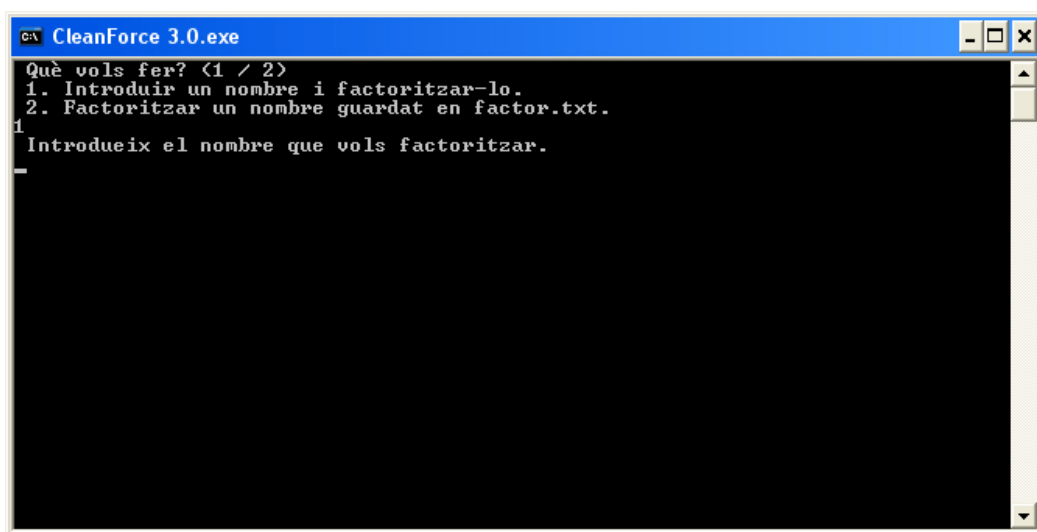
Ara que ja sabem la funció dels arxius mostrats passem a iniciar el programa, executant l'arxiu *CleanForce 3.0*, que té les lletres MS DOS a la icona, i ens apareix la pantalla principal del programa:



**Figura 26:** Captura de pantalla del programa *CleanForce*.

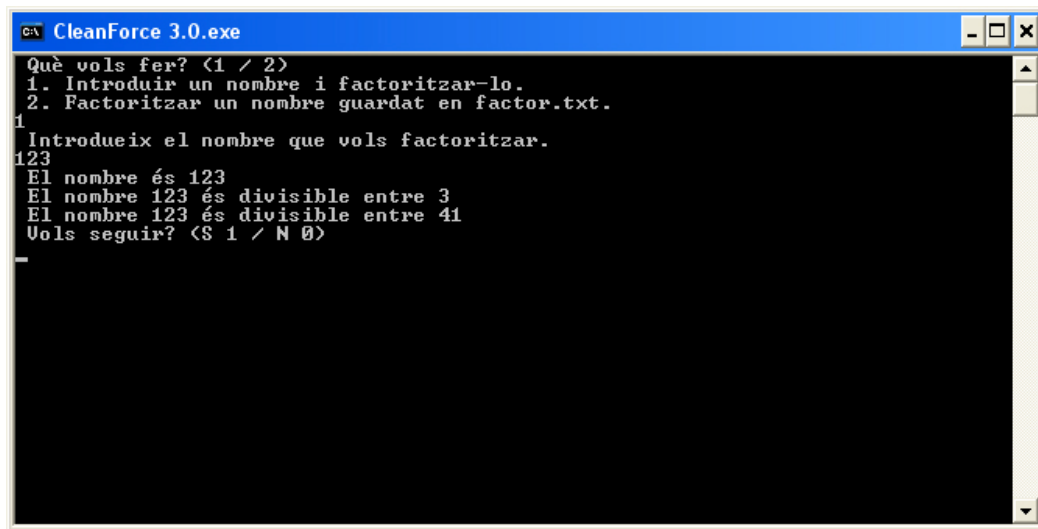
Tal i com podem observar, el programa ofereix dos opcions, i per escollir-ne una només cal escriure 1 o 2 depenent de l'acció que es vulgui realitzar.

Si seleccionem l'opció 1 ens apareixerà la següent pantalla:



**Figura 27:** Captura de pantalla del programa *CleanForce*.

En aquest punt introduïm el nombre que volem factoritzar de forma manual i el programa comprova si algun dels nombres de l'arxiu *primes.txt* és un factor del nombre introduït. Si en troba algun ho indica en la pantalla.

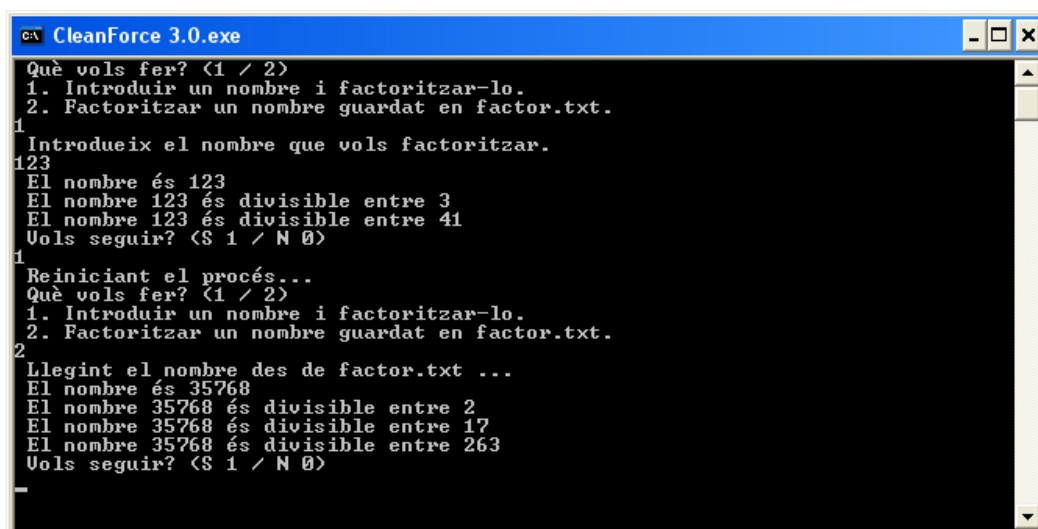


```
C:\> CleanForce 3.0.exe
Què vols fer? <1 / 2>
1. Introduir un nombre i factoritzar-lo.
2. Factoritzar un nombre guardat en factor.txt.
1
Introdueix el nombre que vols factoritzar.
123
El nombre és 123
El nombre 123 és divisible entre 3
El nombre 123 és divisible entre 41
Vols seguir? <S 1 / N 0>
-
```

**Figura 28:** Captura de pantalla del programa *CleanForce*.

Quan acaba, el programa ens dona la opció de continuar treballant o de parar. En cas que vulguem continuar escriurem 1 i en cas que vulguem parar escriurem 0, ja que no accepta la introducció de text. Cal remarcar que si s'introdueixen lletres el programa donarà error i quedarà congelat.

