Criptografia

un repte per a les matemàtiques i la física

IMATGE: http://www.tendencias21.net/photo/art/default/1105229-1409566.jpg?v=1289405777

Pseudònim: Newton

Índex

0 Introducció

Quan el gener de 2011 el programa Joves i Ciència de CatalunyaCaixa em va presentar la proposta d'activitats d'investigació per fer durant l'estiu, no vaig tenir cap dubte en escollir el projecte de Criptografia Quàntica, que tindria lloc a l'Institut de Ciències Fotòniques (ICFO), al Parc Mediterrani de la Tecnologia, a Castelldefels.

El projecte consistia en unes classes personalitzades en les quals dos alumnes tutelats per un investigador de l'ICFO, aprendríem els fonaments de la física quàntica relacionats amb la llum i la seva aplicació en la criptografia. Les classes tindrien lloc del 21 de juny al 18 de juliol.

En el moment de triar aquest projecte, sabia molt poc sobre criptografia, ja fos clàssica o quàntica. Per tal de treure més profit del treball que faríem a l'ICFO, vaig considerar que calia documentar-me i va ser així quan em vaig adonar dels enormes canvis que havia fet la criptografia des dels seus inicis fins a l'actualitat.

Mai m'havia plantejat la rellevància que té la criptografia en la nostra vida diària. Vaig descobrir que en l'actualitat no podríem fer gairebé res del que fem, mantenint la privacitat i confidencialitat, si no hi haguessin unes tècniques criptogràfiques adequades a les tecnologies informàtiques i de comunicació actuals. Els correus electrònics podrien ser interceptats per qualsevol, i les compres o contractació de serveis per Internet, la banca electrònica i els pagaments mitjançant targetes no serien possibles.

Vaig descobrir la gran importància que tenien les matemàtiques en la criptografia actual. Molts d'aquests conceptes matemàtics m'haurien resultat incomprensibles si no fos per les activitats extra-acadèmiques que he estat portant a terme els últims anys. Entre aquestes activitats han tingut un paper predominant les classes de preparació per a les Olimpíades de Matemàtiques, a les quals he assistit els divendres a la tarda, durant els darrers cursos, a la Universitat de Girona (UdG) i a càrrec de professors de la Universitat Politècnica de Catalunya (UPC).

Més tard, al plantejar-me un tema pel Treball de Recerca, em va semblar molt atraient fer-lo sobre criptografia, tant clàssica (que es basa en la intractabilitat de determinats problemes matemàtics) com quàntica (que es basa en les lleis de la física, especialment les relacionades amb els fotons).

El treball s'ha plantejat dedicant una part important a la criptografia clàssica, exposant alguns dels mètodes més significatius, dels quals s'explica el seu funcionament des d'un punt de vista matemàtic; una segona part es dedica a explicar els fonaments de la física quàntica i la seva aplicació a la criptografia; als annexos es fa un repàs de sistemes criptogràfics que han existit al llarg de la història i que actualment estan en desús.

El món de la criptografia és molt extens, ja que hi ha molts mètodes diferents i alguns d'ells amb diverses variants, els quals sovint s'utilitzen de forma combinada. No s'ha aprofundit al màxim ja que un estudi més exhaustiu sobre la criptografia implicaria realitzar una anàlisi molt més extensa del que és raonable per un treball d'aquest tipus.

L'apartat de criptografia quàntica suposa un repte important perquè implica un canvi conceptual profund. A diferència de la física clàssica, o de Newton, que és molt determinista, la física quàntica

és probabilística, o sigui, que es pot analitzar la probabilitat que hi ha que una partícula actuï d'una manera determinada però no es pot tenir prèviament la certesa de com actuarà. Tots els coneixements necessaris per fer aquest apartat els he adquirit aquest estiu, en les activitats en les que he participat. Aquest apartat l'he pogut desenvolupar bastant gràcies a la formació específica que he estat rebent per part d'investigadors i especialistes en aquest camp.

A part d'assistir al curs de Criptografia Quàntica a l'ICFO, en el qual vaig aprendre molt del que s'explica en l'apartat 2.7 Criptografia quàntica, durant l'estiu vaig participar en el programa International Summer School for Young Physicists (ISSYP), al Perimeter Institute for Theorical Physics (PI), Waterloo (Canadà), del 21 de juliol al 6 d'agost. L'activitat estava centrada en l'estudi dels grans temes de la física actual: la Teoria de la Relativitat Especial i General i la Física Quàntica. Tot el programa va ser molt interessant però, a més, va haver-hi activitats que van resultar especialment adients per fer el treball: la conferència "Quantum Cryptography" i la visita a l'Institute for Quantum Computing (IQC).

La criptografia quàntica i els ordinadors quàntics actualment encara estan en fase experimental, però només és possible fer experiments en laboratoris que únicament uns pocs organismes i entitats es poden permetre, tant per la seva complexitat tecnològica com pel cost econòmic que representa. Al ritme que ha avançat la tecnologia en les darreres dècades, no seria estrany que d'aquí a pocs anys els ordinadors quàntics es trobessin ja al mercat.

Tots els exemples presentats per cada un dels mètodes criptogràfics explicats i tots els gràfics són d'elaboració pròpia, si no s'especifica la procedència. Així mateix s'han creat les claus i s'han fet tots els càlculs per xifrar i desxifrar els missatges.

1 Història de la criptografia

En aquest apartat s'explicaran diferents mètodes criptogràfics importants de la història, però, primer de tot, caldria explicar més què és la criptografia, diferenciant-la de l'esteganografia, ja que és un concepte amb el qual sovint es confon.

L'esteganografia (del grec "steganos" (encobert) i "gràphein" (escriptura)) és l'art d'amagar els missatges, però sense modificar-los. En canvi, la criptografia (del grec "kryptós" (secret) i "gràphein" (escriptura)) és l'art de modificar el missatge per tal que, encara que sigui interceptat, sigui incomprensible si no es coneix la clau o el mètode utilitzat al modificar-lo. En aquest treball em centraré en la criptografia, deixant de banda l'esteganografia.[1]

L'objectiu del treball no és explicar els mètodes històrics, ja que, si bé van tenir utilitat en la seva època, actualment han quedat obsolets per la gran facilitat que hi ha, amb els mitjans tecnològics actuals, en descodificar-los sense saber-ne la clau. Per aquest motiu aquí se'n farà una breu explicació, la qual s'ampliarà als annexos.[2]

En aquest treball, en general s'utilitzarà un alfabet de 26 lletres, és a dir, no s'inclourà la *ç* ni la *ñ*, ni vocals accentuades, per no afegir complexitat als exemples. Només en algun cas excepcional s'utilitzaran també les xifres del 0 al 9. A la pràctica es poden utilitzar tants símbols (lletres, números, etc.) com es desitgi o sigui necessari.

Al llarg del temps hi ha hagut molts mètodes criptogràfics diversos, al principi més senzills, però que s'han hagut de complicar més a mesura que augmentaven els coneixements de les tècniques criptogràfiques, per tal d'obtenir missatges més segurs, i aconseguir que fos més difícil desxifrar-los per persones alienes.

Actualment la criptografia no únicament serveix per enviar missatges sense que puguin ser llegits per altra gent, sinó que també s'utilitza per assegurar que el missatge arriba sencer, sense ser modificat (integritat), per demostrar que ha estat una persona concreta que ha enviat el missatge (autentificació) i per poder assegurar-se i demostrar que una persona ha llegit un missatge concret (no-repudiació).

1.1 Xifrat simètric

Són els mètodes en els quals s'utilitza la mateixa clau per xifrar que per desxifrar. Per tant, l'emissor i el receptor han de saber la clau, i per això s'han d'haver reunit per acordar-la. Si hi ha n usuaris i cada missatge té un únic emissor i un únic destinatari, es necessitaran $n(n-1)/2$ claus diferents, ja que cada parella d'usuaris necessitarà una clau per comunicar-se. Els dos tipus de criptografia clàssica més utilitzats són la transposició i la substitució. Els xifrats simètrics són més ràpids i eficients, ja que no necessiten gaire capacitat de computació, però tenen el problema que, quan dos usuaris volen enviar-se un missatge, primerament s'han de trobar per acordar la clau. Aquest tipus de xifrat era l'únic existent des de l'inici de la criptografia fins fa uns 30 anys, quan Diffie i Hellman van inventar el xifrat asimètric.

[1] Per més informació sobre l'esteganografia veure l'annex A: Esteganografia.

[2] Veure annex B: Història de la criptografia.

1.1.1 Transposició

Els mètodes més senzills són els de transposició, en els quals l'únic que es modifica del missatge és l'ordre de les lletres, per exemple un anagrama. L'ordre ha de ser prèviament acordat per l'emissor i el receptor. Alguns exemples de transposició són el mètode de Railfence i la "Scytale" romana.

1.1.2 Substitució

En els mètodes per substitució cada lletra, o grup de lletres, és substituït per una altra lletra, grup de lletres o símbol. De fet, la majoria dels mètodes es basen en la substitució. Alguns exemples de substitució són els xifrats monoalfabètics generals (que inclouen el xifrat de Cèsar, l'afí, etc.), el xifrat de Vigenère, el xifrat de Playfair, etc.

