



Premi Poincaré 2005



Facultat de Matemàtiques
i Estadística

UNIVERSITAT POLITÈCNICA DE CATALUNYA

Títol: *Criptografia: garantia de privacitat?*

Autora: Berta Velasco Casals **Tutora:** Pilar Alcon Baiges

Centre: IES Montserrat

Accèssit a l'esforç realitzat per parlar de manera clara i entenedora sobre la criptografia amb tota la seva complexitat. L'exposició sistemàtica del contingut matemàtic necessari per abordar els problemes que es planteja i pels exemples pràctics proposats, tant els d'aplicació de la teoria com els d'investigació pròpia.

TREBALL DE RECERCA

CRIPTOGRAFIA. GARANTIA DE PRIVACITAT?



2n de Batxillerat

Barcelona, 26 d'abril de 2005

AGRAÏMENTS

A la meva tutora, perquè sempre he tingut la seva ajuda, col·laboració i les orientacions adients per a realitzar aquest treball.

També vull agrair a la Facultat de Matemàtiques de la Universitat Politècnica de Catalunya i en especial al Dr. Josep Grané, l'esforç que fan per fer arribar les matemàtiques a tots els alumnes de secundària. Per fer aquest treball, tota la part d'Aritmètica Entera i Aritmètica Modular, he pogut desenvolupar-la amb l'ajuda que he rebut a les classes de preparació de les Proves Cangur i les Olimpíades Matemàtiques. Aquests temes no formen part dels programes establerts pel departament d'Educació en l'Ensenyament Secundari.

ÍNDIX:

Treball de Recerca	1
Agraïments.....	2
Índex:.....	3
Introducció.....	6
Objectius	7
Metodologia	8
1 UN PASSEIG PER A LA HISTÒRIA DE LA CRIPTOGRAFIA I DE LA ESTEGANOGRAFIA.....	10
1.1 Conceptes bàsics i nomenclatura	10
1.2 Història Breu De La Criptografia.....	12
1.3 Història De L'Esteganografia	20
2 MÈTODES CRIPTOGRÀFICS CLÀSSICS.....	22
2.1 Xifres de Transposició	22
2.1.1 Mètode de riel	22
2.1.2 Mètode de transposició amb període fix (mètode dels blocs).....	23
2.1.3 Mètode de les Caixes	23
2.2 Xifres De Substitució	24
2.2.1 Substitució simple	24
2.2.2 Substitució Homofònica.....	25
2.2.3 Substitució Polialfabètica.....	26
2.2.4 Substitució Poligràfica:	27
3 MÈTODES CRIPTOGRÀFICS MODERNS.....	28
3.1 Sistema De Clau Privada.....	29
3.1.1 El criptosistema DES	29
3.1.2 El criptosistema IDEA	30
3.1.3 El criptosistema AES	30
3.2 Sistemes de clau Pública	32
3.2.1 RSA.....	34
3.2.2 Altres sistemes de clau pública	37
4 SEGURETAT CRIPTOGRÀFICA.....	39

4.1	Seguretat Criptogràfica	39
4.2	Atacs a la seguretat criptogràfica	41
4.3	Aplicacions Criptogràfiques.....	41
4.3.1	Correu electrònic segur	42
4.3.2	Comerç electrònic	44
4.3.3	Situació actual del comerç electrònic.....	47
4.4	Perspectives de futur	49
5	CONCEPTES MATEMÀTICS UTILITZATS AL LLARG DEL TREBALL.....	51
5.1	Tècniques de Comptar.....	51
5.1.1	Permutacions de n elements: P_n	51
5.1.2	Permutacions amb repetició de n objectes. $PR_n^{p_1, \dots, p_r}$	52
5.1.3	Variacions de n elements agafats de p en p: $V_{n,p}$	53
5.1.4	Variacions amb repeticions de n elements agafats de p en p: $VR_{n,p}$...	54
5.1.5	Combinacions de n elements agafats de p en p: $C_{n,p}$	55
5.2	Aplicació	56
5.2.1	Concepte d'aplicació	56
5.3	Funció.....	58
5.3.1	Funció polinòmica.....	58
	Una funció és polinòmica si està definida de la forma:	58
5.3.2	Funció exponencial	58
	Una funció és exponencial si està definida de la següent forma:	58
5.3.3	Funció logarítmica	59
5.4	Àlgebra lineal	60
5.4.1	Concepte de matriu	60
5.4.2	Tipus de matrius.....	60
5.4.3	Operacions amb matrius.....	61
5.4.4	Determinants	62
5.4.5	Matriu inversa	64
5.5	Teoria de nombres.....	65
5.5.1	Sistema de numeració binari	65
5.5.2	Nombres Primers.....	66
5.5.3	Màxim comú divisor de nombres naturals. Algoritme d'Euclides	68
5.5.4	Nombres Congruents.....	69

5.5.5	Funció ϕ d'Euler	71
6	PRÀCTIQUES DE XIFRAR I DESXIFRAR MISSATGES	72
6.1	Xifrat Amb Mètodes Clàssics.	72
6.1.1	Pràctica 1	72
6.2	Xifrat Amb Mètodes Moderns	78
6.2.1	Pràctica 2	78
6.2.2	Pràctica 3	82
6.2.3	Pràctica 4	83
6.2.4	Pràctica 5	86
6.2.5	Pràctica 6	89
6.2.6	Pràctica 7	92
6.2.7	Pràctica 8	96
Conclusions:.....		105
Bibliografia		107
Índex d'Annexos.....		108

INTRODUCCIÓ

La elecció del tema d'aquest treball "Criptografia. Garantia de privacitat?" va venir determinat per la curiositat que em va despertar la lectura del llibre *Lee a Julio Verne* de Susana Mataix. Aquest treball preten introduir de forma molt senzilla els temes bàsics de criptografia clàssica i moderna.



Partint de la *hipòtesi que hi ha relació entre criptografia i matemàtiques*, he volgut comprovar fins a quin punt la criptografia ha necessitat i necessita les matemàtiques per poder continuar evolucionant i així, seguir garantint la privacitat, la integritat, i l'autenticitat en el tractament de la informació en format electrònic a començament d'aquest segle XXI i en un futur.

A grans trets els dos objectius fonamentals del treball són:

Ser entès i assimilat per a qualsevol persona amb una mínima formació científica.

Tenint en compte la hipòtesis del treball (que la criptografia es fonamenta en la matemàtica) contribuir a que el pànic que provoca la paraula *matemàtica* en moltes persones disminueixi, i així, es puguin reconciliar (encara que només sigui una mica) amb el món de les matemàtiques, després de llegir-lo.

Els continguts d'aquest treball són:

Objectius i metodologia emprada:

Capítol 1 i 2: Evolució històrica de la criptografia i les tècniques de xifrar clàssiques.

Capítol 3 i 4: Mètodes de xifrat moderns, remarcant el sistema de clau pública (en particular el criptosistema RSA) i una petita introducció a la seguretat criptogràfica actual i unes reflexions sobre les perspectives de futur de la criptografia.

Capítol 5: Bases matemàtiques per entendre els fonaments bàsics de la criptografia.

Capítol 6: Pràctiques de xifrat i desxifrat de missatges.

Conclusions.

OBJECTIUS

Els dos objectius fonamentals del treball els he exposat en la introducció, en aquest apartat, vull desenvolupar-los de forma més detallada.

Els objectius que m'han pautat el treball són els següents:

- Conèixer a què ens referim quan parlem de criptografia.
- Conèixer la terminologia bàsica emprada en criptografia.
- Tenir una visió de la evolució històrica de la criptografia.
- Conèixer les tècniques clàssiques de xifrat.
- Adonar-se de la feblesa dels criptosistemes clàssics.
- Compendre la diferència entre criptosistemes clàssics i moderns.
- Conèixer l'esquema general dels xifrats moderns de clau privada.
- Entendre el concepte de clau pública.
- Entendre l'algoritme de generació de claus del criptosistema més utilitzat de clau pública: RSA (Rivest, Shamir i Adleman).
- Saber quines són els avantatges i els inconvenients d'utilitzar el sistema RSA.
- Adonar-se de la lluita entre criptògrafs i criptoanalistes.
- Veure que la criptografia s'ha revelat com la eina més poderosa per proporcionar seguretat en els sistemes informàtics.
- Conèixer algun producte criptogràfic per gestionar de manera segura el correu electrònic: PGP (Pretty Good Privacy)
- Ser conscients del problema que hi ha amb el rastre en els pagaments electrònics i adonar-se que això té solució criptogràfica.
- Saber quins són els sistemes de comerç electrònic que hi ha.
- Prendre consciència de la omnipresència de la criptografia en el món actual i reflexionar sobre les perspectives de futur de la criptografia.
- Adquirir o recuperar els coneixements matemàtics per a entendre els fonaments bàsics de la criptografia.
- Saber xifrar i desxifrar missatges utilitzant diferents mètodes de xifrat i diferents procediments de resolució.

METODOLOGIA

La metodologia que he emprat per a realitzar aquest treball ha estat:

Documentar-me amb llibres específics de criptografia, uns més divulgatius i, altres més acadèmics.

Tot aquest procés ha anat acompanyat d'un gran esforç i moltes hores de dedicació per a comprendre i saber utilitzar conceptes matemàtics que anaven sorgint des de les primeres pàgines de qualsevol text dedicat a la criptografia.

He cregut que per donar més coherència al treball seria més entenedor agrupar els conceptes matemàtics que apareixen, en un únic capítol (capítol 5). A més a més, aquest treball va complementat d'un CD ROOM, que conté tot el treball informatitzat i en el qual s'han creat uns hipervincles que cada vegada que apareix un concepte matemàtic et porta al capítol 5, també en aquest CD ROOM hi ha incorporat tota la part pràctica del capítol 6 i una presentació del treball per fer una exposició oral feta amb Power Point.

He de dir que dels conceptes matemàtics a què faig referència només he treballat una petita part (capítol 5), ja que he hagut de deixar moltes coses interessants i necessàries però que, pel seu grau de complexitat superava amb escreix les meves bases matemàtiques per poder-los comprendre (per exemple, poder entendre i fer un exemple pràctic d'algun test de primalitat).

Per facilitar la comprensió de la part teòrica, he desenvolupat una part pràctica (capítol 6). Els passos que he seguit per dur a terme aquest apartat de pràctiques són:

Xifrar una única lletra amb el sistema de clau pública RSA a mà, que tot i ser el procés més senzill de xifrat amb aquest sistema, em va dur una gran quantitat de temps degut a la complexitat matemàtica que aquest procés requereix.

Programar un full de càlcul amb Excel, perquè em calculés l'invers modular de nombres grans molt més ràpidament que fent-ho manualment.

Xifrar una sola lletra amb l'ordinador utilitzant el programa "Derive para Windows". El procés em va resultar una mica difícil al començament perquè no havia utilitzat mai aquest programa, però gràcies al manual d'ajuda del propi programa de seguida m'hi vaig familiaritzar., i vaig aconseguir xifrar una lletra fàcilment, ja que

l'algorisme de xifrat del sistema RSA ja l'havia entès quan havia hagut de xifrar una lletra a mà.

Xifrar un missatge sencer amb el sistema RSA a mà, per així entendre bé tots els passos a seguir. Aquest procés inclou alguns passos no utilitzats en el xifrat d'una única lletra.

Programar un full de càlcul amb Excel per calcular les potències de grans nombres utilitzant el mètode dels quadrats.

Xifrar un missatge amb el programa Derive. El procés per fer-ho em va resultar molt fàcil tenint en compte que ja havia xifrat una lletra utilitzant aquest programa, però em va sorgir un contratemps, doncs hi havia un pas en el procés de xifrat que creava un bucle que s'havia d'anar repetint moltes vegades. Probablement aquest fet va ser degut a que, per la meua poca experiència amb aquest programa, en desconeixia alguna funció que feia aquests passos de manera automàtica.

Per acabar la part pràctica d'utilització del criptosistema RSA, volia utilitzar el programa *Mathemática* per xifrar un missatge. Per la manca de disponibilitat d'aquest programa no he pogut realitzar aquesta pràctica, tot i així, en el treball, hi ha un exemple de xifrat d'un missatge utilitzant l'algoritme de l'RSA amb el programa *Mathemática*.

Xifrats de missatges utilitzant mètodes clàssics (transposició i substitució) programant amb Visual Basic.

Finalment, hi ha el guió d'una pràctica per utilitzar el programa PGP.

Crec que al anar pautant de forma molt detallada tots els passos a seguir a estat una ajuda per dur a bon terme aquest treball, perquè hi ha conceptes prou difícils que no et permeten saltar-te passos per poder seguir avançant.

1 UN PASSEIG PER A LA HISTÒRIA DE LA CRIPTOGRAFIA I DE LA ESTEGANOGRAFIA

1.1 CONCEPTES BÀSICS I NOMENCLATURA

La *criptografia* és l'estudi dels mètodes usats per enviar missatges de manera encoberta per tal que només el receptor (autoritzat per l'emissor) sigui capaç, de llegir-los i entendre'ls. La paraula criptografia prové del grec: κρυπτός (kriptos) “ocult” γραφή (graptos) “escrit”. Parlarem de *text inicial* o *text en clar* quan es refereixi al missatge que es desitja transmetre i de *text xifrat* o *criptograma* quan es faci referència al missatge transformat que finalment es transmet. *Xifrar* és el procés de convertir el text inicial en un text xifrat. El procés invers s'anomena *desxifrar*¹.

En qualsevol procés criptogràfic per transformar el text inicial s'ha de seguir estrictament un procediment sobre el qual s'hauran posat d'acord prèviament l'emissor i el receptor. Aquest protocol dependrà del que s'anomena una *clau*. Aquesta clau pot ser un nombre, una paraula, una taula d'equivalències de dos alfabetes, o qualsevol cosa que calgui fer servir durant els processos de xifrar i desxifrar. El coneixement del protocol i la clau permeten a l'emissor xifrar el text i al receptor desxifrar-lo invertint el procediment.

El conjunt de caràcters amb els quals s'escriu el text s'anomena *alfabet*. Usualment l'alfabet del text inicial coincideix amb el del text xifrat. Una *unitat de missatge* és la mínima part constitutiva d'un text; pot ser una lletra, dues (dígraf), tres (trígraf) o un bloc de n lletres en general. Podem considerar una *transformació xifradora* com una **aplicació bijectiva**: f del conjunt de totes les possibles unitats de missatge del text inicial U_i en el conjunt U_x de totes les possibles unitats de missatge del text xifrat. Com que aquesta aplicació es bijectiva, podem definir la seva **aplicació inversa** f^{-1} que l'anomenarem *transformació desxifradora*.

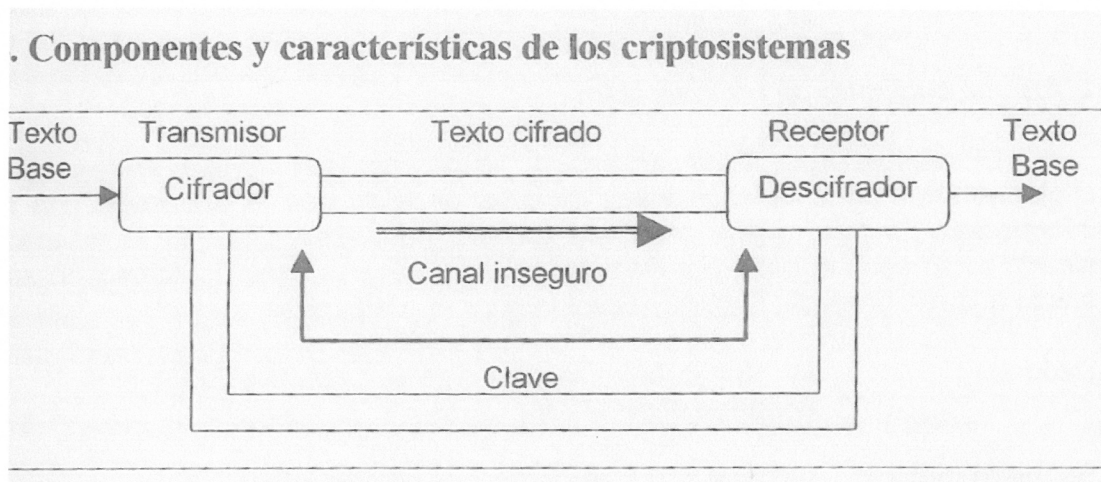
S'anomena *criptosistema* (o bé *xifra* o *xifratge*) la parella f, f^{-1} juntament amb les conjunts U_i i U_x :

¹ En aquest treball s'evitarà les paraules d'ús comú *encriptar*, *text encriptat* i *desencriptar* perquè són anglicismes que encara no han estat acceptats en el nostre idioma, tampoc en castellà.

$$U_i \xrightarrow{f} U_x \xrightarrow{f^{-1}} U_i$$

S'anomena *criptoanàlisi* l'art de vulnerar la seguretat d'un criptosistema. Un atac al sistema pot ser de diferents tipus segons el nivell d'informació del que disposi l'atacant. Criptoanalitzar un sistema vol dir examinar-lo exhaustivament per descobrir-ne les seves possibles febleses i proposar mètodes per endevinar la clau sense tenir-ne permís. Pot semblar que la criptoanàlisi i la criptografia són disciplines oposades, però, això no és cert, ja que per l'avenç de la criptografia és necessari el diàleg crític entre criptògrafs i criptoanalistes.

La criptografia i la disciplina complementària la criptoanàlisi es coneixen conjuntament amb el nom de *criptologia*.



S'anomena *Esteganografia* a l'art i la ciència d'ocultar (del grec **steganoz** (steganos), "cobert" en el sentit d'ocult i **graptoz** (graptos), "escrit") físicament el missatge tapant-lo o fent-lo invisible, tot i que el missatge està en algun lloc. L'esteganografia no ha de ser confosa amb la criptografia, ja que aquesta última tracta de manipular un missatge per tal que tingui una aparença irreconeixible. En canvi, l'esteganografia tracta d'ocultar un missatge secret en un altre públic que sembla inofensiu, que no té cap rellevància.

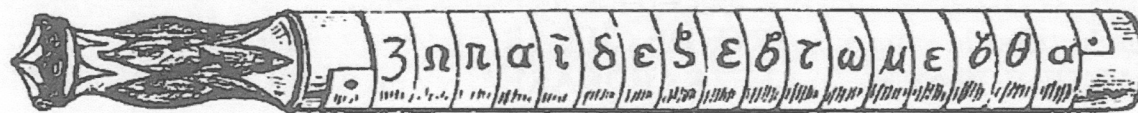
1.2 HISTÒRIA BREU DE LA CRIPTOGRAFIA

L'art de la criptografia és gairebé tan antic com l'escriptura. La comunicació secreta ha estat el protagonista més o menys directe de molts esdeveniments històrics relacionats amb la guerra, la diplomàcia, l'espionatge...

És molt difícil situar els inicis de la criptografia i els primers mètodes utilitzats. No obstant, ja a l'antic Egipte es van emprar sistemes criptogràfics, i prova d'això són els jeroglífics escrits en les parets de les piràmides i algunes tombes. La clau d'aquest llenguatge egipci estava en la pedra *Rosseta* descoberta l'any 1799 i que va ser desxifrada per Champollion l'any 1822.

En el segle V a.C en la guerra del Peloponès els Espartans, van utilitzar la escitala que es considera el primer sistema de criptografia per transposició. És a dir, consisteix en amagar el significat real d'un text, alterant l'ordre lògic dels signes. Per entendre com funcionava Plutarco ho va descriure en la seva obra "*Vida de Lisandro*" de la següent manera:

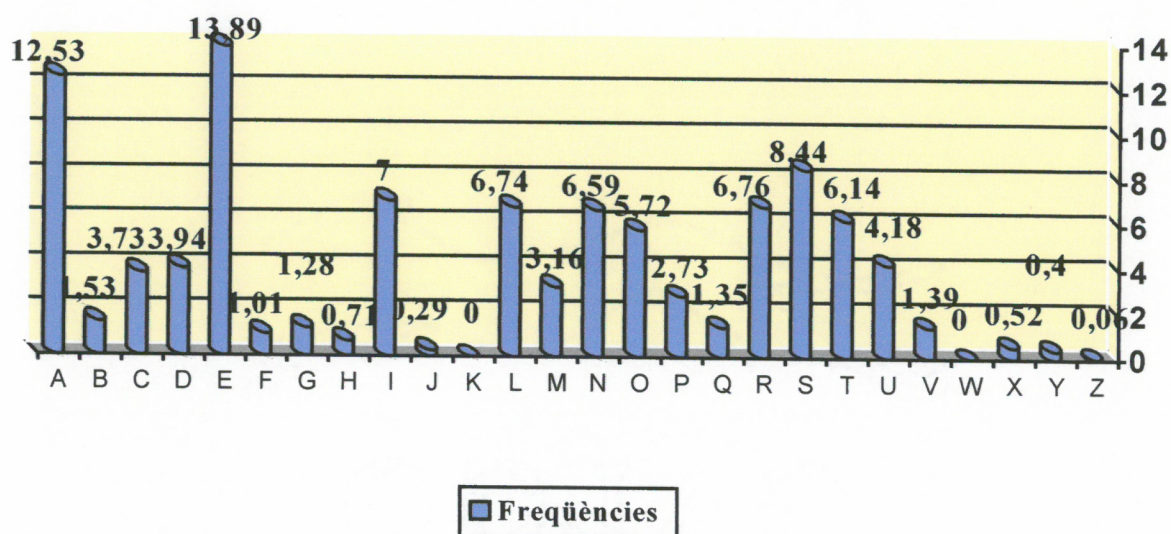
"Cuando un general parte para una expedición de tierra o mar, los ministros toman dos bastones redondos, perfectamente iguales en longitud y grosor, de manera que se correspondan exactamente uno con otro en todas sus dimensiones. Ellos guardan uno de estos bastones, dando el otro al general, y llaman a estos bastones escítalos (ver figura). Cuando quieren enviar al general un secreto de importancia, cortan una tira de pergamino, larga y estrecha como una correa, arrollándola alrededor del escítalo que guardaron, sin dejar el menor intervalo entre los bordes de la banda, de tal suerte que el pergamino cubra enteramente la superficie del bastón. Sobre este pergamino así arrollado alrededor del escítalo, escriben lo que desean y después quitan la cinta y la envían al general sin el bastón. El general que la recibe no sabría leerla, porque las letras, perdida la alineación y dispersas, no tendrían continuidad; pero él toma el escítalo que llevó consigo, y arrollando alrededor la banda del pergamino, se reunirán las vueltas, volviendo las letras a tomar el primitivo orden en que fueron escritas. Esta misiva se llama escítalo, del nombre mismo del bastón, como aquello que se mide toma el nombre de aquello que le sirve de medida."



Escitalo

Un altre mètode del que se'n té coneixement el va utilitzar l'emperador Romà Juli Cèsar (100a.C.- 44a.C.). Aquest mètode consistia en substituir cada lletra del missatge per una altra lletra que ocupava tres llocs endavant a l'alfabet. Tot i semblar un mètode molt segur i molt pràctic, va poder ser desxifrat pels criptoanalistes àrabs. Desxifrar la xifra de substitució monoalfabètica, va ser possible gràcies a la combinació de l'estadística i la lingüística, ja que el mètode per identificar quina lletra o quin símbol del missatge xifrat representava a cada lletra del alfabet, es basava en l'anàlisi de freqüències de cada símbol o lletra del missatge xifrat. Per fer l'anàlisi de freqüència, s'havia de saber en quin idioma estava escrit el text, perquè en cada idioma, les freqüències de les lletres varien. Per exemple, en català la lletra més utilitzada és la E amb un 13'89%, seguida de la A amb un 12'55%, després va la S....,

Freqüències en català



La freqüència de cada lletra en cada idioma, es pot saber analitzant bastants textos i comptant quantes vegades apareix la lletra en el text. Si tenim un text o un missatge una mica llarg, analitzant la freqüència dels símbols o de les lletres, es pot arribar a identificar les lletres. Per exemple, segurament el símbol que representi la lletra E en un text xifrat en català sigui el més utilitzat, a més a més, també s'ha de tenir en compte on està situat cada símbol, ja que hi ha lletres que només apareixen seguides d'altres lletres (com en el cas del català en el qual la lletra q apareix sempre abans de la lletra u, i seguit de que sempre

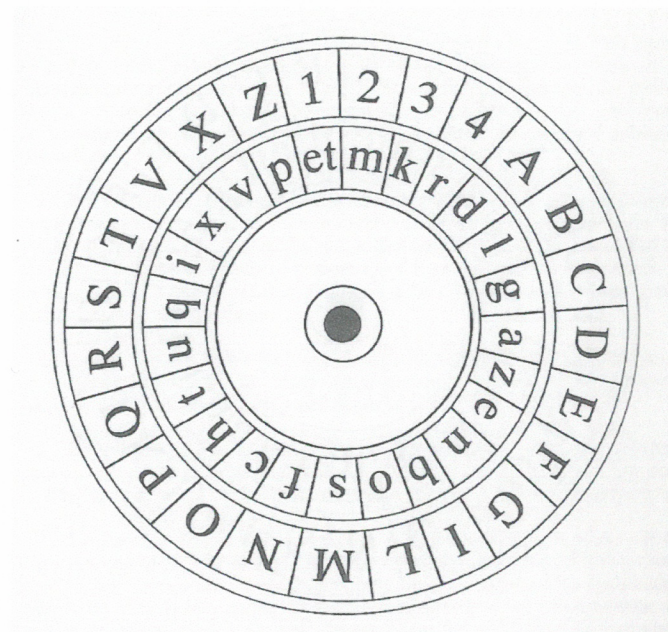
apareix una vocal. Aquesta explicació la va fer Al-Kindi al segle IX en el seu llibre titulat: “*Sobre el desxiframent de missatges criptoràfics*”² on s’explicava detalladament la manera de descodificar missatges de substitució monoalfabètica.

També en alguns textos medievals s’utilitzava l’alfabet del zodíac per amagar noms, també es canviava l’ordre de les lletres o es substituïen les vocals per punts o per consonants aleatòries.

El descobriment de la tècnica de l’anàlisi de freqüències va convertir en insegurs tots els mètodes clàssics de xifratge per substitució monoalfabètica. Però, de tota manera, aquesta troballa no es va difondre uniformement a tot arreu, ni va passar a formar part del corpus teòric de la tradició escrita de la criptografia. De manera que, al llarg de tota l’Edat Mitjana, el Renaixement i el Barroc, no es van deixar d’utilitzar sistemes alternatius. Qui ignorava la potència de l’atac estadístic (com els militars espanyols del regnat de Felip II), tenia unes comunicacions transparents als ulls de les principals potències europees.

En el segle XV, Lleó Battista Alberti (1404-1072) nascut a Gènova i educat a Bologne, que pot ser considerat com un dels pares de la xifra polialfabètica, va idear un aparell que estava format per dos cercles concèntrics de diferent radi, amb un eix comú. Els dos anells, es dividien en 24 caselles i a l’anell exterior hi havia 20 lletres de l’alfabet (es prescindia de les lletres H, J, K, Ñ, U, W, Y) i els 4 primers dígit, i en l’anell interior hi havia 23 lletres posades en qualsevol ordre (hi faltaven les lletres J, Ñ, U, W) i la conjunció *et*. Per xifrar s’escull una clau de correspondència i es substitueix les lletres del text normal localitzades en el cercle interior per les del cercle exterior. Per exemple: Per codificar BERTA amb la clau E-Z s’obté: E-Z.IF4QD.

² Aquesta obra es va trobar l’any 1987 a l’Arxiu Sulaimaniyyah Ottoman de Istanbul.



Disc d'Alberti

Al segle XVI Blaise de Vigenère (1523-1596) va fer una contribució molt important en el desenvolupament de la criptografia. L'any 1586 Vigenère va publicar el *Traicté des chiffres* en el que s'explicava el seu mètode de substitució polialfabètica. Aquest mètode pot ser considerat com una generalització del mètode César, només que, en comptes de desplaçar un nombre fix de posicions per obtenir una lletra xifrada, el desplaçament és variable i ve determinat per una frase o paraula. El xifrat de Vigenère que no es va difondre extensament fins al segle XVIII, és probablement la tècnica criptogràfica més equilibrada que hi ha, en el sentit que aconsegueix ser d'ús fàcil i força segura.

Utilitzant la taula de Vigenère que apareix a la pàgina següent, podríem codificar el missatge "Reunió" tal com segueix a continuació:

Missatge: REUNIÓ

Clau: KRYPTO

Text xifrat: BVSCBC

Aquest mètode per xifrar el missatge relaciona cada lletra del missatge en clar amb el seu corresponent de la clau, en el cas anterior la R es relaciona amb la K, la E amb la R, i així successivament. Tenint en compte aquestes correspondències, cerquem la lletra del missatge a la fila de color verd i la lletra de la clau a la columna blava. La intersecció entre la columna groga delimitada per la lletra del missatge i la fila groga determinada per la lletra de la clau ens dona la lletra xifrada, que s'ha marcat d'un color

BVSCBC.

blau clar. Si fem aquest procés amb REUNIÓ i utilitzem com a clau KRYPTO, el text xifrat serà:

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

Taula de Vigenère utilitzant la clau KRYPTO.

El mètode proposat per Vigenère va resultar indestructible durant 400 anys. Al segle XIX, encara s'utilitzava per protegir transmissions telegràfiques de caràcter comercial; però l'any 1864, un oficial Prussià, retirat: Kasiski (1805-1881) publicà *L'escriptura secreta i l'art del desxiframent* on es descriu per primera vegada una criptoanàlisi de la xifra Vigenère. Aquesta criptoanàlisi està basada en la importància de que el criptoanalista conegui la longitud de la clau i, Kasiski va entendre que l'estructura repetitiva del llenguatge pot ajudar a descobrir aquesta longitud.

Encara que la Xifra Vigenère ja no era segura, durant la segona meitat del segle XIX els criptògrafs no van dissenyar noves xifres, però durant aquesta època va sorgir un gran interès de la societat envers la criptografia. Aquest fet és palpable en la literatura de l'època. Per exemple: *Viatge al centre de la terra* de Julio Verne, *L'aventura dels homes ballarins* de sir Arthur Conan Doyle, *L'escarabat d'or* d'Edgar Allan Poe...

El segle XX va suposar un avenç revolucionari en el món de la criptografia, basant-se en el disc d'Alberti, es van dissenyar teletips que estaven formats per una seqüència de rotors mòbils que giraven amb cada tecla que es premia. Així, en lloc d'escriure la lletra escollida, apareixia un signe escollit per la màquina que es basava amb un codi polialfabètic complex. Aquests aparells es van anomenar *traductors mecànics*. Però, el que marca el punt d'inflexió entre la criptografia clàssica i la moderna és el desenvolupament de la *màquina Enigma*. La màquina Enigma utilitzava el corrent elèctric, però fent servir principis de funcionament mecànic. La màquina enigma va ser patentada per Arthur Scherbius l'any 1918, amb la finalitat de facilitar la comunicació per documents entre comerciants i homes de negocis de forma secreta. El mecanisme estava constituït fonamentalment per un teclat, similar al de les màquines d'escriure, que controlava una sèries d'interruptors elèctrics i un engranatge mecànic.



Vista general de la màquina Enigma oberta a punt per xifrar i desxifrar missatges.

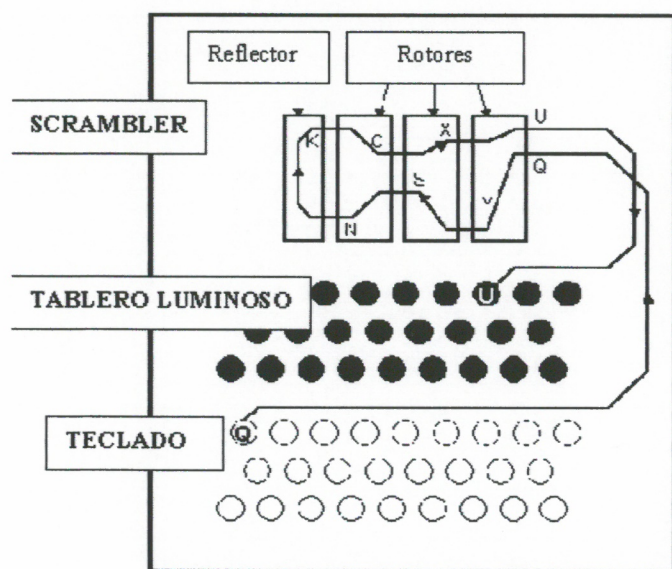


Diagrama d'una Enigma militar de tres rotors.

Aquesta màquina oferia gran possibilitat de combinacions. Com que cada rotor tenia 26 posicions i en la màquina original hi havia 3 rotors, les combinacions inicials possibles eren:

$$VR_{6,3} = 26^3 = 17.576$$

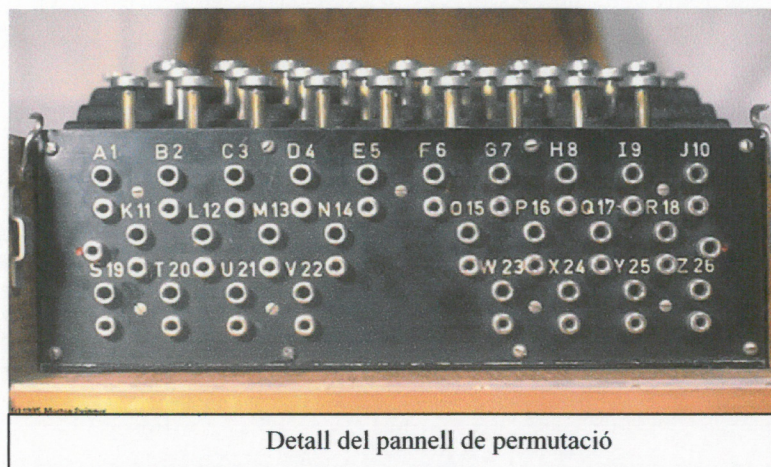
Després es va fer que els rotors poguessin intercanviar-se de posició i, per tant, les posicions inicials ascendien fins a:

$$26^3 \times P_3 = 105.456$$

Més endavant, l'any 1938, durant la segona guerra mundial, els alemanys hi van

afegir 2 rotors més encara que només es podien utilitzar 3 a la vegada. Això feia que el número de posicions inicials possibles en aquell moment fos:

$$26^3 \times C_{5,3} \times P_3 = 1.540.560$$



Detall del pannell de permutació



Detall on es veu la disposició dels tres rotors a la màquina

Aquesta gran quantitat de combinacions possibles va fer que els nazis pensessin que els missatges que transmetien a través de l'Enigma eren completament segurs. Però no van saber que des de 1942, un grup de matemàtics i criptografs britànics, entre altres Alan Turing³ (1912-1954) van aconseguir desxifrar els missatges. Aquest fet, poc conegut, va ser un factor decisiu en el desenllaç de la segona guerra mundial.