Si seleccionem 1 tornarem a la pantalla inicial. Ara seleccionem 2, i el programa automàticament llegeix el nombre escrit a l'arxiu *factor.txt* i comprova si aquest nombre té algun factor primer que estigui escrit en l'arxiu *primes.txt*. En cas afirmatiu, el programa ho passa per pantalla.

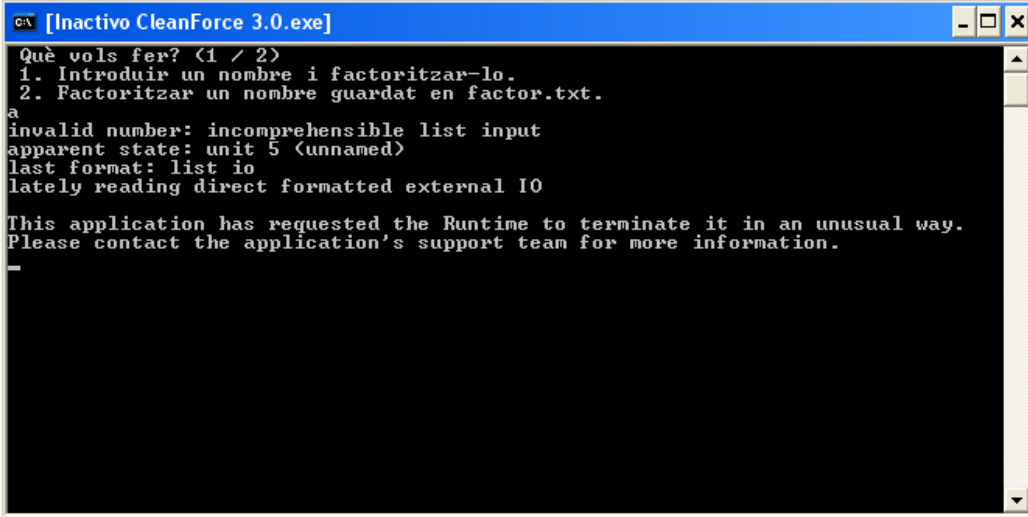


```
C:\> CleanForce 3.0.exe
Què vols fer? <1 / 2>
1. Introduir un nombre i factoritzar-lo.
2. Factoritzar un nombre guardat en factor.txt.
1
Introdueix el nombre que vols factoritzar.
123
El nombre és 123
El nombre 123 és divisible entre 3
El nombre 123 és divisible entre 41
Vols seguir? <S 1 / N 0>
1
Reiniciant el procés...
Què vols fer? <1 / 2>
1. Introduir un nombre i factoritzar-lo.
2. Factoritzar un nombre guardat en factor.txt.
2
Llegint el nombre des de factor.txt ...
El nombre és 35768
El nombre 35768 és divisible entre 2
El nombre 35768 és divisible entre 17
El nombre 35768 és divisible entre 263
Vols seguir? <S 1 / N 0>
-
```

**Figura 29:** Captura de pantalla del programa *CleanForce*.

Un cop finalitzada la tasca, el programa torna a donar l'opció de seguir treballant o de parar. Si seleccionem 0, el programa es congelarà i el podrem tancar sense problemes. Cal remarcar que si el tanquéssim sense congelar-lo ens apareixeria un missatge dient que el programa no respon, per tant hem de procurar parar-lo i posteriorment tancar-lo per evitar problemes.

Anteriorment hem comentat que aquest programa no accepta la introducció de text, ja que el congela i s'ha de reiniciar per poder continuar treballant. A continuació s'adjunta una pantalla on es mostra què passa si hi introduïm lletres i no nombres:



```
CA [Inactivo CleanForce 3.0.exe]
Què vols fer? <1 / 2>
1. Introduir un nombre i factoritzar-lo.
2. Factoritzar un nombre guardat en factor.txt.
a
invalid number: incomprehensible list input
apparent state: unit 5 <unnamed>
last format: list io
lately reading direct formatted external IO

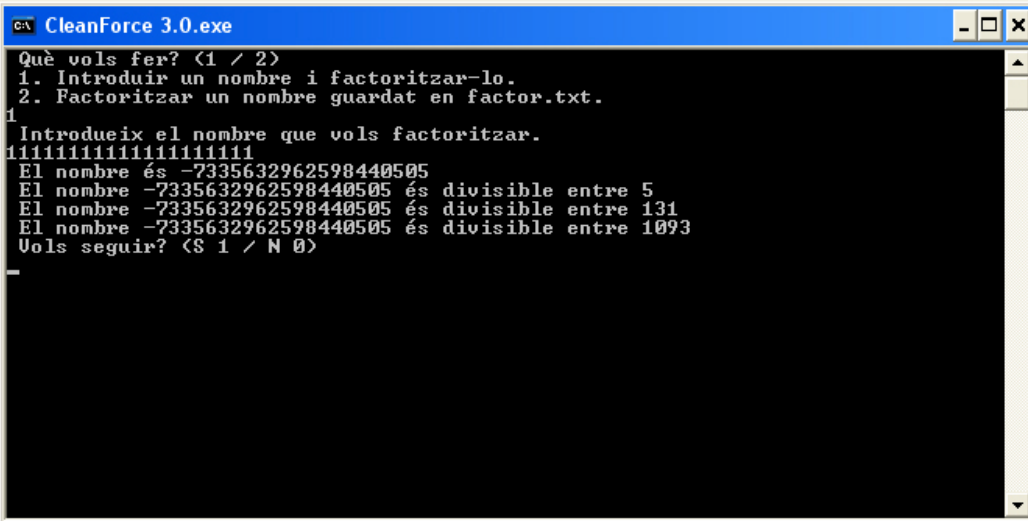
This application has requested the Runtime to terminate it in an unusual way.
Please contact the application's support team for more information.
```

**Figura 30:** Captura de pantalla del programa *CleanForce*.

Tal i com es pot observar, el programa es queda inactiu i mostra un error per pantalla.