1.2 Xifrat asimètric

El 1975, dos matemàtics de la Universitat de Stanford, W. Diffie[3] i M. Hellman[4], que es van conèixer al MIT, van publicar un article, "New Directions in Cryptography", on explicaven la seva idea sobre inventar mètodes en els quals el xifrat fos asimètric, de manera que l'emissor i el receptor no s'haguessin de trobar prèviament per acordar la clau, sinó que cada usuari tingués una clau pública, la qual podria conèixer tothom, i una clau privada, la qual només podria conèixer el propietari de la clau. Això es podria fer utilitzant funcions matemàtiques d'una sola direcció, és a dir, que fossin senzilles de calcular en un sentit, però extremadament complicades en el sentit contrari. Actualment es fan servir bàsicament dos grans problemes de la matemàtica: la factorització de nombres enters i el logaritme discret. Aquests dos problemes constitueixen uns grans reptes pels matemàtics, ja que fer el procés invers (és a dir, multiplicar nombres i l'exponencial discreta) són càlculs més fàcils, en canvi factoritzar nombres i trobar un logaritme discret són dos problemes molt complexos, dels quals encara no s'ha trobat un mètode eficient, i potser no n'existeix cap. Aquest tipus de xifrat té una sèrie d'avantatges. Per exemple, cada usuari necessita només una clau privada, la qual utilitza per crear la seva clau pública, fent una sèrie d'operacions, per tant, si hi ha n usuaris es necessitaran únicament n claus, no $n(n-1)/2$ com en el xifrat clàssic. També, un altre avantatge és que l'emissor i el receptor no s'han de trobar per acordar la clau, sinó que l'emissor utilitza la clau pública del receptor, que pot veure tothom, per codificar el missatge. Com a inconvenients hi ha que, en general, són mètodes molt més complexos, és a dir, requereix més capacitat de càlcul per a un mateix nivell de seguretat.

Per fer-ho més senzill d'entendre es podria comparar amb una oficina de correus, on cada receptor deixés uns quants panys oberts, els quals, quan estan tancats, només es poden obrir amb la clau que únicament té el receptor. Quan algú vol enviar un missatge al receptor, el posa dins d'una caixa i agafa un dels panys oberts del receptor. Seguidament tanca la caixa amb el pany. Des del moment que l'hagi tancat, ningú, exceptuant el receptor, podrà llegir el missatge. Ni tan sols

[3] Bailey Whitfield Diffie va ser matemàtic al MIT (Massachussetts Institute of Technology) i, des de 2002, director de seguretat i vicepresident de Sun Microsystems (Califòrnia)

[4] Monte Hellman va ser enginyer a IBM (International Business Machines) i al MIT.

l’emissor hi tindrà accés. No hi ha cap problema en deixar els panys a la vista de tothom, ja que no serveixen per aconseguir la clau.

Actualment, l’ús que es fa de la criptografia és una combinació de xifrat asimètric, per intercanviar les claus i firmar documents, i de simètric, per intercanviar el gruix de dades sense la necessitat de computació que comporten els xifrats simètrics.

2 Criptografia actual

2.1 DES

2.1.1 Història

El 1972 el NIST (National Institute of Standards and Technology), conegut inicialment com a NBS (National Bureau of Standards) va adonar-se que era necessari un estàndard de xifrat per totes les institucions governamentals dels Estats Units. El maig del 1973 va demanar propostes per un sistema de xifratge, però cap de les presentades complia els rigorosos criteris de disseny demanats. L'agost de 1974 va tornar-ho a demanar i l'IBM va presentar el seu mètode de xifrat intern, que va ser anomenat DES (Data Encryption Standard).

Es tracta d'un xifrat de bloc simètric, en els quals s'agafa un text amb una longitud fixa, es fan una sèrie d'operacions amb cossos finits[5] utilitzant la clau i queda transformat en un text xifrat de la mateixa longitud que l'inicial. En el DES s'utilitzen claus de 56 bits i mides de blocs de 64 bits. Per entendre-ho més fàcilment es podria comparar amb un xifrat monoalfabètic[6], però enlloc d'haver-hi $26!$ (on $n! = n \cdot (n-1)(n-2) \cdot \ldots \cdot 3 \cdot 2 \cdot 1$) permutacions n'hi ha $2^{64}!$, ja que hi ha 64 bits, és a dir, un nombre molt gran, molt superior al nombre d'àtoms que hi ha a l'Univers.

Més tard es van dissenyar nous mètodes, basats en el DES, per exemple el RC5, el Blowfish, l'IDEA, el NewDES, el SAFER, el CAST5, el FEAL, el TDES, el DES-X i el GDES, entre d'altres.

El Triple DES (TDES) va ser descrit i analitzat per un dels inventors del DES, i consistia en aplicar el DES tres vegades, amb dues o tres claus diferents (anomenats 2TDES i 3TDES, respectivament). Aquest mètode era més segur que el DES, però era força més lent. Una alternativa computacionalment menys costosa va ser el DES-X, que consistia en augmentar la mida de la clau fent una operació XOR amb material extra per la clau abans i després del DES.

2.1.2 Avantatges i inconvenients

Un avantatge és que és un xifrat simètric, i per tant no necessita gaire capacitat de computació, però en canvi hi ha dificultat i risc al distribuir les claus. Actualment és considerat insegur per moltes aplicacions, ja que les claus són massa curtes. Va haver-hi uns quants motius de controvèrsia, amb aquest xifrat, per exemple la curta longitud de la clau, elements classificats com a informació confidencial en el seu disseny i la sospita que la NSA (National Security Agency) dels Estats Units tenia un mètode per desxifrar-lo.

[5] Veure definició a Annex C: Demostracions i explicacions.

[6] Veure 7.2.9 Xifrat monoalfabètic general.

2.2 AES

2.2.1 Història

El 1997, el NIST va organitzar un concurs internacional per escollir un nou algoritme de xifrat pel govern d'Estats Units, per substituir el DES. El nom del xifrat seria AES (Advanced Encryption Standard). El 2 de gener anunciava la intenció de desenvolupar l'AES, però no va ser fins al setembre del mateix any que es va fer la convocatòria formal, on s'indicaven les condicions que havien de tenir els algoritmes que es presentessin. Algunes d'aquestes característiques eren que havia de ser un algoritme de xifrat simètric, havia de suportar blocs de 128 bits com a mínim i les claus del xifrat havien de ser de 128, 192 o 256 bits. A finals d'agost del 1998 NIST va anunciar els 15 algoritmes seleccionats. Al cap d'un any NIST va decidir els 5 finalistes (Rijndael, RC6, Serpent, MARS i Twofish), dels quals es va fer una revisió més detallada, fins al maig de l'any 2000. A l'octubre del mateix any es va fer una votació per triar el guanyador del concurs, que va ser el xifrat Rijndael, elaborat pels belgues Joan Daemen i Vincent Rijmen que, curiosament, feia poc temps que havien acabat el doctorat i que es dedicaven a la investigació, però tot i així van guanyar a experts en criptografia.

En realitat, el Rijndael no és igual que l'AES. L'AES consta de blocs fixos de 128 bits i mides de claus de 128, 192 i 256 bits, mentre que el Rijndael permet un major rang de mida de blocs i longitud de claus (les claus han de ser múltiples de 32, entre 128 i 256).

En l'AES, igual que el DES, és comparable amb un xifrat monoalfabètic, però encara hi ha més permutacions, concretament $2^{128}!$, on "!" indica factorial.

2.2.2 Avantatges i inconvenients

Com que es tracta d'un xifrat simètric no necessita gaire capacitat de computació, però és difícil distribuir les claus. Les claus i blocs són més grans que en el DES, la qual cosa implica que és més segur, i el mètode de xifratge és més ràpid.

2.3 RSA

2.3.1 Història

Ron Rivest, informàtic del MIT, es va interessar per l'article de Diffie i Hellman, esmentat anteriorment, sobre el xifrat asimètric. Va anar a parlar amb dos companys seus, Leonard Adleman, matemàtic del MIT, el qual no en va voler saber res, ja que li interessava més provar de demostrar l'últim teorema de Fermat i altres conjectures, i Adi Shamir, un matemàtic i informàtic israelià que estava de visita al MIT. Shamir sí que es va interessar per aquest tema, i amb Rivest sempre n'estaven parlant. Buscaven problemes matemàtics computacionalment durs, perquè els missatges encriptats fossin difícils d'atacar. Com que a Adleman li agradaven els problemes difícils, quan Rivest i Shamir tenien alguna idea, ell l'analitzava en busca de possibles errors.

Després de molt temps de treballar en aquest tema ja començaven a perdre l'esperança, pensant que la teoria funcionava, però que potser la pràctica no. Una nit, a l'abril de 1977 Rivest va trucar a Adleman, explicant-li la idea que acabava de tenir, que consistia en la dificultat de descompondre números en nombres primers. A Adleman li va semblar una idea genial i el dia següent Rivest ja escrivia l'article on explicava el mètode RSA, el nom del qual prové de les inicials dels creadors: Rivest, Shamir i Adleman.