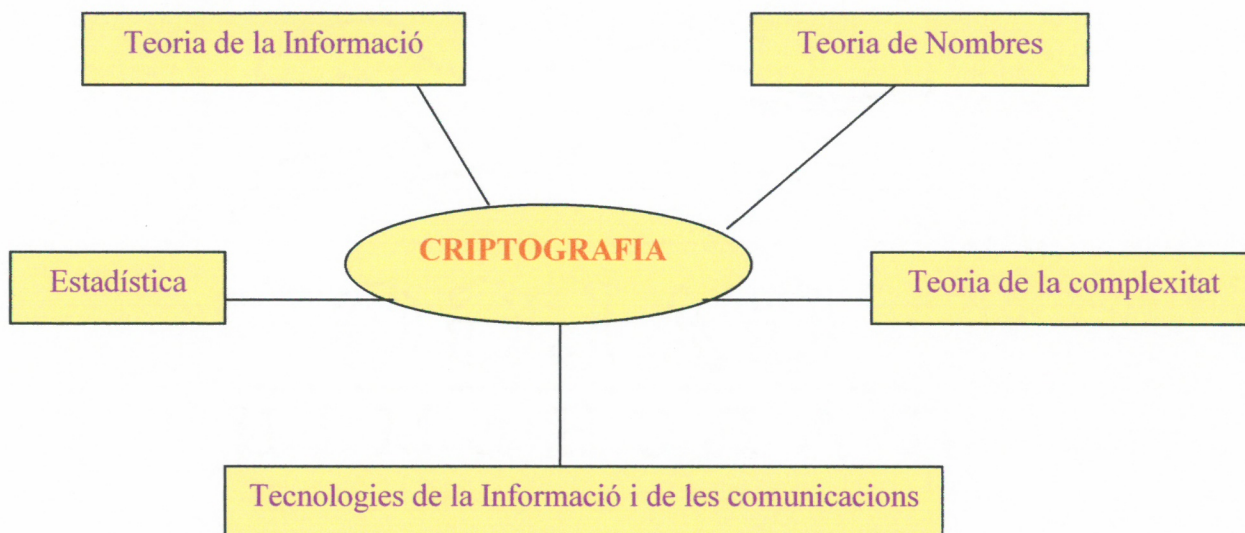
Tot i així, el període que va des de l'antiguitat fins a l'any 1949, es pot considerar com l'era de la criptografia pre-científica. La publicació l'any 1949 per part de C.E. Shannon⁴ de l'article "Communication Theory of

Secrecy Systems" va inaugurar l'era de la criptologia científica ja que va proporcionar un fonament teòric de la criptografia, basat en la teoria de la informació que ell mateix havia

³ Matemàtic anglès. Ideà el concepte teòric d'una màquina calculadora universal, que és anomenada *màquina de Turing*. Treballà especialment en el camp de la lògica matemàtica i s'interessà per la intel·ligència artificial

⁴ Enginyer i matemàtic. Va fundar una nova branca de les matemàtiques: La teoria de la informació i de la codificació.

elaborat l'any anterior. Des d'aleshores, la criptologia va ser considerada com una ciència perquè estava relacionada amb altres ciències com l'estadística, la teoria de nombres, la teoria de la informació i la teoria de la complexitat computacional.



Però aquest article de Shannon no va suposar un gran impuls per a la recerca criptogràfica.

L'eclosió real de la criptografia s'esdevingué amb la publicació l'any 1976 per part de W.Diffie i M.E. Hellman de l'article "*New Directions in Cryptography*". Diffie i Hellman van mostrar per primer cop que era possible la comunicació secreta sense cap transferència de clau secreta entre l'emissor i el receptor, i van encetar així l'època de la criptografia de clau pública en la qual ens trobem actualment.

1.3 HISTÒRIA DE L'ESTEGANOGRAFIA

Al llarg de la història s'han utilitzat multitud de mètodes i variacions per ocultar informació.

Les Històries d'Heròdot: Un dels primers documents en què es descriu l'estenografia és les *Històries* d'Heròdot. A l'antiga Grècia, els textos eren escrits en taules cobertes amb cera. En una història, Demeratus volia comunicar a Esparta que Xerxes tenia pensat envair Grècia. Per evitar la captura ell va treure la cera de les taules i va escriure un missatge a la fusta de sota. Llavors va tornar a cobrir les taules amb cera. Les taules semblaven que no tenien cap missatge i que no havien estat utilitzades, per la qual cosa passaren la inspecció dels sentinelles sense cap pregunta. El mateix Heròdot descriu un truc per puntejar lletres en un text d'encobriment amb una tinta secreta, inventat per Aeneas.

Mètode del missatger: Un altre mètode enginyós va ser afaitar el cap d'un missatger i tatuar un missatge o una imatge al cap del missatger. Després de deixar créixer el seu cabell, el missatge seria indetectable fins que el cap tornés a ser afaitat.

Utilització de tintes invisibles: Un altre mètode conegut per tothom d'esteganografia és la utilització de tintes invisibles. Aquestes tintes van ser utilitzades amb èxit durant la Segona Guerra Mundial i per la resistència als camps nazis. Així, una carta que semblava inofensiva, sense cap missatge important, podia contenir un missatge escrit entre les línies d'aquesta. Entre les tintes més utilitzades hi havia llet, vinagre, suc de fruita i orina, perquè quan s'escalfaven s'enfosquien. Es pot provar d'escriure amb suc de llimona en un full de paper, i després una vegada ja s'ha assecat transmetre calor al full, amb compte i sobretot amb l'ajut d'un adult, però vigileu de no posar massa calor ja que és fàcil que el paper comenci a cremar-se.

La facilitat per descobrir aquests missatges ocults i l'avenç de la tecnologia van fer que s'inventessin tintes que només eren visibles si es feien reaccionar amb certs reactius específics.

Missatges sense xifrat: També van ser utilitzats els anomenats missatges sense xifrat. En aquest tipus de missatges, el missatge real és escrit directament, però els seus elements són camuflats entre altres del missatge inofensiu.

La tecnologia de micropunts: A l'hora que la detecció dels missatges anava progressant, també ho feien les tecnologies per ocultar missatges menys sospitosos, i amb més quantitat útil d'informació. Els alemanys van desenvolupar la tecnologia de micropunts que consistien en fotografies en què els punts es trobaven dispersos de tal manera, i eren tan petits, que no es veien a primera vista. Els missatges que portaven aquesta nova tecnologia no estaven ni ocults ni xifrats, eren tan petits que eren imperceptibles.

L'esteganografia i la computadora: Amb cada nou missatge ocult que es descobria amb aplicacions existents, nous mètodes millorats d'esteganografia es creaven. I així arribem a l'actualitat on la invenció de la computadora ha permès abordar amb més complexitat el tema de l'esteganografia i, en aquest moment, aquesta ciència té cada vegada més interès per moltes raons: Per exemple:

- Les empreses de difusió d'informació s'estan interessant en tècniques per ocultar marques de drets d'autor codificades i nombres de sèrie en pel·lícules digitals, discos compactes, llibres i productes multimèdia.
- Les limitacions que imposen alguns governs a l'hora d'utilitzar mètodes criptogràfics, ha motivat a la gent interessada en comunicar-se amb total confidencialitat, a estudiar mètodes pels quals es pot ocultar un missatge secret en un altre que sembla inofensiu.

2 MÈTODES CRIPTOGRÀFICS CLÀSSICS

S'entenen per mètodes criptogràfics clàssics els que es feien servir abans de l'aparició dels ordinadors, encara que aquests sistemes han servit de base pels mètodes criptogràfics actuals.

Hi ha 2 tipus de xifres elementals:

Les basades en el principi de transposició i les basades en el principi de substitució.

2.1 XIFRES DE TRANSPOSICIÓ

Les xifres de transposició ordenen els caràcters d'acord amb certes regles, a vegades, la reordenació dels caràcters es feia amb l'ajut d'alguna figura geomètrica.

Aquest xifrat s'efectuava amb 2 passos:

1. El text en clar s'escrivia seguint un determinat camí d'entrada.
2. Seguint un determinat camí de sortida s'extreia el text xifrat.

En la transposició, les lletres del missatge simple es col·loquen en diferent ordre, generant d'aquesta manera un anagrama. Les lletres no es transformen, simplement varia la seves posicions a dins del text. Aquest mètode es pot considerar poc segur per missatges amb poques lletres degut a que com menys lletres hi hagi menys nombre de combinacions hi haurà, però, a mesura que s'augmenta el nombre de lletres, el nombre de combinacions es dispara de manera exagerada. Perquè el receptor pugui desxifrar el missatge s'ha d'utilitzar algun mètode determinat. Hi ha diferents mètodes de transposició:

2.1.1 *Mètode de riel*

És un sistema de permutació que va ser adoptat pels escolars anglesos a l'època victoriana. És un dels mètodes més utilitzats. Consisteix en separar el missatge en 2 línies. Posant les lletres en posició senar en la primera fila i les que estan en posició parell a la segona fila, i, finalment, s'escriu la segona fila al darrere de la primera fila, i el resultat final és un conjunt de lletres sense sentit aparent. Utilitzant aquest mètode, el receptor pot desxifrar el missatge invertint el procés que ha fet l'emissor.

EXEMPLE:Missatge per codificar: **QUEDEM A CASA TEVA PER FER EL TREBALL****QEEAAAEAEFRLRBL****UDMCSTVPREETEAL**Missatge Codificat: **QEEAAAEAEFRLRBL UDMCSTVPREETEAL.**

Un altre mètode de transposició és la *escitala* que ja s'ha explicat el seu funcionament en un apartat anterior.

2.1.2 Mètode de transposició amb període fix (mètode dels blocs)

Proposa que emissor i receptor es posin d'acord en una determinada ordenació dels nombres naturals entre 1 i n . Prenem, per exemple, $n = 4$, i suposem que hem convingut la ordenació (3,1,4,2). Aleshores, el text que volem xifrar es divideix en blocs de 4 lletres, i a cada un dels blocs se li aplica la permutació (3,1,4,2), en el sentit de que la tercera lletra del bloc, es col·locarà en el primer lloc i així successivament:

EXEMPLE:TEXT EN CLAR: **DEMA A LES DUES ON SEMPRE****DEMÀ-ALES-DUES-ONSE-MPRE**CLAU: **(3,1,4,2)**TEXT XIFRAT: **EADM-LSAE-USDE-NEOS-PEMR****EADMLSAEUSDENEOSPEMR****2.1.3 Mètode de les Caixes**

Aquest mètode va ser utilitzat per l'exercit espanyol fins la dècada de 1970. És una mena d'encreuament entre el mètode dels blocs i el dels escolars anglesos. La clau és una paraula secreta, coneguda només per l'emissor i el receptor. El mètode consisteix en agafar la columna del primer número que apareix en la clau i copiar les lletres de dalt a baix.

EXEMPLE:PARAULA CLAU: **CRIPTOGRAFIA = 3,10,6,9,12,8,5,11,1,4,7,2**TEXT EN CLAR: **EXEMPLE D'ÚS DEL MÈTODE DE LES CAIXES**TEXT XIFRAT: **EEL-SL-LDS-UE-ES-DD-POE-DE-ELC-MTX-EE-XMA****EEISLLDSUEESDDPOEDEELCMTXEEXMA**

1	2	3	4	5	6	7	8	9	10	11	12
E	X	E	M	P	L	E	D	U	S	D	E
L	M	E	T	O	D	E	D	E	L	E	S
C	A	I	X	E	S						

Hi ha molts altres mètodes per obtenir el text xifrat, però en general, els criptosistemes per transposició es caracteritzen pel fet que el text xifrat que s'obté és sempre una permutació del total de les lletres del text inicial.

2.2 XIFRES DE SUBSTITUCIÓ

Hi ha quatre tipus de xifres de substitució:

- La Simple
- La Homofònica
- La Polialfabètica
- La Poligràfica

2.2.1 Substitució simple

Una xifra de substitució simple canvia cada caràcter d'un alfabet en clar ordenat, anomenat A, per la lletra corresponent d'un alfabet xifrat denotat per C.

Aquesta substitució simple sempre és una aplicació injectiva ja que dues lletres diferents no poden substituir-se per una mateixa, ja que si fos així no es podria desxifrar el missatge.

EXEMPLE 1:

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

TEXT EN CLAR:

MISSATGEXIFRATAMBELMÈTODESIMPLE

TEXT XIFRAT:

WDIIPJBTMDAHPJPWQTVWTJYSTIDWFVT

EXEMPLE 2: MÈTODE DE CÉSAR

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

TEXT EN CLAR: **EXEMPLEDESUBSTITUCIÓAMBELMÈTODECÉSAR**

TEXTXIFRAT: **HAHPSOHGHVXEVWLWXFLRDPEHOPHWRGRGHFHVDU**

Aquest mètode de xifrat el podem posar com una fórmula matemàtica de la següent manera: suposem que estem utilitzant un alfabet de n lletres i unitats de missatge d'una lletra. Podem considerar l'alfabet com el conjunt d'enters $\mathbb{Z}/N$. I considerem la funció afi.

$$\begin{array}{ccc} f: \mathbb{Z}/N & \longrightarrow & \mathbb{Z}/N \\ x & \longrightarrow & f(x) = x + r \pmod{N} \end{array}$$

on r és un enter entre 0 i $N-1$

Aquesta transformació desplaça cada lletra x del text original r lletres endavant. Si $r=3$, s'anomena xifrat de Juli César. Per desxifrar aquest missatge necessitem conèixer r , i per tant r és la clau del criptosistema.

2.2.2 Substitució Homofònica

Les substitucions simples tenen l'inconvenient que conserven les freqüències del text en clar al text xifrat, la qual cosa facilita molts atacs criptoanalítics. Una xifra de substitució homofònica té com a objectiu dissimular les freqüències dels caràcters del text en clar. L'idea és fer correspondre a cada caràcter a del alfabet del text en clar no pas un, sinó un conjunt $f(a)$ de símbols de text xifrat anomenats homòfons. Per amagar les freqüències del text en clar i evitar atacs criptoanalítics, una bona estratègia és que el conjunt d'homòfons $f(a)$ tingui un cardinal proporcional a la freqüència del caràcter en clar a . D'aquesta manera s'aconsegueix que les freqüències dels símbols en el text xifrat siguin pràcticament uniformes.

2.2.3 Substitució Polialfabètica

La substitució polialfabètica també té com a objectiu dissimular la freqüència dels caràcters del text en clar, però a diferència de la substitució homofònica, aplica criteris diferents de substitució en comptes d'un sol criteri. Entre elles se'n poden distingir diferents mètodes.

- Xifra d'Alberti:

Va ser el primer mètode de substitució polialfabètica, documentada per primer cop a Itàlia. La primera xifra d'aquesta mena, fou publicada per Alberti l'any 1568.

- Xifra de Vigenère:

Aquest és un altre exemple de substitució polialfabètica, que ja ha estat explicat en l'apartat de la història de la criptografia.

- Màquina Enigma:

És una altra mostra de substitució polialfabètica.

- Xifrat de Vernam:

Apareix al segle XX i se'l coneix com el cas límit del mètode de Vigenère. Utilitza **l'alfabet binari**. L'operació aritmètica és la suma del mòdul 2 (XOR lògic, disjunció exclusiva) i la clau és una seqüència binària aleatòria de la mateixa longitud que el text, i no reutilitzable

EXEMPLE:

Missatge en clar:	00011011110110100101
Clau:	11011001010101100110
Criptograma:	11000010100011000011
Clau:	11011001010101100110
Missatge en clar:	00011011110110100101

Com que mòdul 2 sumar i restar és el mateix, l'algoritme de xifrar i desxifrar és el mateix.

2.2.4 Substitució Poligràfica:

Les tres substitucions anteriors xifren una sola lletra del text en clar cada cop. Les xifres de substitució poligràfica xifren blocs grans de lletres amb la qual cosa dificulten atacs criptoanalítics basats en les freqüències individuals de les lletres del text en clar. Un exemple d'aquest tipus de substitució en seria *la xifra de Hill*:

L'any 1929 S. Hill, un jove matemàtic va publicar a Nueva York, un article en que proposava utilitzar l'àlgebra, i en particular les matrius en les operacions de xifrar. La clau de la xifra de Hill, és una matriu, K de d files i d columnes. Per a xifrar, s'agafen blocs successius de d caràcters del text en clar com si fossin vectors. Cada vector del text en clar es multiplica per K per obtenir un vector de text xifrat (també amb d caràcters). Els productes són mòdul n , sent n el cardinal de l'alfabet del text xifrat. La matriu K sempre ha de ser una matriu quadrada i ha de tenir inversa en el mòdul amb el que estem treballant perquè si no tingués inversa el missatge no podria ser desxifrat pel receptor.

EXEMPLE:

Per a $d = 2$ els dígrafs es consideren vectors de 2 components i a cada dígraf x se li aplica la següent transformació.

$$F: (\mathbb{Z}/N)^2 \rightarrow (\mathbb{Z}/N)^2$$

$$x = \begin{pmatrix} x_1 \\ x_2 \end{pmatrix} \rightarrow f(x) = A \cdot x + B = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \cdot \begin{pmatrix} x_1 \\ x_2 \end{pmatrix} + \begin{pmatrix} e \\ f \end{pmatrix}$$

La clau del criptosistema la formen els sis nombres enters a, b, c, d, e, f . Observem que un dígraf inicial $x = (x_1, x_2)$ queda xifrat com a:

$$y = (y_1, y_2) \quad \begin{cases} y_1 = ax_1 + bx_2 + e \\ y_2 = cx_1 + dx_2 + f \end{cases}$$

De manera que cada un dels caràcters que formen el dígraf xifrat depèn dels dos caràcters del dígraf inicial. Aquesta barreja dificulta l'atac per anàlisi de freqüències.

3 MÈTODES CRIPTOGRÀFICS MODERNS

La diferència essencial entre els mètodes de criptografia clàssica i els mètodes de criptografia moderna és que, un criptosistema clàssic només és segur si es manté en secret el procediment i les claus. En canvi, en la criptografia moderna, els procediments són públics i les claus es mantenen secretes. Els procediments són tan complicats que fins i tot un atacant que disposi d'una quantitat arbitrària de text xifrat no podrà deduir les claus de xifrat, encara que conegui el mètode que s'ha utilitzat per xifrar el text.

Els sistemes criptogràfics clàssics presentaven una greu dificultat: la relació entre la complexitat - longitud de la clau i el temps necessari per xifrar i desxifrar el missatge. A l'era moderna, aquesta barrera s'ha trencat degut principalment als següents factors:

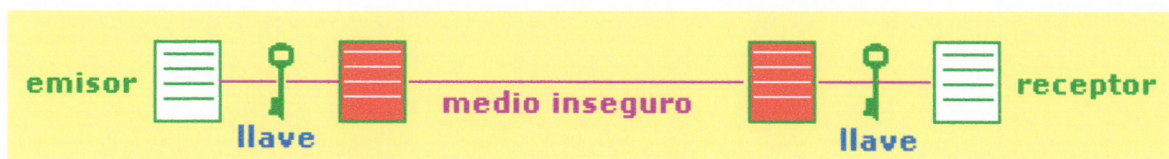
Velocitat de Càlcul: Amb l'aparició de les computadores es va disposar d'una potència de càlcul molt superior a la dels mètodes clàssics.

Avenç en els coneixements matemàtics: Han permès trobar i definir amb claredat sistemes criptogràfics estables i segurs.

Necessitat de seguretat: Han sorgit moltes activitats noves que precisen de l'ocultació de dades.

Partint d'aquests principis, han sorgit nous i complexos sistemes criptogràfics, que els podem classificar en dos grups de criptosistemes: Els de clau privada o simètrica i els de clau pública o asimètrica.

En el de clau privada només l'emissor i el receptor coneixent la clau utilitzada en la transmissió del missatge, i la mateixa clau serveix per xifrar el missatge i per desxifrar-lo.



Esquema de funcionament d'un sistema de clau privada.

En els criptosistemes de clau pública, la característica fonamental és que la clau de desxifrar no es pot calcular a partir de la clau de xifrar. Cada usuari U té un parell de claus, una de les claus és pública i l'altra és secreta i coneguda només per l'U. La clau pública és

utilitzada per a qualsevol altre usuari que vulgui enviar a U un text xifrat. Quan U rep el missatge, fa servir la seva clau privada per desxifrar-lo. Com que U no comparteix amb ningú la seva clau privada, la seguretat d'aquest tipus de criptosistemes és més gran que la dels sistemes simètrics, en els quals cada parell d'usuaris s'ha de posar d'acord en compartir una mateixa clau.



Esquema de funcionament del sistema de clau pública

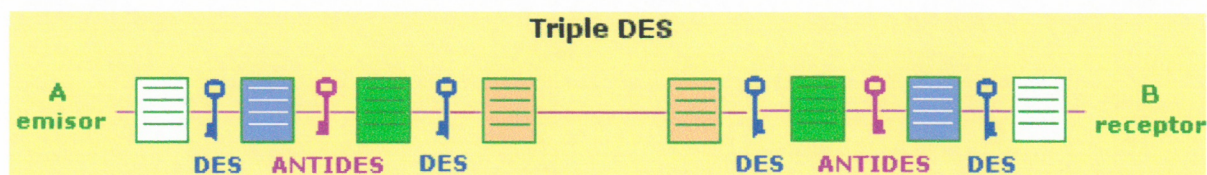
3.1 SISTEMA DE CLAU PRIVADA

3.1.1 El criptosistema DES

L'any 1977 el departament de comerç i la oficina nacional d'Estandards Nord-Americana amb col·laboració amb l'empresa IBM va idear el sistema de clau privada DES (*Data Encryption Standard* 1976). Aquest sistema es va crear per proporcionar al públic en general un algoritme de xifrat estàndard i que pogués garantir la seguretat davant dels atacs d'usuaris no autoritzats. Durant els anys 80 i 90, aquest criptosistema fou el més utilitzat, però aquest sistema va ser trencat l'estiu del 1998.

Actualment el mètode més acceptat com a possible substitut del DES és l'IDEA (*International Data Encryption Algorithmic* universitat politècnica de Zurich 1991), que es fa servir dins del sistema PGP per garantir la seguretat del correu electrònic de la xarxa d'internet.

El DES és un exemple de mètode de xifratge en bloc. Això vol dir que el text inicial (que a partir d'ara suposarem que està xifrat en sistema binari, i per tant serà una cadena de bits) es divideix en blocs de 64 bits, i cada bloc es xifra separatament usant una clau secreta de 56 bits. Per tant, el número de claus totals d'aquest sistema seria $2^{56} = 7,2 \times 10^{16}$. El sistema DES es pot implementar tan en Hardware com en Software, encara que la implementació Hardware permet velocitats de xifrat i desxifrat molt més grans. El sistema DES presenta inconvenients:



- Es considera que en aquests moments la seva clau és massa curta atesa la potència del càlcul actual amb els ordinadors. Per resoldre aquest problema, s'ha proposat el xifrat múltiple que es coneix amb el nom de *triple DES*. Aquests xifrats múltiples consisteixen en aplicar el mateix algoritme varies vegades però amb diferents claus.

El triple DES està format per una clau de 128 bits que es divideix en dues claus diferents de 64 bits. Primer se li aplica al text en clar, una clau C_1 al resultat (Anti DES) se li aplica una segona clau C_2 i al resultat se li torna a aplicar la clau C_1 .

- La seguretat del sistema es redueix molt si es té un nombre suficient de textos aquest procés es coneix amb el nom de *criptoanàlisis diferencial*⁵.

Encara que el sistema DES està sotmès a una crítica contínua, continua sent el sistema més estès.

3.1.2 El criptosistema IDEA

L'any 1992 Biham i Shamir proposen un nou sistema de xifrat simètric l'IDEA. Utilitza una clau secreta de 128 bits que xifra blocs d'informació de 64 bits, el número de claus totals d'aquest sistema seria de 2^{128} aproximadament 3×10^{38} .

El sistema IDEA és aproximadament el doble de ràpid que el sistema DES. En l'actualitat, IDEA és un dels algoritmes de xifrat més segurs i ha augmentat la seva popularitat des de que forma part del xifrat simètric del PGP.

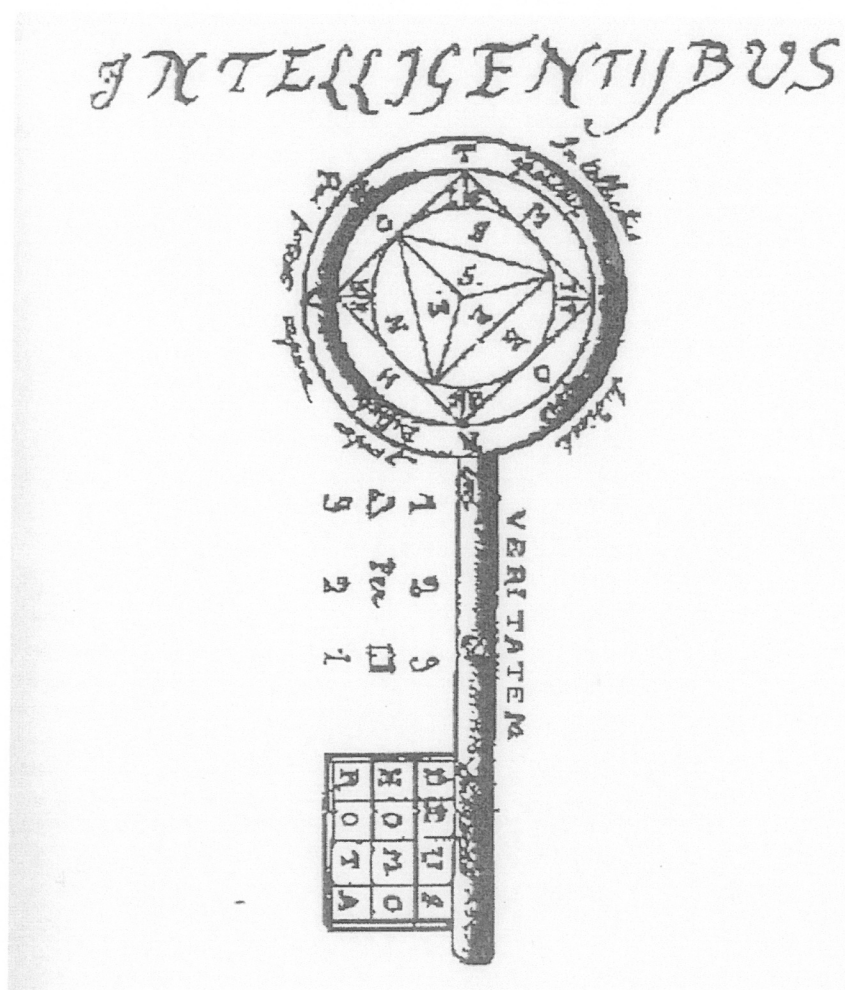
3.1.3 El criptosistema AES

Davant l'augment de la potència de càlcul que aconsegueixen cada dia els ordinadors, i, d'altra banda, a causa de la controvèrsia que hi ha sobre la seguretat del DES en relació amb la llargada de la seva clau, es fa necessari substituir-lo. El *National Institute of Standards & Technology* (NIST) del govern nord - Americà, va fer una crida al Setembre de 1997 perquè es presentessin propostes per a un nou estàndard de xifrat el qual es coneixerà com a AES (*Advanced Encryption Standard*). En la petició de propostes, el

⁵ És un atac amb text original escollit que té èxit només amb algunes implementacions de DES, consisteix en examinar grans quantitats de textos xifrats.

NIST, va demanar un algoritme de xifrat de bloc que fos utilitzable tan en entorns governamentals com en entorns comercials, i que havia de ser més eficient que el triple DES. Així mateix, la clau havia de tenir una longitud variable (128, 192 o 256 bits almenys) i els blocs de xifrat una llargada de 128 bits. L'any 2000 el NIST va escollir el treball presentat pels belgues Rijmen i Daemen, conegut actualment amb el nom d'AES. Respecte a la seguretat de l'AES, és encara un algoritme jove que de moment a passat totes les proves a les que ha estat sotmès. Els seus autors diuen que és immune als atacs per criptoanàlisi diferencial.

3.2 SISTEMES DE CLAU PÚBLICA



El gravat representa la clau de David incloïa en el *Absconditorium clavis* de Guillaume Postel (Amsterdam, 1645). Aquesta clau era considerada com la clau de les coses ocultes necessària per penetrar en el vel de la eterna veritat. Al peu de la mateixa apareixia la llegenda: “Clau que obre i res tanca, que tanca i res obre”, pot ser considerada com una autèntica premonició de la criptografia de clau pública.

Sistemes de clau Pública

La criptografia de clau pública ha suposat una revolució en la criptografia moderna.

La criptografia de clau compartida presenta 3 inconvenients:

- 1) La distribució de claus: Dos usuaris han d'eleger una clau secreta abans de començar-se a comunicar.
- 2) La gestió de claus: En una xarxa de n usuaris, cada parella d'usuaris ha de tenir la seva clau compartida particular. La qual cosa implica un total de

$$C_{n,2} = n \cdot (n-1) / 2$$

- 3) No hi ha signatura digital: La signatura digital és l'equivalent a les signatures manuals en el cas de la informació electrònica; en un criptosistema de clau compartida generalment no hi ha possibilitat de signar els missatges, pel fet que totes les claus són compartides almenys per 2 usuaris.

El concepte de criptosistema de clau pública, que permet superar els inconvenients anteriors, va ser proposat per W.Diffie, M.E.Hellman en l'article: "*New directions in cryptography*". Aparegut l'any 1976. L'idea que es pot qualificar de revolucionària era permetre un intercanvi segur de missatges entre emissor i receptor sense haver-se de trobar prèviament per acordar una clau secreta segura.

Segons Diffie i Hellman tot algoritme de clau pública ha de complir les següents propietats:

- 1) Qualsevol usuari pot calcular les seves pròpies claus pública i privada en temps polinòmic.
- 2) L'emissor pot xifrar el seu missatge amb la clau pública del receptor amb temps polinòmic.
- 3) El receptor pot desxifrar el criptograma amb la clau privada amb temps polinòmic.
- 4) El criptoanalista que intenti esbrinar la clau privada mitjançant la pública es trobarà amb un problema intractable.
- 5) El criptoanalista que intenta desxifrar un criptograma tenint la clau pública és trobarà amb un problema intractable.

En la pràctica dissenyar algoritmes aritmètics és resoldre cinc problemes numèrics diferents. Els tres primers (condicions 1, 2 i 3) són problemes de temps polinòmic i els altres dos (condicions 4 i 5) són problemes molt complexos de temps exponencial. Això

vol dir que aquests criptosistemes es basen en l'existència de problemes fàcils⁶ relacionats amb problemes difícils⁷.

Per aquest motiu, es defineix una transformació criptogràfica: T_k que sigui fàcil d'aplicar, però de manera que sigui molt difícil de trobar la seva transformació inversa: T_k^{-1} sense tenir la clau de desxifrat. Aquesta transformació T_k s'anomena funció unidireccional amb trampa.

Suposant que tenim una màquina que és capaç de processar 10^8 instruccions per segon, es pot veure en la taula següent que segons la complexitat de l'algoritme que s'hagi d'utilitzar els temps de resolució són molt diferents:

ALGORITME	OPERACIONS PER $n=10^8$	TEMPS
Polinomi constant	1	10^{-8} segons
Polinomi lineal	10^8	1 segon
Polinomi quadràtic	10^{16}	1000 dies
Polinomi cúbic	10^{24}	$2,7 \cdot 10^8$ anys
Exponencial	$10^{9030900}$	$10^{9030886}$ anys

3.2.1 RSA

En l'article esmentat l'apartat anterior, Diffie i Hellman van formular la idea d'un criptosistema de clau pública, però no en van donar cap exemple pràctic. La primera aplicació de la proposta va ser el criptosistema RSA publicat per Rivest, Shamir i Adleman el 1978 amb l'article "*A method for obtaining digital signatures and public-key cryptosystems*".

Per entendre l'algoritme de generació de claus del RSA que s'exposa tot seguit es necessiten molts conceptes matemàtics que s'expliquen en el capítol 5 amb els seus exemples corresponents:

- *Algoritme de Generació de Claus del RSA:*

⁶ És aquell problema que es pot resoldre en temps polinòmic

⁷ És aquell problema que no es pot resoldre en temps polinòmic.

- 1) Escollir dos grans⁸ **nombres primers**⁹ (veure annex 1) **p** i **q** (secrets) i calcular el nombre **N** (públic) corresponent al seu producte. $N = p \cdot q$.
- 2) Escollir la clau de desxifrar que haurà de ser un gran nombre enter **d**(secret) que és primer amb el nombre **$\varphi(N)$** (secret) sent

$$\varphi(N) = (p-1) \cdot (q-1)$$

- 3) Calcular l'enter positiu **e** (públic) tal que $1 \leq e \leq \varphi(N)$

$$\text{m.c.d}(\text{de } e \text{ i } \varphi(N)) = 1$$

fent la **congruència** $d \equiv e^{-1} \pmod{\varphi(N)}$ utilitzant **l'algoritme d'Euclides** estès.

- 4) Fer pública la clau de xifrar (**e**, **N**).
- 5) Per xifrar un text, és necessari prèviament xifrar el text en un sistema numèric en base **b** dividint-lo en blocs de mida **j-1** de manera que:

$$b^{j-1} < N < b^j$$

- 6) Xifrar cada bloc **M_i** transformant-lo en un nou bloc de mida **j**: **C_i** d'acord amb l'expressió:

$$C_i \equiv M_i^e \pmod{N}$$

- 7) Per desxifrar el bloc **C_i**, es fa servir la clau privada **d**, segons l'expressió:

$$M_i \equiv C_i^d \pmod{N}$$

Per clarificar el procés que s'acaba de descriure a continuació es mostraran uns exemples realitzats per procediments diferents:

- Dificultats del RSA

Les dues principals dificultats en la implementació de l'RSA són:

- El càlcul de potències modulars. El problema del càlcul d'una potència modular és un problema de temps polinomial utilitzant el mètode del quadrat.
- La recerca de nombres primers adequats. Hi ha diversos mètodes eficients per a confirmar que un nombre gran és primer. Per exemple els tests de primeritat de Solovay-Strassen i el de Lehman i Peralta.