També hem comentat que per nombres superiors a 19 dígits el programa també mostra errors, ja que només pot treballar amb nombres de com a màxim 19 dígits.

Vegem què passa quan introduïm un nombre de 20 dígits:



```
CA CleanForce 3.0.exe
Què vols fer? <1 / 2>
1. Introduir un nombre i factoritzar-lo.
2. Factoritzar un nombre guardat en factor.txt.
1
Introdueix el nombre que vols factoritzar.
11111111111111111111
El nombre és -7335632962598440505
El nombre -7335632962598440505 és divisible entre 5
El nombre -7335632962598440505 és divisible entre 131
El nombre -7335632962598440505 és divisible entre 1093
Vols seguir? <S 1 / N 0>
```

**Figura 31:** Captura de pantalla del programa *CleanForce*.

Tal i com podem observar, el programa no interpreta correctament el nombre introduït i en mostra un altre de negatiu, i a més els nombres primers que mostra no són factors del nombre introduït.

Ara que ja hem vist com funciona el programa i quines són les seves limitacions, passem a descriure l'atac al sistema de xifrat RSA utilitzant el mètode implementat de factorització *BruteForce*.

#### 4.3.2.2.2. Treballant amb el programa informàtic propi *CleanForce*

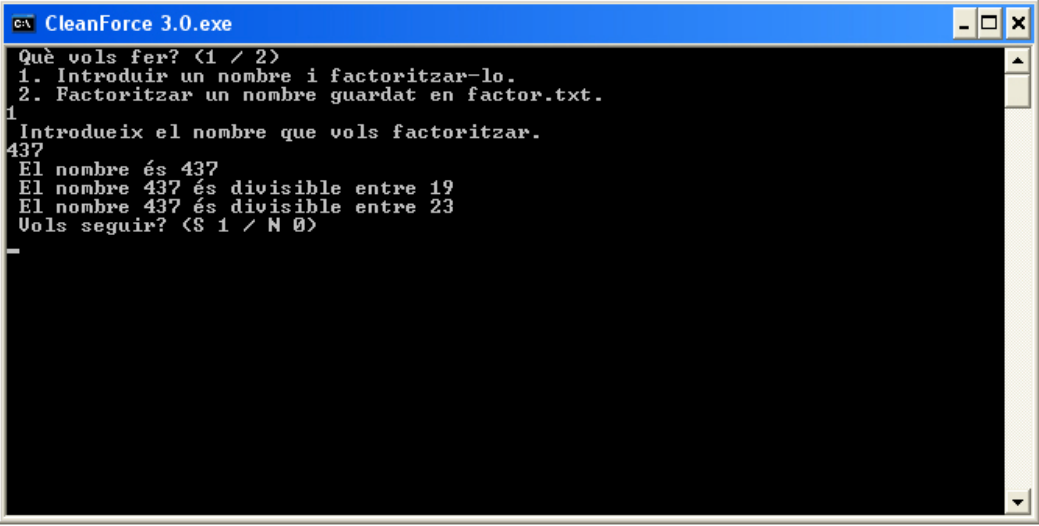
Suposem que tenim un sistema de xifrat RSA definit pels paràmetres següents:

$$\begin{cases} p = 19, \\ q = 23, \\ N = 437, \\ (p-1)(q-1) = 396, \\ e = 17. \end{cases}$$

Sigui  $M = 257$  un missatge i  $C$  el seu xifrat donat per:

$$C \equiv 257^{17} \equiv 2 \pmod{437}.$$

Un atacant podria conèixer la parella de claus públiques  $(N, e)$  i el missatge xifrat  $C$ , de tal forma que per desxifrar-lo necessitaria tenir la clau privada  $d$ . Així doncs, l'atacant factoritza  $N = 437$  utilitzant el mètode implementat:



```

CleanForce 3.0.exe
Què vols fer? <1 / 2>
1. Introduir un nombre i factoritzar-lo.
2. Factoritzar un nombre guardat en factor.txt.
1
Introdueix el nombre que vols factoritzar.
437
El nombre és 437
El nombre 437 és divisible entre 19
El nombre 437 és divisible entre 23
Vols seguir? <S 1 / N 0>

```

**Figura 32:** Captura de pantalla del programa *CleanForce*.

D'aquesta forma l'atacant troba els valors de  $p$  i  $q$ , a partir dels quals calcula  $(19-1)(23-1) = 396$ . Sabent que  $ed \equiv 1 \pmod{(p-1)(q-1)}$ , l'atacant computa el valor de  $d$  de la forma següent:

$$d \equiv \frac{1}{17} \equiv 233 \pmod{396}.$$

I finalment l'atacant recupera el missatge  $M$  de la forma següent:

$$M \equiv C^d \equiv 2^{233} \equiv 257 \pmod{437}.$$

### 4.3.3. Atac al mètode d'intercanvi de claus basat en CE

De la mateixa forma que en el mètode d'intercanvi de claus proposat per *Diffie* i *Hellman*, es poden considerar dos possibles atacs al procediment d'intercanvi de claus basat en corbes el·líptiques: els atacs passius i els actius.

En els primers, l'atacant intenta obtenir informació simplement escoltant la comunicació sense intervenir-hi, és a dir, sense modificar-la.

Pel contrari, en els segons l'atacant intenta obtenir informació i modificar-la. A continuació es descriurà la forma de portar a terme aquests atacs.

Suposem que l'atacant simplement escolta la comunicació durant un intercanvi de claus. En aquest cas, tot i conèixer els paràmetres públics  $E$ ,  $G$ ,  $P_a$  i  $P_b$ , és molt poc probable que l'atacant pugui obtenir la clau secreta comuna, és a dir, el punt  $P_{ab} = P_{ba}$  intercanviat entre  $A$  i  $B$ .