Martin Gardener, un conegut divulgador científic d'Estats Units, va sentir curiositat pel mètode RSA i va demanar permís per publicar un article,"Un nou tipus de xifrat que costaria milions d'anys desxifrar", dedicat al RSA, a la revista "Scientific American".

Els serveis de seguretat governamentals s'hi van interessar ràpidament, mentre que l'ús generalitzat d'aquest sistema no va ser fins a la dècada de 1990, amb la implantació d'internet.

El sistema RSA inicialment només podia ser utilitzat en ordinadors molt potents, degut a les operacions amb nombres molt grans que s'havien de fer. A l'estiu de 1991, Phil Zimmermann, físic d'Estats Units, va oferir PGP (Pretty Good Privacy, és a dir, molt bona privacitat). Es tracta d'un algoritme d'encriptació capaç de funcionar en ordinadors domèstics. Aquest mètode utilitza la codificació simètrica clàssica, la qual cosa el fa més ràpid, però xifra les claus amb un encriptat asimètric RSA. L'ús de PGP s'ha estès des de la seva creació i actualment és l'eina criptogràfica disponible més important.

El 1997 es va anunciar que aquest mètode havia estat descobert prèviament pels criptògrafs del govern britànic James Ellis i Clifford Cocks, però s'havia mantingut en secret fins al moment, ja que no hi havia la necessitat que fos públic.

2.3.2 Mètode

2.3.2.1 Idea utilitzada

Hi ha operacions que són fàcils en un sentit, però resulta molt complicat fer l'invers, les quals s'utilitzen en els xifrats asimètrics. El mètode RSA es basa en la facilitat de multiplicar dos nombres primers grans per obtenir-ne el producte i la dificultat de descompondre el producte de dos

nombres primers grans. També s'utilitza la idea que existeixen infinits primers[7] i que els primers són relativament densos dins del conjunt dels enters, i per tant es poden utilitzar nombres tan grans com es vulgui, és molt improbable que dos usuaris escullin els mateixos a l'atzar i és extremadament difícil fer les suficients permutacions per trobar les claus privades dels diferents usuaris.

2.3.2.2 Fonaments matemàtics[8]

- Nombres coprimers → no tenen cap divisor en comú, és a dir, donats dos nombres coprimers a i b, el màxim comú divisor dels dos nombres és igual a 1 ($mcd\ (a,b) = 1$).

- Aritmètica modular → $a \equiv b\ (mod\ c)$ significa que $a = b + kc$, on a, b, c i k són nombres enters. Així, per exemple, $13 \equiv 1\ (mod\ 6)$, $9 \equiv 4\ (mod\ 5)$, etc. És utilitzat quotidianament en els rellotges, on, com tothom sap, les 15h són les 3h de la tarda, és a dir, $15 \equiv 3\ (mod\ 12)$ o, si anem a dormir a les 23h i dormim 8 hores ens despertem a les 7h, no a les 31h, és a dir $23 + 8 = 31 \equiv 7\ (mod\ 24)$.

- Algoritme d'Euclides → $mcd\ (a,b) = mcd\ (b,r)$, on a i b són dos nombres naturals qualssevol i r és el residu de la divisió d'aquests dos nombres. S'utilitza per calcular els nombres x i y de la identitat de Bézout.

- Identitat de Bézout → $\exists x, y \in \mathbb{Z}$ tals que $xa + yb = mcd\ (a,b)$, és a dir, donats dos nombres enters a i b existeixen uns nombres enters x i y tals que $xa + yb = mcd\ (a,b)$.

- Petit teorema de Fermat→ Sigui p un nombre primer i a un nombre natural coprimer amb p. Aleshores $a^{p-1} \equiv 1\ (mod\ p)$. En general es podria enunciar que, $\forall\ a, a^p \equiv a\ (mod\ p)$.

- Adaptació del petit teorema de Fermat → Siguin p i q dos nombres primers, i a un nombre natural coprimer amb pq, de manera que $a \not\equiv 0\ (mod\ p)$. Aleshores $a^{(p-1)(q-1)} \equiv 1\ (mod\ pq)$.

2.3.2.3 Creació de les claus

Primerament es trien 2 nombres primers diferents, que anomenarem p i q. Per més seguretat, és recomanable que siguin triats a l'atzar i que siguin d'una llargada similar.

Seguidament es calcula $n = pq$. Aquest nombre serà utilitzat tant en la clau pública com en la privada.

Llavors es calcula $\varphi(n) = (p-1)(q-1)$, on $\varphi(n)$ és la funció φ d'Euler, que indica la quantitat de nombres menors que n que no tenen cap divisor en comú amb n, és a dir, que són coprimers. Després es tria un enter e que compleixi que $1 < e < \varphi(n)$ i que el $mcd\ (e, \varphi(n)) = 1$, és a dir, que e i $\varphi(n)$ siguin coprimers. e serà l'exponent de la clau pública. Si e és molt petit la seguretat és menor. Sovint s'utilitza el nombre primer $e = 65537 = 2^{16} + 1$, ja que amb binari s'expressa $100 \ldots 001$, és a dir, només hi ha dos 1, i el nombre de càlculs que es fan per calcular

[7] Demostració a l'annex C: Demostracions i explicacions.

[8] Veure l'annex C: Demostracions i explicacions.

l'exponencial discreta tenen a veure amb el nombre d'1 que hi ha, per tant els càlculs són més ràpids.

Finalment es calcula d, tal que $d \cdot e \equiv 1 \, mod \, \varphi(n)$. Per tant, $ed + k\varphi(n) = 1$, on $k \in \mathbb{Z}$. Per calcular d, normalment s'utilitza la identitat de Bézout (explicada anteriorment), substituint $a = e$, $b = \varphi(n)$, $mcd\left(e, \varphi(n)\right) = 1$, $x = k$ i $y = d$.

La clau pública és (n, e) i la clau privada és d.

2.3.2.4 Encriptar

L'Alice[9] vol enviar un missatge M a en Bob, per tant agafa la clau pública d'en Bob (n, e).

Primerament substitueix M per un enter, o més d'un, m, tal que $0 < m < n$. Per realitzar aquesta substitució podem utilitzar el nostre propi codi, per exemple A→00, B→01, C→02, …, Y→24, Z→25, o utilitzar codis coneguts, per exemple ASCII (American Standard Code for Information Interchange). Normalment, els diferents *m* utilitzats són grans, ja que si fossin de lletres individuals el sistema RSA seria semblant a un xifrat monoalfabètic general.

Finalment calcula el text encriptat $c = m^e \ (mod \, n)$ i l'envia a en Bob.

2.3.2.5 Desencriptar

En Bob pot obtenir m a partir de c utilitzant d, que només es pot saber si es coneixen els dos nombres primers que formen la clau. Per obtenir m, en Bob realitza el càlcul $m = c^d \ (mod \, n)$. Això funciona ja que $c = m^e \ (mod \, n)$, per tant $c^d = (m^e)^d \ (mod \, n)$. Per altra banda, $ed \equiv 1 \ (mod \, \varphi(n))$, per tant $ed = 1 + k\varphi(n)$, on k és un nombre enter. Per tant $m^{ed} = m^{1+k\varphi(n)} = m \cdot m^{k\varphi(n)}$. Finalment, $m \cdot m^{k\varphi(n)} \equiv m \ (mod \, n)$, degut a l'adaptació del petit teorema de Fermat (esmentada anteriorment).

Finalment, en Bob pot obtenir el missatge M utilitzant el codi que ha utilitzat l'Alice per canviar de M a m.

2.3.2.6 Exemple

Seguidament s'explicarà un exemple per aclarir una mica el procediment, però es farà amb nombres petits, per tal que sigui més fàcil d'operar i també d'entendre. A la vida real, però, s'utilitzen nombres de fins a centenars de xifres!

Creació de les claus

[9] Els noms utilitzats per anomenar cadascun dels personatges (Alice, Bob i, més tard, Eve) són els usats habitualment, en lloc de A, B i E, en articles, llibres, conferències, etc. Eve, en anglès, té una fonètica semblant a la primera part del mot "eavesdropper" (el que escolta secretament converses privades), i s'utilitza per designar l'espia o intrús, el qual es suposa que té coneixements de criptografia i té els mitjans adequats per atacar els missatges, per exemple ordinadors potents. L'Alice habitualment s'utilitza per designar l'emissor i en Bob per designar el destinatari. L'Alice i en Bob no necessàriament són persones; també poden ser màquines, targetes de crèdit, ordinadors, etc.

En Bob tria, a l'atzar, $p = 97$ i $q = 53$. Llavors calcula $n = pq = 97 \cdot 53 = 5141$. Seguidament calcula $\varphi(n) = \varphi(5141) = (p-1)(q-1) = (97-1)(53-1) = 96 \cdot 52 = 4992$.

Després tria un enter e que sigui coprimer amb 4992 i compleixi que $1 < e < 4992$. En Bob tria, per exemple, 925.

Finalment calcula d, recordem que $d \cdot e \equiv 1\ (mod\ \varphi(n))$, utilitzant la identitat de Bézout[10]. S'obté que $1333 \cdot 925 - 247 \cdot 4992 = 1$. Per tant, $d = 1333$. Es pot comprovar fàcilment que $d \cdot e = 1333 \cdot 925 = 1 + 4992 \cdot 247 \equiv 1\ (mod\ 4992)$.