⁸ Actualment, es recomana que cadascun d'aquests nombres primers tingui més de dos-cents dígit.

⁹ Veure annex 1. "Hi ha algú aquí a fora?" (perquè ens calen primers tan grans?) Article publicat per Pilar Bayer.

- El test de Solovay-Strassen és una tècnica que permet determinar amb una probabilitat molt gran si un nombre p és o no primer.

- Velocitat de l'RSA

En la pràctica, perquè el procés de xifratge en l'RSA sigui més ràpid, se sol escollir un exponent públic e petit; sovint es pren $e = 3$. Aquesta tria no compromet la seguretat del sistema, ja que aquesta depèn del secret de la clau privada d .

Si ens fixem en la velocitat que s'aconsegueix en les implementacions de l'RSA, cal reconèixer dos fets:

- En programari, el criptosistema DES arriba a funcionar 100 vegades més de pressa que l'RSA.
- En maquinari, el DES arriba a ser, entre 1000 i 10.000 vegades més ràpid que l'RSA.

Malgrat la lentitud relativa, l'RSA i els altres criptosistemes de clau pública, es fan servir perquè permeten també, signar digitalment els missatges enviats. Normalment es fa per mitjà d'una combinació de clau pública i de clau secreta coneguda com a *Sobre digital*, que ofereix la velocitat de la clau compartida i la flexibilitat de la clau pública.

- Seguretat de l'RSA

Per a trencar el criptosistema RSA, un criptoanalista, ha de trobar el valor d , que és la trampa de la funció unidireccional, però això requereix conèixer $\phi(N)$ però, no és fàcil trobar-la a partir de N si no és que se sap factoritzar $N = p \cdot q$. D'aquí es dedueix que la seguretat del criptosistema RSA, es basa en el problema de la factorització (encara que no s'ha pogut demostrar que la única manera de trobar d a partir de e , passi per factoritzar N).

Convé doncs, elegir els dos primers p i q de manera que la factorització sigui tan difícil com es pugui. El que se sol fer és triar p i q aleatòriament entre els primers que compleixen les següents condicions:

- 1) p i q han de tenir una magnitud semblant però no han de ser massa propers.
- 2) p i q han de ser de més de 512 bits.
- 3) $(p-1)$ i $(q-1)$ han de tenir factors primers grans.
- 4) m.c.d. $(p-1, q-1)$ ha de ser petit.

Una manera d'elegir p i q perquè compleixin les condicions anteriors és triar un primer r gran, tal que $p = 2r+1$ i $q=2p+1$ siguin primers. Un nombre p triat així, s'anomena primer segur.

És lògic pensar que a mesura que s'aprofundeixi en la investigació es descobriran noves propietats d'aquests paràmetres, que s'han de verificar perquè el sistema resulti cada vegada més segur.

3.2.2 Altres sistemes de clau pública

- Sistema d' ELGAMAL (1985):

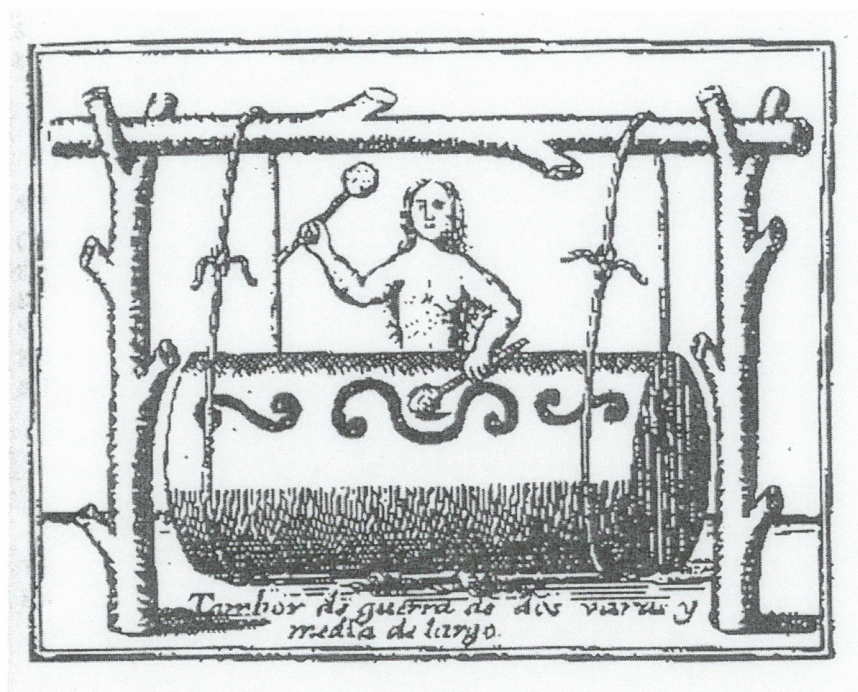
Funciona de manera diferent als altres sistemes de clau pública ja que el xifrat es fa utilitzant la clau pública del receptor i la clau privada de l'emissor.

- Sistema de Merkle-Hellman (1978):

Aquest sistema de clau pública ja no s'utilitza, perquè totes les seves versions han estat trencades pels criptoanalistes. Aquest sistema tenia una avantatge respecte als altres sistemes de clau pública: la seva alta velocitat.

- Altres sistemes basats en la teoria de corbes el·líptiques.
- Sistemes probabilístics, que es diferencien dels altres sistemes de clau pública perquè en aquest cas els algoritmes de xifrat són probabilístics en comptes de deterministes.

Seguretat Criptogràfica:



La figura representa un gravat pres del llibre "El Orinoco" Il·lustrat per P. Joseph Gumilla, de la Companyia de Jesús (any 1714) , conservat a la Biblioteca General de la Universitat de Zaragoza.

Aquesta il·lustració mostra un model primitiu de comunicacions digitals amb canal obert per la transmissió de missatges guerrers, pel que sembla l'assumpte més important de la època. És senzill donar-se compte de que la comunicació es trobava exposada a atacs passius (oïda), però era immune a possibles modificacions del missatge a través del canal de transmissió (excepte quan hi havia turmenta). De la mateixa manera, l'atac actiu que té com a finalitat suplantar la personalitat del emissor requeria matar al timbaler. En el nostre món digital, les comunicacions telemàtiques, si bé són més ràpides i sofisticades que les antigues, continuen exposades com elles a atacs actius i passius, a modificacions de missatges i a la suplantació de la identitat dels comunicants (afortunadament incrementa en la majoria dels casos). En aquest context, les eines criptogràfiques presentades en els capítols anteriors serveixen com a base pel desenvolupament de nombroses aplicacions que permeten comunicacions entre els éssers humans de forma confidencial i segura

4 SEGURETAT CRIPTOGRÀFICA

4.1 SEGURETAT CRIPTOGRÀFICA

Durant 2000 anys els creadors de xifres han lluitat per conservar secrets, mentre que els desxifradors s'han esforçat per revelar-los.

La protecció de la informació deixa d'ésser una exigència de minories i es converteix en una necessitat global. Això comporta també major vulnerabilitat i inseguretat: El nombre d'atacants potencials i els mitjans al seu abast són igual de sofisticats que els dels sistemes de protecció.

La criptografia s'ha revelat com l'eina més poderosa per proporcionar serveis de seguretat en els sistemes informàtics.

Aquesta ciència té com a objectiu:

Confidencialitat: La informació ha d'estar disponible únicament pels usuaris autoritzats.

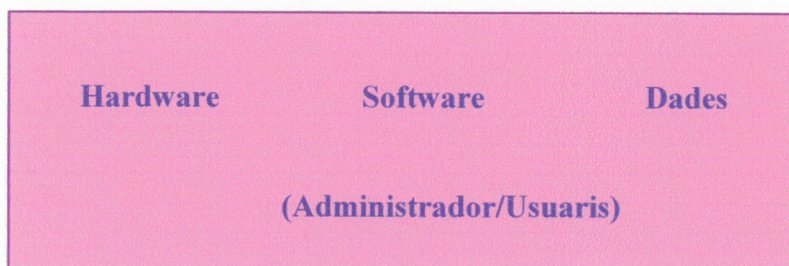
Integritat: S'ha de garantir que la informació no ha estat falsejada, accidentalment o intencionadament.

Autenticitat: S'ha d'assegurar l'origen i el destí de la informació (firma electrònica, copyright electrònic...)

No repudi: S'ha d'impossibilitar al·legar que certa informació no ha estat enviada o rebuda (correu electrònic certificat...).

En un sistema informàtic tots els seus elements són vulnerables.

Sistema Informàtic



Les mesures de seguretat per protegir la informació abasten diferents àmbits: legals, administratius, físics i lògics.

Per exemple, una implementació dolenta en Hardware o Software d'un algorisme matemàtic teòricament segur pot inutilitzar el sistema. També és cert, que molts sistemes de seguretat es trenquen a causa de la inconsciència dels usuaris: elecció dolenta de Passwords, no manteniment del secret de claus, desconnexió inadequada.... Però un sistema ben dissenyat, ha de tenir en compte els seus usuaris, perquè moltes vegades prefereixen la simplicitat i no estan conscienciats de la importància de les mesures de seguretat.

En l'àmbit legal, la llei de protecció de dades personals (Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal (BOE núm. 298, de 14-12-1999, pp. 43088-43099)) regula la protecció de dades i estableix un llistat de drets relatius a les persones físiques amb la finalitat que puguin dur a terme un control sobre les seves pròpies dades. Però respecte a la protecció de dades, s'ha de partir d'una ponderació entre els diferents drets en conflicte: la protecció de la intimitat de la persona i el lliure desenvolupament de l'activitat de les empreses i les Administracions Públiques. És necessari doncs, cercar un punt d'equilibri entre la protecció de la intimitat de l'individu i el correcte desenvolupament de les relacions tant amb les empreses com de l'Administració amb els ciutadans.

La seguretat no és un valor absolut, perquè no es pot dir que un sistema informàtic és segur, únicament que no es coneixen atacs que puguin vulnerar-lo. La criptografia únicament és capaç de posar barreres més o menys difícils per poder garantir un cert nivell de confiança.

La seguretat que ofereix la criptografia es considera violada quan a sigut possible obtenir la clau secreta del sistema. Des d'aquest punt de vista es poden diferenciar els següents nivells de seguretat:

- Seguretat incondicional: És la que ofereixen els mètodes de xifrat, en els quals es pot demostrar, des del punt de vista de la teoria de la informació que no existeix la possibilitat de predir la clau secreta de xifrat, conegut aquest. Els xifrats que compleixen aquesta condició s'anomenen xifrats perfectes. Des del punt de vista de la teoria de la informació hi ha només un xifrat perfecte: La xifra de Vernam.
- Seguretat Computacional: És la que ofereixen aquells mètodes de xifrat pels quals no existeix capacitat de càlcul suficient en l'univers per obtenir la seva clau secreta associada. La seguretat computacional està

definida d'acord amb la teoria de la complexitat, els coneixements matemàtics actuals i les prestacions dels ordinadors.

- Seguretat probable: Són aquells mètodes de xifrats que no han pogut ser violats encara, perquè l'esforç computacional que requereixen per trencar-los és superior a la capacitat de càlcul de l'atacant.
- Seguretat condicional: És la que ofereixen aquells mètodes dissenyats amb una finalitat específica i pels quals la dificultat de violació és més gran que la capacitat d'atac d'un atacant.

S'ha de tenir en compte que la seguretat criptogràfica representa un cost d'implementació i manteniment, per tant, el nivell de seguretat pràctica ha d'estar relacionada amb aquest cost, així com, amb l'avaluació dels riscos potencials que podria ocasionar una possible violació del sistema.

4.2 ATACS A LA SEGURETAT CRIPTOGRÀFICA

Existeixen dos tipus d'atacs en les comunicacions digitals: actius i passius.

En els atacs passius, l'atacant intenta només, obtenir la informació sense modificar-la. Aquests atacs no poden ser detectats pels comunicants.

En els atacs actius, l'atacant pretén, no només obtenir la informació, sinó també modificar-la. Els atacs actius poden classificar-se en dos grups: Atacs als operadors i atacs als protocols:

- Els atacs als operadors criptogràfics es fonamenten en l'ús del text en clar o del text xifrat per obtenir la clau.
- Els atacs als protocols són aquells que es basen en conèixer la clau, suplantar la personalitat (violar el PIN).

4.3 APLICACIONS CRIPTOGRÀFIQUES

La confidencialitat de la informació, és a dir, l'establiment de comunicacions secretes sobre canals insegurs no és l'únic propòsit de la criptografia, encara que, històricament, aquest a estat el seu objectiu durant molts anys. La criptografia moderna, té moltes altres aplicacions en la nostra societat. No és fàcil fer una classificació de totes les

aplicacions en que hi intervé, perquè a més a més, està en constant evolució fruit de les necessitats creades per les diferents situacions de relació social i comercial entre persones, institucions i organismes.

Per citar-ne algunes:

- comunicacions entre ordinadors.
- Comunicacions telefòniques.
- Transaccions electròniques.
- Aplicacions de les firmes digitals.
- Contractes electrònics.
- Eleccions electròniques.
- Correu electrònic.
- Comerç electrònic.

4.3.1 Correu electrònic segur

Entre les eines informàtiques, a nivell d'usuaris d'informàtica en general i en particular dels usuaris que envien i reben informació a través d'internet, algunes de les més conegudes són aquelles que amb els seus algorismes de clau privada i pública permeten xifrar i firmar documents de correu electrònic.

Dos gestors de correu electrònic segur són: el PGP (Pretty Good Privacy) i el PEM (Privacy Enhanced Mail)

El PGP (Pretty Good Privacy) va ser creat per P.Zimmermann¹⁰ l'any 1991. És un programari de lliure distribució que fa operacions criptogràfiques associades amb el sistema de correu electrònic. Aquest gestor permet enviar missatges electrònics signats, xifrats o totes dues coses.

Les característiques més importants que ofereix el PGP són les següents:

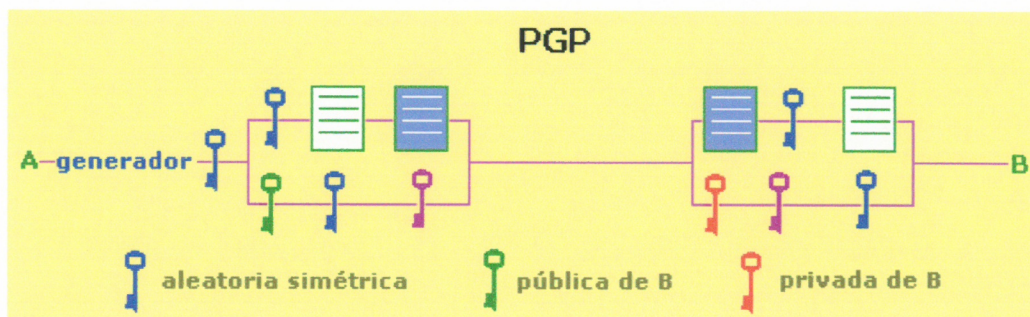
- 1) **Confidencialitat:** El missatge només pot ser llegit pel seu destinatari.
- 2) **Integritat:** El destinatari té la certesa que el missatge no ha estat modificat per ningú i que rep de la mateixa manera que el remitent l'ha enviat.
- 3) **Autenticitat:** El destinatari té la certesa de la identitat del remitent.
- 4) **No-repudiació:** El remitent no pot negar el fet d'haver enviat el missatge que el destinatari ja ha rebut.

¹⁰ Llicenciat en física i Informàtica per La universitat Atlàntica de Florida.

En l'àmbit de la confidencialitat, el PGP utilitza una combinació de clau pública i clau compartida per a aprofitar la velocitat de xifrat que ofereix la clau compartida i la versatilitat de la clau pública.

Pel que fa a l'integritat, l'autenticitat i la no-repudiació, el PGP utilitza la combinació d'una funció *hash*¹¹ i un esquema de *signatura digital*¹².

Quan enviem un missatge xifrat, el PGP el xifra utilitzant un sistema simètric, generalment, fa servir el sistema simètric l'IDEA, encara que a vegades també utilitza el DES. Utilitzant un generador pseudoaleatòri que posteriorment es xifra amb el sistema RSA. S'envia el document xifrat amb la clau pseudoaleatòria i aquesta clau xifrada amb la clau RSA pública del destinatari, quan aquest rep el correu i vol desxifrar-lo el seu programa PGP primer desxifra la clau asimètrica amb la seva clau privada RSA i després desxifra el document fent servir la clau desxifradora. Aquest procés es pot veure en el següent esquema:



En el cas que, quan s'envia un missatge es vulgui obtenir alhora autenticació i privacitat, primer caldrà signar-lo i després xifrar-lo.

La llargada de les claus RSA que empra el PGP, és diferent segons el grau de seguretat que es vulgui obtenir. N'hi ha de tres tipus: *Casual* (384 bits), *Commercial* (512 bits), i *Military* (1024 bits).

¹¹ Mecanisme criptogràfic irreversible que a partir d'una entrada qualsevol genera una sortida única de longitud constant. Els algoritmes que utilitza no necessiten claus i es basen en transformacions de substitució i permutació.

¹² Mecanisme criptogràfic en el qual l'autor d'un missatge genera un codi, que s'anomena signatura, que depèn del missatge i d'un secret que només coneix ell, de manera que aquest codi pot ser verificat pel receptor del missatge. Alguns dels algoritmes de signatura digital més coneguts i utilitzats són els que es basen en el criptosistema RSA i amb una funció Hash.

Les claus que s'utilitzen per xifrar amb Idea que s'anomenen claus de cessió, per a obtenir privacitat, les genera el programari mateix a partir d'un generador pseudoaleatòri. Aquest generador és el mateix xifrador Idea. Tant les claus RSA que genera el PGP com l'estat inicial del xifrador Idea per a obtenir les claus de cessió les aconsegueix aleatòriament el programari; com a llavor, utilitza una combinació del temps que tarda l'usuari a prémer una tecla i el valor d'aquesta.

En el capítol 6 es presenta de forma detallada el guió d'una pràctica per utilitzar els conceptes bàsics del programa PGP.

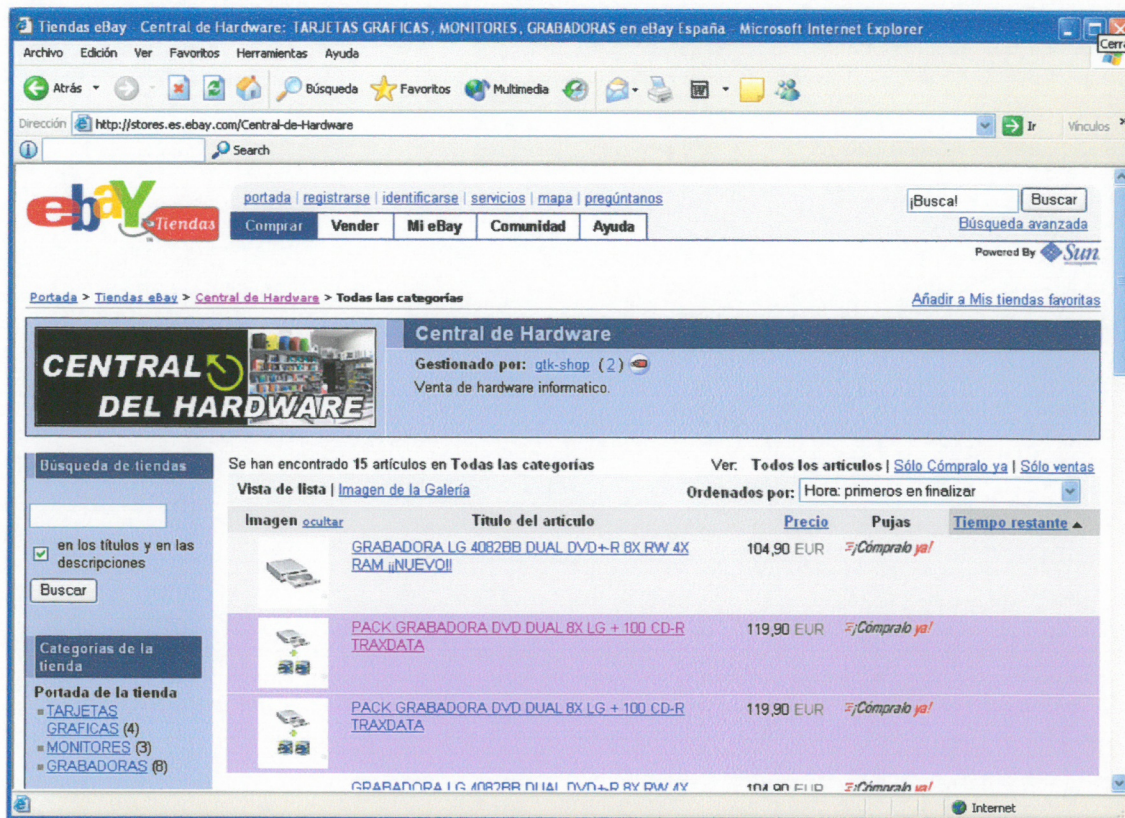
4.3.2 Comerç electrònic

El comerç electrònic és el procés de comprar o vendre béns i serveis entre empreses, clients i proveïdors a traves de xarxes d'ordinadors.

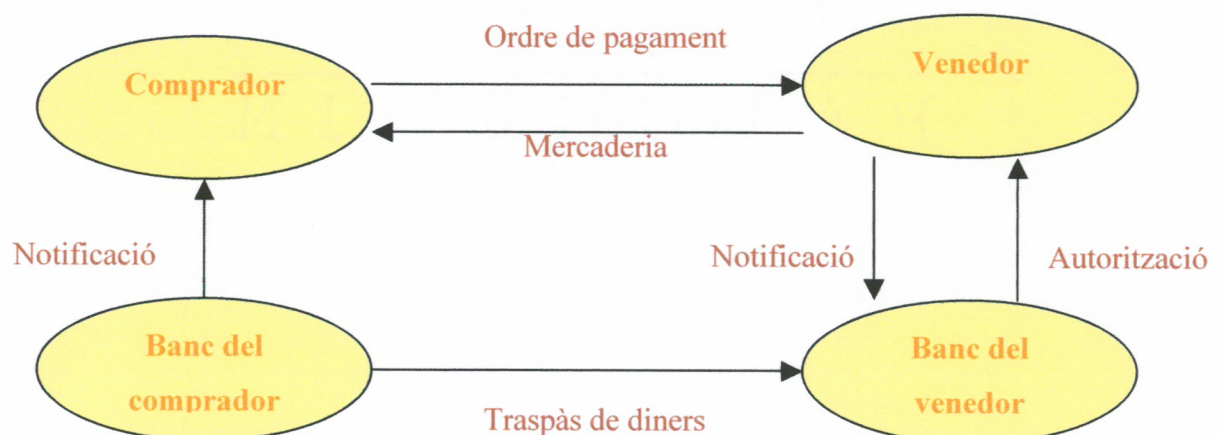
Podríem situar l'inici del comerç electrònic amb les primeres targetes de crèdit als anys 60 i, de manera més general amb els caixers automàtics de principi dels 80. Actualment, el comerç electrònic inclou no solament l'intercanvi de béns, sinó també el fet de poder fer negocis de qualsevol tipus a traves de les xarxes d'ordinadors, sobretot d'internet. En el comerç electrònic es poden diferenciar dos grups:

- Comerç electrònic d'empresa a empresa (business to business). Des d'in punt de vista econòmic no està destinat a obtenir guanys.
- Comerç electrònic d'empresa a consumidor (business to costumers). El seu objectiu és obtenir beneficis aprofitant el fet bàsic de supressió de distàncies que ofereix internet.

En el comerç electrònic podem considerar un subconjunt de transaccions que s'agrupen amb el nom de *comerç electrònic pur*, que són aquelles transaccions que es poden fer totalment a traves de la xarxa informàtica, des de la comanda fins a la recepció del producte. Això és possible gràcies al fet que el producte venut es pot obtenir amb suport electrònic (fotos, revistes, pel·lícules, llibres...)



- Sistemes de pagament electrònic: Les parts que intervenen en un sistema de pagament electrònic són el comprador, el venedor i les entitats bancàries que representen el comprador i el venedor. En l'esquema següent, es mostra com es produeix el sistema de compra amb pagament electrònic.



L'aspecte més important del comerç electrònic és la seva seguretat. Un sistema de pagament electrònic haurà de tenir les característiques següents:

- Integritat: Ningú no pot agafar diners d'un usuari sense l'autorització explícita d'aquest.
- Autorització: Els pagaments han de poder ser autoritzats per mitjà de contrasenyes o signatures digitals.
- Confidencialitat: Les transaccions han de tenir un cert grau de confidencialitat pel que fa a les identitats del comprador i del venedor, el contingut de la venda i el seu preu.
- Disponibilitat: Totes les parts involucrades han de poder fer pagaments. Aquests pagaments s'han de fer totalment per evitar que el sistema quedi inconsistent.

Els sistemes de pagament electrònic permeten moltes classificacions, segons les característiques en què ens fixem:

1) Valor total del pagament:

- Macropagaments: Pagaments de quantitats superiors a 10 €.
- Micropagaments: Pagaments de quantitats inferiors a 10€.

2) Situació de les entitats bancàries:

- On line: El venedor necessita una connexió en línia amb el banc per a validar el pagament.
- Off line: No es necessita cap connexió amb línia amb el banc quan es fa el pagament

3) Tipus de transacció econòmica:

- Dèbit: L'import de la compra es carrega en el mateix moment al compte del comprador.
- Crèdit: L'entitat bancària del comprador liquida totes les compres al final d'un període establert.

4) Situació del comprador:

- Anònim: El venedor no coneix la identitat del comprador.
- No anònim: El venedor coneix la identitat del comprador.

Els sistemes de pagament electrònic que s'utilitzen són diferents en el cas de macropagaments i micropagaments.

En els macropagaments, el sistema més important és el SET (Secure Electronic Transactions). El SET és un conjunt d'especificacions que han desenvolupat Visa i Master Card amb el suport d'empreses informàtiques com IBM, Microsoft, VeriSign... que tenen com a objectiu permetre pagaments segurs mitjançant internet, el seu funcionament es basa en targetes de crèdit i en certificats electrònics. Aquests certificats serveixen per validar la clau pública de les parts i són emesos per autoritats de certificació electrònica en les quals confien totes les parts que hi intervenen en l'esquema de pagament.

En els micropagaments no s'utilitza el sistema SET ja que, per quantitats tan petites, el preu de la transacció del pagament superaria al de la mercaderia comprada, perquè els protocols criptogràfics que s'utilitzen són cars degut a que utilitzen eines criptogràfiques complexes com ara les signatures digitals que tenen un cost computacional i de transmissió elevat, motiu pel qual, es substitueix la signatura digital per funcions *hash* (un ordinador amb una potència de càlcul normal, tarda 0'5 segons a fer una signatura digital utilitzant el criptosistema RSA i en aquest mateix període de temps, és capaç de calcular 10.000 imatges d'una funció *hash*).

4.3.3 Situació actual del comerç electrònic

Una preocupació que tenia, era conèixer el grau de seguretat que oferia el comerç electrònic: compres per internet, transaccions bancàries...

M'he posat en contacte amb algunes empreses perquè em facilitessin informació sobre quins mitjans utilitzaven per garantir la seguretat de les dades dels clients: *el Corte Ingles, Caprabo, Caixa Catalunya*.

Totes les empreses que he visitat m'han dit que són totalment segures:

- Corte Ingles (veure annex 2): M'han dit que confiaven la seguretat a l'empresa Safelayer i no han sabut explicar-me quins eren els protocols de seguretat que feien servir.
- Caixa Catalunya(veure annex 3): La seguretat de Caixa Catalunya també està en mans de l'empresa Safelayer.

- Caprabo: M'han dit que l'empresa que certifica la confidencialitat de les seves dades és VeriSign i adjunto la pàgina d'internet on deien que estaven explicats els protocols de seguretat que utilitza l'empresa.

Caprabo manté una política de confidencialitat de les dades aportades pels clients, i es compromet a protegir les dades personals dels clients de capraboacasa.com. La protecció de dades s'estén també a la recollida i a l'ús de la informació proporcionada a través del portal.

En aquest sentit, Caprabo garanteix que tractarà confidencialment les teves dades personals, i que el servidor en què s'emmagatzemaran i tractaran aquestes dades disposa de les mesures de seguretat necessàries per evitar que hi puguin accedir persones no autoritzades.

A aquest efecte, Caprabo ha adoptat les mesures oportunes de caràcter tècnic i de seguretat en les seves instal·lacions, en els sistemes i en els fitxers. Els pagaments que s'efectuen a Capraboacasa utilitzen un servidor segur per garantir la confidencialitat de les dades personals que viatgen per la xarxa mitjançant tècniques criptogràfiques.

Aquestes tècniques criptogràfiques consisteixen a xifrar les dades que s'envien per Internet mitjançant un protocol de comunicació denominat SSL (Secure Socket Layers). Aquest protocol utilitza un sistema de clau asimètrica per garantir una transacció segura i una autoritat de certificació per assegurar l'autenticitat dels participants en les transaccions. L'autoritat de certificació de Capraboacasa és Verisign.



Al veure que dues de les tres empreses que havia consultat confiaven la seva seguretat a l'empresa Safelayer (verue annex 4), vaig buscar informació i em vaig posar en contacte amb el Dr. Francisco Jordan., però no ha estat possible poder tenir una entrevista amb ell, atesos els seus compromisos professionals.

L'empresa Safelayer és una de les poques organitzacions que desenvolupen productes relacionats amb la criptografia en el nostre País.

Després de tots els llibres que he llegit i del contacte per via email amb el Sr. Francisco Jordan, m'he adonat que encara que la seguretat absoluta no existeix, sí que, el comerç electrònic gaudeix d'un alt grau de seguretat i que es segueix treballant per millorar cada dia aquesta seguretat.

4.4 PERSPECTIVES DE FUTUR

En aquests moments només una quantitat mínima de la informació que flueix pel món està xifrada amb seguretat, la resta està mal xifrada o sense xifrar.

Encara que s'utilitzi el criptosistema RSA correctament, els desxifradors poden fer moltes coses per obtenir informació dels missatges xifrats: atac de tempesta¹³, virus, cavalls de Troya... Però l'objectiu dels criptoanalistes és trencar la xifra de l'RSA, però fins ara, tots els intents de desenvolupar un mètode per factoritzar ràpidament han acabat fracassant. Els matemàtics han estudiat al llarg dels segles el problema de la factorització, i les tècniques actuals de factorització no són gaire millors que les tècniques antigues.

Els criptoanalistes, doncs, sense molta esperança d'un gran avenç teòric, s'han vist obligats a buscar una innovació tecnològica. És a dir, necessiten una tecnologia que faci aquests passos amb molta més rapidesa: *l'ordinador quàntic*. L'ordinador quàntic, seria capaç de realitzar càlculs amb una gran velocitat que faria que l'ordinador més modern d'aquests moments semblés un àbac trencat. Però en aquests moments encara s'ha de dir que la tecnologia per construir ordinadors quàntics operatius segueix sent molt primitiva. Només el temps ens podrà dir si es poden superar els problemes de construir un ordinador quàntic i quan serà possible.

Actualment, el problema més gran per a la implementació dels ordinadors quàntics és la seva capacitat de difusió en recorreguts llargs. No s'ha aconseguit una estabilitat que mantingui la polaritat dels fotons amb la distància. Encara que en el any 2003, un grup d'investigadors de Toshiba Reserch Europe, van aconseguir travessar la barrera de 100 Km. utilitzant fibra òptica.

La criptografia quàntica és un sistema de xifrat indesxifrabable. Tot i que aquesta afirmació no sigui la primera vegada que s'ha utilitzat en els últims 2000 anys, en aquest cas, és diferent de totes les afirmacions anteriors, ja que, si un missatge protegit per la criptografia quàntica fos desxifrat alguna vegada, significaria que la teoria quàntica és errònia, la qual cosa tindria efectes desastrosos pels físics, ja que s'hauria de reconsiderar com funciona tot l'univers.

¹³ És un sistema que detecta les diferents senyals electromagnètiques emeses per un ordinador cada vegada que es tecleja una lletra.

Com diu Simon Singh¹⁴ en el seu llibre *Los Códigos Secretos*:

“Si se pueden construir sistemas criptográficos cuánticos que operen entre grandes distancias, la evolución de las cifras se detendrá. La búsqueda de la privacidad habrá llegado a su fin. Habrá disponible una tecnología que garantice las comunicaciones seguras a los gobiernos, el ejército, las empresa y el público. La única cuestión que queda es si los gobiernos nos permitirían usar esa tecnología. ¿Cómo regularían los gobiernos la criptografía cuántica para que enriquezca la Era de la Información sin proteger a los criminales?”