Això és degut a que per calcular aquest punt, l'atacant hauria de calcular la clau secreta  $a$  de  $A$  o la clau secreta  $b$  de  $B$  a partir de les respectives claus públiques associades  $P_a = aG$  i  $P_b = bG$ . En aquestes condicions, aquest és el problema del logaritme el·líptic, la complexitat del qual és molt elevada sempre que  $G$  sigui el generador de punts de la corba  $E$  definida sobre  $\mathbb{Z}/p\mathbb{Z}$ , amb  $p$  suficientment gran.

No obstant això, també existeix la possibilitat que l'atacant pugui violar el sistema sense necessitat de calcular la clau secreta comuna entre  $A$  i  $B$ . Això és possible si l'atacant no només escolta la comunicació sinó que a més hi pren part activa. Per descriure aquest atac, considerem un atacant  $C$  que intercepta la línia de comunicació. En aquestes condicions, l'atac es porta a terme tal i com es descriurà a continuació.

El comunicant  $A$  tria un valor aleatori secret  $a \in \mathbb{Z}/p\mathbb{Z}$  i envia a  $B$  el punt de la corba

$$P_a = aG.$$

L'atacant  $C$  intercepta el punt  $P_a$  evitant que  $B$  el rebí. A continuació tria un valor enter aleatori secret  $c \in \mathbb{Z}/p\mathbb{Z}$ , calcula el punt  $P_{ca} = cP_a = caG$  i envia a  $B$  el punt  $P_c = cG$ .

El comunicant  $B$  rep  $P_c$  pensant que prové de  $A$  tria un valor enter aleatori secret  $b \in \mathbb{Z}/p\mathbb{Z}$  i calcula el punt  $P_{bc} = bP_c = bcG$ . A continuació,  $B$  envia a  $A$  el punt  $P_b = bG$ .

L'atacant  $C$  intercepta  $P_b$  evitant que sigui rebut per  $A$  i calcula  $P_{cb} = cP_b = cbG$  i seguidament envia a  $A$  el punt  $P_c$ .

Aleshores  $A$  rep  $P_c$  pensant que prové de  $B$  i calcula  $P_{ac} = aP_c = acG$ .

Evidentment els punts  $P_{ca}$  i  $P_{cb}$  calculats per l'atacant  $C$  són respectivament iguals als punts  $P_{ac}$  i  $P_{bc}$  recuperats per  $A$  i  $B$ . D'aquesta forma, quan  $A$  envia a  $B$  un missatge xifrat amb la clau  $P_{ac}$ , l'atacant  $C$  pot interceptar-lo, desxifrar-lo amb la clau  $P_{ca}$ , modificar-lo, xifrar-lo amb la clau  $P_{cb}$  i enviar-lo a  $B$ , que el desxifrarà amb la clau  $P_{bc}$ . Ara que ja hem vist la part teòrica d'aquest atac passarem a exposar un exemple pràctic per tal de comprendre'n el funcionament correctament.

Suposem que tenim un sistema d'intercanvi de claus secretes basat en corbes el·líptiques definit pels següents paràmetres:

$$\begin{cases} E : y^2 \equiv x^3 + 4x + 4 \pmod{5}, \\ G = (0, 2). \end{cases}$$

Suposem també que dos comunicants  $A$  i  $B$  volen intercanviar una clau secreta en un canal obert.

En aquestes condicions,  $A$  tria un valor enter aleatori  $a = 2$ , i calcula la seva clau pública  $P_a = (1, 2)$ , que posteriorment envia a  $B$ .

Aleshores l'atacant  $C$  intercepta el punt  $P_a = (1, 2)$  evitant que el rebí  $B$ . A continuació tria un valor enter aleatori  $c = 3$ , calcula el punt  $P_{ca} = cP_a = 3 \cdot (1, 2) = (1, 3)$  i envia a  $B$  el punt  $P_c = cG = 3 \cdot (0, 2) = (4, 3)$ .

El comunicant  $B$  rep  $P_c$  creient que prové de  $A$  tria un valor aleatori  $b = 3$  i calcula el punt  $P_{bc} = bP_c = 3 \cdot (4, 3) = 2 \cdot (4, 3) + (4, 3) = (1, 3) + (4, 3) = (x_R, y_R)$ :

$$\begin{aligned} m &\equiv \frac{(y_P - y_Q)}{(x_P - x_Q)} \equiv \frac{3 - 3}{1 - 4} \equiv 0 \pmod{5}, \\ x_R &\equiv m^2 - x_P - x_Q \equiv 0 - 1 - 4 \equiv 0 \pmod{5}, \\ y_R &\equiv -y_P + m(x_P - x_R) \equiv -3 \equiv 2 \pmod{5}, \end{aligned}$$

$$P_{bc} = (x_R, y_R) = (0, 2).$$

Posteriorment envia a  $A$  el punt  $P_b = (4, 3)$ .

Aleshores l'atacant  $C$  intercepta  $P_b = (4, 3)$  evitant que el rebí  $A$  i calcula  $P_{cb} = cP_b = 3 \cdot (4, 3) = (0, 2)$ . Seguidament  $C$  envia a  $A$  el punt  $P_c = (4, 3)$ .

Seguidament  $A$  rep  $P_c$  creient que prové de  $B$  i calcula  $P_{ac} = aP_c = 2 \cdot (4, 3) = (1, 3)$ .

Tal i com podem comprovar,  $P_{ac} = P_{ca} = (1, 3)$  i  $P_{bc} = P_{cb} = (0, 2)$ , per tant l'atacant  $C$  podrà modificar tota la informació que es transmeti xifrada amb aquestes claus.

En aquestes condicions suposem que  $A$  vol enviar el missatge  $M = (4, 3)$  a  $B$ , i que el xifrat  $C(M)$  és un punt de la corba  $E$  obtingut al sumar  $M$  amb la clau secreta  $P_{ac} = (1, 3)$ :

$$C(M) = (4, 3) + (1, 3) = (0, 2).$$

Aleshores  $C$  intercepta el xifrat i recupera el missatge en clar amb la clau  $P_{ca} = (1, 3)$ :

$$M = (0, 2) - (1, 3) = (0, 2) + (1, 2) = (4, 3).$$

Posteriorment  $C$  modifica el missatge, i envia a  $B$  un nou missatge  $M' = (4, 2)$ , que xifra amb la clau  $P_{cb} = (0, 2)$ :

$$C(M') = (4, 2) + (0, 2) = (1, 3).$$

Aleshores  $B$  recupera el missatge  $M'$  pensant que prové de  $A$ , amb la clau  $P_{bc} = (0, 2)$ :

$$M = (1, 3) - (0, 2) = (1, 3) + (0, 3) = (4, 2).$$

D'aquesta forma un atacant  $C$  pot prendre part activa en una conversació, modificant els missatges xifrats que es transmeten.