La clau pública és $(n, e) = (5141, 925)$ i la clau privada és $d = 1333$.

Encriptar

L'Alice vol enviar el missatge "aquest es el missatge" a en Bob.

Per substituir el missatge per un enter, o més d'un, utilitza el codi següent:

a	b	c	d	e	f	g	h	i	j	k	l	m
00	01	02	03	04	05	06	07	08	09	10	11	12

n	o	p	q	r	s	t	u	v	w	x	y	z
13	14	15	16	17	18	19	20	21	22	23	24	25

Per tant el missatge substituït, i traient els espais, per poder fer les separacions adequades, ens quedarà:

00162004181904180411120818180019060 4

Com s'ha dit abans, *0<m<n*, per tant les els grups de lletres haurien de ser de menys de 4 xifres, ja que sinó pot ser que n'hi hagi algun de més gran que *n*. Per tant farem separacions de 3 xifres, és a dir:

m_1*=001*; m_2*=620*; m_3*=041*; m_4*=819*; m_5*=041*; m_6*=804*; m_7*=111*; m_8*=208*; m_9*=181*; m_{10}*=800*; m_{11}*=190*; m_{12}*= 604*

Seguidament s'agafa cada grup de 3 xifres i s'encripta, tal com s'ha explicat abans, $c=m^e\ (mod\ n)$. És a dir:

$c_2 = m_2^e\ (mod\ n) = 620^{925}\ (mod\ 5141) = 620 \cdot (620^2)^{462}\ (mod\ 5141) = 620 \cdot 384400^{462}\ (mod\ 5141) = 620 \cdot 3966^{462}\ (mod\ 5141) = 620 \cdot (3966^2)^{231}\ (mod\ 5141) = 620 \cdot 15729156^{231}\ (mod\ 5141) = 620 \cdot 2837^{231}\ (mod\ 5141) = 620 \cdot 2837 \cdot (2837^2)^{115}\ (mod\ 5141) = 1758940 \cdot 8048569^{115}\ (mod\ 5141) = 718 \cdot 2904^{115}\ (mod\ 5141) = 718 \cdot 2904 \cdot (2904^2)^{57}\ (mod\ (5141) = 2085072 \cdot 8433216^{57}\ (mod\ 5141) = 2967 \cdot 1976^{57}\ (mod\ 5141) = 2967 \cdot 1976 \cdot (1976^2)^{28}\ (mod\ 5141) = 5862792 \cdot 3904576^{28}\ (mod\ 5141) = 2052 \cdot 2557^{28}\ (mod\ 5141) = 2052 \cdot (2557^2)^{14}\ (mod\ 5141) = 2052 \cdot 6538249^{14}\ (mod\ 5141) = 2052 \cdot 4038^{14}\ (mod\ 5141) = 2052 \cdot (4038^2)^7\ (mod\ 5141) = 2052 \cdot 16305444^7\ (mod\ 5141) = 2052 \cdot 3333^7\ (mod\ 5141) = 2052 \cdot 3333 \cdot (3333^2)^3\ (mod\ 5141) = 6839316 \cdot 11108889^3\ (mod\ 5141) = 1786 \cdot 4329^3\ (mod\ 5141) =$

[10] Veure el procés realitzat a l'annex C: Demostracions i explicacions.

$1786 \cdot 4329 \cdot 4329^2 \pmod{5141} = 7731594 \cdot 18740241 \pmod{5141} = 4671 \cdot 1296 \pmod{5141} = 6053616 \pmod{5141} =$ ***2659***

Tal com es veu a l'exemple anterior, una manera ràpida d'aconseguir el resultat és anar separant el nombre utilitzant propietats de les potències. En els següents exemples, que es poden calcular de la mateixa manera, es posarà el resultat directament, ja que el càlcul és prescindible. En aritmètica modular, encara que una base sigui molt gran, no necessàriament dóna un valor molt alt a l'elevar-lo a la mateixa potència que les altres, tal com es pot veure a continuació.

$c_1 = m_1^e \pmod n = 001^{925} \pmod{5141} =$ ***0001***
$c_2 = m_2^e \pmod n = 620^{925} \pmod{5141} =$ ***2659***
$c_3 = m_3^e \pmod n = 041^{925} \pmod{5141} =$ ***3206***
$c_4 = m_4^e \pmod n = 819^{925} \pmod{5141} =$ ***4710***
$c_5 = m_5^e \pmod n = 041^{925} \pmod{5141} =$ ***3206***
$c_6 = m_6^e \pmod n = 804^{925} \pmod{5141} =$ ***2092***
$c_7 = m_7^e \pmod n = 111^{925} \pmod{5141} =$ ***2499***
$c_8 = m_8^e \pmod n = 208^{925} \pmod{5141} =$ ***2984***
$c_9 = m_9^e \pmod n = 181^{925} \pmod{5141} =$ ***2966***
$c_{10} = m_{10}^e \pmod n = 800^{925} \pmod{5141} =$ ***1916***
$c_{11} = m_{11}^e \pmod n = 190^{925} \pmod{5141} =$ ***1168***
$c_{12} = m_{12}^e \pmod n = 604^{925} \pmod{5141} =$ ***3902***

Seguidament, l'Alice ajunta tots els missatges, és a dir, escriu 0001 2659 3206 4710 3206 2092 2499 2984 2966 1916 1168 3902. Les separacions les pot fer com vulgui ja que, com que *e* té 4 xifres, els nombres han de ser com a molt de 4 xifres, i per tant en Bob ja sabrà que per desxifrar-lo correctament ha de fer aquestes separacions. Finalment, l'Alice envia el missatge encriptat a en Bob.

Desencriptar

En Bob agafa els diferents missatges i els desxifra calculant $m = c^d \ (mod\ n)$, tal com hem vist abans. Per reduir els nombres, també es pot fer com abans, quan s'explicava l'exemple d'encriptar.

$m_1 = c_1^d \pmod n = 0001^{1333} \pmod{5141} =$ ***001***
$m_2 = c_2^d \pmod n = 2659^{1333} \pmod{5141} =$ ***620***
$m_3 = c_3^d \pmod n = 3206^{1333} \pmod{5141} =$ ***041***
$m_4 = c_4^d \pmod n = 4710^{1333} \pmod{5141} =$ ***819***
$m_5 = c_5^d \pmod n = 3206^{1333} \pmod{5141} =$ ***041***
$m_6 = c_6^d \pmod n = 2092^{1333} \pmod{5141} =$ ***804***
$m_7 = c_7^d \pmod n = 2499^{1333} \pmod{5141} =$ ***111***
$m_8 = c_8^d \pmod n = 2984^{1333} \pmod{5141} =$ ***208***
$m_9 = c_9^d \pmod n = 2966^{1333} \pmod{5141} =$ ***181***
$m_{10} = c_{10}^d \pmod n = 1916^{1333} \pmod{5141} =$ ***800***
$m_{11} = c_{11}^d \pmod n = 1168^{1333} \pmod{5141} =$ ***190***
$m_{12} = c_{12}^d \pmod n = 3902^{1333} \pmod{5141} =$ ***604***

Seguidament en Bob escriu els resultats tots seguits, i fa les separacions necessàries per poder substituir els nombres per les lletres i obtenir el missatge que li ha enviat l'Alice. Per tant en bob escriu: 00 16 20 04 18 19 04 18 04 11 12 08 18 18 00 19 06 04 i, substituint-ho per les lletres utilitzant el mateix codi que l'Alice, obtindrà "aquesteselmissatge". Finalment pot fer les separacions entre paraules i llegir el missatge "aquest es el missatge".

2.3.2.7 Firma electrònica

L'Eve podria enviar un missatge a en Bob, fent-se passar per l'Alice, ja que també sap la clau pública d'en Bob. Com pot assegurar-se en Bob que un missatge que li arriba és de l'Alice? Com pot l'Alice demostrar que ha estat ella qui ha enviat el missatge i no ha estat l'Eve? Doncs firmant el missatge. Però no serveix firmar-lo posant el nom, ja que això també ho podria fer l'Eve. S'ha de

fer d'alguna manera que l'Eve no pugui fer. La única informació que l'Alice sap i l'Eve no sap és la clau privada de l'Alice, per tant aquesta serà la única manera que l'Eve no es pugui fer passar per l'Alice.

La clau pública de l'Alice serà (n_A, e_A) i la seva clau privada serà d_A. La clau pública d'en Bob serà (n_B, e_B) i la clau privada serà d_B.

L'Alice, per demostrar que ha estat ella qui ha enviat el missatge, l'encriptarà primerament amb la clau pública d'en Bob, i seguidament amb la seva clau privada. Per desencriptar-lo, en Bob utilitzarà la clau pública de l'Alice i finalment la seva clau privada.