¹⁴ Referència en l'apartat de bibliografia

5 CONCEPTES MATEMÀTICS UTILITZATS AL LLARG DEL TREBALL

5.1 TÈCNIQUES DE COMPTAR

5.1.1 Permutacions de n elements: P_n

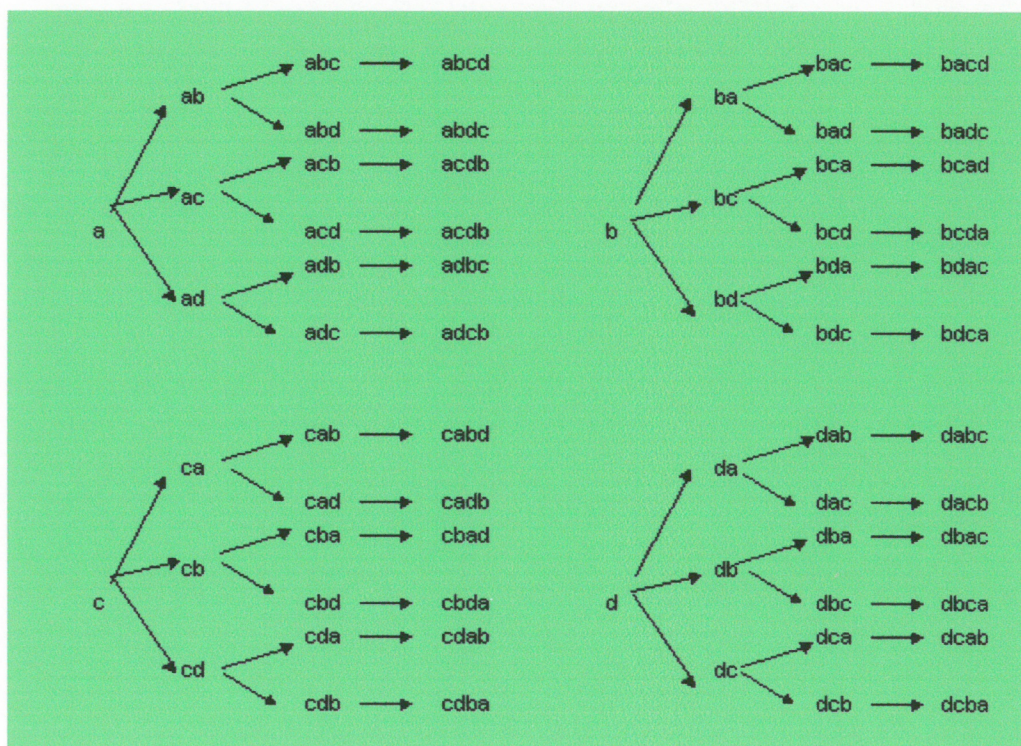
Sigui A un conjunt de n elements, una permutació de n elements del conjunt A és el resultat de col·locar els n elements en n llocs (o cel·les o també caselles) de manera que cada lloc contingui solament un element.

Si tenim n elements $\{a_1, a_2, \dots, a_n\}$ en n cel·les. A la primera cel·la s'hi poden col·locar n , a la segona només $n-1$, atès que ja n'hi ha un a la primera cel·la i no es poden repetir, i així successivament. Per tant, el nombre de P_n és:

$$P_n = n \cdot (n-1) \cdot \dots \cdot 2 \cdot 1 = n!$$

Nota: $n!$ És lleix factorial de n , o bé n factorial. Per conveni, $0! = 1$.

Exemple: Volem col·locar quatre llibres diferents de totes les maneres possibles en un prestatge. Els llibres els senyalem amb les lletres : $\{a, b, c, d\}$



Per saber quines són aquestes ordenacions construirem un diagrama d'arbre:

En aquest diagrama es veu que de cada un dels 4 elements originals surten 3 fletxes i que de cada una d'aquestes en surten 2 i de cada una d'aquestes dues en surt 1. Per tant, el nombre total de grups de quatre elements que es poden formar, serà $4 \times 3 \times 2 \times 1 = 4!$

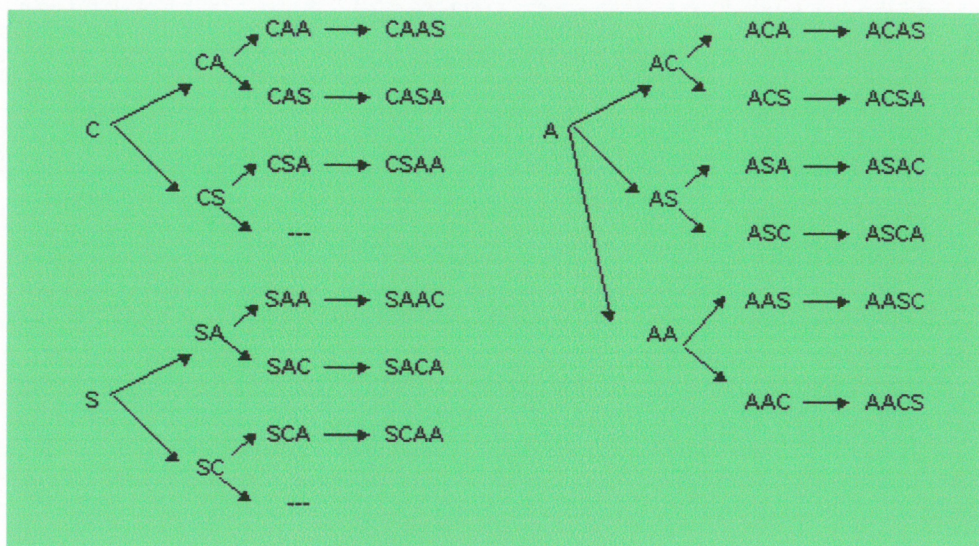
5.1.2 Permutacions amb repetició de n objectes. $PR_n^{p_1, \dots, p_r}$

Si disposem de n objectes però n'hi ha p_1 d'indistingibles, p_2 d'indistingibles,..., p_r d'indistingibles amb $p_1 + p_2 + \dots + p_r = n$ aleshores, quan els permutem, tenim les permutacions amb repetició de n objectes amb $p_1, p_2, \dots, p_r$ de repetits. El nombre de $PR_n^{p_1, \dots, p_r}$ és:

$$PR_n^{p_1, \dots, p_r} = \frac{n!}{p_1! \dots p_r!}$$

Exemple 1: Amb les lletres de la paraula "CASA". Quantes ordenacions diferents podem escriure?

Per saber quines són aquestes ordenacions construirem un diagrama d'arbre:



Fixem-nos que ens surten les següents possibilitats: 12

Això respon a l'expressió: $PR_4^{2,1,1} = \frac{4!}{2!} = \frac{4 \cdot 3 \cdot 2 \cdot 1}{2 \cdot 1} = 12$

5.1.3 Variacions de n elements agafats de p en p : $V_{n,p}$

Suposem que tenim n objectes però només disposem de p caselles, $p \leq n$. Cada una de les diferents maneres de col·locar p dels n objectes sense repetir-ne cap, en les p caselles s'anomena variació de n elements agafats de p en p . Dues variacions amb els mateixos objectes però col·locats de maneres diferents, són diferents.

Com abans, és clar que el nombre de $V_{n,p}$ de variacions de n elements agafats de p en p és:

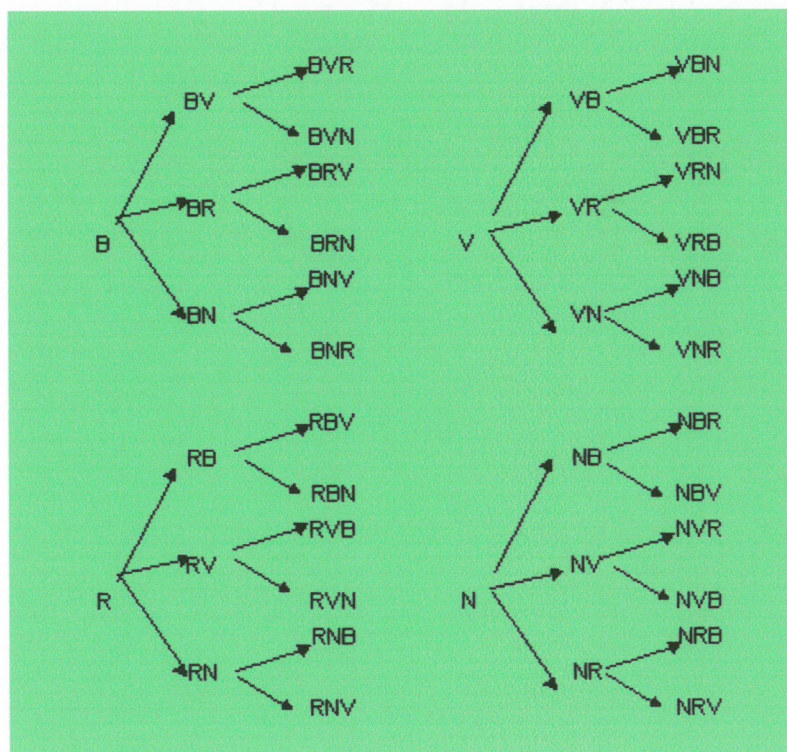
$$V_{n,p} = n(n-1) \cdots (n-p+1) = n! / (n-p)!$$

És clar que $V_{n,n} = P_n$ i $V_{n,0} = 1$, atès que $0! = 1$.

Exemple 1: Ens interessa saber quantes i quines banderes tricolors es poden formar amb els colors: { blau, verd, rosa, negre }

Per saber quantes utilitzarem la fórmula anterior: $V_{4,3} = 4 \cdot 3 \cdot 2 = 24$

Per saber quines utilitzarem el diagrama d'arbre :



5.1.4 Variacions amb repeticions de n elements agafats de p en p : $VR_{n,p}$

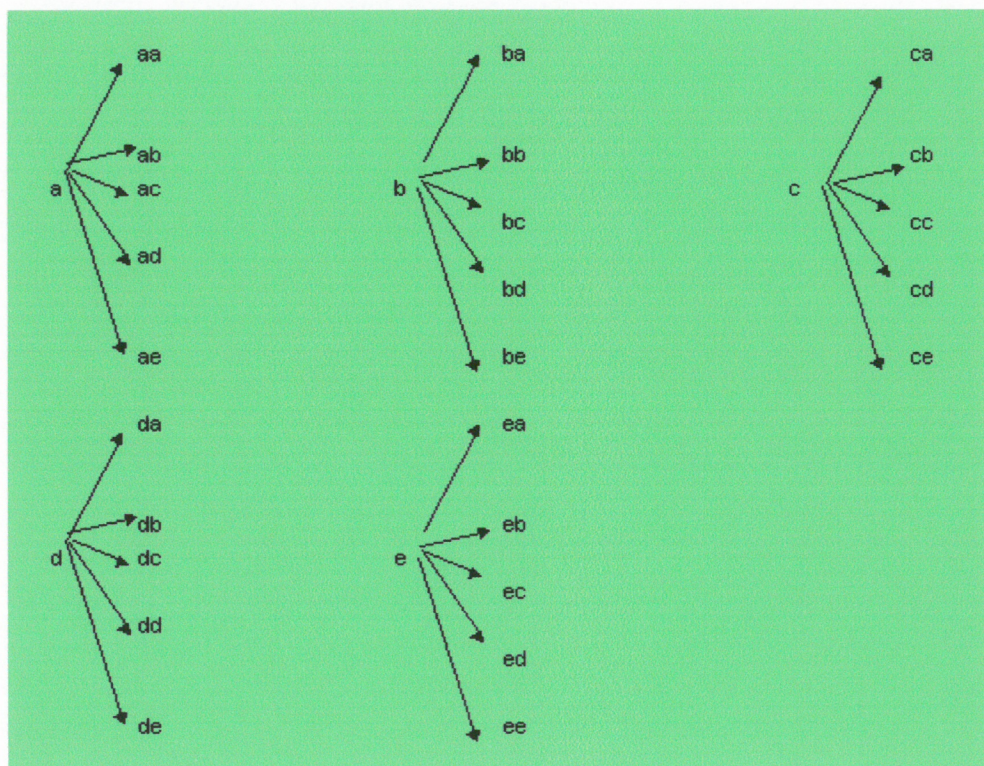
Suposem que tenim n objectes però només disposem de p caselles. Cada una de les diferents maneres de col·locar p dels n objectes podent-se repetir, en les p cel·les s'anomena variació amb repetició de n elements agafats de p en p . Dues variacions amb repetició amb els mateixos objectes però col·locats de maneres diferents, són diferents. Observem que en aquest cas p pot ser més gran igual o més petit que n , ja que es poden repetir elements.

El nombre de variacions amb repetició de n elements agafats de p en p és:

$$VR_{n,p} = n^p$$

Exemple: Volem saber quants i quins grups de dos elements es poden formar amb els elements del conjunt: $\{a, b, c, d, e\}$, si en els grups hi poden haver elements repetits.

Per saber quins construirem un diagrama d'arbre:



En aquest diagrama veiem que de cada un dels 5 elements originals surten 5 fletxes, per tant es poden formar : 5.5 grups de dos elements. Per tant, el nombre total de possibilitats serà: $VR_{5,2} = 5^2 = 25$

5.1.5 Combinacions de n elements agafats de p en p : $C_{n,p}$

Una combinació de n elements agafats de p en p , consisteix en agafar p elements dels n donats. És evident que $p \leq n$.

Això fa que dues variacions de n objectes agafats de p en p , amb els mateixos p elements, però col·locats de manera diferent, donin la mateixa combinació. I de variacions diferents que donen una mateixa variació n'hi ha exactament $p!$ Per tant:

$$C_{n,p} = \binom{n}{p} = \frac{1}{p!} \cdot V_{n,p} = \frac{n!}{p! \cdot (n-p)!}$$

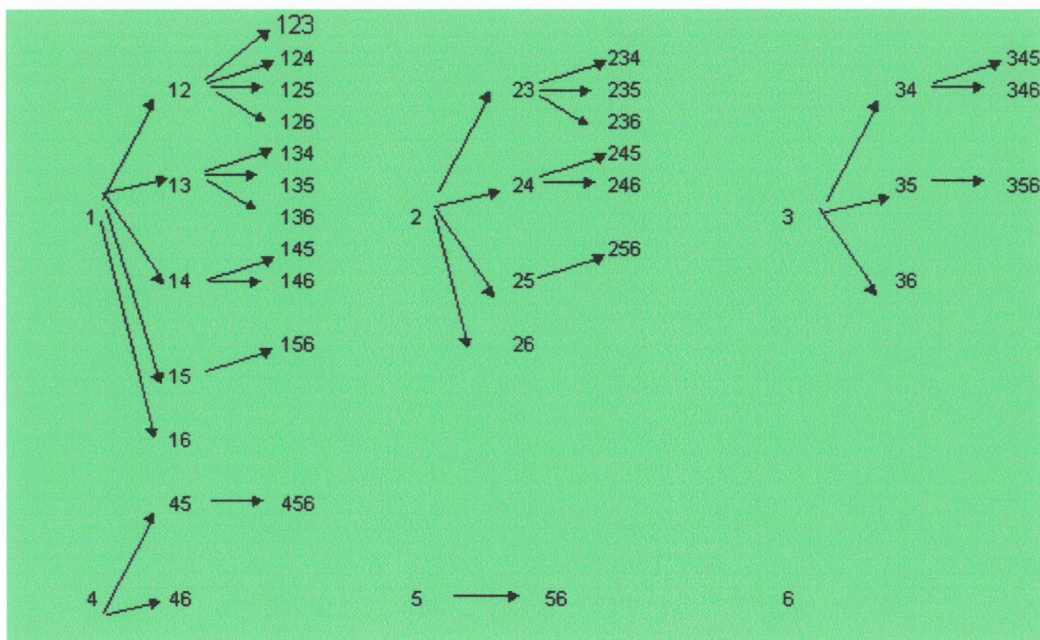
Nota: Els nombres $\binom{n}{p}$ s'anomenen nombres combinatoris.

Exemple: Una oficina disposa de 3 llocs de treball iguals que pot cobrir amb 6 persones. De quantes i quines maneres pot omplir-los si numerem les persones de l'1 al 6?

Per saber quantes utilitzarem la fórmula anterior: $C_{6,3} = 20$

Per tant, les combinacions possibles seran:

$$C_{6,3} = \binom{6}{3} = \frac{6!}{3! \cdot (6-3)!} = \frac{6 \cdot 5 \cdot 4 \cdot 3!}{3! \cdot 3!} = \frac{6 \cdot 5 \cdot 4}{3 \cdot 2} = 5 \cdot 4 = 20$$



5.2 APLICACIÓ

5.2.1 Concepte d'aplicació

Donats dos conjunts A i B, s'anomena aplicació entre A i B a tota relació entre A i B tal que, tot element del conjunt d'A té una i només una imatge en el conjunt B.

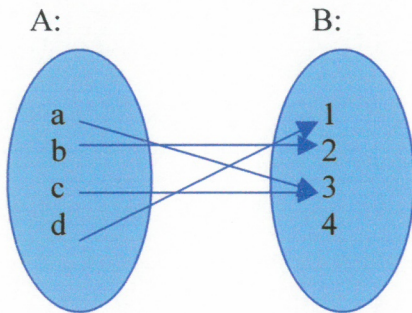


Figura 1

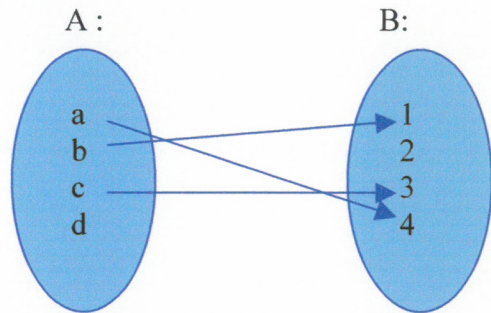


Figura 2

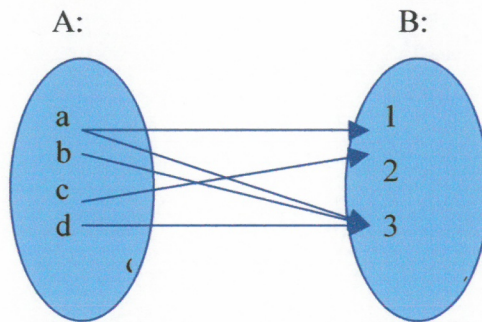


Figura 3

Figura 1 : Aquesta relació és una aplicació.

Figura 2: Aquesta relació no és una aplicació perquè l'element d no té cap imatge en el conjunt B.

Figura 3: Aquesta relació no és una aplicació perquè l'element a té dues imatges en el conjunt B.

Tipus d'aplicacions:

Aplicació injectiva: És una aplicació en la que els elements del conjunt B estan relacionats com a màxim amb un element del conjunt A.

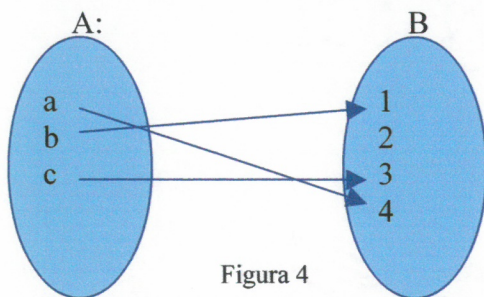


Figura 4

Figura 4: Aquesta aplicació és una aplicació injectiva.

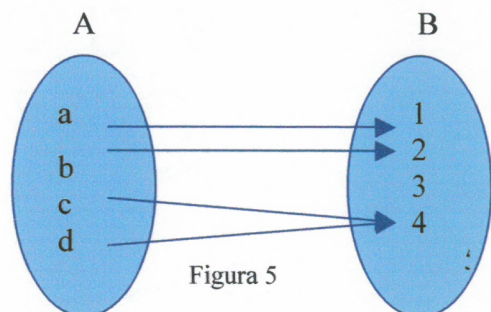


Figura 5

Figura 5: Aquesta aplicació no és una aplicació injectiva perquè l'element (5) del conjunt B està relacionat amb 2 elements (c i d) del conjunt B.

Aplicació exhaustiva: És una aplicació en la que tots els elements del conjunt B han d'estar relacionats com a mínim amb un element del conjunt A.

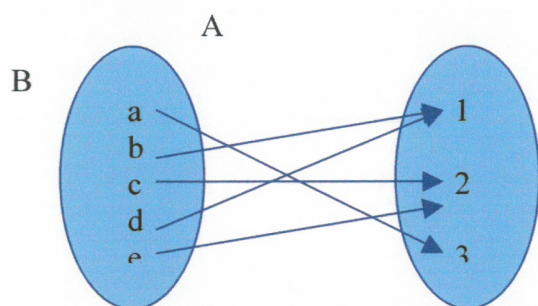


Figura 6

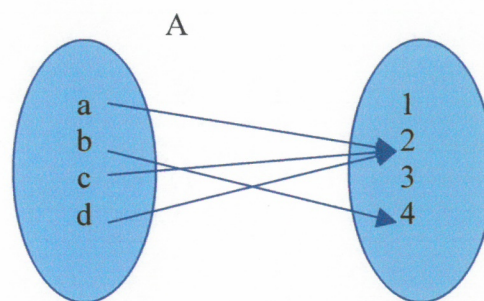


Figura 7

Figura 6: Aquesta aplicació és una aplicació exhaustiva.

Figura 7: Aquesta aplicació no és una aplicació exhaustiva perquè hi ha dos elements del conjunt B (1 i 3) que no estan relacionats amb cap element del conjunt A.

Aplicació bijectiva: És una aplicació en la que tots els elements del conjunt B estan relacionats una vegada i només una, amb els elements del conjunt A. Per tant, perquè una aplicació sigui bijectiva, és condició necessària, però no suficient, que el conjunt A i el conjunt B tinguin el mateix nombre d'elements. També es pot dir que una aplicació és bijectiva si és a la vegada injectiva i exhaustiva.

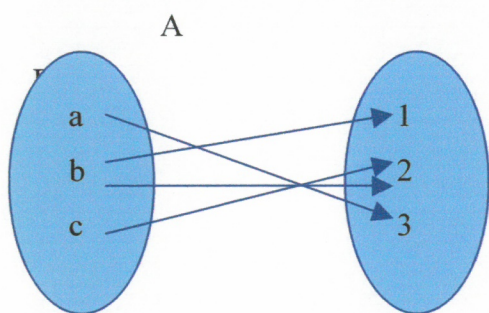


Figura 8

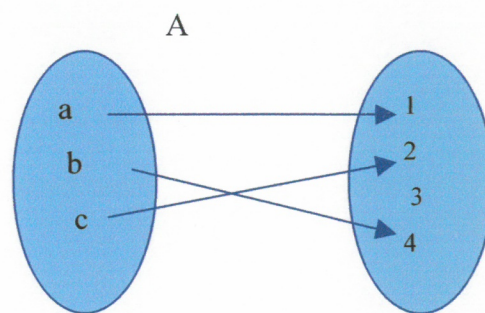


Figura 9

Figura 8: Aquesta aplicació és una aplicació bijectiva.

Figura 9: Aquesta aplicació no és una aplicació bijectiva perquè no tenen el mateix nombre d'elements (el conjunt A té 3 elements i conjunt B té 4 elements).

Aplicació Inversa: Si f és una aplicació bijectiva entre els conjunts A i B , es pot definir l'aplicació inversa de f que es representarà f^{-1} com una aplicació entre els conjunts B i A .

5.3 FUNCIO

Anomenem funció real de variable real a l'aplicació entre un subconjunt dels nombres reals (domini de la funció) en el conjunt dels nombres reals.

5.3.1 Funció polinòmica

Una funció és polinòmica si està definida de la forma:

$$f(x) = a_n x^n + a_{n-1} x^{n-1} + \dots + a_2 x^2 + a_1 x + a_0$$

On $a_n, a_{n-1}, \dots, a_1, a_0 \in \mathbb{R}$ i $n \in \mathbb{N}$.

Si $n = 1$, s'obté la funció polinòmica de primer grau: $f(x) = ax + b$, que s'anomena **funció afi**. La seva representació gràfica és una recta.

a s'anomena pendent de la recta (angle que forma la recta amb el semieix positiu d'abscisses).

b s'anomena ordenada a l'origen (punt de tall de la recta amb l'eix d'ordenades).

5.3.2 Funció exponencial

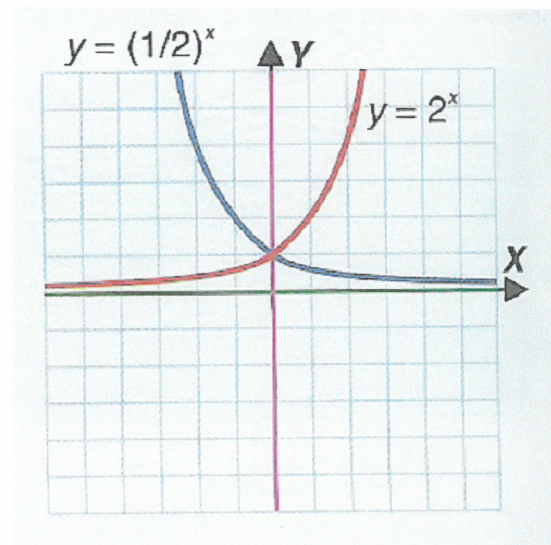
Una funció és exponencial si està definida de la següent forma:

$$f(x) = a^x$$

On $a \in \mathbb{R}^+$ i $a \neq 1$

Les característiques generals de les funcions exponencials són:

- El seu domini és el conjunt dels nombres reals.
- El seu recorregut és el conjunt dels nombres reals positius.
- És contínua.



- L'eix d'abscisses és una asímptota horitzontal
- No talla l'eix d'abscisses. Talla l'eix d'ordenades en el punt (0,1).
- Si $a > 1$, la funció és creixent, i si $0 < a < 1$, és decreixent.
- És sempre còncava.
- La inversa de la funció exponencial és la funció logarítmica

5.3.3 Funció logarítmica

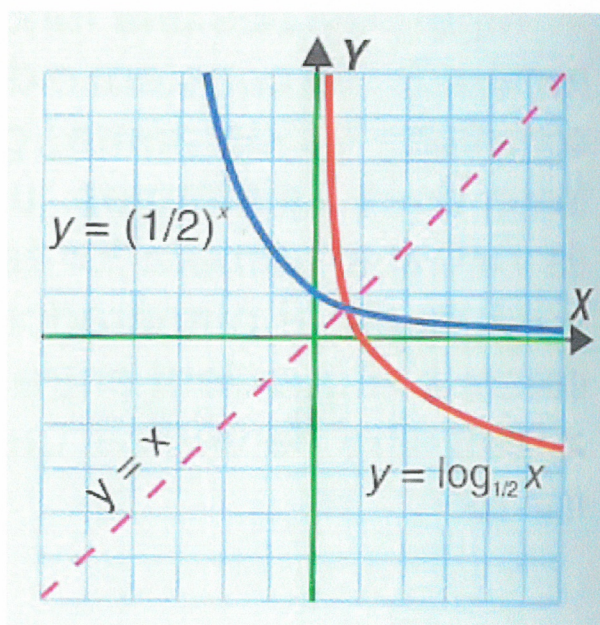
Una funció és logarítmica si esta definida de la següent forma:

$$f(x) = \log_a \text{ de } x$$

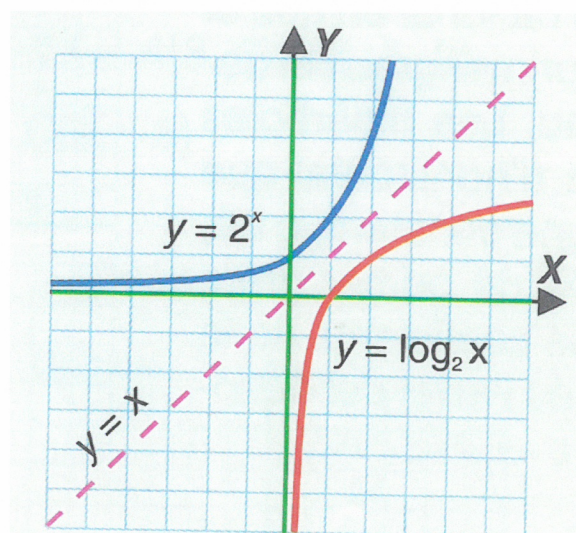
$$\text{On } a \in \mathbb{R}^+ \text{ i } a \neq 1$$

Les característiques generals de la funció logarítmica són:

- El seu domini és el conjunt dels nombres reals positius.
- El seu recorregut és el conjunt dels nombres reals.
- És contínua.
- L'eix d'ordenades és una asímptota vertical.
- No talla l'eix d'ordenades. Talla l'eix d'abscisses en el punt (1,0).
- Si $a > 1$, la funció és creixent, i si $0 < a < 1$, és decreixent.
- Si $a > 1$, és convexa i si $0 < a < 1$, és còncava.



Les gràfiques d'una funció exponencial i la de la seva logarítmica corresponent, són simètriques respecte de la bisectriu del primer i tercer quadrants.



5.4 ÀLGEBRA LINEAL

5.4.1 Concepte de matriu

Fa més de vint-i-un segles, es va publicar a la China el llibre: *Nou capítols sobre l'art de les matemàtiques*. En el capítol vuitè es resolen problemes d'equacions lineals (fins i tot, de 4 equacions amb 5 incògnites) i els resolen amb matrius que les consideren com capses numèriques en les quals es resumeix una informació estructurada. D'aquesta manera les van utilitzar ocasionalment al llarg de la història molts matemàtics.

No obstant això, el seu tractament sistemàtic, va tenir lloc al segle XIX. Van destacar com artífexs del seu desenvolupament Hamilton (1805-1865), Sylvester (1814-1897) i sobretot, Arthur Cayley (1821-1895). Els estudis d'aquest últim, per descriure les transformacions geomètriques van donar lloc a les operacions amb matrius. Es va arribar així a l'àlgebra matricial, en la qual les matrius passen de ser elements aïllats a conjunts amb una sòlida estructura algebraica.

Direm doncs, que una **matriu** és una taula de nombres col·locats en files i columnes. Les representarem incloent les dades entre uns parèntesis grans.

Les files són horitzontals i les columnes verticals. El primer índex indica la fila i el segon la columna.

Direm que una matriu és de *dimensió* $n \times p$ quan té n files i p columnes:

$$A = (a_{ij})_{n \times p} = \begin{pmatrix} a_{11} & a_{12} & \dots & a_{1p} \\ a_{21} & a_{22} & \dots & a_{2p} \\ \dots & \dots & \dots & \dots \\ a_{n1} & a_{n2} & \dots & a_{np} \end{pmatrix}$$

5.4.2 Tipus de matrius

Si $n = p$ es diu que la **matriu és quadrada**.

S'anomena *diagonal principal* d'una matriu a la diagonal que va d'esquerra a dreta i de dalt a baix.

- *Matriu transposada* d'una matriu $A = (a_{ij})_{n \times p}$ és una altra matriu $A^T = (a_{ji})_{p \times n}$ que s'obté en canviar en A les files per les columnes i les columnes per les files. EXEMPLE:

$$A_{3 \times 2} = \begin{pmatrix} 1 & 0 \\ -5 & 3 \\ 4 & -2 \end{pmatrix} \quad A_{2 \times 3}^T = \begin{pmatrix} 1 & -5 & 4 \\ 0 & 3 & -2 \end{pmatrix}$$

- *Matriu amb una sola fila*: **vector fila**
- *Matriu amb una sola columna*: **vector columna**
- *Matriu nul·la*: Tots els elements són **zero**
- *Matriu diagonal*: $a_{ij}=0 \quad \forall i \neq j$
- *Matriu unitat o matriu identitat*: matriu diagonal tal que $a_{ij}=1 \quad \forall i=j$.
- *Menor adjunt d'ordre k d'una matriu*: És qualsevol subconjunt de **k** files i **k** columnes que pertanyi a la matriu, mantenint l'ordre en les files i les columnes.

5.4.3 Operacions amb matrius

En el conjunt de les matrius podem definir les següents operacions:

- *Suma de matrius*: Dos matrius es poden sumar si tenen les mateixes dimensions.
- *Producte d'un nombre per una matriu*: Per multiplicar un nombre per una matriu, es multiplica pel nombre cada terme de la matriu.
- *Producte d'una matriu fila per una matriu columna*: S'obté multiplicant element per element i sumant-ne els resultats.

$$(a_1, a_2, a_3, \dots, a_n) \cdot \begin{pmatrix} b_1 \\ b_2 \\ b_3 \\ \dots \\ b_n \end{pmatrix} = a_1 b_1 + a_2 b_2 + a_3 b_3 + \dots + a_n b_n$$

- *Producte de matrius*: Per poder multiplicar dues matrius, la primera ha de tenir tantes columnes com files té la segona. El resultat de la operació serà una matriu que té tantes files com la primera i tantes columnes com la segona.

$$A_{n \times p} \cdot B_{p \times q} = C_{n \times q}$$

EXEMPLE:

$$\begin{pmatrix} 2 & 3 & 4 \\ 1 & 5 & 6 \\ 3 & 0 & 7 \\ 4 & 1 & 2 \end{pmatrix} \cdot \begin{pmatrix} 7 & 2 \\ 0 & 1 \\ 3 & 5 \end{pmatrix} = \begin{pmatrix} 2 \cdot 7 + 3 \cdot 0 + 4 \cdot 3 & 2 \cdot 2 + 3 \cdot 1 + 4 \cdot 5 \\ 1 \cdot 7 + 5 \cdot 0 + 6 \cdot 3 & 1 \cdot 2 + 5 \cdot 1 + 6 \cdot 5 \\ 3 \cdot 7 + 0 \cdot 0 + 7 \cdot 3 & 3 \cdot 2 + 0 \cdot 1 + 7 \cdot 5 \\ 4 \cdot 7 + 1 \cdot 0 + 2 \cdot 3 & 4 \cdot 2 + 1 \cdot 1 + 2 \cdot 5 \end{pmatrix} = \begin{pmatrix} 26 & 27 \\ 25 & 37 \\ 42 & 41 \\ 34 & 19 \end{pmatrix}$$

5.4.4 Determinants

- És una operació que associa una matriu quadrada amb un escalar. Utilitzarem la següent notació

$$\det(A) = \begin{vmatrix} a_{11} & \cdot & \cdot & \cdot & \cdot & a_{1n} \\ \cdot & \cdot & \cdot & \cdot & \cdot & \cdot \\ \cdot & \cdot & \cdot & \cdot & \cdot & \cdot \\ \cdot & \cdot & \cdot & \cdot & \cdot & \cdot \\ a_{n1} & \cdot & \cdot & \cdot & \cdot & a_{nn} \end{vmatrix} = k$$

- **Determinants de segon ordre**

Donada una matriu de segon ordre:

$$A = \begin{pmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{pmatrix}$$

s'anomena determinant de la matriu el nombre $a_{11} a_{22} - a_{12} a_{21}$, que es

representa per:

$$\begin{vmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{vmatrix}$$

- **Determinants de tercer ordre**

Donada una matriu de tercer ordre:

$$\begin{pmatrix} a_{11} & a_{12} & a_{13} \\ a_{21} & a_{22} & a_{23} \\ a_{31} & a_{32} & a_{33} \end{pmatrix}$$

S'anomena *menor complementari* de qualsevol dels elements, la matriu de segon ordre que s'obté de suprimir a la matriu la seva fila i la seva columna. Es representa el

$$M_{23} = \begin{pmatrix} a_{11} & a_{12} \\ a_{31} & a_{32} \end{pmatrix}$$

menor complementari de l'element a_{ij} per M_{ij} .