## 5. PROTOCOLS CRIPTOGRÀFICS

### 5.1. Introducció

Passem a descriure un tipus de procediments relacionats amb la Criptografia, als que anomenarem protocols criptogràfics.

Actualment la Criptografia cobreix objectius molt diversos, de vegades molt allunyats del tradicional i més conegut, que és el de transmetre informació modificada per tal que només pugui ser interpretada per la persona a la qual va dirigida.

Aquest tipus d'aplicacions s'engloben dins del grup dels protocols criptogràfics. Bàsicament podem dir que un protocol criptogràfic és un conjunt definit d'etapes designat per realitzar una tasca específica, que utilitza com a eina algun algoritme criptogràfic.

Existeix una àmplia varietat de protocols criptogràfics, que donen resposta a diferents objectius. Es tracta d'un tema molt ampli i en constant creixement.

A continuació es citen alguns del protocols criptogràfics més comuns, tot i que cal remarcar que nosaltres en aquest apartat només en tractarem un d'ells, el protocol de secrets compartits.

1. **Protocols d'autenticació d'usuari:** permeten garantir que el remitent d'un missatge o l'usuari amb el qual establir comunicació és realment la persona que afirma ser.
2. **Protocols d'autenticació del missatge:** garanteixen que el missatge enviat no ha estat substituït o alterat.
3. **Distribució de claus:** permeten solucionar un dels principals problemes de la Criptografia que és l'intercanvi de claus de forma segura.
4. **Protocols de secrets compartits:** l'objectiu és distribuir un cert secret, per exemple la clau per obrir una caixa forta, entre un conjunt  $K$  de participants, de forma que certs subconjunts predefïnits de  $K$  puguin recuperar el secret unint les seves parts del secret.
5. **Proves de coneixement zero:** permeten a un individu convèncer a un altre de que posseeix una certa informació, sense revelar cap aspecte sobre el contingut de la mateixa.
6. **Transaccions electròniques segures:** permeten realitzar de forma electrònica segura les operacions bancàries habituals, tals com la firma electrònica de contractes.
7. **Tècniques de compromís amb un bit:** permeten a una de les parts  $A$  a comprometre's amb una elecció sense revelar-la fins un moment posterior. El protocol garanteix a una altra part  $B$  que  $A$  no canvia la seva elecció.

8. ***Transferències transcordades:*** permeten que els usuaris adquireixin les seves claus secretes de forma anònima a través d'un distribuïdor, és a dir, sense que aquest conegui quin usuari posseeix cada clau.
9. ***Eleccions electròniques:*** permeten realitzar un procés electoral electrònicament, garantint la privacitat de cada votant i la impossibilitat d'estafa.
10. ***Partides de Poker per Internet:*** permet que dues persones, físicament separades, puguin mantenir una partida de Poker o similar comunicant-se per correu electrònic, telèfon, etc. garantint la impossibilitat de fer trampes.

Ara que ja hem comentat els aspectes generals relacionats amb els protocols criptogràfics, passarem a descriure més detalladament un dels tipus mencionats anteriorment, més concretament, els protocols criptogràfics de secrets compartits.

Per fer-ho, estudiarem un dels mètodes més coneguts per compartir secrets i posteriorment plantejarem una possible implementació d'aquest mètode juntament amb una proposta d'un procediment alternatiu per compartir secrets. Cal remarcar que tant la implementació com la proposta mencionades s'han dissenyat exclusivament per ser exposades en aquest treball.

## 5.2. Protocols criptogràfics de secrets compartits

Les claus secretes utilitzades en els protocols criptogràfics plantegen diversos problemes pràctics relatius tant a la seva generació com a la seva memorització i distribució.

Pel que fa a l'aspecte de la distribució, en molts casos pràctics és necessari que la clau secreta sigui distribuïda entre els diferents membres d'un mateix grup, de forma que no pugui ser recuperada sense la cooperació d'un nombre mínim de membres del grup.

D'aquesta forma, cap membre posseeix la clau secreta completa, però sí una participació de la mateixa. Aquest esquema de distribució és especialment adequat si les claus secretes són responsabilitat d'un grup i no d'un sol individu, o si els integrants d'un grup han de cooperar sense que hi hagi confiança mútua entre els mateixos.

També és probable que en algunes situacions sigui necessari recuperar una determinada clau sense la presència del seu responsable directe, és a dir, que una mateixa clau pugui ser recuperada pel seu propietari o per determinats grups jeràrquics escollits per aquest.

Pel contrari, en altres ocasions és convenient que la distribució es realitzi de tal forma que el propietari mai pugui ser suplantat per altres membres del sistema. Això es pot portar a terme fent que algunes de les participacions de la clau tinguin un caràcter preferencial sobre les altres.

Existeix per tant una gran varietat de problemes pràctics associats a les tècniques de distribució de les claus criptogràfiques. La Criptografia moderna els ha anat resolent, desenvolupant procediments per distribuir secrets amb els requeriments mencionats anteriorment i amb mesures de seguretat suficients.

Alguns d'aquests procediments s'utilitzen molt freqüentment, mentre que altres estan en procés de desenvolupament.

A continuació es descriurà un dels procediments bàsics de distribució de secrets, el mètode de *Shamir*.

### 5.2.1. Esquema de Shamir per compartir secrets

L'objectiu d'aquest procediment és distribuir un secret  $S$  en  $n$  participacions, de tal forma que  $t \leq n$  participacions qualsevol permetin reconstruir el secret, però no un nombre de participacions inferior a  $t$ .

Aquest sistema de distribució va ser proposat per *A. Shamir* i es basa en la idea que dos punts són suficients per a definir una línia recta, tres punts ho són per a definir una paràbola, quatre per a definir una corba cúbica i així successivament. És a dir, són necessaris  $d+1$  punts per definir un polinomi de grau  $d$ . Es tracta, en definitiva, d'un problema d'interpolació polinomial amb una variable.