És a dir, l'Alice primer calcula $c = m^{e_B}\ (mod\ n_B)$. Seguidament el firma calculant $f = c^{d_A}\ (mod\ n_A)$ i envia f a en Bob. La clau privada de l'Alice només la sap ella, per tant només ella pot haver enviat aquest missatge. Per desencriptar-lo, en Bob primer calcula $f^{e_A}\ (mod\ n_A) = c^{d_A \cdot e_A}\ (mod\ n_A) = c$. Això funciona pel motiu explicat en l'apartat 2.3.2.5 Desencriptar. Finalment, en Bob calcula $c^{d_B}\ (mod\ n_B) = m^{e_B \cdot d_B} (mod\ n_B) = m$, i funciona pel mateix motiu. Aquest últim pas només el pot fer en Bob, ja que és l'únic que posseeix la clau privada d'en Bob.

2.3.3 **Avantatges i inconvenients**

Com que, a diferència dels mètodes anteriors, es tracta d'un xifrat asimètric, cada usuari té la seva pròpia clau i, per tant, se'n necessiten només *n* (suposant que la clau d'un usuari és el conjunt de la clau pública i la privada).

Un dels problemes del mètode RSA és que consumeix molt temps de computació i, per tant, es necessiten ordinadors de gran capacitat. A més, algunes organitzacions no el consideren un mètode prou segur, ja que es coneixen alguns algoritmes que redueixen la complexitat del problema de la factorització i, per tant, exigeixen claus molt més llargues, la qual cosa significa encara més temps de computació. Fins als anys 80 només els governs, l'exèrcit i les grans empreses podien utilitzar aquest sistema, ja que només ells tenien ordinadors suficientment potents per treballar amb el mètode RSA. Per solucionar aquest tema, va ajudar molt l'oferiment de PGP, per part de Zimmermann.

Com a inconvenients també té la possible creació d'ordinadors quàntics en un futur pròxim, els quals podrien fer operacions molt ràpid, degut a la superposició d'estats, i per tant seria molt més senzill atacar-los i descobrir els nombres primers que formen la clau.

Hi ha un dels set problemes del mil·lenni, dels quals un ja ha estat demostrat, que es demana demostrar que P=NP o P≠NP, on P és el conjunt de problemes computacionalment fàcils (per exemple la multiplicació de dos nombres) i NP és el conjunt de problemes dels quals és computacionalment fàcil comprovar la resposta a partir dels resultats (per exemple comprovar la factorització d'un nombre multiplicant els nombres en els quals es factoritza). $P \in NP$, per tant si $P = NP$ aleshores significarà que els problemes utilitzats en criptografia, és a dir, la factorització de nombres i el logaritme discret, són fàcils computacionalment, per tant aquests mètodes deixaran de ser útils.

Per tant, amb poques dècades d'existència, el mètode RSA podria quedar obsolet si les tècniques matemàtiques fessin un progrés important en la factorització de nombres molt grans o amb la millora de la física quàntica i la construcció d'ordinadors quàntics.

Però de moment, mentre no s'avanci suficientment en aquests camps, el mètode RSA és segur.

2.4 ElGamal

2.4.1 Història

El mètode d'ElGamal va ser inventat per Tahel Elgamal el 1984.

Encara que aquest mètode criptogràfic tingui una existència molt breu, es basa en problemes i tècniques matemàtiques que fa molts anys que s'intenten resoldre.

2.4.2 Mètode

2.4.2.1 Idea utilitzada

Aquest mètode es basa en la dificultat de trobar un logaritme discret, és a dir, un logaritme quan treballem amb aritmètica modular. Es tracta, també, d'un xifrat asimètric, és a dir, que cada usuari té una clau pública, que coneix tothom, però en té una de privada que només coneix aquell usuari, i que li permet desxifrar els missatges.

2.4.2.2 Fonaments matemàtics

Grup → És una estructura algebraica formada per un conjunt G, en els elements del qual s'ha definit una operació denominada $\diamondsuit$. L'estuctura $(G,\diamondsuit)$ és un grup si compleix les següents propietats:

- Associativa: no importa l'ordre en el qual s'operen les parelles d'elements, és a dir, $(a \diamondsuit b) \diamondsuit c = a \diamondsuit (b \diamondsuit c)$.
- Existència d'un element neutre: existeix un element e al grup tal, al ser operat amb qualsevol altre, no el modifica, és a dir, $a \diamondsuit e = e \diamondsuit a = a$.
- Existència d'un element invers per cada element de G: tots els elements del grup tenen un element invers, a^{-1}, amb el que, al operar-lo amb a, s'obté l'element neutre, és a dir, $a \diamondsuit a^{-1} = a^{-1} \diamondsuit a = e$.

Grup cíclic → un grup és cíclic si existeix un element g tal que, per qualsevol element a del grup existeix un nombre n tal que $\exp_g n = a$, on $\exp_g n$ és $g \diamondsuit g \diamondsuit \ldots \diamondsuit g$ n vegades. Per exemple $\mathbb{Z}_p^* = \{1, 2, \ldots, p-2, p-1\}$ amb l'operació de multiplicar mòdul p, és un grup cíclic, i és utilitzat en ElGamal aplicat a un grup multiplicatiu.

Logaritme discret en una operació qualsevol → Sigui $(G,\diamondsuit)$ un grup i a i b dos elements d'aquest grup. Anomenarem $b = \exp_a x$ l'operació $b = a \diamondsuit a \diamondsuit \ldots \diamondsuit a \diamondsuit a$ x vegades. Aleshores, $x = \log_a b$, on $\log_a b$ serà el logaritme discret.

2.4.2.3 Creació de les claus

Es tria un grup G, un nombre primer p i un generador g. En Bob tria aleatòriament una clau privada x_B, pertanyent al grup G. Seguidament calcula $h_B = \exp_g x_B$. La clau pública serà (h_B, p, g) i la clau privada x_B.

2.4.2.4 Encriptar

L'Alice vol enviar-li un missatge m a en Bob. Per fer-ho necessita una clau privada x_A. Seguidament calcula $h_A = \exp_g x_A$ i $c = m \cdot \exp_{h_B} x_A$. El missatge xifrat és (h_A, c).

2.4.2.5 Desencriptar

En Bob vol obtenir el missatge m a partir de h_A i c. Per tant calcula:

$$\mathrm{m} = \mathrm{c} \cdot \left(\exp_{h_B} x_A\right)^{-1} (mod\ p) = c \cdot \left(\exp_g (x_A x_B)\right)^{-1} (mod\ p) = c \cdot \left(\exp_{h_A} x_B\right)^{-1} (mod\ p)$$

2.4.2.6 Avantatges i inconvenients

Aquest mètode pot ser utilitzat en qualsevol grup, però normalment només s'utilitza en el grup multiplicatiu i en les corbes el·líptiques, ja que són els que presenten més avantatges.

2.4.2.7 ElGamal aplicat a un grup multiplicatiu

2.4.2.7.1 Fonaments matemàtics

Logaritme discret en un grup multiplicatiu → és relativament fàcil calcular el logaritme d'un nombre, és a dir, calcular, per una *x* concreta, $x = log_b y$, ja que la gràfica de la funció exponencial és creixent (veure Fig. 2.4.2.7.1.1). Però, si volem calcular el logaritme discret, és a dir, $x = \log_b y\ (mod\ p)$ es complica molt, ja que la gràfica es torna caòtica (veure Fig. 2.4.2.7.1.2). Es coneixen alguns mètodes més eficaços que anar provant tots els casos, però tot i així no són suficientment eficients.

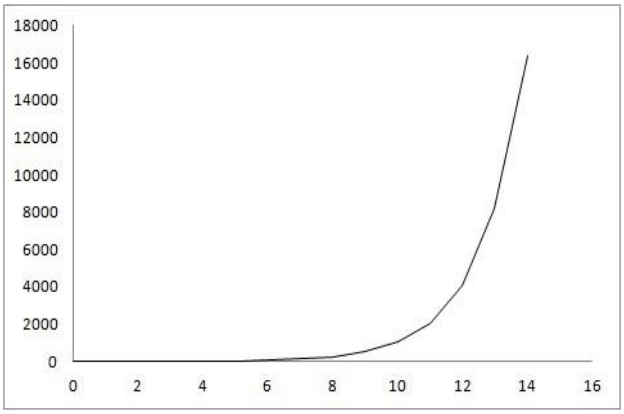


Fig. 2.4.2.7.1.1 Gràfica de la funció $y=2^x$.

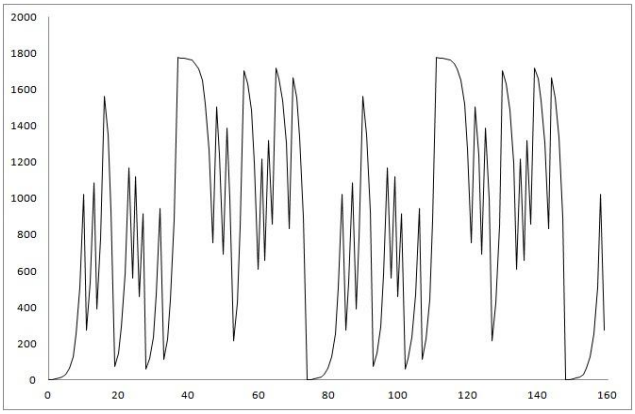


Fig. 2.4.2.7.1.2 Gràfica de la funció $y=2^x\ (mod\ 1777)$.