S'anomena *adjunt o cofactor* d'un element qualsevol de la matriu el determinant del seu menor complementari afectat de signe positiu o negatiu segons la situació de l'element a la matriu, d'acord amb l'esquema

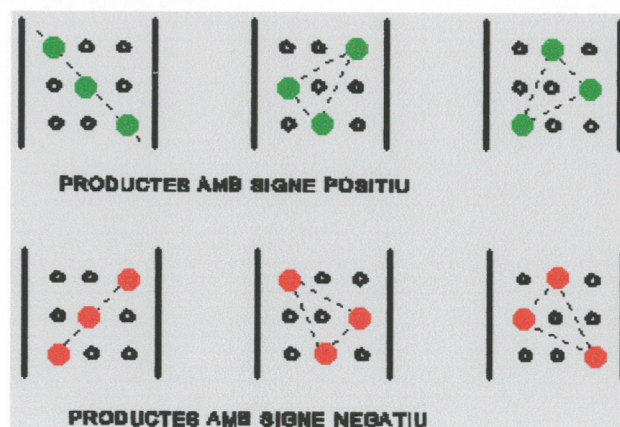
$$\begin{pmatrix} + & - & + \\ - & + & - \\ + & - & + \end{pmatrix}$$

Es representa l'adjunt de l'element a_{ij} per A_{ij} , es pot observar que el signe corresponent a aquest adjunt A_{ij} és positiu si $i+j$ és parell i és negatiu si $i+j$ és senar.

Donada una matriu de tercer ordre s'anomena determinant de tercer ordre el nombre obtingut en sumar el resultat de multiplicar cada element d'una de les seves línies (files o columnes) pel seu adjunt.

$$\begin{vmatrix} 4 & 2 & -3 \\ 5 & 1 & 2 \\ -2 & 4 & 3 \end{vmatrix} = 4 \begin{vmatrix} 1 & 2 \\ 4 & 3 \end{vmatrix} - 5 \begin{vmatrix} 2 & -3 \\ 4 & 3 \end{vmatrix} - 2 \begin{vmatrix} 2 & -3 \\ 1 & 2 \end{vmatrix} = 4(3-8) - 5(6+12) - 2(4+3) =$$

El càlcul d'un determinant de tercer ordre és molt senzill de realitzar amb la **Regla de Sarrus**: el determinant és la suma de la multiplicació de diferents conjunts de tres elements, tal com s'indica a l'esquema.



$$\begin{vmatrix} 4 & 2 & -3 \\ 5 & 1 & 2 \\ -2 & 4 & 3 \end{vmatrix} = [4 \times 1 \times 3] + [(-3) \times 5 \times 4] + [(-2) \times 2 \times 2] - \\ - [(-3) \times 1 \times (-2)] - [4 \times 4 \times 2] - [3 \times 2 \times 5] = -124$$

5.4.5 Matriu inversa

Donada una matriu quadrada A, s'anomena **inversa de A**, a una altra matriu que es representa per A^{-1} i que compleix: $A \cdot A^{-1} = I$

Solament tenen inversa les matrius quadrades el determinant de les quals és diferent de 0.

- Procediment per calcular la matriu inversa utilitzant determinants:

- Es calcula el determinant de la matriu.
- Es forma una nova matriu amb els menors complementaris de cada element.
- Es canvia el signe alternativament per obtenir els adjunts.
- Es transposa la matriu que s'acaba d'obtenir.
- Es divideix cada elements d'aquesta nova matriu pel valor del determinant que s'ha obtingut en el pas a).

La matriu inversa d'A és: $A^{-1} = \frac{1}{|A|} \cdot (Adj(A))^T$

Exemple per calcular la inversa d'una matriu quadrada d'ordre 3.

$$A = \begin{pmatrix} 4 & 5 & -2 \\ 2 & 1 & 1 \\ -3 & 2 & 3 \end{pmatrix}$$

- a) Calcular el determinant de A:

$$|A| = \begin{vmatrix} 4 & 5 & -2 \\ 2 & 1 & 1 \\ -3 & 2 & 3 \end{vmatrix} = (4 \cdot 1 \cdot 3) + (2 \cdot 2 \cdot (-2)) + (5 \cdot 1 \cdot (-3)) - ((-3) \cdot 1 \cdot (-2)) - (4 \cdot 1 \cdot 2) - (5 \cdot 3 \cdot 2) = 12 + (-8) + (-15) - 6 - 8 - 30$$

11 Com que el determinant és diferent de 0, ja podem calcular la seva inversa:

b i c) Calculem:

$$Adj(A) = \begin{pmatrix} \begin{vmatrix} 1 & 1 \\ 2 & 3 \end{vmatrix} & -\begin{vmatrix} 2 & 1 \\ -3 & 3 \end{vmatrix} & \begin{vmatrix} 2 & 1 \\ -3 & 2 \end{vmatrix} \\ -\begin{vmatrix} 5 & -2 \\ 2 & 3 \end{vmatrix} & \begin{vmatrix} 4 & -2 \\ -3 & 3 \end{vmatrix} & -\begin{vmatrix} 4 & 5 \\ -3 & 2 \end{vmatrix} \\ \begin{vmatrix} 5 & -2 \\ 1 & 1 \end{vmatrix} & -\begin{vmatrix} 4 & -2 \\ 2 & 1 \end{vmatrix} & \begin{vmatrix} 4 & 5 \\ 2 & 1 \end{vmatrix} \end{pmatrix} = \begin{pmatrix} 1 & -9 & 7 \\ -19 & 18 & -23 \\ 7 & -8 & -6 \end{pmatrix}$$

d) Calculem $(Adj(A))^T$

$$(Adj(A))^T = \begin{pmatrix} 1 & -19 & 7 \\ -9 & 18 & -8 \\ 7 & -23 & -6 \end{pmatrix}$$

La inversa d'aquesta matriu serà doncs: $A^{-1} = \frac{1}{|A|} \cdot (Adj(A))^T$

$$A^{-1} = \frac{1}{-55} \cdot \begin{pmatrix} 1 & -19 & 7 \\ -9 & 18 & -8 \\ 7 & -23 & -6 \end{pmatrix}$$

5.5 TEORIA DE NOMBRES

5.5.1 Sistema de numeració binari

El sistema de numeració binari, és un sistema de numeració posicional on totes les quantitats es representen utilitzen com a base el nombre 2, per tant, només disposem de dues xifres: el 0 i l'1.

Els ordinadors treballen internament amb dos nivells de voltatge, el seu sistema de numeració, és doncs, el binari (encès 1 i apagat 0).

Conversió de Binari a Decimal:

Qualsevol nombre binari es pot convertir amb el seu equivalent en el sistema de numeració decimal (sistema en base 10).

Exemple: 111011_2

$$1 \cdot 2^5 + 1 \cdot 2^4 + 1 \cdot 2^3 + 0 \cdot 2^2 + 1 \cdot 2 + 1 = 69_{10}$$

Conversió de Decimal a Binari:

Existeixen dues maneres de transformar un nombre enter escrit en base 10 a base 2. Un mètode és l'invers del procés descrit anteriorment; el nombre decimal s'expressa com a

suma de potències de 2 i aleshores els uns i els zeros s'escriuen en les seves posicions corresponents.

$$\text{Exemple: } 45_{10} = 32 + 8 + 4 + 1 = 2^5 + 0 \cdot 2^4 + 2^3 + 2^2 + 0 \cdot 2^1 + 2^0 = 101101_2$$

El segon mètode consisteix en dividir successivament el nombre escrit en sistema decimal per 2, fins que el quocient sigui 0. Aleshores el nombre escrit en sistema binari estarà format pels residus de les divisions successives, tenint en compte que el primer dígit serà l'últim residu, i així successivament.

Exemple:

174	2								
0	87	2							
	1	43	2						
		1	21	2					
			1	10	2				
				0	5	2			
					1	2	2		
						0	1	2	
							1	0	

$$174_{10} = 10101110_2$$

5.5.2 Nombres Primers

Un nombre natural es diu que és primer quan només té dos divisors (1 i ell mateix). Quan té més de dos divisors es diu que és compost. El nombre 1 no és ni primer ni compost; es diu que és una unitat.

El nom de primer, ve suggerit pel següent problema, que per la seva importància s'anomena:

TEOREMA FONAMENTAL: Tot nombre natural compost, es descompon de manera única en producte de factors primers.

Si n descompon en factors primers de manera que: $n = p_1^{a_1} \cdot p_2^{a_2} \cdot \dots \cdot p_r^{a_r}$ amb p_i , ($i = 1, 2, \dots, r$) nombres primers diferents. Es compleix que:

Nombre de divisors de n serà: $d(n) = (a_1+1) \cdot (a_2+1) \cdots (a_r+1)$.

La suma de tots aquests divisors serà: $s(n) = \frac{p_1^{a_1+1}-1}{p_1-1} \cdot \frac{p_2^{a_2+1}-1}{p_2-1} \cdots \frac{p_r^{a_r+1}-1}{p_r-1}$

Si el nombre de primers fos finit, evidentment no caldria ni plantejar-se el problema de la factorització d'un nombre enter en producte de nombres primers, ja que ni hauria prou en comprovar si el candidat és a la llista o no de nombres primers. Però aquesta no és la situació ja que es coneix que existeixen infinits nombres primers. La primera demostració d'aquest fet la va donar el gran matemàtic Euclides. Una altra demostració ben diferent a la de Euclides la va donar Euler, i en aquesta demostració ens mostra una relació entre l'aritmètica i l'anàlisi.

Tenint en compte que molts mètodes de xifrat i de desxifrat es basen en la factorització de nombres molt grans en producte de primers, es podria pensar que és fàcil fer un algoritme que prenent com a entrada un enter $n > 1$, proporcioni com a sortida la factorització de n com a producte de potències de nombres primers. Si el nombre d'entrada n és



un nombre primer, cap de les divisions fetes dona exacte i la sortida és el mateix nombre n . Però es cometria un greu error si es penses que aquesta és la única manera de determinar si un nombre és primer i que, per tant, la complexitat computacional per determinar la primalitat d'un nombre n és idèntica a la de factoritzar la del mateix nombre.

Hi ha molts mètodes deterministes (certificats) i probabilístics (tests) per esbrinar la primalitat d'un nombre enter $n > 1$. Els mètodes deterministes es basen en condicions necessàries i suficients sobre un nombre n perquè sigui primer. Els mètodes probabilístics es basen en condicions necessàries i en la probabilitat que un nombre senar compost les

pugui satisfer. Així, s'aconsegueixen algorismes que permeten determinar de manera efectiva la primalitat de nombres grans.

Ambdós mètodes tenen un grau de dificultat que sobrepassen els nivells matemàtics d'un estudiant de 2n de batxillerat, de tota manera es vol deixar constància de la seva existència.

Per acabar, es vol esmentar que el *garbell d'Erastotenes* és un mètode que requereix molta memòria, que no requereix operacions, ni productes ni divisions, convé fer-lo servir per generar una taula de primers petits que s'emmagatzemen i s'utilitza com a pas previ de qualsevol test de primalitat. Per exemple, per veure si $n < 10^6$ és primer, només cal veure si és divisible per algun primer més petit que 10^3 i, com a molt fer 168 divisions.

5.5.3 Màxim comú divisor de nombres naturals. Algoritme d'Euclides

El màxim comú divisor de dos nombres naturals a i b és el nombre natural d que divideix a i b i que tot altre divisor de a i b el divideix. S'indica per m.c.d. (a , b). Si $d = 1$ es diu que els dos nombres són primers entre si o primers entre ells.

Algoritme d'Euclides: Per tal de determinar el m.c.d. de dos nombres naturals cal tenir en compte que es disposa d'un algorisme molt útil que només fa ús de la divisió entera.

Siguin a i b dos nombres naturals, $a > b$. La divisió entera de a per b dona dos nombres q_1, r_1 que compleixen $a = bq_1 + r_1$, $r_1 < b$. Dividint b per r_1 tindrem $b = r_1q_2 + r_2$ amb $r_2 < r_1$; dividint r_1 per r_2 serà $r_1 = r_2q_3 + r_3$ amb $r_3 < r_2$. Seguint aquest procés, com que els residus formen una successió de nombres naturals decreixent, s'arribarà a un residu 0. L'últim residu no nul obtingut és el màxim comú divisor de a i b .

Per facilitar el càlcul, s'acostumen a posar els diversos nombres que intervenen a l'algorisme en la següent forma:

	q_1	q_2	...	q_{k+1}	q_{k+2}	q_{k+3}
a	b	r_1	...	r_k	r_{k+1}	r_{k+2}
r_1	r_2	r_3	...	r_{k+2}	0	

$$\text{m.c.d.}(a, b) = r_{k+2}$$

Algoritme d'Euclides estès (Identitat de Bézout):

Sigui a i b dos nombres enters tal que el m.c.d. (a i b) = d .

En aquest cas sempre existiran dos nombres enters r i s , tals que :

$$d = a \cdot r + b \cdot s$$

L'algorisme d'Euclides estès ens permet donats dos nombres enters, calcular el seu m.c.d. i els dos nombres enters r i s .

EXEMPLE: Donats els nombres enters 1547 i 560, trobar el seu màxim comú divisor i trobar els nombres enters r i s que fan certa la igualtat:

$$1547 \cdot r + 560 \cdot s = \text{mcd}(1547, 560)$$

Aplicant l'algorisme d' Euclides es trobarà el màxim comú divisor:

	2	1	3	4	1	3
1547	560	427	133	28	21	7
427	133	28	21	7	0	

Per tant, el m.c.d. $(1547, 560) = 7$

Si escrivim els resultats parcials, quedarà:

$$7 = 28 - 1 \cdot 21$$

$$133 = 560 - 1 \cdot 427$$

$$21 = 133 - 4 \cdot 28$$

$$427 = 1547 - 2 \cdot 560$$

$$28 = 427 - 3 \cdot 133$$

I fent les successives substitucions, es trobaran els valors r i s :

$$\begin{aligned} 7 &= 28 - 1 \cdot 21 = 28 - 1 (133 - 4 \cdot 28) = 5 \cdot 28 - 1 \cdot 133 = 5 \cdot (427 - 3 \cdot 133) - 1 \cdot 133 = \\ &= 5 \cdot 427 - 16 \cdot 133 = 427 - 16 (560 - 1 \cdot 427) = 21 \cdot 427 - 16 \cdot 560 = 21 (1547 - 2 \cdot 560) - 16 \cdot 560 \\ &= 21 \cdot 1547 - 58 \cdot 560. \end{aligned}$$

D'aquí es dedueix que $r = 21$ i $s = -58$.

Aquest algorisme s'ha utilitzat per fer l'invers modular en el sistema RSA.

5.5.4 Nombres Congruents

Tota la teoria de congruències va ser estudiada de forma sistemàtica per Carl Friederich Gauss a finals del s.XIX i s'aplica en teoria de nombres, àlgebra extracta, criptografia i en arts visuals i musicals.

Les operacions aritmètiques que avui en dia fan la majoria de les computadores són aritmètiques modulars.

Dos nombres enters a i b són congruents segons el mòdul m ($m > 1$) quan donen el mateix residu en dividir-los per m . S'escriu:

$$a \equiv b \pmod{m}$$

També es pot definir que dos nombres enters a i b són congruents segons el mòdul m quan la diferència $a-b$ és múltiple de m .

Propietats de les Congruències:

- 1) Si $a \equiv b \pmod{m}$ i $c \equiv d \pmod{m}$, llavors $a + c \equiv b + d \pmod{m}$.
- 2) Si $a \equiv b \pmod{m}$ i c és un enter qualsevol, llavors $ca \equiv cb \pmod{m}$.
- 3) Si $a \equiv b \pmod{m}$ i $c \equiv d \pmod{m}$, llavors $ac \equiv bd \pmod{m}$.
- 4) Si $a \equiv b \pmod{m}$ i d divideix m , llavors $a \equiv b \pmod{d}$.
- 5) Si $ca \equiv cb \pmod{m}$ i $\text{mcd}(c, m) = 1$, llavors $a \equiv b \pmod{m}$.

Si es té sempre present que s'està treballant sempre amb aritmètica d'enters, es pot manipular les congruències gairebé com equacions ja que tenint en compte les propietats anteriors sempre es pot sumar o multiplicar un nombre als dos costats de la congruència i, suma o multiplicar dues congruències tal com es fa amb les equacions.

És fàcil trobar tots els enters que són congruents $\pmod{m}$ a un enter donat, ja que tots ells compleixen la condició que tenen el mateix residu quan es divideixen per n . Per exemple tots els enters congruents amb $15 \pmod{4}$ són 15, 19, 23, 27..., i també 13, 7, 3, -1, -3... Tots aquests enters comparteixen el mateix residu quan els dividim per 4. Es pot veure que la llista de tots els enters congruents amb $A \pmod{m}$ sempre hi ha un enter que està entre 0 i $m-1$ (en aquest exemple el 3). Aquest enter és, justament, la resta de la divisió entre A i m . Quan s'escriu l'expressió $A \pmod{m}$, s'entén que ens estem referint a aquesta resta. Per exemple, $39 \pmod{4} = 3$, $40 \pmod{4} = 0$, i $41 \pmod{4} = 1$.

Definim doncs el *conjunt de residus d'ordre m* , com el conjunt dels enters entre 0 i $m-1$: $\mathbb{Z}/m = \{0, 1, \dots, m-1\}$ amb un parell d'operacions, suma i producte (modulars) definides a $\mathbb{Z}/m$. Aquestes dues operacions són *operacions internes*, això vol dir que la suma i el producte de dos elements de $\mathbb{Z}/m$ també és un element de $\mathbb{Z}/m$.

5.5.5 Funció φ d'Euler

La funció φ d'Euler d'un nombre enter positiu n es representarà per: $\varphi(n)$ i es definirà com: el nombre d'enters entre 1 i $n-1$ (ambdós inclosos) que són coprimers¹⁵ amb n és a dir:

$$\varphi(n) = |\{1 \leq k < n : m.c.d.(k, n) = 1\}|$$

¹⁶

Propietats de la funció $\varphi(n)$.

- $\varphi(1) = 1$.
- Per a p primer, $\varphi(p) = p-1$.
- Per a $n = p \cdot q$ amb p i q primers:

$$\varphi(n) = \varphi(p) \cdot \varphi(q) = (p-1) \cdot (q-1).$$
- Si $m.c.d.(a, m) = 1$, llavors $a^{\varphi(m)} \equiv 1 \pmod{m}$



EXEMPLE: $\varphi(10) = 4$ perquè hi ha quatre elements que són a $\{1, \dots, 9\}$ que són coprimers amb 10; concretament són l'1, el 3, el 7 i el 9.

Com a conseqüència de les propietats que compleix la funció φ d'Euler, es pot deduir el següent resultat: Si p és primer i $a \in \mathbb{Z}$, llavors $a^{p-1} \equiv 1 \pmod{p}$. Aquest resultat es coneix amb el nom de teorema petit de Fermat. Aquest teorema proporciona una condició necessària perquè p sigui primer i s'utilitza sovint com un dels mètodes probabilístics per estudiar la primalitat d'un nombre.

La funció φ d'Euler s'utilitza en criptografia per a desxifrar el missatge en el sistema RSA.

¹⁵ Dos nombres són coprimers si són primers entre ells, també es pot dir que dos nombres són coprimers i el m.c.d. és 1.

¹⁶ S'acaba d'utilitzar l'anotació $|C|$ que indica la mida o el nombre d'elements d'aquest conjunt.

6 PRÀCTIQUES DE XIFRAR I DESXIFRAR MISSATGES

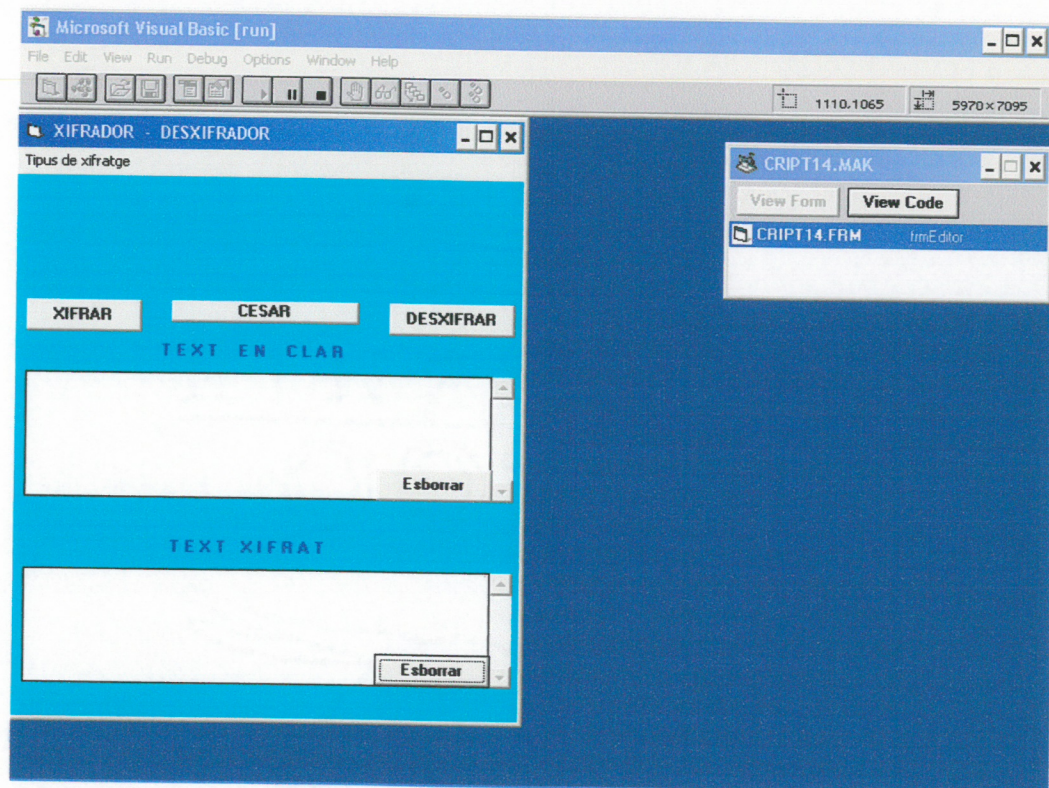
6.1 XIFRAT AMB MÈTODES CLÀSSICS.

6.1.1 Pràctica 1

Pràctica 1.- Elaboració d'un programa en Visual Basic per xifrar o desxifrar missatges segons el mètode de César i segons una permutació dels caràcters de un text.

Inicialment es genera un senzill menú que permet triar entre els dos tipus de xifrat i que en el cas del xifrat de César permet escollir el desplaçament de les lletres segons una llista de 1 fins a 26, i en el cas de permutació obra una finestra de text on s'introdueix una paraula o frase clau que genera una permutació de igual longitud a la clau introduïda i que s'anirà repetint en el text a xifrar (la raó de fer la permutació segons una clau es per facilitar la memorització, la transferència a qui hagi de tenir accés a ella i evitar errors en la seva aplicació).

A continuació es dissenya l'entorn on hi figuren: el quadre combinat per escollir el desplaçament (amagat), l'etiqueta i el quadre de text per introduir la clau (també amagats), els botons per xifrar i desxifrar, una etiqueta on es mostra el tipus de xifrat en ús, i els dos quadres de text per introduir i mostrar el text en clar i el text xifrat amb els corresponents botons d'esborrat (veure figura).



Després es programen les diferents accions:

- Les associades a les opcions de menú.
 - Les accions disponibles a qualsevol punt del programa com a subrutines.
 - Les associades a cada un dels objectes de la finestra del programa i que responen a interaccions amb aquests objectes.
- En primer lloc es declaren la major part de les variables

```
C:\ARCHIV~1\VBASIC\WB\SCRIPT15.FRM
Object: [general] Proc: [declarations]
Option Explicit

Dim d As Integer      'd es el desplaçament
Dim i As Integer
Dim j As Integer      'i,j,k són índexs de bucles
Dim k As Integer
Dim n As Integer      'n és nombre
Dim t As Integer      't és el tipus de xifratge

Dim nc As Integer     'nc és el nombre de caràcters que es permuten
Dim pp(20) As Integer 'pp és posició de permutació
Dim pi(20) As Integer 'pi és posició d'inversa
Dim lls(52) As Integer 'lls és la llista de substitució

Dim cado As String    'Cado és la cadena Original
Dim cadx As String     'Cadx és la cadena xifrada
```

- Després s'associa a les opcions de tipus de xifrat del menú, la variable numèrica t, que segons el valor que pren permet desviar la programació; i s'amaguen o es presenten els objectes relacionats amb cada una d'elles.

```
C:\ARCHIV~1\VBASIC\WB\SCRIPT15.FRM
Object: mnuCes Proc: Click

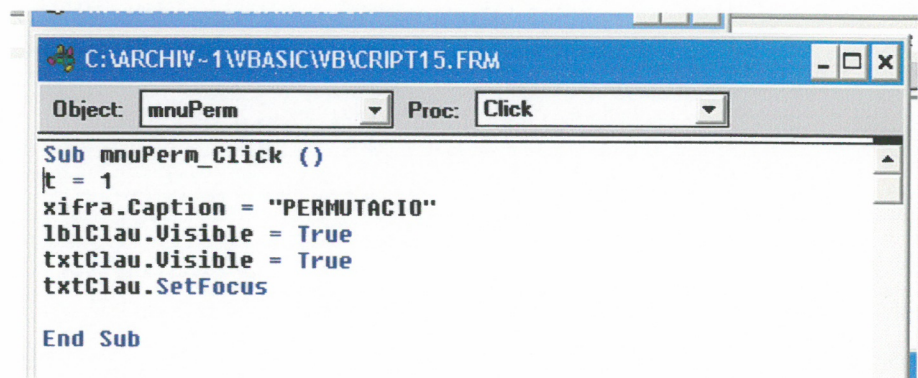
Sub mnuCes_Click ()

    t = 0
    xifra.Caption = "CESAR"
    lblClau.Visible = False
    txtClau.Visible = False

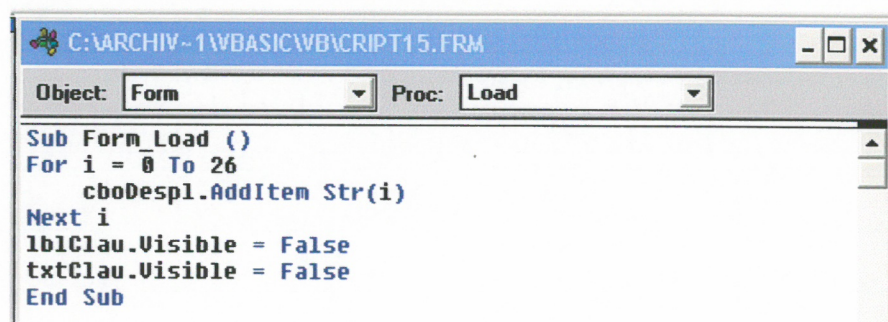
End Sub
```

```
C:\ARCHIV~1\VBASIC\WB\SCRIPT15.FRM
Object: mnuCesDesp Proc: Click

Sub mnuCesDesp_Click ()
    cboDespl.Visible = True
End Sub
```

- Les etiquetes i els quadres de text no tenen cap programació associada.
- Al carregar la finestra es generen els items del quadre combinat per escollir el desplaçament de Cesar i s'amaguen l'etiqueta i el quadre de text de la clau de permutació.



- La programació dels botons de xifrat i desxifrat incorporen el xifrat de César però el de permutació es desvia cap a les subrutines.

```

C:\ARCHIV-1\WBASIC\WB\SCRIPT15.FRM
Object: cmdXif Proc: Click

Sub cmdXif_Click ()
    Dim cado As String
    txtCodificat.Text = ""
    Dim l, b, m, modul As Integer
    Dim lletra As String

    txtCodificat.Enabled = True

    Select Case t
        Case 0
            l = Len(txtOriginal.Text)
            d = cboDespl.ListIndex
            For m = 1 To l
                lletra = Mid(txtOriginal.Text, m, 1)
                Select Case Asc(lletra)
                    Case 48 To 57
                        modul = 48 + (Asc(lletra) + 2 + d) Mod 10
                    Case 65 To 90
                        modul = 65 + (Asc(lletra) + 13 + d) Mod 26
                    Case 97 To 122
                        modul = 97 + (Asc(lletra) + 7 + d) Mod 26
                    Case Else
                        modul = Asc(lletra)
                End Select
                txtCodificat.Text = txtCodificat.Text & Chr(modul)
            Next m
        Case 1
            cado = txtOriginal.Text
            genera_permu (txtClau.Text)
            Call permuta(Len(txtClau.Text), cado)
        End Select
    End Sub

```

- La selecció dels diferents casos es fa per desplaçar majúscules en majúscules, minúscules en minúscules i nombres en nombres, no transformant la resta de caràcters.
- La programació del desxifrat es fa canviant les finestres de lectura i d'escriptura, i restant el desplaçament en comptes de sumar-lo.


```

C:\ARCHIV-1\VBASIC\VBSCRIPT15.FRM
Object: cmdDesx Proc: Click
Sub cmdDesx_Click ()
|
Dim l, m, modul As Integer
Dim lletra As String
txtOriginal.Text = ""
l = Len(txtCodificat.Text)

Select Case t
    Case 0
        d = cboDespl.ListIndex
        For m = 1 To l
            lletra = Mid(txtCodificat.Text, m, 1)
            Select Case Asc(lletra)
                Case 48 To 57
                    modul = 48 + (Asc(lletra) + 2 - d) Mod 10
                Case 65 To 90
                    modul = 65 + (Asc(lletra) + 13 - d) Mod 26
                Case 97 To 122
                    modul = 97 + (Asc(lletra) + 7 - d) Mod 26
                Case Else
                    modul = Asc(lletra)
            End Select
            txtOriginal.Text = txtOriginal.Text & Chr(modul)
        Next m
    Case 1
        cadx = txtCodificat.Text
        genera_permu (txtClau.Text)
        Call permuinv(Len(txtClau.Text), cadx)
End Select

End Sub

```

Les rutina de permutació genera_permu ens crea una permutació a partir de la ordenació alfabètica dels caràcters de la clau, utilitzant el mètode de la bombolla, i l'últim bucle crea la permutació inversa per fer el desxifrat.

```

C:\ARCHIV-1\VBASIC\VBSCRIPT15.FRM
Object: [general] Proc: genera_permu
Private Sub genera_permu (clau As String)
|
    ReDim CarPermu(20) As String
    Dim CarCanvi As String
    Dim NumCanvi As Integer
    ' Quan no fa cap canvi és que
    ' les lletres són per ordre alfabètic
    ' i a pp hi ha la posició
    ' que tenien originalment les lletres

    For i = 1 To Len(clau)
        pp(i) = i
        CarPermu(i) = Mid(clau, i, 1)
    Next i

    k = 1
    While k = 1
        k = 0
        For i = 1 To Len(clau) - 1
            If CarPermu(i) > CarPermu(i + 1) Then
                CarCanvi = CarPermu(i)
                NumCanvi = pp(i)
                CarPermu(i) = CarPermu(i + 1)
                pp(i) = pp(i + 1)
                CarPermu(i + 1) = CarCanvi
                pp(i + 1) = NumCanvi
                k = 1
            End If
        Next i
    Wend

    For i = 1 To Len(clau)
        ni/pp(i) = i
    Next i
End Sub

```

- Per últim, les rutines permuta i permuinv són la mateixa fent el canvi de text en clar per text xifrat i utilitzant la permutació inversa en cas de la segona.

C:\ARCHIV~1\VBASIC\WB\SCRIPT15.FRM

Object: [general] Proc: permuta

```
Private Sub permuta (nc, cado)
    Dim NumVegades As Integer

    cadx = cado
    NumVegades = Int(Len(cado) / nc)

    For i = 0 To NumVegades - 1
        For j = 1 To nc
            Mid(cadx, i * nc + pp(j), 1) = Mid(cado, i * nc + j, 1)
        Next j
    Next i

    For j = 1 To Len(cado)
        txtCodificat.Text = txtCodificat.Text & Mid(cadx, j, 1)
    Next j

End Sub
```

C:\ARCHIV~1\VBASIC\WB\SCRIPT15.FRM

Object: [general] Proc: permuinv

```
Private Sub permuinv (nc, cadx)
    Dim NumVegades As Integer

    cado = cadx
    NumVegades = Int(Len(cadx) / nc)

    For i = 0 To NumVegades - 1
        For j = 1 To nc
            Mid(cado, i * nc + pi(j), 1) = Mid(cadx, i * nc + j, 1)
        Next j
    Next i

    For j = 1 To Len(cadx)
        txtOriginal.Text = txtOriginal.Text & Mid(cado, j, 1)
    Next j

End Sub
```


6.2 XIFRAT AMB MÈTODES MODERNS

6.2.1 Pràctica 2

Xifrar i desxifrar una lletra utilitzant l'algoritme de generació de claus de l'RSA., sense fer ús d'eines informàtiques:

En aquest exemple els nombres primers utilitzats són petits, per tal de poder realitzar a mà totes les operacions fet que provoca que la seguretat sigui molt escassa.

Per iniciar la pràctica de xifrat d'una lletra hem de passar la lletra al codi ASCII a partir de la taula d'equivalències següent:

Lletra	Codi ASCII	Equivalència en Decimal
A	1000001	65
B	1000010	66
C	1000011	67
D	1000100	68
E	1000101	69
F	1000110	70
G	1000111	71
H	1001000	72
I	1001001	73
J	1001010	74
K	1001011	75
L	1001100	76
M	1001101	77
N	1001110	78
O	1001111	79
P	1010000	80

Q	1010001	81
R	1010010	82
S	1010011	83
T	1010100	84
U	1010101	85
V	1010110	86
W	1010111	87
X	1011000	88
Y	1011001	89
Z	1011010	90
Taula 1: Només hi ha 26 dels 256 caràcters del codi ASCII		

Els passos que s'han de seguir són els següents:

- 1) Escollir dos nombres primers p i q que constituïran la clau privada. Per l'exemple que ve a continuació, s'ha escollit:

$$p=11 \text{ i } q=13$$

- 2) Es fa públic el resultat de la multiplicació d'aquests dos primers: $N = p \cdot q$ En aquest cas:

$$N = 11 \cdot 13 = 143$$

- 3) Escollir un nombre e de tal manera que $(p-1) \cdot (q-1)$ i e siguin primers entre ells. I que sigui menor que N :

$$e=17$$

- 4) Es fan públics els nombres e i N (clau pública).