Per començar cal elegir un polinomi  $P(x)$  de grau  $(t-1)$  amb coeficients enters aleatoris excepte el terme independent, que serà  $S$ :

$$P(x) = S + a_1x + a_2x^2 + \dots + a_{t-1}x^{t-1}, \forall a_i \in \mathbb{Z}.$$

Aleshores calculem  $n$  punts  $(x, y)$  a partir d'ell, de tal forma que cadascun d'aquests punts serà una participació del secret  $S$ . A més, per tal de poder-lo recuperar faran falta  $t$  o més participacions, mentre que per un nombre de participacions inferior a  $t$  resultarà impossible recuperar el secret  $S$ .

Per fer-ho, només caldrà calcular els coeficients del polinomi partint dels punts donats i posteriorment recuperar el terme independent d'aquest, que és el secret  $S$ .

Vegem un exemple pràctic per tal de comprendre'n correctament el funcionament.

Suposem que volem distribuir el secret  $S = 65537$  en  $n = 5$  participacions, de tal forma que amb  $t = 3$  participacions es pugui recuperar  $S$ .

Així doncs, escollim un polinomi de grau 2 amb coeficients enters aleatoris i  $S$  com a terme independent:

$$P(x) = 65537 + 257x + 17x^2.$$

A continuació calculem  $n = 5$  punts qualsevol, que seran les participacions del secret  $S$ :

$$\begin{cases} P_1 = (1, 65811), \\ P_2 = (2, 66119), \\ P_3 = (3, 66461), \\ P_4 = (4, 66837), \\ P_5 = (5, 67247). \end{cases}$$

En cas de voler recuperar el secret  $S$ , farien falta com a mínim 3 participacions, ja que han estat calculades amb un polinomi de grau 2, la qual cosa implica que són necessaris 3 punts per poder calcular els coeficients del mateix.

Per exemple suposem que disposem de les participacions  $P_2$ ,  $P_3$  i  $P_5$ , i volem recuperar el secret  $S$ .

Així doncs, haurem de resoldre el següent sistema d'equacions:

$$\begin{cases} 2^2 a_2 + 2a_1 + S = 66119, \\ 3^2 a_2 + 3a_1 + S = 66461, \\ 5^2 a_2 + 5a_1 + S = 67247, \end{cases} \xrightarrow{\frac{f_2 - f_1}{f_3 - f_1}} \begin{cases} 4a_2 + 2a_1 + S = 66119, \\ 5a_2 + a_1 = 342, \\ 21a_2 + 3a_1 = 1128, \end{cases} \xrightarrow{f_3 - 3f_2} \begin{cases} 4a_2 + 2a_1 + S = 66119, \\ 5a_2 + a_1 = 342, \\ 6a_2 = 102, \end{cases}$$

$$\begin{cases} a_2 = \frac{102}{6} = 17, \\ a_1 = 342 - 5 \cdot 17 = 257, \\ S = 66119 - (4 \cdot 17 + 2 \cdot 257) = 65537. \end{cases}$$

Tot i que hem hagut de calcular els valors de  $a_2$  i  $a_1$  cal remarcar que es poden desestimar, ja que no guarden cap relació amb el secret  $S$  i només serveixen per poder obtenir el polinomi utilitzat.

Així doncs recuperem el secret  $S = 65537$  a partir de les tres participacions.

Per acabar cal remarcar que la combinació de tres participacions qualsevol del secret ens permetrien obtenir-lo de la mateixa manera que com s'ha fet a l'exemple anterior.

### 5.2.2. Modificació de l'esquema de Shamir: hiperplans i punts

Tal i com hem mostrat en l'apartat anterior, l'esquema de Shamir permet distribuir un secret  $S$  en  $n$  particions utilitzant un polinomi  $P(x)$ , el grau del qual depèn del nombre mínim de participacions  $t$  que són necessàries per recuperar el secret.

Aquí es proposa una possible modificació d'aquest mètode, en la qual no es treballa amb polinomis  $P(x)$  sinó amb equacions d'hiperplans, de tal forma que al augmentar el nombre mínim de participacions  $t$  que són necessàries per recuperar el secret no augmenta el grau sinó la dimensió de l'hiperplà afegint variables. Es tracta doncs, d'un problema d'interpolació lineal en varies variables.

**Definició 5.2.2.1.** Un *hiperplà* és un objecte geomètric de dimensió  $d - 1$  definit sobre un espai de dimensió  $d$ . L'equació general d'un hiperplà de dimensió 2 a coeficients enters és la següent:

$$\alpha x + \beta y + \gamma z + \delta = 0, \forall \alpha, \beta, \gamma, \delta \in \mathbb{Z}.$$

Així doncs, agafarem com a base del mètode l'equació anterior lleugerament modificada:

$$z = Ax + By + S, \forall A, B, S \in \mathbb{Z}.$$

Cal remarcar que  $S$  és el secret que es vol distribuir i que en el cas anterior, on l'equació representa un hiperplà de dimensió 2, podrem calcular-lo a partir de tres participacions, ja que per poder calcular l'equació d'un hiperplà de dimensió 2 necessitem 3 punts, i, en general, per poder calcular l'equació d'un hiperplà de dimensió  $d - 1$  necessitem  $d$  punts.

En cas de voler obtenir un sistema que requereixi  $t$  participacions per recuperar  $S$ , s'haurà de treballar amb un hiperplà de dimensió  $t - 1$ , amb  $t$  variables, l'equació del qual tindrà una estructura semblant a la de l'hiperplà de dimensió 2, però amb  $t$  variables.

Vegem un exemple pràctic per tal de comprendre'n correctament el funcionament. Suposem que volem distribuir el secret  $S = 65537$  en  $n = 5$  participacions, de tal forma que amb  $t = 4$  participacions es pugui recuperar  $S$ .

Així doncs, escollim un hiperplà de dimensió 3, l'equació del qual tingui coeficients enters aleatoris i  $S$  com a terme independent:

$$w = 5x - 17y + 257z + 65537.$$

A continuació calculem  $n = 5$  punts qualsevol, que seran les participacions del secret  $S$ :

$$\begin{cases} P_1 = (1, 1, 1, 65782), \\ P_2 = (1, 1, 2, 66039), \\ P_3 = (1, 2, 1, 65765), \\ P_4 = (1, 3, 1, 65748), \\ P_5 = (2, 1, 1, 65787). \end{cases}$$

En cas de voler recuperar el secret  $S$ , farien falta com a mínim 4 participacions, ja que han estat calculades amb l'equació d'un hiperplà de dimensió 3, la qual cosa implica que són necessaris 4 punts per poder calcular els coeficients d'aquesta.