2.4.2.7.2 Creació de les claus

En Bob, que serà el receptor, tria un nombre primer, que anomenarem *p*. Tria també dos nombres naturals aleatòriament, que anomenarem *g* i *x*, de tal manera que $0 \leq x \leq p - 1$.

Seguidament, calcula $h = g^x\ (mod\ p)$.

La clau pública serà *(h, p, g)*, mentre que la clau privada serà *x*.

Tot i que quan es treballa amb números molt grans és pràcticament impossible que s'escullin, aleatòriament, uns nombres concrets és recomanable, per més seguretat, que $2 \leq x \leq p-2$, ja que:

$g^0=1 \pmod p$
$g^1=g \pmod p$
$g^{p-1} \equiv 1 \pmod p$, degut al petit teorema de Fermat[11].

2.4.2.7.3 Encriptar

L'Alice vol enviar-li un missatge *m* a en Bob. *m* ha de ser més petit que *p*. Després, l'Alice tria aleatòriament un nombre, que anomenarem *y*, de tal manera que $0 \leq y \leq p-1$. Seguidament calcula:

$a=g^y \pmod p$
$b=m \cdot h^y \pmod p$

El missatge xifrat és: (a, b).

2.4.2.7.4 Desencriptar

Per desencriptar el missatge, en Bob calcula $a^{p-1-x} \cdot b \pmod p$. Això funciona perquè:

$a^{p-1-x} \cdot b = g^{y(p-1-x)} \cdot m \cdot g^{xy} = g^{-xy} \cdot g^{(p-1)y} \cdot m \cdot g^{xy} = g^{(p-1)y} \cdot m$

Finalment, degut al petit teorema de Fermat, explicat anteriorment:

$g^{(p-1)y} \cdot m \pmod p \equiv 1^y \cdot m \pmod p = m \pmod p = m$

2.4.2.7.5 Exemple

Seguidament s'explicarà un exemple, per tal d'aclarir una mica més el procediment per obtenir les claus, encriptar i desencriptar utilitzant el mètode ElGamal. Utilitzaré nombres petits, ja que sinó seria difícil d'operar i d'entendre el procediment, però a la vida real s'utilitzen nombres primers de 40 o més xifres!

Creació de les claus

En Bob tria el nombre primer *p*=1777. Tria també, aleatòriament, *g*=111 i *x*=1479. Seguidament calcula $h=g^x \pmod p$. S'utilitzarà el mètode explicat en el sistema RSA, quan s'havia d'elevar un nombre a una potència molt gran.

$h = g^x \pmod p = 111^{1479} \pmod{1777} = 1761$.

Per tant, la clau pública és $(h = 1761, p = 1777, g = 111)$ i la clau privada és $x = 1479$.

Encriptar

L'Alice vol enviar el missatge "aquest es el missatge" a en Bob. Igual que en el mètode RSA, es substitueixen les lletres per nombres segons un codi establert i es separen en grups de 3 xifres, per

[11] Veure 2.3.2.2. Fonaments matemàtics del mètode RSA.

assegurar-nos que els missatges seran més petits que p, que té 4 xifres. Per tant, els diferents missatges seran m_1=001, m_2=620, m_3=041, m_4=819, m_5=041, m_6=804, m_7=111, m_8=208, m_9=181, m_{10}=804, m_{11}=190, m_{12}= 604.

Seguidament l'Alice tria un nombre *y*, per exemple *y=1312*, i calcula *a* i b_i, per tot *1≤i≤12*.

$a = g^y \pmod p = 111^{1312} \pmod{1777} = \mathbf{64}$

$b_1 = m_1 \cdot h^y \pmod p = 001 \cdot 1761^{1312} \pmod{1777} = \mathbf{1305}$
$b_2 = m_2 \cdot h^y \pmod p = 620 \cdot 1761^{1312} \pmod{1777} = \mathbf{0565}$
$b_3 = m_3 \cdot h^y \pmod p = 041 \cdot 1761^{1312} \pmod{1777} = \mathbf{0195}$
$b_4 = m_4 \cdot h^y \pmod p = 819 \cdot 1761^{1312} \pmod{1777} = \mathbf{0818}$
$b_5 = m_5 \cdot h^y \pmod p = 041 \cdot 1761^{1312} \pmod{1777} = \mathbf{0195}$
$b_6 = m_6 \cdot h^y \pmod p = 804 \cdot 1761^{1312} \pmod{1777} = \mathbf{0790}$
$b_7 = m_7 \cdot h^y \pmod p = 111 \cdot 1761^{1312} \pmod{1777} = \mathbf{0918}$
$b_8 = m_8 \cdot h^y \pmod p = 208 \cdot 1761^{1312} \pmod{1777} = \mathbf{1336}$
$b_9 = m_9 \cdot h^y \pmod p = 181 \cdot 1761^{1312} \pmod{1777} = \mathbf{1641}$
$b_{10} = m_{10} \cdot h^y \pmod p = 800 \cdot 1761^{1312} \pmod{1777} = \mathbf{0901}$
$b_{11} = m_{11} \cdot h^y \pmod p = 190 \cdot 1761^{1312} \pmod{1777} = \mathbf{0947}$
$b_{12} = m_{12} \cdot h^y \pmod p = 604 \cdot 1761^{1312} \pmod{1777} = \mathbf{1009}$

Seguidament, l'Alice ajunta tots els missatges, és a dir, escriu 1305 0565 0195 0818 0195 0790 0918 1336 1641 0901 0947 1009. Les separacions les pot fer com vulgui, ja que, com que p, que és el mòdul, té 4 xifres, els nombres poden tenir 4 xifres, però no poden tenir-ne més, per tant en Bob sabrà que per desxifrar-lo ha de fer aquestes separacions. Finalment l'Alice envia el missatge xifrat a en Bob.

Desencriptar

En Bob agafa els diferents missatges i, tal com s'ha explicat abans, calcula $a^{p-1-x} \cdot b_i \pmod p$, per tot *1≤i≤12*.

$a^{p-1-x} \cdot b_1 = 64^{1777-1-1479} \cdot 1305 \pmod{1777} = \mathbf{001}$
$a^{p-1-x} \cdot b_2 = 64^{1777-1-1479} \cdot 565 \pmod{1777} = \mathbf{620}$
$a^{p-1-x} \cdot b_3 = 64^{1777-1-1479} \cdot 195 \pmod{1777} = \mathbf{041}$
$a^{p-1-x} \cdot b_4 = 64^{1777-1-1479} \cdot 818 \pmod{1777} = \mathbf{819}$
$a^{p-1-x} \cdot b_5 = 64^{1777-1-1479} \cdot 195 \pmod{1777} = \mathbf{041}$
$a^{p-1-x} \cdot b_6 = 64^{1777-1-1479} \cdot 790 \pmod{1777} = \mathbf{804}$
$a^{p-1-x} \cdot b_7 = 64^{1777-1-1479} \cdot 918 \pmod{1777} = \mathbf{111}$
$a^{p-1-x} \cdot b_8 = 64^{1777-1-1479} \cdot 1336 \pmod{1777} = \mathbf{208}$
$a^{p-1-x} \cdot b_9 = 64^{1777-1-1479} \cdot 1641 \pmod{1777} = \mathbf{181}$
$a^{p-1-x} \cdot b_{10} = 64^{1777-1-1479} \cdot 901 \pmod{1777} = \mathbf{800}$
$a^{p-1-x} \cdot b_{11} = 64^{1777-1-1479} \cdot 947 \pmod{1777} = \mathbf{190}$
$a^{p-1-x} \cdot b_{12} = 64^{1777-1-1479} \cdot 1009 \pmod{1777} = \mathbf{604}$

Llavors, en Bob ajunta tots els missatges i utilitza el codi que ha utilitzat anteriorment l'Alice, per substituir els números per lletres i poder llegir el missatge. Per tal de facilitar la feina, els separa en grups de 2. Cada grup equivaldrà a una lletra del codi utilitzat per l'Alice:

00 16 20 04 18 19 04 18 04 11 12 08 18 18 00 19 06 04

00 → a; 16 → q; 20 → u; etc.

Missatge descodificat: "aquesteselmissatge"

Finalment, separant les paraules adequadament, en Bob pot obtenir el missatge "aquest es el missatge".

2.4.2.8 Avantatges i inconvenients

Es tracta d'un mètode segur, degut a la dificultat de calcular logaritmes discrets. Hi ha alguna manera més ràpid per calcular-los, que la simple força bruta, però tampoc són gaire bons. Si es troba algun mètode per calcular-los eficientment, aleshores esdevindrà un mètode inefectiu ja que es podran atacar els missatges xifrats amb ElGamal molt fàcilment. D'altra banda, si evolucionen els ordinadors quàntics, que poden fer càlculs molt ràpidament, ElGamal deixarà de ser un bon mètode, també. Però actualment és un xifrat segur.

Un inconvenient d'aquest mètode és que, el missatge xifrat, és aproximadament el doble de llarg que el missatge original. Per tant, només s'utilitza per enviar missatges relativament curts.