- 5) Per la codificació de la lletra, s'ha de convertir la lletra (el missatge en clar) en un nombre **M** (a partir de la transformació en dígit binari ASCII) En cas de voler codificar per exemple la lletra "S" (si anem a la taula d'equivalències 1) podem veure que la "S" $\rightarrow$ 83

$$M=83$$

- 6) M es codifica per donar lloc al missatge xifrat C, segons la formula:

$$C = M^e \pmod{N} \rightarrow C = 83^{17} \pmod{143}$$

- 7) Com que amb una calculadora no es pot fer directament 83^{17} ja que és un nombre molt gran, es divideix el nombre amb: $83^5 \cdot 83^5 \cdot 83^5 \cdot 83^2 \pmod{143}$

- 8) S'opera separatament: $83^5 \pmod{143} = 3939040643 \pmod{143} = 109$
 $83^2 \pmod{143} = 6889 \pmod{143} = 25$

- 9) Després d'haver operat separatament, s'obté que:

$$C = 109^3 \cdot 25 \pmod{143} = 96.$$

Aquest nombre 96 és el codi ASCII de la lletra ja xifrada del missatge (en aquest cas una lletra) que l'emissor envia al receptor.

Una vegada enviat el missatge, per poder desxifrar-lo, el receptor ha de fer ús de la clau privada (p i q):

- 10) Trobar la ϕ de N a partir de la qual es podrà trobar un nombre d, necessari per desxifrar el missatge. La ϕ de N és el resultat del producte de $(q-1) \cdot (p-1)$. En aquest cas:

$$\phi(143) = (11-1) \cdot (13-1) = 10 \cdot 12 = 120$$

- 11) Un cop trobada la ϕ de N, per continuar el procés de desxifrat del missatge, hem de conèixer el valor d, de l'equació: $e \cdot d = 1 \pmod{\phi(N)}$. Com que el receptor coneix els valors de e i de ϕ de N, es pot resoldre a partir de l'algoritme d'Euclides estès: $17d = 1 \pmod{120}$:

$$120 = 17 \cdot 7 + 1$$

$$17 = 1 \cdot 17 + 0$$

	120	17	1
120	(1,0)	-	-
17	-	(0,1)	-
1	(1,0)	-7·(0,1)	(1,-7)

$$1 = 120 \cdot 1 + 17 \cdot (-7)$$

$$1 = 120 + 17 \cdot (120-7)$$

$$1 = 120 + 113 \cdot 17 \rightarrow d = 113$$

$$d = 113$$

En cas que surti un nombre negatiu, per passar-lo a positiu es fa sumant-li el nombre negatiu al mòdul.

En l'exemple anterior, -7 es converteix en $120 - 7 = 113$

12) Una vegada trobat el valor de d, s'aplica la següent formula per trobar el missatge inicial M:

$$M = C^d \pmod{N}$$

$$M = 96^{113} \pmod{143}$$

$$M = ((96^4)^4 \cdot (96^5)^4 \cdot (96^5)^4 \cdot (96^3)^3) \pmod{143}$$

$$M = (92^4)^4 \cdot 109^4 \cdot 109^4 \cdot 138^3 \pmod{143}$$

$$M = 14^4 \cdot 1 \cdot 1 \cdot 18 \pmod{143}$$

$$M = 92 \cdot 1 \cdot 1 \cdot 18 \pmod{143}$$

$$M = 83$$

6.2.2 Pràctica 3

Algoritme d'Euclides estès

En aquesta pràctica s'ha creat un full de càlcul en EXCEL en que figuren no només els successius residus i quocients sinó també l'expressió de cada residu com a combinació lineal dels nombres originals, que proporciona la identitat de Bezout en la fila corresponent al m.c.d. (anterior a la fila de residu zero).

	A	B	C	D	E	F
1						
2	ALGORITME D'EUCLIDES ESTÈS					
3						
4						
5		introduïu un nombre:	46480			
6		un altre:	39423			
7						
8						
9	46480		1	0		
10	39423		0	1		
11	7057	1	1	-1		
12	4138	5	-5	6		
13	2919	1	6	-7		
14	1219	1	-11	13		
15	481	2	28	-33		
16	257	2	-67	79		
17	224	1	95	-112		
18	33	1	-162	191		
19	26	6	1067	-1258		
20	7	1	-1229	1449		
21	5	3	4754	-5605		
22	2	1	-5983	7054		
23	1	2	16720	-19713		
24	0	2	-39423	46480		
25	#DIV/0!	#DIV/0!	#DIV/0!	#DIV/0!		

A la columna A apareixen els residus de la divisió entera dels dos elements immediatament superiors amb la fórmula: **=RESIDUO(A9;A10)**, fins que aquest sigui zero, per tant el residu anterior es el m.c.d. dels dos nombres introduïts.

A la columna B hi figuren els quocients corresponents a les divisions enteres que permeten calcular les columnes posteriors: **=ENTERO(A9/A10)**

A les columnes C i D apareix la corresponent combinació lineal dels dos nombres donats que proporciona cada un dels residus, i que en el cas de la fila del m.c.d. ens proporciona els coeficients de la identitat de Bézout, (fila 23) les fórmules que figuren a les cel·les són: **=C9-C10*B11** i **=D9-D10*B11**

6.2.3 Pràctica 4

Càlcul de potències modulars de grans enters utilitzant el [mètode del quadrat](#).

1. Per fer aquesta pràctica hem fet un full de càlcul amb EXCEL
2. Hem introduït al principi, un títol, una breu explicació i un formulari, sobre el propi full, per la introducció de les tres dades (base de la potència, exponent i l'enter amb el qual s'han de fer les classes de residus (veure **fig.1**).

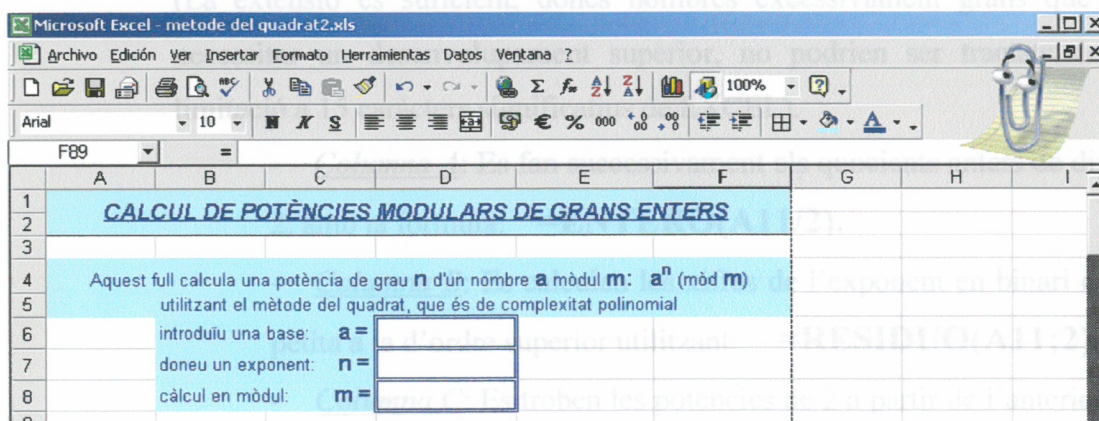


fig. 1

3. A partir de la fila 10 comença pròpiament el full de càlcul.
 - Per fer càlculs mòdul **m** utilitzem la fórmula **RESIDUO(; D\$8)**, on **m** s'anirà a buscar sempre a la cel·la **D8**, ja que el **símbol \$** evita que al copiar les fórmules en la pròpia fila la referència es traslladi a la posició relativa respecte a la cel·la original
 - Les cel·les **A11** i **C11** incorporen respectivament el exponent i la base per iniciar el càlcul, fent referència a les corresponents **D7** i **D6**, i a la cel·la **E10**, que serà la potència zero de la base, i posarem un **1** fix perquè puguem relacionar ja amb ella la cel·la inferior amb la fórmula iterativa.

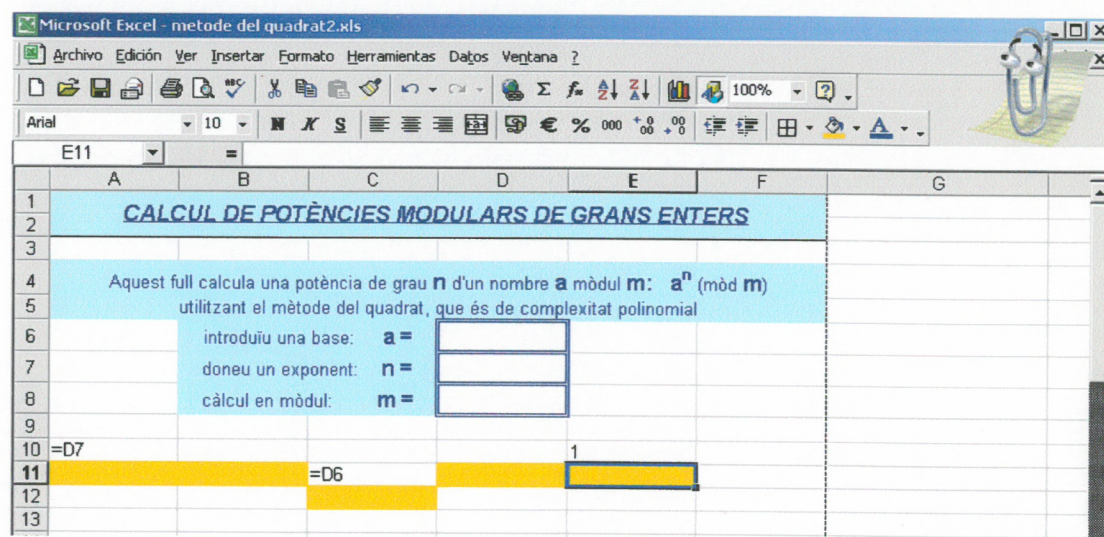


fig 2

4. Fórmules introduïdes a les columnes. Les escriurem a les cel·les que figuren en color daurat en la **fig. 2** i després les copiarem a tota la columna d'aquest full (La extensió és suficient, doncs nombres excessivament grans que podrien necessitar un desenvolupament superior, no podrien ser tractats donada la limitació a 15 caràcters significatius de EXCEL).
 - Columna A: Es fan successivament els quocients enters de dividir per 2, amb la fórmula: **=ENTERO(A11/2)**.
 - Columna B: Es calculen les xifres de l'exponent en binari de la més petita a la d'ordre superior utilitzant: **=RESIDUO(A11;2)**.
 - Columna C: Es troben les potències de 2 a partir de l'anterior, havent fet ja, la seva conversió modular a la columna següent:

$$=SI(A12>0;POTENCIA(D11;2);0)$$

- Columna D: Es fa la conversió modular: $=RESIDUO(C11;D\$8)$

- Columna E: Va calculant els productes modular d'aquestes potencies, en el cas de que el nombre en binari tingui xifra 1, condicionat a que encara hi hagin xifres del binari, doncs sinó la taula continuarà fen càlculs innecessaris i així els aturem

:

$$=SI(A11>0;RESIDUO(E10*POTENCIA(D11;B11);D\$8);0),$$

aquesta multiplicació selectiva es fa elevat a la xifra del binari, amb la qual cosa en cas de que sigui zero, multiplica per una potència de zero que és un 1 i per tant retorna a l'anterior.

6.2.4 Pràctica 5

Xifrar i desxifrar una lletra amb el programa *Derive para Windows*.

- 1) Passar la lletra al sistema decimal, per iniciar el procés amb Derive.
- 2) Obrir el programa “*Derive para Windows*”.
- 3) Arxiu obrir, i en la carpeta Math, obrir l’arxiu que diu Number. Amb aquest arxiu, s’obriran un seguit de funcions de càlcul numèric. Obrir l’arxiu Number Math és imprescindible per fer l’invers modular (pas 10).
- 4) Cada vegada que es vulgui fer qualsevol tipus d’operació (invers modular, trobar un nombre primer molt gran,...) s’haurà d’anar al menú i seleccionar Simplificar: Normal. Tal com ho mostra el dibuix següent:

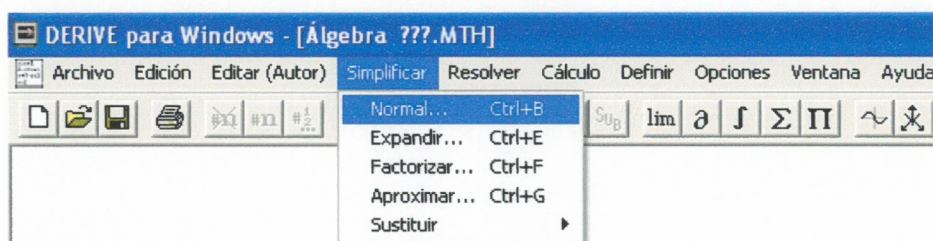


Figura 1

- 5) Escollir un nombre p (primer molt gran). Una vegada s’hagi fet el que diu en el pas 3, s’obrirà una pàgina com la de la Figura 1. Aleshores s’ha d’escriure **next_prime** (9^{10}) (en el cas que es volgués escriure el nombre primer següent de 9^{10}). A la pantalla general apareixerà:

p=1#: 3486784409.

- 6) Escollir un nombre q , que ha de ser un nombre primer molt gran. El procediment per escollir-lo és el mateix que per escollir el nombre p : **next_prime** (11^{10}) . Una vegada posada aquesta ordre, a la pantalla general apareixerà a sota del nombre #1:

$q = \#2: 25937424629$ (que és el nombre primer següent a 11^{10}).

- 7) Trobar el nombre N , que és el producte de $p \cdot q$: $\#1 \cdot \#2$ o també es pot escriure els 2 nombres ($3486784409 \cdot 25937424629$). Després d'aquest pas, s'obtindrà el nombre:

$$N = \#3: 90438207806009809261.$$

- 8) Escollir un nombre e [ha de ser primer amb $(p-1) \cdot (q-1)$] i més petit que N . Per assegurar-se que serà primer amb $(p-1) \cdot (q-1)$ és recomanable escollir un nombre primer qualsevol no massa gran (ja que els nombres primers tenen com a propietat ser divisibles únicament per 1 i per ells mateixos. En aquest cas s'ha escollit el nombre primer següent de 5^7 .

$$e = \#4: 78137$$

- 9) Xifrar el missatge a partir de la fórmula: $C = M^e \pmod{N}$ On M és l'equivalència de la lletra en el sistema decimal. En el cas que es volgués codificar la lletra B ($M=66$). S'hauria d'escriure: $\text{mod } (66^{\#4, \#3}) = \text{mod } (66^{78137}, 90438207806009809261)$ com a resultat d'això, obtenim

$$C = \#5: 89582771394594569249$$

Fins aquí arriba el que ha de fer l'emissor del missatge si vol codificar un text, (només ha d'utilitzar la clau pública (N i e)).

El receptor rep el missatge codificat i es disposa a iniciar el procés de descodificació del missatge (en aquest cas una sola lletra) tenint en compte que ha d'utilitzar la clau pública (p i q).

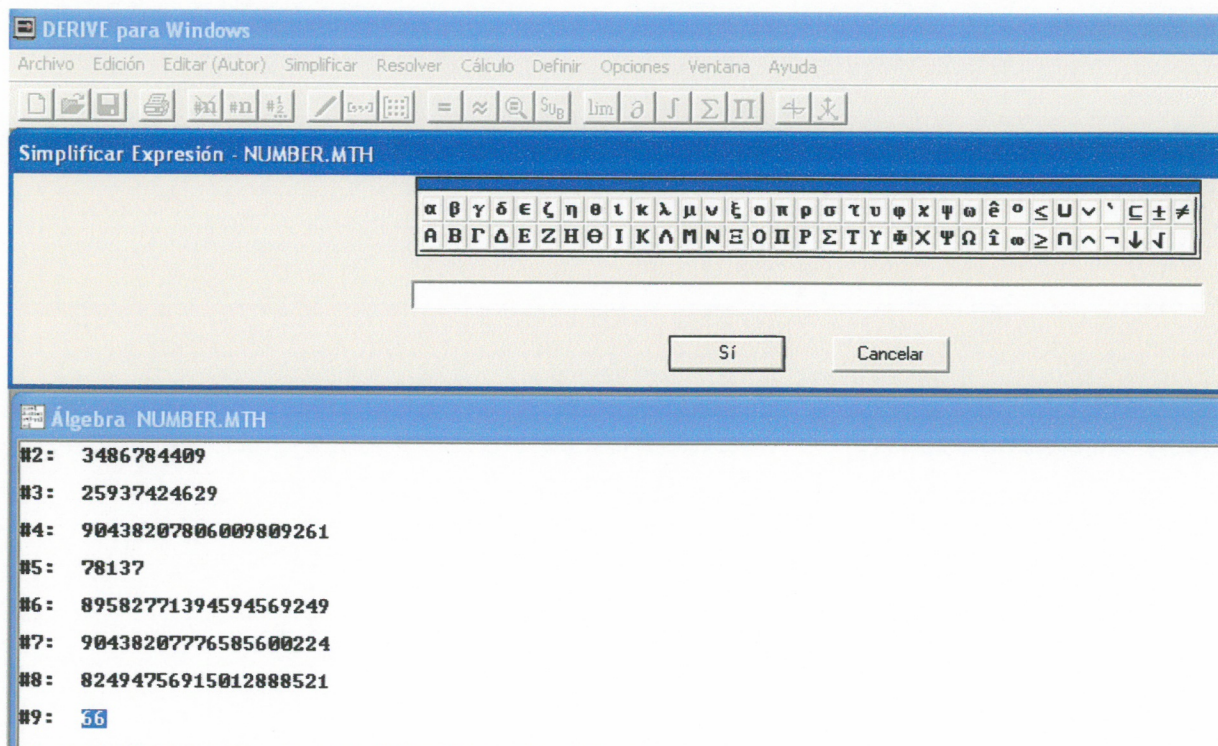
- 10) Trobar la ϕ de N : $(p-1) \cdot (q-1)$. Calcular: $(\#1-1) \cdot (\#2-1) = (3486784409 \cdot 25937424629)$.

$$\phi(N) = \#6: 90438207776585600224.$$

11) Trobar un nombre d (a partir de l'invers modular). Aquest nombre d és imprescindible per descodificar el missatge. Per trobar aquest nombre d , s'ha de fer l'invers modular de e , en mòdul $(p-1)*(q-1)$. Per tant s'ha de fer: **inverse_mod (#4,#6).** = inverse_mod (78137 ,90438207776585600224).

$$d = \#7: 82494756915012888521.$$

Finalment, una vegada s'ha obtingut el nombre d , ja es pot aplicar la fórmula $M = C^d \pmod{N}$: **mod (#5^#7,#3)** = mod (89582771394594569249^82494756915012888521, 90438207806009809261) i obtenim el nombre 66 = Missatge en clar (la lletra B en el sistema decimal)



Pantalla que apareix quan es posa simplificar, normal.

6.2.5 Pràctica 6

Xifrar i desxifrar un missatge utilitzant l'algoritme de generació de claus de l'RSA, sense fer ús d'eines informàtiques.

Per resoldre aquest exemple s'ha utilitzat el mètode del quadrat.

- 1) Triar els nombres primers $p = 281$ i $q = 167$ (clau privada).
- 2) Fer públic el producte de $p \cdot q = N = 46927$. (clau pública)
- 3) Trobar la $\varphi(N) = (p-1) \cdot (q-1) = 280 \cdot 166 = 46480$ (clau privada).
- 4) Tot seguit es tria l'enter $e = 39423$ (clau pública) que ha de complir que: $\text{m.c.d.}(e, p-1) = 1$ i $\text{m.c.d.}(e, q-1) = 1$, (dues condicions que impliquen l'aterior i que són més fàcilment comprovables, ja que es manipulen enters petits).
- 5) Finalment, l'usuari A (receptor del missatge) calcula:

$$d = e^{-1} \pmod{\varphi(N)} = 39423^{-1} \pmod{46480}$$

mitjançant l'algorisme d'Euclides, i s'obté $d = 19713$

- 6) Un usuari B (emissor del missatge) del sistema vol enviar el missatge "ENCARA" a l'usuari A. La transformació xifradora és:

$$F: \mathbb{Z} / 46927 \rightarrow \mathbb{Z} / 46927$$

$$x \rightarrow f(x) = x^{39423} \pmod{46927}$$

On x és una unitat de missatge, que ha de tenir un valor numèric entre 0 i 46926.

- 7) L'alfabet emprat és l'A-Z de 26 lletres.
- 8) Recordem que quan les unitats de missatge són blocs de k lletres, el valor numèric que associem a cada bloc correspon a pensar-lo com un nombre de k xifres escrit en base 26, i el rang d'enters que es pot

representar amb k xifres va des 0 fins a $26^k - 1$. Com que les unitats de missatge del text original han d'estar dins del rang $0 - 46926$, tenint en compte que $26^3 < 46926 < 26^4$, triarem unitats de llargada 3 per el text en clar i unitats de llargada 4 per al text xifrat

- 9) El missatge ENCARA consta de dues unitats, "ENC" i "ARA", amb equivalents numèrics $ENC = 4132 = 4 \cdot 26^2 + 13 \cdot 26 + 2 = 3044$ i $ARA = 0170 = 0 \cdot 26^2 + 17 \cdot 26 + 0 = 442$. Posem:

$$X_1 = 3044$$

$$X_2 = 442$$

- 10) La transformació del missatge x_1x_2 és y_1y_2 on:

$$y_1 = f(x_1) = 3044^{39423} \pmod{46927}$$

$$y_2 = f(x_2) = 442^{39423} \pmod{46927}$$

- 11) El següent pas és trobar y_1 i y_2 , a partir del mètode del quadrat¹⁷. En aquest cas $y_1 = 39896$ i $y_2 = 31017$.

- 12) Finalment hem d'expressar el resultat anterior en mòdul 26:

$$Y_1 = 39896 \pmod{26} = 2 \cdot 26^3 + 7 \cdot 26^2 + \cdot 26 + 12 \rightarrow 2/7/0/12 =$$

CHAM

$$Y_2 = 31017 \pmod{26} = 1 \cdot 26^3 + 19 \cdot 26^2 + 22 \cdot 26 + 25 \rightarrow 1/19/22/25 =$$

BTWZ

Missatge Xifrat = CHAMBTWZ

Una vegada l'usuari A hagi rebut el missatge xifrat de B, es disposarà a desxifrar-lo a partir de:

- 13) Codificar CHAM = 39896, BTWZ = 31017 i aplicant la transformació inversa que utilitza la clau secreta $d = 26767$ i que només coneix l'usuari A.

$$f^{-1} : Z / 46927 \rightarrow Z / 46927$$

¹⁷ Utilitzant el full de càlcul d'EXCEL de la pràctica 4.

$$y \rightarrow f(y) = y^{26767} \pmod{46927}$$

14) Es pot comprovar pel mètode del quadrat que:

$$39896^{26767} \pmod{46927} = 3044 = \text{ENC}$$

$$31017^{26767} \pmod{46927} = 442 = \text{ARA}$$

15) Per acabar el procés de desxiframent unim els dos trossos del missatge i obtenim el missatge en clar inicial del emissor: ENCARA

6.2.6 Pràctica 7

Xifrat i desxifrat d'un missatge amb el programa "Derive para Windows"

- 1) Com en els anteriors casos, haurem d'obrir el programa "Derive para Windows"
- 2) Després obrir l'arxiu Number de la Carpeta Math.
- 3) Escollir un nombre primer molt gran (q): next_prime 3^9 . 75# = 19687
- 4) Escollir un segon nombre primer amb molts dígit (p) : next_prime 7^5 . 76# = 16811
- 5) Trobar el producte de $p \cdot q = N = 75 \cdot 76$.

$$N = \#77 : 330958157$$

- 6) Trobar la $\phi(N) = (p-1) \cdot (q-1) = (75-1) \cdot (76-1)$:

$$\phi(N) = \#78 : 330921660$$

- 7) Buscar un nombre e que sigui primer amb $\phi(n)$ i més petit que N. En aquest cas, s'ha escollit:

$$e = \#79 = 347$$

- 8) Trobar d, a partir de e i $\phi(n)$: inverse_mod (#79, #78).

$$d = \#80 = 250813823$$

- 9) Saber en quantes lletres hem de dividir els blocs (k). Per realitzar aquest procés, es parteix de que s'està utilitzant un alfabet amb 26 lletres. Per trobar k l'emissor s'haurà de quedar amb la part sencera del resultat de $\log N / \log 26$: $\log(\#77, 10) / \log(26, 10)$.

$$\#81 = \text{LN}(330958157)/\text{LN}(26)$$

- 10) Per obtenir el resultat, s'ha de marcar el quocient de logaritmes i clicar Simplificar:
Aproximar. Com a conseqüència $\#82 = 6.02115$ (com ja hem dit anteriorment,
l'emissor s'ha de quedar amb la part entera, en aquest cas 6).

$$K = \#82 : 6$$

- 11) Dividir el missatge en blocs de k lletres: PRACTI-CAAMBD-ERIVE

- 12) Per fer l'exemple només codificarem el primer bloc de lletres (PRACTI). Passar les
lletres a base 26 tenint en compte l'ordre alfabètic. (M = missatge en clar)

$$M = \text{PRACTI} = 15 \cdot 26^5 + 17 \cdot 26^4 + 0 \cdot 26^3 + 2 \cdot 26^2 + 19 \cdot 26 + 8 = 185991086$$

$$M = \#83: 185991086$$

- 13) Xifrar el missatge seguint la fórmula : $C = M^e \pmod{N} = 185991086^{347} \pmod{330958157} = \pmod{(185991086^{\#79}, \#77)} = 204514807$.

$$C = \#84 : 204514807$$

- 14) Fer un seguit de divisions per anar obtenint les diferents lletres:

$$\#85: \text{mod}(204514807/26, 26) = 3$$

$$\#86: (\#84 - 3)/26 = 7865954$$

$$\#87: \text{mod}(7865954, 26) = 18$$

$$\#88: (\#86 - 18)/26 = 302536$$

$$\#89: \text{mod}(302536, 26) = 0$$

$$\#90: (\#88 - 0)/26 = 11636$$

$$\#91: \text{mod}(11636, 26) = 14$$

$$\#92: (\#90-14)/26=447$$

$$\#93: \text{mod}(447,26) = 5$$

$$\#94: (\#92-5)/26=17$$

$$\#95: \text{mod}(17,26) = 17$$

15) Escriure les lletres equivalents als números 17-5-14-0-18-3 (tenint present que l'últim nombre obtingut serà la primera lletra).

$$\#107: \text{mod}(407,26) = 17$$

16) Finalment, el missatge quedaria xifrat de la següent manera: RFOASD

$$\#108: (18106-17)/26 = 15$$

Una vegada el receptor del missatge rebés el text xifrat es disposaria a descodificar-lo seguint els passos següents:

17) Passar les lletres al número corresponent al seu ordre en l'alfabet: 17-5-14-0-18-3

$$\#19) \text{ Un cop trobat els nombres que componen el text en clar (15, 17, 0, 2, 19, 8),}$$

18) Trobar l'expressió polinòmica que converteix en potències de 26: l'ordre de l'alfabetari, en

$$\#96 = 17*26^5 + 5*26^4 + 14*26^3 + 0*26^2 + 18*26 + 3 = 204514807$$

18) Elevar a d el nombre obtingut en mòdul N, i el resultat donat es resta el nombre anterior, fent aquest procés repetidament fins que el resultat del mòdul sigui el mateix que el del residu:

$$\#98: \text{mod}(204514807^{250813823}, 330958157) = 185991086$$

$$\#99: \text{mod}(185991086, 26) = 8$$

$$\#100: (\#98-8)/26=7153503$$

$$\#101: \text{mod}(7153503, 26) = 19$$

$$\#102: (\#100-19)/26=275134$$

$$\#103: \text{mod}(275134,26) = 2$$

$$\#104: (\#102-2)/26=10582$$

$$\#105: \text{mod}(10582,26) = 0$$

$$\#106: (\#104-0)/26=407$$

$$\#107: \text{mod}(407,26) = 17$$

$$\#108: (\#106-17)/26 = 15$$

$$\#109: \text{mod}(15,26) = 15$$

19) Un cop trobat els nombres que componen el text en clar (15, 17, 0, 2, 19, 8). S'ha de trobar l'equivalència a la lletra corresponent en el número, segons l'ordre de l'abecedari, en aquest cas seria: PRACTI.

6.2.7 Pràctica 8

Xifrat i desxifrat d'un missatge amb el programa *Mathematica*.

- 1) Trobar els nombres primers molt grans que formaran part de la clau privada:

$$p = \text{Prime}[10^{10}] = 252097800623$$

$$q = \text{Prime}[10^9] = 22801763489$$

- 2) Fer el producte de p i q , obtenint així el nombre N , corresponent a la clau pública:

$$N = p * q = 5748274425902722853647$$

- 3) Buscar $\phi(N)$, coneixent la clau privada p i q (per tant, $\phi(N)$ formarà part de la clau privada).

$$\phi(N) = (p-1)*(q-1) = (252097800623-1)*(22801763489-1) = \\ 5748274425627823289536$$

- 4) Buscar un nombre e que compleixi les directrius explicades en l'apartat de l'RSA:

$$e = 2371$$

- 5) Comprovar que e és primer amb $\phi(N)$:

$$\text{GCD}[e, \phi(N)] = 1 \text{ (l'únic divisor comú és 1, per tant } e \text{ és primer amb } \phi(N)).$$

- 6) Fer l'invers modular de e i $\phi(N)$:

$$d = \text{PowerMod}[e, -1, \phi(N)] = 366085802728722613547$$

- 7) Trobar k (sent k el número de lletres corresponent a cada bloc). Aquest procés es realitza agafant la part entera del quocient del logaritme de N i el log de 256 (nombre de caràcters en el codi ASCII):

$$k = \text{Floor}[\text{Log}[256, 5748274425902722853647]] = 9$$

- 8) Comprovar que el nombre n es troba entre 256^k i 256^{k+1} :

$$\begin{aligned} 256^k < n < 256^{(k+1)} &= 256^k < 5748274425902722853647 \\ < 256^{(k+1)} \\ \text{True} \end{aligned}$$

9) Passar el missatge que volem xifrar a Codi ASCII:

Mens = ToCharCode ["Què embolicat que és això del RSA"]
 {81, 117, 232, 32, 101, 109, 98, 111, 108, 105, 99, 97, 116, 32, 113, 117, 101, 32, 233, 115, 32, 97, 105, 120, 242, 32, 100, 101, 108, 32, 82, 83, 65, 33}.

10) Veure la longitud del missatge:

l = Length [mens] = 34

11) Completar el missatge amb blancs de tal manera que el missatge tingui una longitud que sigui múltiple de 9, per poder-lo dividir en blocs de 9 lletres:

Comp = Table [32, {i, k - Mod [1, k]}]
 {32, 32}

12) Afegir al missatge en clar els dos blancs:

Menscomp = Flatten@Append [mens, comp]
 {81, 117, 232, 32, 101, 109, 98, 111, 108, 105, 99, 97, 116, 32, 113, 117, 101, 32, 233, 115, 32, 97, 105, 120, 242, 32, 100, 101, 108, 32, 82, 83, 65, 33, 32, 32}.

13) Partir els el missatge en blocs de k lletres:

Blocs = Partition [menscomp, k]
 {{81, 117, 232, 32, 101, 109, 98, 111, 108},
 {105, 99, 97, 116, 32, 113, 117, 101, 32},
 {233, 115, 32, 97, 105, 120, 242, 32, 100},
 {101, 108, 32, 82, 83, 65, 33, 32, 32}}

14) Agafar el primer bloc de lletres i obtenir un nombre únic passant-lo a base 256.

m1 = FromDigits [b1, 256] = 1502682346287507074924

15) Xifrar el el bloc 1 amb la fórmula: $C = M^e \pmod{N}$:

$c1 = \text{PowerMod } [m1, e, N] = 899443616636926071215$

16) La següent acció que s'ha de fer serà transformar la cadena de nombres $c1$ en les lletres del bloc 1 xifrat.