Per exemple suposem que disposem de les participacions  $P_1, P_2, P_3$  i  $P_5$ , i volem recuperar el secret  $S$ .

Així doncs, haurem de resoldre el següent sistema d'equacions:

$$\begin{aligned} \begin{cases} A + B + C + S = 65782, \\ A + B + 2C + S = 66039, \\ A + 2B + C + S = 65765, \\ 2A + B + C + S = 65787, \end{cases} & \xrightarrow[\substack{f_3 - f_1}]{\substack{f_2 - f_1}} \begin{cases} A + B + C + S = 65782, \\ C = 257, \\ B = -17, \\ 2A + B + C + S = 65787, \end{cases} & \xrightarrow{f_4 - f_1} \begin{cases} A + B + C + S = 65782, \\ C = 257, \\ B = -17, \\ A = 5, \end{cases} \\ & & \begin{cases} S = 65537, \\ C = 257, \\ B = -17, \\ A = 5. \end{cases} \end{aligned}$$

Tot i que hem hagut de calcular els valors de  $A, B$  i  $C$ , cal remarcar que es poden desestimar, ja que no guarden cap relació amb el secret  $S$  i només serveixen per poder obtenir el polinomi utilitzat.

Així doncs recuperem el secret  $S = 65537$  a partir de les quatre participacions.

Per acabar cal remarcar que la combinació de quatre participacions qualsevol del secret ens permetrien obtenir-lo de la mateixa manera que com s'ha fet a l'exemple anterior.

### 5.2.3. Proposta: esquema basat en hiperplans i coeficients

En l'apartat anterior hem introduït el concepte d'hiperplà i hem vist com poden ser utilitzats per distribuir un secret  $S$  en  $n$  participacions.

En aquest apartat continuarem treballant amb hiperplans per distribuir secrets, però descriurem un altre mètode. Cal remarcar que en aquest cas no podrem recuperar el missatge amb un nombre de participacions  $t \leq n$ , la qual cosa vol dir que es necessitaran totes les participacions per poder recuperar  $S$ .

En l'apartat anterior calculàvem punts d'un hiperplà, que passaven a ser les participacions del secret  $S$ . En aquest cas les participacions són els coeficients de l'equació de l'hiperplà i els valors d'algunes de les variables.

De forma general podem dir que per generar  $n$  participacions d'un secret  $S$ , obtindríem un hiperplà de dimensió  $n-1$ , amb  $n$  variables i  $a$  coeficients  $a_i \in \mathbb{Z}^+$ . D'aquesta forma, la primera variable de l'equació la substituiríem per  $S$ , l'última ens generaria la primera participació, les altres variables les substituiríem per valors enters aleatoris que passarien a ser participacions i finalment l'última participació s'obtindria a partir de les expressions següents:

$$P_n = \sum_{i=0}^{i=n} a_i N^i, \text{ on } N = \sum_{i=0}^{i=n} a_i^2.$$

Vegem un exemple pràctic per tal de comprendre'n el funcionament.

Suposem que treballem amb un hiperplà de dimensió 2, l'equació general del qual seria la següent:

$$a_3x + a_2y + a_1z + a_0 = 0, \forall a_i \in \mathbb{Z}^+.$$

Aleshores podríem obtenir 3 participacions d'un secret  $S$ . Suposem que  $S = 257$ . Per obtenir les participacions substituiríem les  $x$  per  $S$ , triaríem  $(a_3, a_2, a_1, a_0) = (1, 3, 5, 8)$ , triaríem un valor enter aleatori  $b = 10$  i el substituiríem per les  $y$ , i calcularíem el valor de  $z$ . En aquestes condicions, l'equació de l'hiperplà i les participacions  $P_1, P_2, P_3$  del missatge serien les següents:

$$\begin{aligned} x + 3y + 5z + 8 &= 0, \\ P_1 = z &= \frac{257 + 3 \cdot 10 + 8}{-5} = -59, \\ P_2 = y &= 10, \\ N &= \sum_{i=0}^{i=3} a_i^2 = a_0^2 + a_1^2 + a_2^2 + a_3^2 = 64 + 25 + 9 + 1 = 99, \\ P_3 &= \sum_{i=0}^{i=3} a_i N^i = a_0 N^0 + a_1 N^1 + a_2 N^2 + a_3 N^3 = 8 + 5 \cdot 99 + 3 \cdot 99^2 + 1 \cdot 99^3 = 1000205. \end{aligned}$$

Per tal de recuperar el secret  $S$  a partir de la participacions  $P_1 = -59$ ,  $P_2 = 10$ ,  $P_3 = 1000205$  i  $N = 99$ , que és un valor públic, començaríem obtenint els coeficients de l'equació a partir de  $P_3$  i  $N$ , dividint  $P_3$  entre  $N$  obtenint el quocient  $q_1$  i el residu  $r_1$ . Posteriorment dividiríem  $q_1$  entre  $N$ , obtenint el quocient  $q_2$  i el residu  $r_2$ , i així successivament fins que ja no sigui possible continuar dividint. Aleshores recuperariem tots els residus obtinguts, que correspondrien als coeficients de l'equació.

$$\begin{cases} 1000205 = 10103 \cdot 99 + 8 \Rightarrow a_0 = 8, \\ 10103 = 102 \cdot 99 + 5 \Rightarrow a_1 = 5, \\ 102 = 1 \cdot 99 + 3 \Rightarrow a_2 = 3, \\ 1 = 0 \cdot 99 + 1 \Rightarrow a_3 = 1. \end{cases}$$

Partint dels coeficients reconstruïm l'equació de l'hiperplà utilitzat, que és la següent:

$$x + 3y + 5z + 8 = 0.$$

Substituint  $P_1 = z = -59$  i  $P_2 = y = 10$  podem recuperar el secret  $S = x$  de la següent forma:

$$x + 3 \cdot 10 + 5(-59) + 8 = 0 \Rightarrow x = 257.$$

D'aquesta forma recuperem el secret  $S = 257$  a partir de les tres participacions utilitzant aquest mètode propi basat en hiperplans, que s'ha dissenyat exclusivament per ser exposat en aquest treball.