Un altre inconvenient és que, encara que sigui molt improbable, si dos usuaris trien la mateixa *y* per enviar un missatge a una mateixa persona, aleshores, sabent el missatge que han enviat poden calcular el missatge que ha enviat l'altre de la següent manera:

L'usuari 1 envia $a_1=g^y$ i $b_1=m_1 \cdot h^y$, i l'usuari 2 envia $a_2=g^y$ i $b_2=m_2 \cdot h^y$. L'usuari 2 vol descobrir m_1. Aleshores, $b_1/b_2=m_1 \cdot h^y/m_2 \cdot h^y=m_1/m_2$, per tant, $m_1=m_2 \cdot b_1/b_2$. L'usuari 2 pot saber fàcilment b_1, ja que s'envia per un canal públic, i sap m_2 i b_2.

2.5 El Gamal aplicat a les corbes el·líptiques

2.5.1 Història

Les propietats de les corbes el·líptiques han estat estudiades des de fa uns 150 anys. El seu ús en la criptografia va ser proposat per primera vegada el 1985, separadament, per Neal Koblitz, de la Universitat de Washington i Victor Miller, a l'IBM.

Tenen el seu origen en l'estudi per aproximar la longitud d'una corba mitjançant un nombre finit de segments que uneixen punts d'aquesta corba. Aquest mètode va ser utilitzat per estudiar les longituds d'arc de les el·lipses i en van sorgir les funcions el·líptiques i, finalment, les corbes el·líptiques.

2.5.2 Mètode

2.5.2.1 Idea utilitzada

La criptografia de corbes el·líptiques es basa en la dificultat de trobar els logaritmes discrets de les corbes el·líptiques.

2.5.2.2 Fonaments matemàtics

Corbes el·líptiques → Una corba el·líptica és el conjunt de punts *(x, y)* tals que $y^2=x^3+ax+b$, exceptuant els casos en els quals $4a^3+27b^2=0$. Les corbes el·líptiques van ser utilitzades per demostrar l'últim teorema de Fermat.

Les corbes el·líptiques en cossos finits poden ser utilitzades en ElGamal perquè, juntament amb un punt anomenat punt a l'infinit, formen un grup. Una característica de les corbes el·líptiques molt valuosa per la criptografia és, com en altres processos criptogràfics, que hi ha operacions molt fàcils de realitzar, en aquest cas l'exponencial discreta, però molt difícils de revertir, és a dir, el logaritme discret.

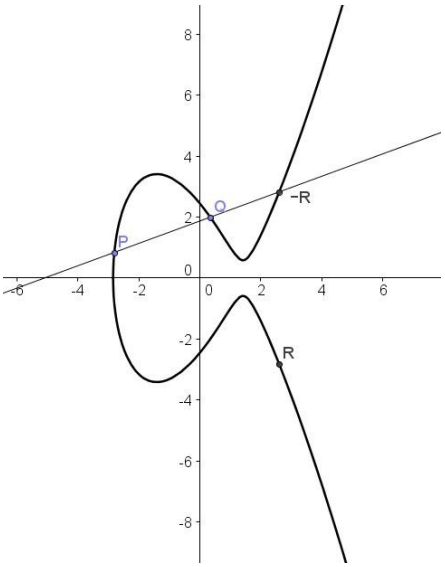


Fig. 2.5.2.2.1. Imatge de la corba el·líptica $y^2=x^3+6x+6$.

Suma de punts en corbes el·líptiques

Sigui $P=(x_p,y_p)$ un punt de la corba el·líptica i -P la seva reflexió en l'eix de la x, és a dir, $-P=(x_p,-y_p)$. Per sumar dos punts diferents, P i Q, on $Q\neq -P$, es dibuixa la recta que passa per aquests dos punts, la qual talla la corba el·líptica en un altre punt, que anomenarem –R. La reflexió d'aquest punt en l'eix de la x serà R, i serà la suma dels punts P i Q, és a dir, P+Q=R.

Si Q=-P, la recta que passa pels dos punts (P i –P) és paral·lela a l'eix de la y, no talla la corba el·líptica en cap altre punt. És per això que existeix el punt O, a l'infinit, que és l'element neutre de la suma, ja que P+(-P)=O, per tant P+O=P.

Finalment, si Q=P, per sumar P+P es dibuixa una línia tangent a la corba en el punt P, que tallarà la corba en un altre punt, que serà –R. La reflexió d'aquest punt en l'eix de la x serà R=2P.

Algebraicament, el punt R es pot calcular així:

$x_R=s^2-x_P-x_Q$ i $y_R=s(x_P-x_R)-y_P$, on *s* és el pendent, és a dir, si $P\neq Q$, aleshores $s=(y_P-y_Q)/(x_P-x_Q)$ i si $P=Q$, aleshores $s=(3x_P^2+a)/(2y_P)$.

En la criptografia s'utilitzen cossos finits $\mathbb{F}_p$, és a dir, utilitza nombres entre 0 i p-1, per tant els resultats es donen en mòdul p.

Multiplicant un punt de la corba per un nombre k, és a dir, sumar $P_1+P_2+\ldots+P_k=kP$ mòdul p, produirà un altre punt de la corba, però és molt difícil trobar el nombre k encara que es coneguin el punt original i el punt resultant.

Si s'agafa, per exemple[12], p=23, s'obtindran 23·23=529 corbes, ja que es poden substituir els paràmetres *a* i *b* per 23 valors diferents cadascun. D'aquestes n'hi haurà unes quantes, en aquest cas 18, que no podran ser utilitzades, ja que no compleixen que $4a^3+27b^2\neq 0 \pmod{23}$. La resta de corbes tenen diferents solucions, que depenen de la corba. En el cas de p=23 hi ha entre 14 i 32 solucions en cada corba de les utilitzades. Per exemple, en el cas *a=10* i *b=18* s'obtindria una corba el·líptica amb els següents punts:

	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22
22																X							
21															X				X				
20						X				X													
19																							
18																							
17																						X	
16													X										
15	X																X						
14									X														
13																							
12		X		X																X			
11		X		X																X			
10																							
9									X														
8	X																X						
7													X										
6																						X	
5																							
4																							
3						X				X													
2															X				X				
1																X							
0			X																				

En aquest cas hi ha 29 solucions. Es pot observar que és simètrica, entre els valors y=11 i y=12.

[12] Exemple obtingut a partir d'aplicacions de http://www.certicom.com/index.php/solutions/7-ecc-tutorial/144-ecc-tutorial.

Si en aquest mateix exemple s'escull un punt, per exemple *P=(0,8)* es poden calcular *2P=(18,21)*, *3P=(9,20)*, etc. Però si se sap que *P=(0,8)* i que *kP=(0,15)*, es pot deduir el valor de *k* a partir d'aquestes dades? En aquest exemple només caldria anar sumant $P_1+P_2+\ldots+P_k$. Però si és fàcil fer-ho és únicament perquè s'està treballant amb nombres molt petits. Si *p* és prou gran es pot aconseguir que sigui una tasca inassolible, fins i tot pels ordinadors potents.

Si anem sumant punts semblen tenir una relació molt caòtica. A continuació es mostren els diferents resultats obtinguts en l'exemple anterior:

P=(0,8)	7P=(19,11)	13P=(12,16)	19P=(1,11)	25P=(21,6)
2P=(18,21)	8P=(6,8)	14P=(14,21)	20P=(8,14)	26P=(3,12)
3P=(9,20)	9P=(17,15)	15P=(2,0)	21P=(17,8)	27P=(9,3)
4P=(3,11)	10P=(8,9)	16P=(14,2)	22P=(6,15)	28P=(18,2)
5P=(21,17)	11P=(1,12)	17P=(12,7)	23P=(19,12)	29P=(0,15)
6P=(5,3)	12P=(15,1)	18P=(15,22)	24P=(5,20)	30P=O

Per tant, en aquest exemple k=29. Es pot observar que en aquest cas concret s'ha passat per tots els punts de la corba el·líptica, la qual cosa no és habitual.

30P és el punt a l'infinit, ja que *29P=-P*, i per tant, *29P+P=O*. Es pot observar també, que *28P=-2P*, *27P=-3P*, etc. És a dir, generalitzant, que *nP=-(30-n)P*.

2.5.2.3 Creació de les claus

Es trien una sèrie de paràmetres $E = (a, b, p)$ que definiran la corba el·líptica $y^2 = x^3 + ax + b\ (mod\ p)$ en la qual es treballarà. També es tria un generador G, que serà un punt de la corba el·líptica. En general no tots els punts de la corba formen un grup cíclic, per tant el generador no passarà per tots els punts, només passarà per un subgrup, que sí que serà cíclic. És interessant que passi per tants punts com sigui possible, ja que així el grup cíclic que formarà serà més gran. Finalment també es busca n, que és l'ordre de G, és a dir, el nombre no negatiu més petit pel qual $nG = O$, que ens indicarà el nombre d'elements que hi ha en el subgrup escollit. L'Alice i en Bob trien aleatòriament les seves claus privades, que seran d_A i d_B, respectivament.

En Bob, que serà el receptor del missatge, calcula $Q_B = d_B \cdot G$. Aquest mètode es basa en trobar d_B a partir de G i Q_B. La seva clau pública serà (E, G, Q_B) i la privada d_B.