$cc1 = \text{StringJoin } [\text{Map}[\text{FromCharCode}, \text{IntegerDigits}[c1, 256, k+1]]]$

I finalment, obtenim que $c1 = \text{OÄËßð}^{\sim}$

17) Repetir els passos 14, 15 i 16 pels 3 blocs de lletres següents:

- Bloc 2:

$m2 = \text{FromDigits } [[2], 256]$

$c2 = \text{PowerMod } [m2, e, N] = 1057760289999951889630$

$cc2 = \text{StringJoin } [\text{Map}[\text{FromCharCode}, \text{IntegerDigits}[c2, 256, k+1]]]$

Finalment s'obtenen els caràcters següents: 9W_s 1N

- Bloc 3

$m3 = \text{FromDigits } [[3], 256]$

$c3 = \text{PowerMod } [m3, e, N] = 4358214861141262587371$

$cc3 = \text{StringJoin } [\text{Map}[\text{FromCharCode}, \text{IntegerDigits}[c3, 256, k+1]]]$

Els caràcters que s'obtenen són els següents: iBa eaUÖë

- Bloc 4

$m4 = \text{FromDigits } [[3], 256]$

$c4 = \text{PowerMod } [m3, e, N] = 848468694135602449343$

$cc4 = \text{StringJoin } [\text{Map}[\text{FromCharCode}, \text{IntegerDigits}[c4, 256, k+1]]]$

El darrer bloc de notes queda xifrat: -pUiÀ\$ ¿

18) Ajuntar els diferents blocs per obtenir tot el missatge xifrat:

$\text{OÄËßð}^{\sim} \quad 9W_s \ 1N \quad iBa \ eaUÖë \quad -pUiÀ\$ \ ¿$

Per desxifrar el missatge hem d'invertir el procés anterior pas a pas:

19) Passa els caràcters a codi ASCII:

$mx1 = \text{ToCharCode } [\text{missatgexifrat}]$

{0, 48, 194, 73, 163, 223, 240, 154, 145, 175, 0, 57,
87, 95, 115, 128, 49, 78, 4, 222, 0, 236, 66, 97, 141, 101,
97, 85, 213, 235, 0, 45, 254, 222, 85, 239, 192, 36, 139, 191}

20) Partir el missatge en blocs de $k+1$ caràcters:

$mx2 = \text{Partition } [mx1, k+1]$
{ {0, 48, 194, 73, 163, 223, 240, 154, 145, 175}
{0, 57, 87, 95, 115, 128, 49, 78, 4, 222}
{0, 236, 66, 97, 141, 101, 97, 85, 213, 235}
{0, 45, 254, 222, 85, 239, 192, 36, 139, 191}}

21) Agafar cada bloc per separat i aplicant-li la fórmula: $M = C^d \pmod{N}$, trobar el valor inicial de cada caràcter:

a. Bloc 1:

21.1. Agafar el primer bloc i transformar-lo fent base 256 en un sol nombre:

$cc1 = \text{FromDigits } [mx2 [[1]], 256] = 899443616636926071215.$

21.2. Elevar a d el resultat obtingut en el pas 21.1 en mòdul n :

$mm1 = \text{PowerMod } [cc1, d, n]$

21.3. Transformar el valor $mm1$, en k caràcters:

$mmm1 = \text{IntegerDigits } [mm1, 256, k] = \{81, 117, 232, 32, 101, 109, 98, 111, 108\}$

21.4. Passar al codi ASCII els nombres corresponents a $mmm1$:

$md1 = \text{StringJoin } [\text{Map}[\text{FromCharCode}, mmm1]] = \text{Què embol}$

En els següents blocs ja no s'explicaran els passos detalladament, ja que són els mateixos que en el Bloc 1:

b. Bloc 2:

$cc2 = \text{FromDigits } [mx2 [[2]], 256]$

$mm2 = \text{PowerMod } [cc2, d, n]$

$mmm2 = \text{IntegerDigits } [mm2, 256, k] = \{105, 99, 97, 116, 32, 113, 117, 101, 32\}$

$md2 = \text{StringJoin } [\text{Map}[\text{FromCharCode}, mmm2]] = \text{icat que}$

c. Bloc 3:

`cc3 = FromDigits [mx3 [[3]], 256]`

`mm3 = PowerMod [cc3, d, n]`

`mmm3 = IntegerDigits [mm3, 256, k] = {233, 115, 32, 97, 105, 120, 242, 32, 100}`

`md3 = StringJoin [Map[FromCharacterCode, mmm3]] = és això d`

d. Bloc 4:

`cc4 = FromDigits [mx4 [[4]], 256]`

`mm4 = PowerMod [cc4, d, n]`

`mmm4 = IntegerDigits [mm4, 256, k] = {101, 108, 32, 82, 83, 65, 33, 32, 32}`

`md4 = StringJoin [Map[FromCharacterCode, mmm4]] = el RSA!`

Finalment, al usuari B només li falta ajuntar els diferents blocs de lletres per obtenir el missatge sencer:

`22) StringJoin [md1, md2, md3, md4]`

Com a resultat d'aquest darrer pas, l'usuari B, pot llegir el missatge que l'usuari A li ha enviat:

Què embolicat que és això del RSA!

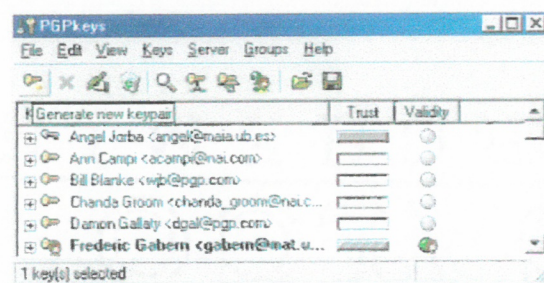
Pràctica de Criptografia: PGP

L'objectiu d'aquesta pràctica és arribar a enviar correu electrònic xifrat i signat. Usarem el programa **PGP (Pretty Good Privacy)**. Podeu baixar-vos la versió freeware del software de la pàgina de ftp de RedIris: <ftp://ftp.rediris.es/software/security/crypt/pgp/pgpi/6.5/6.5.3/>

Per començar, cal crear el parell de claus (clau pública – clau privada) que ens permetrà xifrar i signar, i obtenir la clau pública d'algú altre (per exemple, dels companys de l'ordinador del costat) per tal de poder comunicar-nos amb aquest “algú altre” de forma segura.

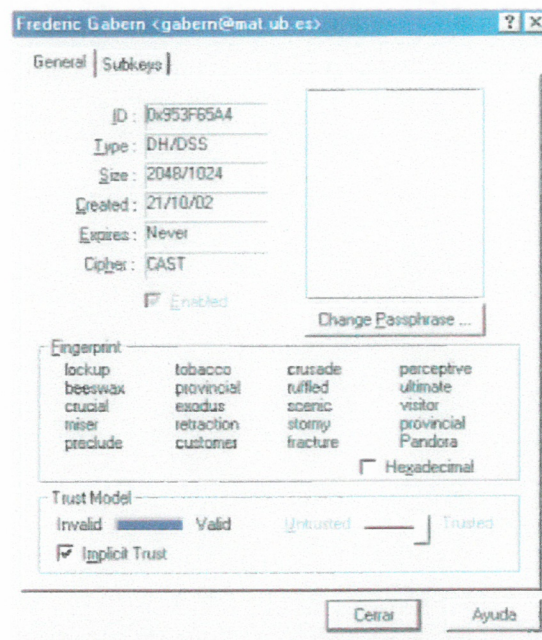
1. **Crear el parell de claus.** Per tal de generar el parell de claus amb el programa PGP, seguiu els següents passos:

- Obriu el PGPKeys. Aquest és el programa gestor de claus. El podem trobar a: “Menú Inicio – Programs – PGP – PGPKeys ”.
- Feu “Generate new keypair” des del menú “Keys – New Key”, o bé usant la icona amb el dibuix d'una clau.



- Seguiu les indicacions del programa d'ajuda “Key Generation Wizard” que us demanarà tot un seguit d'informació per tal de crear el parell de claus:
 - Introduïu el vostre nom i cognoms a on hi diu *Full name*, i l'adreça de correu electrònic a on hi diu *E-mail adress*¹.
 - Escolliu el tipus de claus *Diffie-Helman/DSS*.
 - Seleccioneu una llargada de clau de 2048 bits.
 - Trieu la caducitat de la clau. Per defecte, que no caduqui mai (*Key pair never expires*).
 - Introduïu la contrasenya *passphrase* (fins que la barra de qualitat estigui al màxim) i verifiqueu-la (repetint-la en la finestra inferior).
 - Feu “Següent” fins a finalitzar.
- Podem veure les propietats de les claus tot seleccionant-ne una de la llista de claus i anant al menú “Keys – Properties”. Feu-ho pel parell de claus que acabeu de crear.

¹Per accedir al correu electrònic: adreça: a01@ub052021.mat.ub.es contrasenya: Pgp/2POP



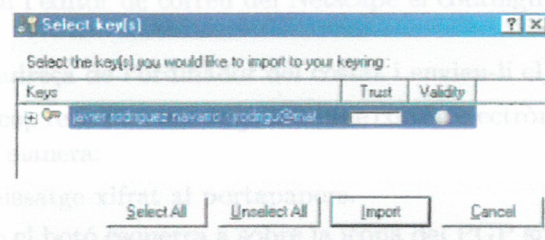
- Exporteu la vostra clau pública a un arxiu .asc usant el menú "Keys – Export". Guardeu-la en el disc (per exemple, en la carpeta *claus* de la unitat D:, que podeu crear, si no hi és, vosaltres mateixos), sota el nom que hi ha per defecte. D'aquesta manera podem compartir la clau pública amb altres usuaris de PGP per tal de que ens puguin enviar correu encriptat, sempre i quan disposin de la vostra clau pública. Podeu visualitzar la clau pública amb un editor de text qualsevol (per exemple, el "Bloc de Notes-Notepad"):



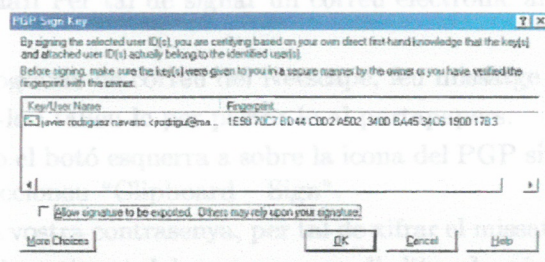
2. **Importar la clau pública d'una altra persona.** Per tal d'enviar correu xifrat a una altra persona, ens cal la seva clau pública. Per a obtenir-ne una, importarem la dels companys de l'ordinador del costat seguint els següents passos:

- Envieu un e-mail, usant el programa de correu del Netscape, a l'ordinador del costat, adjuntant-hi l'arxiu .asc que conté la vostra clau pública.
- Guardeu en el disc (a D:\claus) l'arxiu .asc que us acaben d'enviar els vostres companys de l'ordinador del costat.

- Importeu (amb el menú “Keys – Import”) la clau pública que acabeu de guardar en un arxiu.



- Per tal d'incloure aquesta clau en el vostre anell de confiança i, així, poder enviar correu xifrat al propietari d'aquesta clau, cal que previament la verifiqueu. La verificació d'una clau es fa, simplement, signant-la (xifratge amb clau privada). Aneu al menú “Keys – Sign”, cliqueu OK i introduïu la vostra contrasenya.

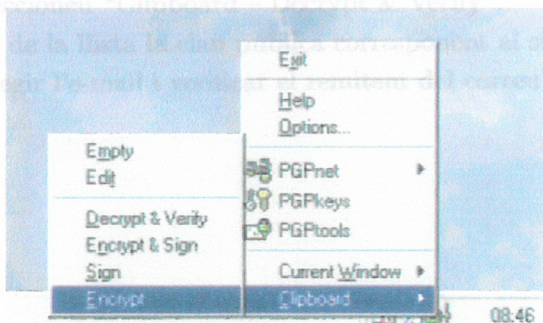


- Xifrar i Signar un correu electrònic.** Enviar un e-mail sense xifrar és equivalent, en el correu convencional, a enviar una postal. Qualsevol persona que hi tingui accés en podrà llegir el contingut. Si us interessa, pel que sigui, guardar la privacitat del e-mail, el PGP ens permet xifrar-lo, usant la clau pública del destinatari, de tal manera que només aquest podrà accedir al contingut, ja que és l'únic que té la clau privada que pot desxifrar-lo.

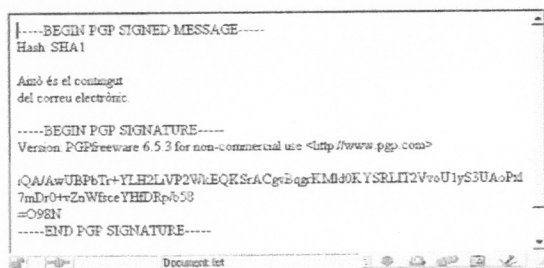
D'altra banda, quan rebem un e-mail d'alguna persona, com sabem que realment el remitent és qui diu que és? Una eina que ajuda a certificar que un correu pertany a qui diu que pertany és la signatura electrònica.

- Xifrar.** Envieu un correu xifrat a l'ordinador del costat, seguint els següents passos:

- Obriu el programa de correu del Netscape, feu missatge nou i escriviu un curt e-mail.
- Seleccioneu-lo i talleu-lo per tal de passar-lo al portapapers.
- Cliqueu amb el botó esquerra a sobre la icona del PGP situada a la barra de programes actius i seleccioneu “Clipboard – Encrypt”:



- Seleccioneu la clau del destinatari de la llista, clickant dues vegades a sobre. El nom del destinatari apareixerà a la finestra inferior. Feu OK.
 - Enganxeu en l'editor de correu del Netscape el contingut del portapapers (que ja està encriptat).
 - Introduïu l'adreça de l'ordinador del costat i envieu-li el correu xifrat.
- (b) **Desxifrar.** Un cop rebeu un missatge xifrat de correu electrònic amb el Netscape, desxifreu-lo de la següent manera:
- Copieu el missatge xifrat al portapapers.
 - Cliqueu amb el botó esquerra a sobre la icona del PGP situada a la barra de programes actius i seleccioneu "Clipboard - Decrypt & Verify".
 - Introduïu la contrasenya per tal d'accedir a la vostra clau privada, que és la única que pot desxifrar el missatge (ja que suposadament està encriptat amb la vostra clau pública). Ja podeu llegir l'e-mail.
- (c) **Signar un e-mail** Per tal de signar un correu electrònic amb el PGP, cal que seguiu els següents passos:
- Obriu el programa de correu del Netscape, feu missatge nou i escriviu un curt e-mail.
 - Seleccioneu-lo i tal·leu-lo per passar-lo al portapapers.
 - Cliqueu amb el botó esquerra a sobre la icona del PGP situada a la barra de programes actius i seleccioneu "Clipboard - Sign".
 - Introduïu la vostra contrasenya, per tal de xifrar el missatge amb la vostra clau privada.
 - Enganxeu el contingut del portapapers a l'editor de missatge del Netscape:



```
-----BEGIN PGP SIGNED MESSAGE-----
Hash: SHA1

Això és el contingut
del correu electrònic.

-----BEGIN PGP SIGNATURE-----
Version: PGPFreeWare 6.5.3 for non-commercial use <http://www.pgp.com>
iQA/AwUBPbTr+YLEZLVp2WbEQK5rACgZegqKMB40KYSRLIT2VroU1yS3UAoPd
7mDr0+ZaWbceYHEDRp6:58
=O98N
-----END PGP SIGNATURE-----
```

- Introduïu l'adreça de correu de l'ordinador del costat i envieu-li el missatge signat.
- (d) **Verificar la signatura d'un e-mail.** Seguiu els següents passos per tal de verificar la signatura electrònica d'un e-mail:
- Al rebre un e-mail signat (com el de la darrera figura), copieu-lo sencer al portapapers.
 - Cliqueu amb el botó esquerra a sobre la icona del PGP situada a la barra de programes actius i seleccioneu "Clipboard - Decrypt & Verify".
 - Seleccioneu de la llista la clau pública corresponent al signant del missatge.
 - Ja podeu llegir l'e-mail i verificar el remitent del correu electrònic.

criptografia quàntica serà el final d'aquesta ciència. Però jo prefereixo subscriure la frase d'un gran afecçional a la criptografia.

CONCLUSIONS:

"Es dubta que el genari hagi pogut crear un enigma que el mateix enginy humà no pugui resoldre."
L'elaboració d'aquest treball m'ha permès aprendre els conceptes bàsics de criptografia i així deixar la porta oberta a la possibilitat d'enriquir-los. Encara que, en el moment que estic redactant aquest apartat, pensí que no vull saber-ne mai més res d'aquest tema, també se, que això és degut al cansament que tinc després d'aquests últims dies de dedicació intensiva a la redacció i a la transcripció definitiva del treball. Són molts els dies i hores que he emprat per poder-me sentir mínimament segura sobre un tema, que ja pensava que no seria fàcil, però no podia imaginar-me el gran grau de complexitat que té.

La criptografia no és només històries d'espionatge, secrets d'estat, sempre envoltats d'un aire de misteri; sinó que en els últims trenta anys, paral·lelament a l'aparició dels ordinadors digitals i a la popularització de les xarxes mundials de telecomunicacions, ha adquirit un protagonisme inesperat en la vida de qualsevol usuari d'internet que vulgui garantir la privacitat de les seves comunicacions.

La hipòtesi inicial del treball era: Hi ha relació entre matemàtiques i criptografia, i després de concloure'l, he de dir que he arribat a la conclusió que la criptografia sense les matemàtiques no existiria.

L'alt grau de dificultat d'aquests conceptes matemàtics, que formen part de qualsevol sistema criptogràfic, ha estat la dificultat més gran que se m'ha plantejat i ha sigut tot un repte aconseguir seguir endavant (unes vegades trobant-hi la solució i altres no m'ha quedat cap altra possibilitat que deixar sense treballar una part que jo considerava important.

Però una vegada acabat el treball, penso que aquest tema que vaig escollir és un tema molt ampli, obert i que està en constant evolució. I que encara que han quedat moltes coses per explicar, els objectius que em vaig proposar s'han complert, i per tant, en faig una valoració positiva.

Per acabar, voldria dir que en el treball he tractat els missatges des de l'antiguitat fins al moment actual; també s'ha reflexionat sobre el futur de la criptologia. Es diu que les

criptografia quàntica serà el final d'aquesta ciència. Però jo prefereixo subscriure la frase d'un gran afeccionat a la criptografia: Edgar Allan Poe:

“És dubtós que el gènere humà pugui crear un enigma que el mateix enginy humà no pugui resoldre”.

BIBLIOGRAFIA

Llibres:

CABALLERO, Pino; *Introducción a la Criptografía*. Ed. Ra-Ma, 2a Edición 2002.

COLERA, J; OLIVERA, M^a.J.; GARCÍA, R. *Matemàtiques 2. Modalitat Ciències de la Terra i de la salut tecnologia*. Ed. Barcanova, 2003.

COROMINA, Eusebi; CASACUBERTA, Xavier; QUINTANA, Dolors. *El treball de recerca. Procés d'elaboració, memòria escrita, exposició oral i recursos*. Santa Perpètua de Mogoda; Ed. Eumo, 2000.

DOMINGO, Josep; HERRERA, Jordi; *Criptografia per als Serveis telemàtics i el comerç electrònic*. Edicions de la Universitat Oberta de Catalunya, 99.

JUHER, David; *L'art de la comunicació secreta. El llenguatge de la criptografia*. Llibres de l'índex, 2004.

MATAIX, Susana; *Lee a Julio Verne*. Ed. Rubes, 2002.

PASTOR, José; SARASA, Miguel Àngel; SALAZAR, José Luis. *Criptografia Digital (Fundamentos y aplicaciones)*. Colección de textos docentes. Ed. Prensas Universitarias de Zaragoza, 2a Edición, 2001.

RAMIÓ, Jorge; *Aplicaciones Criptográficas*. Universidad politécnica de Madrid. 2a Edició, 1999.

Sessions de preparació per a l'Olimpíada Matemàtica; Societat Catalana de Matemàtiques; Barcelona 2002

SINGH, Simon. *Los códigos secretos*. Ed. Debate, 2000.

Xambó, Sebastià. *Álgebra lineal y geometrias lineales (volumen I)*. Ed. Eunibar, 1978.

Pàgines web:

<http://www.portalmundos.com/mundoinformatica/seguridad/cuantica.htm>

<http://www.xtec.es/~dobrador/cripto/>

<http://civil.udg.es/normacivil/estatal/persona/PF/Lo15-99.htm>

<http://webs.ono.com/usr005/jsuarez/colabora/enigma/enigma.html>

http://www.verisign.es/products/site/faq/identity_auth.html

ÍNDEX D'ANNEXOS

Annex 1: Article <i>Hi ha algú aquí a fora?</i> Autora: Pilar Bayer (doctora en matemàtiques de la Universitat de Barcelona), aquest article ha estat publicat per la revista <i>mètode</i> de la universitat de València.....	109
Annex 2: Tríptic d'informació sobre la garantia de seguretat de l'empresa "El Corte Inglés"	114
Annex 3: Tríptic d'informació sobre la garantia de seguretat de "La Caixa de Catalunya"	117
Annex 4: Tríptic informatiu sobre l'empresa de seguretat Safelayer amb informació sobre la seva filosofia, productes i clients.....	119
Annex 5: Funcions de càlcul numèric del programa " <i>Derive para Windows</i> "	127

Hi ha algú aquí fora?

per Pilar Bayer, Facultat de Matemàtiques. Universitat de Barcelona.

Is anybody out there? In the paper our aim is to describe some basic facts about prime numbers and the Riemann zeta function. After discussing their importance, we mention some open problems and applications.

CONTACTE

Actualment, ningú no sap si hi ha o no vida intel·ligent o bé, simplement, vida en alguna altra part de l'univers. Amb tot, si n'hi hagués, establir-hi contacte no seria fàcil. Caldria, com a mínim, que alguns extraterrestres emetessin senyals racionals, que nosaltres els interceptéssim i que, a més, fóssim capaços de descodificar-los. No obstant això, en el film de ciència ficció *Contact*, dirigit l'any 1997 per Robert Zemeckis amb l'aval científic de Carl Sagan, la radioastrònoma Ellie Arroway (Jodie Foster) aconsegueix captar per primera vegada senyals intel·ligents procedents de l'espai exterior.

El missatge dels alienígenes de *Contact* és: 2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47, etc. Arroway s'adona que un missatge així no pot ser degut a cap radiació fortuïta, ja que hi reconeix la successió dels nombres primers i, per tant, la intervenció d'una acció intel·ligent. Com que la notícia és rebuda amb l'escepticisme previsible, la científica es veu abocada a defensar el seu parer. Així, en una escena que és força inusual en el cinema, Jodie Foster explica a un comitè d'experts de Washington que "els nombres primers són aquells que només es poden dividir per ells mateixos i per l'1 [...]". Com que l'escena és molt curta, i l'espectador només assisteix a una part del debat, utilitzarem l'ocasió per parlar d'aquests nombres i de com els éssers humans han anat escorcollant les seves propietats.

SOBRE LA QUANTITAT DE NOMBRES PRIMERS

Considerem la successió dels nombres naturals 1, 2, 3, 4, 5, 6, 7, etc. Els nombres primers són els constituents bàsics dels nombres naturals, en tant que tot nombre natural factoritza com a producte de nombres primers. Des del segle III a. C., es coneix que la successió dels nombres primers, a l'igual de la dels nombres naturals, no s'acaba mai. Euclides demostrà que hi ha una quantitat infinita de nombres primers en

el capítol IX dels *Elements*. La demostració d'Euclides es fonamenta en propietats elementals de la divisibilitat dels nombres.

L'any 1748, Leonhard Euler redemonstrà el teorema d'Euclides d'una manera molt més elaborada. En el seu raonament, Euler utilitzà la identitat:

$$Sn^{-s} = P(1 - p^{-s})^{-1}$$

on el sumatori de l'esquerra s'estén a tots els nombres naturals, el producte de la dreta ho fa a tots els nombres primers i $s > 1$ denota un nombre real. La validesa de la identitat és deguda al fet que tot nombre natural es descompon en factors primers *de manera única* (la qual cosa no seria provada rigorosament fins una cinquantena d'anys més tard per Carl Friedrich Gauss). Euler s'adonà que si el conjunt dels nombres primers fos finit, el producte de la dreta representaria una quantitat finita, per a tot s , mentre que el sumatori de l'esquerra representa una quantitat no finita quan s tendeix cap a 1. Com que les dues afirmacions es contradiuen, el conjunt dels nombres primers és infinit.

Euler lamentà el desconcert imperant en la successió dels nombres primers. Considerava que el comportament d'aquests nombres és tan misteriós que la seva comprensió restaria per sempre fora de l'abast de la ment humana. Euler no podia sospitar, però, que la seva identitat seria el punt de partida d'una intensa recerca que es produiria en el decurs dels segles subsegüents.

SOBRE LA QUANTITAT DE NOMBRES PRIMERS INFERIORS A UNA QUANTITAT DONADA

Més amunt hem escrit tots els nombres primers inferiors a 50. N'hi ha quinze. Si escrivíssim tots els nombres primers inferiors a 100, en trobaríem vint-i-cinc. I d'inferiors a 1.000, cent seixanta-vuit, etc. L'any 1785, Adrien-Marie Legendre introduí una funció, que es designa per $p(x)$, que compta el nombre de primers inferiors o iguals a x . Al mateix temps, Carl Friedrich Gauss construï taules molt extenses de primers (fins a sis milions) i comptà el seu nombre en cada miler de nombres naturals. De manera independent, Legendre i Gauss conclogueren que la funció $x / \log x$ aproximava bé, i que ho havia de fer cada cop millor en créixer x , el valor $p(x)$. Avui, que tenim tants mitjans de càlcul a l'abast, és interessant comprovar l'encert de les prediccions de Legendre i Gauss. Observem-ho en els resultats continguts a la taula:

x	$p(x)$	$x / \log x$
100	25	21.71
1000	168	144.76
10000	1229	1085.74
100000	9592	8685.89
1000000	78498	72382.41

LA FUNCIO ZETA DE RIEMANN

L'any 1859, Bernhard Riemann reprenqué l'estudi de la successió dels nombres primers en el punt on l'havia deixat Euler. En l'època de Riemann, l'ús dels nombres complexos i la manipulació de sèries eren pràctiques més habituals que no en la d'Euler. D'aquesta manera, Riemann pogué considerar una funció:

$$z(s) = \sum n^{-s}$$

definida per a tots els nombres complexos s de part real més gran que 1. En la memòria *Ueber die Anzahl der Primzahlen unter einer gegebenen Grösse*, Riemann estengué la funció anterior a tots els nombres complexos per mitjà d'una representació integral. Riemann intuï que la localització dels seus zeros havia de tenir una forta influència en el nombre de primers inferiors a una quantitat donada, la qual cosa formulà d'una manera precisa. Però les eines disponibles en l'època no li permeteren anar més lluny. La funció en qüestió s'anomenà la funció zeta de Riemann i quedà lligada indefectiblement a l'estudi de les lleis que regeixen el comportament dels nombres primers.

EL TEOREMA DELS NOMBRES PRIMERS

Jacques Hadamard (1865-1963) i Charles-Jean de la Vallée Poussin (1866-1962), dues vides paral·leles en la història de la matemàtica, provaren l'any 1896, de manera simultània i independentment, l'anomenat teorema dels nombres primers. Veritable fita matemàtica del segle XIX, el teorema afirma que la funció $x / \log x$ és asimptòticament equivalent a la funció $p(x)$, d'acord amb les conjectures formulades per Legendre i Gauss. Les demostracions d'ambdós autors són llargues i difícils. Un punt delicat en què es basa el resultat final és la prova que la funció zeta no té cap zero

punt delicat en què es basa el resultat final és la prova que la funció zeta no té cap zero de part real igual a 1. O sigui, que el nombre complex $z(1+bi)$ és sempre diferent de zero. La sola demostració d'aquest fet ocupa en l'article de De la Vallée Poussin més de vint pàgines.

Al llarg del segle XX, diversos autors han intentat simplificar les demostracions del teorema dels nombres primers. L'any 1949, A. Selberg i P. Erdős n'aconseguien una prova amb recursos elementals, però encara massa llarga per esdevenir popular. Successives simplificacions han conduït, finalment, a una demostració del teorema molt més assequible.

Les simplificacions més recents aconseguides en la demostració del teorema dels nombres primers són degudes, bàsicament, a D. J. Neumann (1980) i D. Zagier (1997). Aquests autors presenten de manera compacta molts recursos deguts als seus predecessors. La demostració que en resulta és analítica i, per descomptat, s'hi empra la funció zeta de Riemann a bastament. Avui, transcorreguts més de cent anys després de les primeres demostracions, el teorema dels nombres primers es pot aprendre en unes quatre o cinc hores de classe.

LA HIPÒTESI DE RIEMANN

En l'*International Congress of Mathematicians*, celebrat a París l'any 1900, David Hilbert presentà una llista de 23 problemes oberts, d'una rellevància especial. Els problemes de Hilbert han esperonat una part molt significativa de la recerca matemàtica del segle XX. El problema número 8 de Hilbert se centra en l'anomenada hipòtesi de Riemann. La hipòtesi de Riemann controla els zeros de la funció zeta en la banda crítica, tal com s'expressà en la memòria de Riemann de l'any 1859. Concretament, el problema demana demostrar que si un nombre complex $a+bi$ és un zero (no trivial) de la funció zeta, $\zeta(a+bi) = 0$ aleshores $a = 1/2$. La seva prova permetria obtenir, entre d'altres, bones fites del terme d'error $p(x) - x / \log x$.

Malgrat els nombrosos intents portats a terme durant gairebé 150 anys per provar la hipòtesi de Riemann, aquesta resta inassequible. En aquest sentit, els matemàtics entrem en l'any 2000 amb els deures proposats per Hilbert inacabats i la hipòtesi de Riemann emergeix com un repte matemàtic per a les noves generacions. Interpretacions espectrals i cohomològiques, fórmules de traces, trencament de simetries, transicions de fase, etc. són recursos que s'han presentat com a probables vies

d'atac de la hipòtesi de Riemann i que actualment són objecte d'una intensa recerca. D'altra banda, una forta experimentació numèrica la corrobora.

PER A QUÈ ENS CALEN PRIMERS TAN GRANS?

En arribar a aquest punt, algú podria interpretar la tasca exposada com un exercici intel·lectual pur, desconnectat de la *realitat*. El més sorprenent, però, és que l'existència de primers grans s'ha convertit en els darrers anys, i a causa de circumstàncies originades per la tecnologia d'última hora, en salvaguarda dels nostres interessos. En efecte, la circulació d'informació privada en xarxa i el nombre creixent d'usuaris obliga, cada cop més, al maneig de mètodes fiables de codificació de la informació. Un dels mètodes més populars emprats en criptografia és l'anomenat RSA, en honor dels seus creadors R. L. Rivest, A. Shamir, L. Adleman. La seguretat del mètode es basa, precisament, en la dificultat de factoritzar de manera eficient els nombres naturals que són producte de dos nombres primers molt grans. Les implementacions més elaborades del mètode RSA (així com també d'altres similars) utilitzen lleis aritmètiques profundes, el coneixement de les quals seria inimaginable sense el suport teòric que s'ha desenvolupat a l'entorn de la funció zeta.

EPÍLEG

Ara com ara, si en una pel·lícula o novel·la de ciència ficció es volgués donar a entendre que una civilització d'alienígenes es troba un punt més avançada que la nostra, n'hi hauria prou que transmetés, a més de la successió dels nombres primers, una prova de la hipòtesi de Riemann.



Garantía de seguridad

En El Corte Inglés estamos especialmente preocupados por la seguridad y por asegurar la confidencialidad de los datos aportados por nuestros clientes. Por ello, además de ser socios fundadores de la @ECE (Asociación Española de Comercio Electrónico) estamos adheridos a Confianza Online, un sistema de resolución de las posibles controversias que se puedan dar entre consumidores y empresas en el ámbito del Comercio Electrónico y la Publicidad Interactiva, apoyado por un gran número de asociaciones empresariales, el Instituto Nacional de Consumo, la Agencia de Protección de Datos y por el Ministerio de Ciencia y Tecnología.

En el momento que un cliente se registra en nuestro servidor seguro o realiza un pedido, sus datos personales, domiciliarios, y los relativos a su forma de pago, son incorporados a nuestra base de datos, utilizándose únicamente para tramitar el pedido, así como para enviar información sobre ofertas y servicios que puedan resultar de su interés. El Corte Inglés asegura la confidencialidad de los datos aportados por nuestros clientes, y garantiza que en ningún caso será cedida a terceras empresas ajenas a nuestro grupo.

Ley de Protección de datos: LOPD.

En cumplimiento de lo dispuesto en la Ley Orgánica 15/1999 de 13 de Diciembre, de Protección de Datos de Carácter Personal, el cliente de El Corte Inglés podrá en todo momento ejercitar los derechos de acceso, rectificación, cancelación y oposición, comunicándolo por escrito a El Corte Inglés, C/ Alfonso Gómez, 8 - 28037 Madrid o mediante correo electrónico.

Información adicional sobre nuestros sistemas de seguridad y de garantía de protección de Datos Personales

Internet es un medio de comunicación y también un nuevo medio que posibilita el realizar transacciones comerciales a través de la red. Por ello, una de las principales preocupaciones por parte de los usuarios que utilizan internet es la seguridad de los datos en la red. Como transacción de Comercio Electrónico se entiende todo el proceso de realización de un acuerdo comercial incluyendo el contacto entre ambas partes: cliente y empresa. Los aspectos que debe reunir toda transacción comercial deben ser:

La **Autenticación** que nos garantiza la personalidad jurídica o física con la que nos comunicamos.

La **Integridad**, es decir, que el contenido de la comunicación entre ambas partes no puede ser modificado.

La **Confidencialidad**, que consiste en la garantía de que nadie no autorizado pueda conocer el contenido de la comunicación.

Proceso de compra en El Corte Inglés

A continuación se describen los procesos que intervienen en la compra a través del servidor de El Corte Inglés:

1. Registro de clientes.

El cliente se registra rellenando en un formulario sus datos personales y de pago, dándose de alta en el sistema con un nombre de usuario y una clave determinada por él mismo. Este proceso implica el envío de datos, el cual se realiza de forma segura mediante el empleo de un sistema avanzado de seguridad SSL (Secure Socket Layers). La mayoría de los navegadores existentes aceptan el SSL, pero ante cualquier duda diríjase a su proveedor de acceso a internet.

Al realizar una transacción que implique intercambio de información confidencial, se accede automáticamente a la zona segura del servidor, indicando el navegador esta circunstancia mediante la visualización de una URL del tipo <https://libros.elcorteingles.es>, y se visualiza en el navegador un icono en forma de candado cerrado. A partir de este momento, cualquier envío de datos se realiza de forma totalmente segura.

2. Cesta de la compra.

El cliente navega por nuestras tiendas incorporando a su cesta de la compra aquellos artículos que desee comprar.

Las cookies son pequeñas piezas de información que El Corte Inglés necesita para conocer los intereses de nuestros clientes y que no contienen ningún tipo de información personal. La mayoría de los navegadores aceptan automáticamente cookies, pero también es normalmente posible configurarlos para su no aceptación. En ese caso podrá navegar, pero quizá no tenga acceso a algunas funciones de nuestras tiendas.

3. Tramitación del pedido.

Una vez finalizado el proceso de selección de artículos, se pasa al apartado de confirmación del pedido, en el que se solicita al cliente que se identifique en caso de que se hubiera registrado anteriormente o en caso contrario se le pide que se registre. En el caso de que el cliente esté registrado, sus datos personales ya están alojados en nuestro servidor seguro y no viajan por la red. Además, si es titular de la Tarjeta El Corte Inglés y lo indicó en su ficha de registro, el número de la misma tampoco viaja en el caso de que la utilice como forma de pago del pedido.

Esta fase se realiza de forma totalmente segura al estar integrada dentro de nuestro servidor seguro.

Recomendaciones y Precauciones.

Estas son algunas de las precauciones que aconsejamos deben de tomar nuestros clientes:

No facilitar a nadie el usuario, ni la contraseña.

No apuntarla en lugares de fácil acceso: ordenador, agenda,

Utilizar siempre nuestro sistema de seguridad SSL.

Desconectar siempre la sesión del navegador con posterioridad de haber accedido a una zona de seguridad o de haber introducido al sistema el usuario o contraseña.