## 6. VALORACIÓ PERSONAL

Totes les coses tenen un final, i aquest treball no és una excepció. Sembla ser que ja ha arribat l'hora d'acabar, i he de dir que no és fàcil. Quan es fa un treball dedicat a un tema del qual hi ha gran quantitat d'aspectes importants a tenir en compte, un sempre pensarà que per molt extens que sigui el document, sempre estarà incomplert.

Sembla mentida que fa només quatre mesos encara no sabia com tirar endavant aquest projecte, i ara que ha arribat l'hora de donar-lo per finalitzat, irònicament tampoc se com fer-ho.

He de dir que quan vaig començar a recopilar informació hi havia molts coneixements matemàtics que desconeixia per complet. Coneixements que actualment conformen els apartats principals d'aquest projecte. La primera vegada que hem vaig enfrontar a les corbes el·líptiques va ser en una videoconferència organitzada per *La Caixa*.

He de confessar que quan es va acabar em vaig adonar de que no havia entès res. I això va suposar una motivació per començar una investigació exhaustiva dedicada a les corbes el·líptiques. Investigació que no va finalitzar fins que no es va resoldre l'últim dubte, fins que no es va trobar la demostració de les equacions per sumar i multiplicar punts d'una corba el·líptica.

Aquest treball ha requerit hores i hores davant d'un paper en blanc, realitzant càlculs per intentar entendre el funcionament dels procediments descrits. En algunes situacions vaig pensar que no ho aconseguiria, però no vaig desistir i al final l'esforç es va veure recompensat amb la dissipació dels dubtes existents.

He de dir que aquest projecte ha suposat un esforç per part meua, tant a nivell físic com psicològic. Ha canviat la meua manera de pensar. Ha augmentat la meua passió per la Criptografia i m'ha obert les portes d'alguns coneixements que no hauria adquirit en les classes de Batxillerat.

Abans d'emprendre aquest projecte, jo no era res més que un observador extern del món de les Matemàtiques. Però això ha canviat completament. El fet d'haver de realitzar un treball de Matemàtiques m'ha suposat un repte, ja que havia de deixar de ser un observador extern per passar a pensar i actuar tal i com ho fan els Matemàtics de veritat. Em veig obligat a reconèixer que no ha estat gens fàcil. És més, m'he hagut d'enfrontar a problemes dels quals no tenia clar que pogués trobar una solució, però finalment sembla que s'ha aconseguit.

Estic satisfet perquè s'han assolit els objectius inicials d'aquest treball. S'han adquirit nous coneixements matemàtics que em seran útils en un futur proper, s'ha après a pensar d'una forma més rigorosa, s'ha aconseguit reconstruir tot un bloc temàtic a partir de petits fragments d'informació recopilats de diverses fonts, finalment, el més important de tots, s'ha gaudit realitzant aquesta investigació. És més, si s'hagués de tornar a fer, es tornaria a fer, i es tindrien les mateixes ganes d'aprendre i el mateix entusiasme que s'ha tingut durant la realització d'aquesta investigació.

Aquest projecte ha posat de manifest un fet que la gran majoria de la gent ignora i és que les Matemàtiques estan a tot arreu. La Criptografia només és un dels molts exemples pràctics d'aplicació de les Matemàtiques en el món real. És més, si no existissin les Matemàtiques el món seria molt diferent. Les Matemàtiques intervenen en els processos de fabricació de tots els elements que ens envolten, des dels electrodomèstics fins a les rajoles, les Matemàtiques hi són presents. Tenint en compte això, resulta evident que sense les Matemàtiques, el món estaria condemnat a la destrucció i al caos.

Però bé, el cert és que aquest projecte ha arribat al seu final, i ja és hora de tancar-lo definitivament, per tant ho deixarem aquí. No obstant això cal remarcar que es continuarà estudiant el món de la Criptografia i dels codis, ja que ens proporciona el que tota persona desitja més intensament: la capacitat de guardar els seus secrets més preuats en el lloc més segur de tots, el món dels nombres.

## 7. REFERÈNCIES

- [1] M. Alcubierre, *Introducción a FORTRAN*, Instituto de Ciencias Nucleares, UNAM. (2005).
- [2] P. Caballero, *Introducción a la Criptografía*, Ed. Ra-Ma. (2002).
- [3] A. Fúster, D. G. Martínez, L. Hernández, F. Montoya i J. Muñoz, *Técnicas Criptográficas de protección de datos*, Ed. Ra-Ma. (2004).
- [4] A. Lozano, *Buscando puntos racionales en curvas elípticas: Métodos explícitos*. (2006).
- [5] A. R. Mateos, *El reto de Fermat*, Ed. Ciencia abierta, 10. (2005).
- [6] P. Morillo, *Las Matemáticas en la Criptografía*, Matemática Aplicada IV. Universidad Politécnica de Catalunya.
- [7] J. Pastor, M. A. Sarasa i J. L. Salazar, *Criptografía Digital: Fundamentos y aplicaciones*, Ed. Prensas Universitarias de Zaragoza, 55. (2001).
- [8] O. Roig, *La Conspiración de los Números*, Ed. Libros Cúpula. (2009).
- [9] E. Ruiz, *Criptografía asimétrica con curvas elípticas*, Universidad Nacional Autónoma de México – Facultad de Ciencias.
- [10] D. Zurdo i A. Gutiérrez, *La Guerra de los Códigos Secretos*, Ed. Libros Cúpula. (2009).
- [11] *Programing Praxis*, <http://programmingpraxis.com/2009/07/28/elliptic-curves/>.
- [12] *Wikipedia*:
  - [12.1] [http://es.wikipedia.org/wiki/Infinitud\\_de\\_los\\_n%C3%BAmeros\\_primos](http://es.wikipedia.org/wiki/Infinitud_de_los_n%C3%BAmeros_primos).
  - [12.2] <http://es.wikipedia.org/wiki/Jerogl%C3%ADficos>.
  - [12.3] [http://es.wikipedia.org/wiki/Maquina\\_enigma](http://es.wikipedia.org/wiki/Maquina_enigma).
  - [12.4] [http://es.wikipedia.org/wiki/C%C3%B3digo\\_Lorenz](http://es.wikipedia.org/wiki/C%C3%B3digo_Lorenz).
- [13] *Sttmedia*, <http://www.sttmedia.com/wordcreator>.