Política de protecció de dades

A Caixa Catalunya garantim la protecció de les dades dels nostres clients. El segell de l'Associació Espanyola de Comerç Electrònic (AECE), ens avala com a entitat financera adherida al seu Codi Ètic de Protecció de dades a Internet.

Per tal de millorar el servei i adequar-lo a les preferències de l'usuari, el site de Caixa Catalunya www.caixacatalunya.es utilitza cookies en la navegació pel seu web. L'usuari pot optar per configurar el seu navegador de manera que l'avis de la recepció de les cookies i impedeixi que s'instal·lin al disc dur.

Caixa Catalunya garanteix que les dades personals (nom, telèfon, adreça postal, e-mail...) proporcionades dins el seu Web seran utilitzades exclusivament pel motiu amb què hagin estat sol·licitades.

En cas que l'usuari sol·liciti informació sobre serveis, productes o desitgi realitzar tramitació de reclamacions o incidències, a través de l'enviament de formularis inclosos al Web de Caixa Catalunya, serà necessari recollir aquelles dades personals imprescindibles per poder atendre la seva sol·licitud.

Caixa Catalunya assegura la confidencialitat de les dades facilitades, que s'incorporaran a un fitxer automatitzat del que ella mateixa n'és responsable. L'interessat autoritza Caixa Catalunya perquè pugui cedir les seves dades a les societats del seu grup amb finalitats comercials i operatives. L'interessat té dret a obtenir informació d'aquestes dades, a oposar-se al seu tractament, així com a sol·licitar la rectificació o cancel·lació si fossin inexactes o incompletes, a través del Servei CC On-Line i/o de la xarxa d'oficines, en els termes previstos per la Llei Orgànica de Protecció de Dades de Caràcter Personal.

Per garantir un correcte funcionament del sistema, recomanem que mantingui sempre actualitzat el seu programari. Si no disposa de la versió correcta pot obtenir-la

Caixa d'Estalvis de Catalunya, Plaça Antoni Maura, 6 - 08003 Barcelona, tel. 93 484 50 00, fax 93 484 51 41, télex 50722 CADC, entitat subjecta a supervisió del Banc d'Espanya, inscrita al Registre de Caixes d'Estalvis del Banc d'Espanya amb el número 16.

Seguretat de la connexió

A Caixa Catalunya som conscients de la necessitat de garantir el trànsit d'informació entre la Caixa i els seus clients. Per aquest motiu, Caixa Catalunya compta

amb mesures per a garantir la seguretat i confidencialitat del sistema.



La informació que es transmet per la xarxa està xifrada mitjançant el protocol SSL i claus de 128 bits. El xifrat és un procés que assegura que la informació tramesa només és intel·ligible per l'ordinador de l'usuari el servidor de Caixa Catalunya. D'aquesta manera s'evita que tercers puguin veure o capturar la informació que s'intercanvia.

El servidor de Caixa Catalunya ha estat certificat per l'autoritat certificadora internacional Verisign, que garanteix al client que s'està connectant realment a Caixa Catalunya de forma segura. El navegador informa que la connexió és segura mostrant un cadenat la part inferior de la pantalla.

El control d'accés al servei de banca per Internet, Caixa Catalunya On-Line, es realitza mitjançant la introducció necessària de dos codis de seguretat. Addicionalment, existeix un import d'operatòria màxim diari, i en la realització d'operacions amb transcendència econòmica el sistema sol·licita una de les coordenades que consten a la targeta de claus del servei CC On-Line.

Per altra banda en cada connexió al servei CC On-Line, s'informa el dia i l'hora de l'última connexió, dada que permet a l'usuari controlar els accessos al servei. Aquest Web està optimitzat per a ser visualitzat amb una resolució de 800x600 píxels i per a les següents versions de navegador:

Internet Explorer 4.01, 5.01, 5.5.

Si accedeix des de navegador Netscape Communicator, li recomanem les versions 4.06, 4.51, 4.73, 4.76.

En el cas d'entorn Macintosh, li recomanem les versions Internet Explorer 5.0 i Netscape Communicator 4.77.

Per garantir un correcte funcionament del sistema, recomanem que mantingui sempre actualitzat el seu programari. Si no disposa de la versió correcta pot obtenir-la de la web del proveïdor corresponent:

Microsoft Internet Explorer: www.microsoft.com

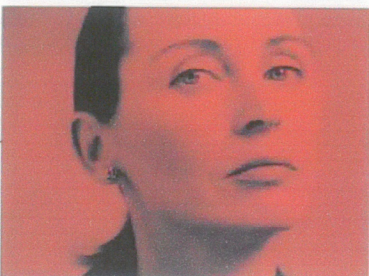
Netscape Communicator: www.netscape.com

Per a qualsevol dubte o aclariment l'atendrem al telèfon 902 42 55 42, a la nostra xarxa d'oficines o, si ho prefereix, a través de correu electrònic.





LA NUEVA SOCIEDAD Y SAFELAYER



La sociedad actual tiende hacia una cultura cuyo soporte central es el BIT. Los hábitos y los procesos que hoy tienen como soporte el papel quedarán sustituidos por el bit, alcanzando entonces la sociedad tal grado de eficiencia que las economías y los hábitos sociales se transformarán completamente.

La mutación no es sencilla, pero ya ha comenzado, y los documentos de identidad, métodos de pago, documentos legales, etc. formarán parte de este cambio. Pero un cheque endosado, un contrato firmado, un protocolo notarial, conllevan un compromiso y aceptación ya que aparece la firma manuscrita de un individuo social. Es

decir, la seguridad que los individuos depositan en el papel y en la firma es vital en esta sociedad actual.

En este momento, sólo la tecnología de criptografía de clave pública mediante el despliegue de una infraestructura de PKI garantiza esa misma confianza

cuando se produce el paso del papel al bit.

Safelayer Secure Communications es un fabricante de software de seguridad basado en PKI (Infraestructura de Clave Pública) con una oferta completa de soluciones, aplicaciones y herramientas necesarias para la implantación e integración de la tecnología en cualquier entorno. El conjunto de determinados aspectos de nuestros productos hace diferente y única a Safelayer. Nuestra tecnología y productos han sido diseñados teniendo en cuenta las siguientes premisas:

- Basada exclusivamente en estándares.
- Tecnología y productos abiertos e integrables.
- Disponibilidad y escalabilidad ilimitada.
- Máxima seguridad.

A nivel mundial, Safelayer es la compañía que reúne el mayor número de certificados de conforme técnicamente y de interoperable de las comunidades del sector más exigentes y reconocidas.

Un departamento de Investigación y Desarrollo (I+D) propio con un profundo conocimiento de la tecnología, una experiencia a nivel internacional de más de 15 años en el sector de los sistemas de información en general y de más de 10 años en el campo de la seguridad en particular. Un equipo altamente capacitado con una alta cualificación al provenir sus principales responsables del área de investigación de Universidades líderes en estas tecnologías.

La familia de productos KeyOne nace como respuesta a los retos de confianza que han generado las relaciones virtuales tan comunes en nuestros días. KeyOne, propor-

ciona los niveles de confianza requeridos en entornos abiertos mediante la correcta implantación de los más avanzados servicios de seguridad y el uso de las más contrastadas técnicas criptográficas de forma transparente a la organización que las incorpora, convirtiéndose en el eje principal de la credibilidad en cualquier proceso de negocio on-line.

KeyOne, tecnología PKI, es por tanto un sistema de gestión de confianza entre las distintas partes que constituyen una organización, y está compuesto por:

KEYONE CA Autoridad de certificación responsable de implementar las prácticas y políticas de certificación. Genera un completo sistema de gestión de certificados x.509v3 que garantiza la correcta identidad de sus poseedores además de establecer el ámbito de su actuación y responsabilidad.

KEYONE RA Autoridad de registro está formada por un completo conjunto de componentes que permiten a la organización poner en práctica aquellos mecanismos necesarios para la correcta identificación de los usuarios que conformaran relaciones confiables entre sí.

KEYONE OCSP Solución que permite constatar la validez de un certificado digital en tiempo real, es decir, un sistema que permite la verificación del estado que tiene el certificado del usuario para llevar a cabo una operación, transacción o acceso en el instante en que se lleva a cabo.

KEYONE TSA Solución que permite establecer con carácter no-repudiable el instante en el que una operación se llevó a cabo, mediante la emisión de sellos de tiempo.

KEYONE Desktop Solución que permite a los usuarios de la PKI hacer un uso completo de todos y cada uno de los servicios de confianza y seguridad que ésta presta, para ello implementa mecanismos como el de múltiple-firma, firma avanzada, etc.

KEYONE Toolkits Completo set de herramientas de desarrollo que permiten la integración de servicios tales como: confidencialidad, integridad, autenticidad y no repudio en las aplicaciones que implementan los procesos productivos de la organización.

Una familia de productos que permiten desarrollar soluciones escalables, fácilmente personalizables y sencillas de instalar y administrar. ¡Que se adapten a lo que Vd. necesita!

NUESTRAS SOLUCIONES



W3C WORLD WIDE WEB

Secure Electronic Transaction

JAVA

SOFTWARE
SAP

NIST

GET S/MIME.

Common Criteria

identrus
COMPLIANT

GLOBAL TRADING
GTA

Microsoft

EESSI
The European Electronic Signature Standardization Initiative

CUANDO LA CALIDAD ES MÁS QUE UNA EXIGENCIA

El suministrar uno de los elementos claves en la nueva sociedad, la PKI para la e-economy, obliga a Safelayer Secure Communications a

mantener una exigente labor de I+D como única forma de garantizar su confianza en nuestros sistemas y productos.

Esta garantía se consigue no sólo diseñando y desarrollando nuestros procedimientos de software seguro, sino por la continua evaluación que terceras empresas hacen de nuestros productos, y también, por la participación en el desarrollo de normativas y estándares en seguridad y PKI.

Una garantía y una calidad que no sólo se refleja en nuestras soluciones, sino asimismo en el cumplimiento de estándares de seguridad e interoperabilidad emitidos por EESSI, NIST o W3C, o por la certificación de nuestros productos conforme a ISO 9001:2000 y COMMON CRITERIA, así como por nuestras soluciones homologadas por Identrus, GTA, Microsoft, SAP...

Y es que en Safelayer entendemos la calidad como la única forma de garantía.

LA EXPERIENCIA SE DEMUESTRA TRABAJANDO

Hay una frase muy conocida que dice que el movimiento se demuestra andando. Nosotros creemos que en el trabajo se puede aplicar una filosofía muy parecida. Y que la capacidad se demuestra por la envergadura de los proyectos que uno acomete. Por eso, en Safelayer Secure Communications nos sentimos más que capaces de desarrollar su proyecto. Porque nuestra amplísima experiencia en múltiples campos así lo demuestra. Y nuestra experiencia es, al mismo tiempo, su mejor garantía.

Aquí tiene algunas de nuestras referencias:



ADMINISTRACIONES PÚBLICAS

Ministerio de Presidencia, Ministerio del Interior, Ministerio de Defensa, Generalitat de Catalunya, Junta de Andalucía, Gobierno Vasco, Gobierno de Aragón, Ministerio de Justicia (Portugal), Ministerio de Agricultura (Portugal)...



ENTIDADES FINANCIERAS

Banco Sabadell, Banesto, Banco Guipuzcoano, Caixa de Catalunya, ABN Amro (Uruguay)...



TELECOMUNICACIONES

Relevión, Amena, Euskaltel, Telefónica, Canarias Telecom, Retena, Supercable Andalucía, RSL COM, Tele-Cable, R Galicia, Able, Reteval, Menta, Madritel...



PRESTADORES DE SERVICIOS DE CERTIFICACIÓN

Cámaras de Comercio (Camerfirma), Consejo Superior de Notarios (Feste), Cámara Nacional de Comercio y Servicios de Uruguay, Bolsa de Comercio, Confederación Colombiana de Cámaras de Comercio Certificadora...



INDUSTRIA Y OTROS SECTORES

Schlumberger Sema, Abitab, G&D, Universidad UPC, El Corte Inglés, Colegio de Arquitectos de Catalunya, Agencia Catalana del Agua...

Si desea recibir más información de Safelayer, por favor póngase en contacto con nosotros en:
e-mail: info@safelayer.com ó www.safelayer.com

PORQUE SÓLO UN GRAN EQUIPO OFRECE GRANDES RESULTADOS

Sólo trabajando con los mejores se consiguen grandes resultados.

Por eso, en Safelayer Secure Communications colaboramos con las empresas líderes en cada sector. Para ofrecerle lo mejor en cada campo, operando con diferentes perfiles que se ajusten al suyo y a sus necesidades, sean las que sean. Consultoras, integradoras, partners tecnológicos... un conjunto de compañías que garantizan la integración e interoperabilidad de nuestros productos y de las soluciones que le ofrecemos. A nivel local o internacional. Del tamaño y las necesidades que usted tenga.

Expertos en seguridad e integración y en el desarrollo de proyectos para cualquier cliente. Un gran equipo que le garantiza los mejores resultados.

AIG

Andersen

Bull Portugal

Camerfirma

Cap Gemini Ernst&Young

CMG

Consult Hyperion

Deloitte&Touche

DMR Consulting

Euskaltel

G&D

Gemplus

Ibermática

Indra

Innosec

Integris

Larraby

Microsa

Nakua

nCipher

Novabase

Schlumberger Sema

Secartis

Secunet

Semarket

SGI

Soluziona (Grupo Unión Fenosa)

Unicom

Unisys

Worldplex

¿POR QUÉ SAFELAYER?

POR NUESTRA TECNOLOGÍA PROPIA

- Flexibilidad, modularidad y escalabilidad.
- Facilidad en la customización de nuestros productos.
- Interoperabilidad.
- Ahorro significativo en costes y tiempo de integración.



POR NUESTRA CALIDAD Y CERTIFICACIÓN

- Única compañía europea cuyos productos han sido homologados por: Identrus, SAP y GTA
- Estándares de Calidad: ISO 9001, Common Criteria "EAL4 augmented"



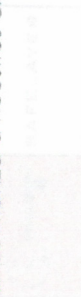
POR NUESTRA EXPERIENCIA

- Gran experiencia en implantación de proyectos a nivel vertical (banca, corporaciones...) con especialización en e-Government y Consultoría Estratégica
- Integración de nuestras soluciones en aplicaciones de clientes.



NUESTRO OBJETIVO

- Aportar confianza a nuestros clientes en esta nueva sociedad.



SAFELAYER ES UNA EMPRESA DE CONSULTORÍA

SAFELAYER, S.A. - C/Alfonso de Ercilla, 10 - 28014 Madrid - España - Tel: +34 91 400 00 00 - Fax: +34 91 400 00 01

SAFELAYER, S.A. - C/Alfonso de Ercilla, 10 - 28014 Madrid - España - Tel: +34 91 400 00 00 - Fax: +34 91 400 00 01

SAFELAYER, S.A. - C/Alfonso de Ercilla, 10 - 28014 Madrid - España - Tel: +34 91 400 00 00 - Fax: +34 91 400 00 01



SAFELAYER SECURE COMMUNICATIONS S.A.

C./Basauri, 17. Edificio Valreality. Edif.B. Planta baja iza. Ofic.B. 28023 Madrid (SPAIN) Tel.: +34 91 7080480 Fax: +34 91 3076652

Edificio World Trade Center (S-4) Moll de Barcelona S/N 08039 Barcelona (SPAIN) Tel.: +34 93 5088090 Fax: +34 93 5088091

WWW.SAFELAYER.COM

Nueva
#1: "File NUMBER.MTH, copyright (c) 1994-1997 by Soft Warehouse, Inc."

Nueva
#2: "Many functions in this file were contributed by Johann Wiesenbauer"

#3: "of Vienna, Austria." Nueva

#4: default1 := 1 Nueva

#5: CEILING(a, default1) := - FLOOR(-a, default1) Nueva

#6: $\text{ROUND}(a, \text{default1}) := \text{FLOOR}\left(\frac{a}{\text{default1}} + \frac{1}{2}\right)$ Nueva

#7: $\text{SQUARE_WAVE}(x) := (-1)^{\text{FLOOR}(x)}$ Nueva

Nueva
#8: $\text{EXTENDED_GCD}(a, b) := \text{ITERATE}\left(\left[v_{-2}, \left[v_{-4}, v_{-6}\right]\right], v_{-}, \right.$
 $\text{ITERATE}(\text{IF}(\text{MOD}(v_{-1}, v_{-2}) = 0, v_{-}, \left[v_{-2}, \text{MOD}(v_{-1}, v_{-2}), v_{-4}, v_{-3} - \right.$
 $\left. \text{FLOOR}(v_{-1}, v_{-2}) \cdot v_{-4}, v_{-6}, v_{-5} - \text{FLOOR}(v_{-1}, v_{-2}) \cdot v_{-6}\right]), v_{-}, [a, b, 1,$
 $0, 0, 1]), 1)$

Nueva
#9: $\text{INVERSE_MOD}(a, m) := \text{IF}(\text{GCD}(a, m) = 1, \text{MOD}(\text{ITERATE}(\text{IF}(\text{MOD}(\alpha_{-}, \beta_{-}) =$
 $0, [\alpha_{-}, \beta_{-}, \gamma_{-}, \delta_{-}], [\beta_{-}, \text{MOD}(\alpha_{-}, \beta_{-}), \delta_{-}, \gamma_{-} - \text{FLOOR}(\alpha_{-}, \beta_{-}) \cdot \delta_{-}]),$
 $[\alpha_{-}, \beta_{-}, \gamma_{-}, \delta_{-}], [a, m, 1, 0])), m)$

#10: $\text{POWER_MOD}(a, n, m) := \text{MOD}(\text{IF}(n \geq 0, a, \text{INVERSE_MOD}(a, m))^{|n|}, m)$ Nueva

Nueva

#11:

$$\text{SOLVE_MOD}(u, x, m) := \text{ITERATE} \left(\text{IF} \left(\text{MOD} \left(\lim_{x \rightarrow 0} (\text{RHS}(u) - \text{LHS}(u)), t_- \right) = 0, \right. \right. \\ \left. \left. \text{ITERATES} \left(s_- + \frac{m}{t_-}, s_-, \right. \right. \right. \\ \left. \left. \text{MOD} \left(\frac{\text{INVERSE_MOD} \left(\frac{\frac{d}{dx} \text{LHS}(u)}{t_-}, \frac{m}{t_-} \right) \cdot \lim_{x \rightarrow 0} (\text{RHS}(u) - \text{LHS}(u))}{t_-}, \frac{m}{t_-} \right), \right. \right. \\ \left. \left. t_- - 1 \right), [] \right), t_-, \text{GCD} \left(\frac{d}{dx} \text{LHS}(u), m \right), 1 \right)$$

Nueva

$$\text{\#12: CRT}(a, m) := \text{ITERATE} \left(\text{MOD} \left(a \cdot \text{VECTOR} \left(\frac{p_-}{m_-} \cdot \text{INVERSE_MOD} \left(\frac{p_-}{m_-}, m_- \right), m_-, m \right), \right. \right. \\ \left. \left. p_- \right), p_-, \Pi(m_-, m_-, m), 1 \right)$$

$$\text{\#13: NTH_PRIME}(n) := \text{ITERATE}(\text{NEXT_PRIME}(k), k, 1, n)$$

Nueva

Nueva

$$\text{\#14: PRIMEPI}(x, d, a) := \text{IF} \left(d, 0, \lim_{[true, false] \rightarrow [1, 0]} \frac{(x - a)/d}{\sum_{n=0}^{\infty} \text{PRIME}(d \cdot n_+ + a)}, \text{PRIMEPI}(x, 6, 1) + \text{PRIMEPI}(x, 6, 5) + \text{IF}(x \geq 3, 2, \text{FLOOR}(x, 2)) \right)$$

Nueva

$$\begin{aligned} \#15: \text{FAREY}(n) &:= \text{SORT} \left(\left(\text{ITERATE} \left(\text{IF} \left(v_{-1} = v_{-2} \wedge v_{-2} = n, v_{-}, \left[\text{IF}(v_{-1} = v_{-2}, \right. \right. \right. \right. \right. \\ & \quad \left. \left. \left. \left. 1, v_{-1} + 1 \right), \text{IF}(v_{-1} = v_{-2}, v_{-2} + 1, v_{-2} \right), \text{IF} \left(\text{GCD}(v_{-1}, v_{-2}) = 1, \right. \right. \right. \\ & \quad \left. \left. \left. \left. \text{APPEND} \left(v_{-3}, \left[\frac{v_{-1}}{v_{-2}} \right], v_{-3} \right) \right], v_{-}, [1, 1, []] \right] \right) \right) \right) \end{aligned}$$

Nueva

$$\begin{aligned} \#16: \text{PRIME_FACTORIZATION}(n) &:= \text{VECTOR}(\text{ITERATE}(\text{IF}(\text{PRIME}(p_{-}), [p_{-}, k_{-}], \\ & \quad [p_{-}^{k_{-}/(k_{-} + 1)}, k_{-} + 1], [p_{-}^{k_{-}/(k_{-} + 1)}, k_{-} + 1]), [p_{-}, k_{-}], [f_{-}, \\ & \quad 1]), f_{-}, \text{FACTORS}(\text{FACTOR}(n))) \end{aligned}$$

Nueva

$$\begin{aligned} \#17: \text{DIVISORS}(n) &:= \text{SORT} \left(\left(\text{ITERATE}(\text{IF}(\text{DIMENSION}(v_{-}) = 0, [u_{-}, v_{-}], \right. \right. \\ & \quad \left. \left. [\text{APPEND}([u_{-}] \cdot [\text{ITERATES}(v_{-1,1} \cdot b_{-}, b_{-}, 1, v_{-1,2})]), \right. \right. \\ & \quad \left. \left. \text{DELETE_ELEMENT}(v_{-}) \right]), [u_{-}, v_{-}], [[1], \text{PRIME_FACTORIZATION}(n)]) \right) \end{aligned}$$

Nueva

$$\#18: \text{DIVISOR_SIGMA}(k, n) := \prod_{j=0}^{v_{-1} \downarrow 2} v_{-1}^{k \cdot j_{-}}, v_{-}, \text{PRIME_FACTORIZATION}(n)$$

$$\#19: \text{DIVISOR_TAU}(n) := \prod_{2}^{v_{-} + 1, v_{-}}, \text{PRIME_FACTORIZATION}(n)$$

Nueva

$$\#20: \text{EULER_PHI}(n) := n \cdot \prod \left(1 - \frac{1}{v_{-1}}, v_{-}, \text{PRIME_FACTORIZATION}(n) \right)$$

Nueva

$$\#21: \text{MOEBIUS_MU}(n) := \prod(\text{IF}(\text{PRIME}(k_{-}), -1, 0), k_{-}, \text{FACTORS}(\text{FACTOR}(n)))$$

Nueva

$$\#22: \text{SQUAREFREE}(n) := \text{IF}(\text{MOEBIUS_MU}(n) = 0, \text{false}, \text{true})$$

Nueva

$$\#23: \text{CYCLOTOMIC}(n, x) := \prod \left((x^{n/d_{-}} - 1)^{\text{MOEBIUS_MU}(d_{-})}, d_{-}, \text{DIVISORS}(n) \right)$$

Nueva

$$\#24: \text{CATALAN}(n) := \frac{\text{COMB}(2 \cdot n, n)}{n + 1}$$

Nueva

#25: $\text{BERNOULLI}(n) := \text{IF}\left(n = 0, 1, \text{IF}\left(n = 1, -\frac{1}{2}, -n \cdot \text{ZETA}(1 - n)\right)\right)$ Nueva

Nueva

```

#26: BERNOULLI_POLY(n, x) := IF  $\left( n = 1, x - \frac{1}{2}, n \cdot \lim_{x \rightarrow x} \frac{x - 1}{\sum_{k=1}^{n-1} k} + \right.$ 
    BERNOULLI(n)  $\left. \right)$ 

```

Nueva

$$\#27: \text{EULER_POLY}(n, x) := \frac{2}{n+1} \cdot \left(\text{BERNOULLI_POLY}(n+1, x) - 2^{n+1} \cdot \text{BERNOULLI_POLY}\left(n+1, \frac{x}{2}\right) \right)$$

#28: $\text{EULER}(n) := \text{IF} \left(\text{MOD}(n, 2) = 1, 0, 2^{\frac{n}{2}} \cdot \text{EULER_POLY} \left(n, \frac{1}{2} \right) \right)$ Nueva

#29:
$$\text{GEN_LUCAS}(n, p, q, 10, 11) := \left(\begin{bmatrix} 0 & 1 \\ -q & p \end{bmatrix}^n \cdot [10, 11] \right)_1$$
 Nueva

```
#30: U_LUCAS(n, p, q) := GEN_LUCAS(n, p, q, 0, 1) Nueva
```

```
#31: V_LUCAS(n, p, q) := GEN_LUCAS(n, p, q, 2, p) Nueva
```

Nueva

$$\begin{aligned} \#32: U_MOD(n, p, q, m) := IF & \left(n = 0, 0, ITERATE \left(MOD \left((-p \cdot l_{-1} + \right. \right. \right. \\ & 2 \cdot l_{-2}) \cdot INVERSE_MOD(p^2 - 4 \cdot q, m), m), l_{-1}, ITERATE \left(IF \left((n \wedge v_{-4}) = 0, \right. \right. \\ & \left[MOD \left(v_{-1}^2 - 2 \cdot MOD(q^{v_{-3}}, m), m), MOD(v_{-1} \cdot v_{-2} - p \cdot MOD(q^{v_{-3}}, m), m), \right. \right. \\ & \left. \left. 2 \cdot v_{-3}, \frac{v_{-4}}{2} \right], \left[MOD(v_{-1} \cdot v_{-2} - p \cdot MOD(q^{v_{-3}}, m), m), MOD(v_{-2}^2 - \right. \right. \\ & \left. \left. 2 \cdot MOD(q^{v_{-3}+1}, m), m), 2 \cdot v_{-3} + 1, \frac{v_{-4}}{2} \right] \right), v_{-1}, [2, p, 0, \\ & \left. \left. \left. FLOOR(LOG(n, 2)) \right], FLOOR(LOG(n, 2)) + 1 \right], 1 \right) \end{aligned}$$

$$\begin{aligned} \#33: V_MOD(n, p, q, m) := & IF \left(n = 0, MOD(2, m), \left(ITERATE \left(IF \left((n \wedge v_{-4}) = 0, \right. \right. \right. \\ & \left[MOD \left(v_{-1}^2 - 2 \cdot MOD(q^{v_{-3}}, m), m \right), MOD(v_{-1} \cdot v_{-2} - p \cdot MOD(q^{v_{-3}}, m), m), \right. \\ & \left. 2 \cdot v_{-3}, \frac{v_{-4}}{2} \right], \left[MOD(v_{-1} \cdot v_{-2} - p \cdot MOD(q^{v_{-3}}, m), m), MOD(v_{-2}^2 - \right. \\ & \left. 2 \cdot MOD(q^{v_{-3} + 1}, m), m), 2 \cdot v_{-3} + 1, \frac{v_{-4}}{2} \right] \right), v_{-}, [2, p, 0, \\ & \left. \left. \left. FLOOR(LOG(n, 2)) \right], FLOOR(LOG(n, 2)) + 1 \right) \right) \end{aligned}$$

```
#35: LUCAS(n) := V_LUCAS(n, 1, -1)
```

```
#37: PELL(n) := GEN_LUCAS(n, 2, -1, 1, 0)
```

```
#38: LUCAS_LEHMER_TEST(p) := IF(ITERATE(MOD(s_2 - 2, 2^p - 1), s_, 4, p - 2)
    = 0, true, false)
```

```
#39: NEXT_MERSENNE_DEGREE(n) := IF(n < 2, 2,
    ITERATE(IF(LUCAS_LEHMER_TEST(p_), p_, NEXT_PRIME(p_)), p_,
    NEXT_PRIME(n)))
```

```
#40: MERSENNE LIST(n) := ITERATES(NEXT MERSENNE DEGREE(n_), n_, 2, n - 1)
```

```
#41: MERSENNE(n) := 2ITERATE(NEXT_MERSENNE_DEGREE(j), j, 1, n) - 1 Nueva
```

```
#42: MERSENNE_DEGREE(n) := ELEMENT([2, 3, 5, 7, 13, 17, 19, 31, 61, 89,
107, 127, 521, 607, 1279, 2203, 2281, 3217, 4253, 4423, 9689, 9941,
11213, 19937, 21701, 23209, 44497, 86243, 110503, 132049, 216091,
756839, 859433, 1257787, 1398269, 2976221, 3021377], n)
```

```
#43: MERSENNE(n) := 2MERSENNE_DEGREE(n) - 1
```

#44: $\text{PERFECT}(n) := \text{ITERATE}\left(\frac{(m_- + 1) \cdot m_-}{2}, m_-, \text{MERSENNE}(n), 1\right)$ Nueva

#45: CONTINUED_FRACTION(u, n) := FLOOR $\left(\text{ITERATES} \left(\frac{1}{\text{MOD}(x_-)}, x_-, u, n \right) \right)$ Nueva

Nueva

#46: CONVERGENT_AUX(v, k, a) := IF $\left(k = 0, a, \text{CONVERGENT_AUX} \left(v, k - 1, v_k + \frac{1}{a} \right) \right)$

#47: CONVERGENT(v) := CONVERGENT_AUX(v, DIMENSION(v), ∞) Nueva

Nueva

#48: PARTS_AUX(n, m) := IF $\left(n < 2 \cdot m, 1, 1 + \sum_{k=m}^{\text{FLOOR}(n, 2)} \text{PARTS_AUX}(n - k, k_-) \right)$

#49: PARTS(n) := IF(n < 0, 0, PARTS_AUX(n, 1)) Nueva

Nueva

#50: DISTINCT_PARTS_AUX(n, m) := IF $\left(n < 2 \cdot m, 1, 1 + \sum_{k=m}^{\text{FLOOR}(n, 2)} \text{DISTINCT_PARTS_AUX}(n - k, k_- + 1) \right)$

#51: DISTINCT_PARTS(n) := IF(n < 1, 0, DISTINCT_PARTS_AUX(n - 1, 1)) Nueva

Nueva

$$\begin{aligned} \#52: \text{PARTS}(n) &:= \text{IF} \left(n < 2, 1, \text{FLOOR} \left(\text{APPROX} \left(\frac{\sqrt{n/\text{LOG}(n, 11)}}{\sum_{k_=1}^{\infty}} \cdot \frac{1}{\pi} \cdot \sqrt{\frac{k_-}{2}} \right) \cdot \left(\frac{k_-}{\sum_{h_=1}^{\infty}} \right. \right. \right. \\ &\quad \left. \left. \left. \text{IF} \left(\text{GCD}(h_-, k_-) = 1, \text{COS} \left(\pi \cdot \left(\left(\frac{k_- - 1}{\sum_{i_=1}^{\infty}} \left(\frac{i_-}{k_-} - \frac{1}{2} \right) \cdot \left(\text{MOD} \left(\frac{i_- \cdot h_-}{k_-} \right) - \right. \right. \right. \right. \right. \right. \right. \right. \right. \right. \right. \right. \right. \\ &\quad \left. \left. \left. \frac{1}{2} \right) \right) - \frac{2 \cdot n \cdot h_-}{k_-} \right) \right), 0 \right) \cdot \left(- \right. \\ &\quad \left. \frac{2 \cdot \sqrt{6 \cdot \hat{e}} - \pi \cdot \sqrt{(24 \cdot n - 1)/(6 \cdot k_-)} \cdot (\hat{e})^{\pi \cdot \sqrt{(24 \cdot n - 1)/(3 \cdot k_-)}} \cdot (6 \cdot k_- - \pi \cdot \sqrt{(24 \cdot n - 1)/(6 \cdot k_-)})^{3/2}}{k_- \cdot (24 \cdot n - 1)} \right. \\ &\quad \left. \cdot (n - 1) - 6 \cdot k_- - \pi \cdot \sqrt{(24 \cdot n - 1)} \right) \cdot \text{LOG} \left(\frac{1}{4 \cdot n \cdot \sqrt{3}} \cdot \text{EXP} \left(\pi \cdot \sqrt{\frac{2 \cdot n}{3}} \right) \right), \\ &\quad \left. 10 \right) + 5 + 0.5 \right) \end{aligned}$$

Nueva

$$\begin{aligned} \#53: \text{PARTS_LIST}(n) &:= \text{REVERSE_VECTOR} \left(\left(\text{ITERATE} \left(\text{IF} \left(n < \text{DIMENSION}(p_-), [p_-, \right. \right. \right. \right. \\ &\quad \left. \left. \left. v_-, m_- \right], \left[\text{APPEND}([p_- \cdot v_-], p_-), \text{APPEND} \left(v_-, \left[\text{IF} \left(\frac{3 \cdot m_-^2 - m_-}{2} = \right. \right. \right. \right. \right. \right. \right. \right. \\ &\quad \left. \left. \left. \text{DIMENSION}(p_-) + 1 \vee \frac{3 \cdot m_-^2 + m_-}{2} = \text{DIMENSION}(p_-) + 1, (-1)^{m_- + 1}, \right. \right. \right. \\ &\quad \left. \left. \left. 0 \right] \right] \right), \text{IF} \left(\frac{3 \cdot m_-^2 + m_-}{2} = \text{DIMENSION}(p_-) + 1, m_- + 1, m_- \right) \right) \right), [p_-, v_-, \\ &\quad \left. m_- \right], [[1], [1], 1], n \end{aligned}$$

#64: PENTATOPE(n) := POLYGONAL_PYRAMID(n, 3, 4) Nueva

#65: "The nth p-sided dth-dimensional centered pyramid number, p>=2:" Nueva
Nueva

#66: CENTERED_PYRAMID(n, p, d) := COMB(n + d - 3, d - 2) + p·COMB(n + d - 2, d)

#67: "The nth p-sided centered number, p>=2:" Nueva

#68: CENTERED(n, p) := CENTERED_PYRAMID(n, p, 2) Nueva

#69: HEX(n) := CENTERED(n, 6) Nueva

#70: STAR(n) := CENTERED(n, 12) Nueva

#71: OCTAHEDRAL(n) := CENTERED_PYRAMID(n, 4, 3) Nueva

#72: CENTERED_CUBE(n, d) := $n^d + (n - 1)^d$ Nueva

#73: CENTERED_HEX(n, d) := $n^{d+1} - (n - 1)^{d+1}$ Nueva

#74: RHOMBIC_DODECAHEDRAL(n) := CENTERED_HEX(n, 3) Nueva