2.5.2.4 Encriptar

L'Alice vol enviar-li el missatge m a en Bob. Primerament calcula $Q_A = d_A \cdot G$. Calcula també $k = (x_k, y_k) = d_A \cdot Q_B$ i finalment $c = m \cdot x_k\ (mod\ p)$. El missatge xifrat és (Q_A, c).

2.5.2.5 Desencriptar

En Bob calcula $k = (x_k, y_k) = d_B \cdot Q_A$. El punt k coincideix amb el que ha calculat l'Alice ja que $k = d_A \cdot Q_B = d_A \cdot d_B \cdot G = d_B \cdot Q_A$.

Per obtenir m a partir de x_{Q_A} i c, en Bob calcula $m = c \cdot x_k^{-1} \ (mod\ p) = c \cdot x_k^{-1} \ (mod\ p) = c \cdot x_k^{p-2} (mod\ p)$

2.5.2.6 Exemple

Com en els exemples anteriors (RSA i ElGamal aplicat a un grup multiplicatiu), l'Alice vol enviar el missatge "aquest es el missatge" a en Bob. Substitueix les lletres per nombres, segons el codi indicat a RSA. En aquest cas, excepcionalment, prescindirem de les lletres x, y i z de l'alfabet, ja que en el missatge que es vol encriptar no hi apareixen i els diferents missatges han de ser menors de *p*, que és 23 i, per tant, si utilitzéssim tot l'alfabet, per assegurar-nos que cadascun dels missatges és menor que p cada missatge hauria de correspondre a una sola xifra. Per tant, els missatges són els següents: m_1=00, m_2=16, m_3=20, m_4=04, m_5=18, m_6=19, m_7=04, m_8=18, m_9=04, m_{10}=11, m_{11}=12, m_{12}=08, m_{13}=18, m_{14}=18, m_{15}=00, m_{16}=19, m_{17}=06 i m_{18}=04.

Creació de les claus

S'utilitzarà la corba el·líptica anterior, és a dir $y^2 = x^3 + 10x + 18 \ (mod\ 23)$. S'escull el generador *G=(0,8)*. Per aquest generador, l'ordre és *n=30*. En Bob tria, aleatòriament, la clau privada $d_B = 13$ i calcula $Q_B = d_B \cdot G = 13 \cdot (0,8) = (1,12)$.

Encriptar

L'Alice tria aleatòriament la seva clau privada $d_A = 7$ i calcula $Q_A = d_A \cdot G = 7 \cdot (0,8) = (19,11)$. Seguidament calcula $k = d_A \cdot Q_B = 7 \cdot (1,12) = (12,7)$. Per tant, $x_k = 12$. Calcula també c_i, per tot $1 \leq i \leq 18$.

$c_1 = m_1 \cdot x_k \ (mod\ p) = 00 \cdot 12 \ (mod\ 23) = 00$
$c_2 = m_2 \cdot x_k \ (mod\ p) = 16 \cdot 12 \ (mod\ 23) = 08$
$c_3 = m_3 \cdot x_k \ (mod\ p) = 20 \cdot 12 \ (mod\ 23) = 10$
$c_4 = m_4 \cdot x_k \ (mod\ p) = 04 \cdot 12 \ (mod\ 23) = 02$
$c_5 = m_5 \cdot x_k \ (mod\ p) = 18 \cdot 12 \ (mod\ 23) = 09$
$c_6 = m_6 \cdot x_k \ (mod\ p) = 19 \cdot 12 \ (mod\ 23) = 21$
$c_7 = m_7 \cdot x_k \ (mod\ p) = 04 \cdot 12 \ (mod\ 23) = 02$
$c_8 = m_8 \cdot x_k \ (mod\ p) = 18 \cdot 12 \ (mod\ 23) = 09$
$c_9 = m_9 \cdot x_k \ (mod\ p) = 04 \cdot 12 \ (mod\ 23) = 02$
$c_{10} = m_{10} \cdot x_k \ (mod\ p) = 11 \cdot 12 \ (mod\ 23) = 17$
$c_{11} = m_{11} \cdot x_k \ (mod\ p) = 12 \cdot 12 \ (mod\ 23) = 06$
$c_{12} = m_{12} \cdot x_k \ (mod\ p) = 08 \cdot 12 \ (mod\ 23) = 04$
$c_{13} = m_{13} \cdot x_k \ (mod\ p) = 18 \cdot 12 \ (mod\ 23) = 09$
$c_{14} = m_{14} \cdot x_k \ (mod\ p) = 18 \cdot 12 \ (mod\ 23) = 09$
$c_{15} = m_{15} \cdot x_k \ (mod\ p) = 00 \cdot 12 \ (mod\ 23) = 00$
$c_{16} = m_{16} \cdot x_k \ (mod\ p) = 19 \cdot 12 \ (mod\ 23) = 21$
$c_{17} = m_{17} \cdot x_k \ (mod\ p) = 06 \cdot 12 \ (mod\ 23) = 03$
$c_{18} = m_{18} \cdot x_k \ (mod\ p) = 04 \cdot 12 \ (mod\ 23) = 02$

Finalment l'Alice ajunta tots els missatges, és a dir, escriu "00 08 10 02 09 21 02 09 02 17 06 04 09 09 00 21 03 02" i ho envia a en Bob. Li envia també $Q_A = (19,11)$.

Desencriptar

En Bob calcula $k = d_B \cdot Q_A = 11 \cdot (19,11) = (12,7)$. Seguidament agafa els diferents missatges i calcula:

$m_1 = c_1 \cdot x_k^{p-2} \ (mod\ p) = 00 \cdot 12^{21} \ (mod\ 23) = 00$
$m_2 = c_2 \cdot x_k^{p-2} \ (mod\ p) = 08 \cdot 12^{21} \ (mod\ 23) = 16$
$m_{10} = c_{10} \cdot x_k^{p-2} \ (mod\ p) = 17 \cdot 12^{21} \ (mod\ 23) = 11$
$m_{11} = c_{11} \cdot x_k^{p-2} \ (mod\ p) = 06 \cdot 12^{21} \ (mod\ 23) = 12$

$m_3 = c_3 \cdot x_k^{p-2} \pmod p = 10 \cdot 12^{21} \pmod{23} = 20$
$m_4 = c_4 \cdot x_k^{p-2} \pmod p = 02 \cdot 12^{21} \pmod{23} = 04$
$m_5 = c_5 \cdot x_k^{p-2} \pmod p = 09 \cdot 12^{21} \pmod{23} = 18$
$m_6 = c_6 \cdot x_k^{p-2} \pmod p = 21 \cdot 12^{21} \pmod{23} = 19$
$m_7 = c_7 \cdot x_k^{p-2} \pmod p = 02 \cdot 12^{21} \pmod{23} = 04$
$m_8 = c_8 \cdot x_k^{p-2} \pmod p = 09 \cdot 12^{21} \pmod{23} = 18$
$m_9 = c_9 \cdot x_k^{p-2} \pmod p = 02 \cdot 12^{21} \pmod{23} = 04$
$m_{12} = c_{12} \cdot x_k^{p-2} \pmod p = 04 \cdot 12^{21} \pmod{23} = 08$
$m_{13} = c_{13} \cdot x_k^{p-2} \pmod p = 09 \cdot 12^{21} \pmod{23} = 18$
$m_{14} = c_{14} \cdot x_k^{p-2} \pmod p = 09 \cdot 12^{21} \pmod{23} = 18$
$m_{15} = c_{15} \cdot x_k^{p-2} \pmod p = 00 \cdot 12^{21} \pmod{23} = 00$
$m_{16} = c_{16} \cdot x_k^{p-2} \pmod p = 21 \cdot 12^{21} \pmod{23} = 19$
$m_{17} = c_{17} \cdot x_k^{p-2} \pmod p = 03 \cdot 12^{21} \pmod{23} = 06$
$m_{18} = c_{18} \cdot x_k^{p-2} \pmod p = 02 \cdot 12^{21} \pmod{23} = 04$

Per tant el missatge desxifrat serà 00 16 20 04 18 19 04 18 04 11 12 08 18 18 00 19 06 04, que substituint-ho per les lletres del codi, es transforma en “aquesteselmissatge” i, separant-ho correctament obté “aquest es el missatge”.

2.5.3 Avantatges i inconvenients

Les claus necessàries per aconseguir suficient seguretat són molt petites, comparades amb les claus utilitzades en altres sistemes, ja que els millors algoritmes que es coneixen són molt complexos computacionalment. La mida de clau recomanada per la criptografia de corbes el·líptiques és de l’ordre de 160 bits, mentre que la del RSA és de l’ordre de 1024 bits. Això és degut al fet que, encara que no es coneguin mètodes eficients per descompondre un número, o trobar un logaritme discret en un grup $\mathbb{Z}_p^*$, es coneixen alguns mètodes millors que provar tots els casos. En canvi, amb els logaritmes discrets de les corbes el·líptiques no es coneixen mètodes gaire millors que la força bruta.

Nigel Smart, investigador del Hewlett Packard, va descobrir un error en el qual certes corbes són extremadament vulnerables. Aquest casos és quan no formen una corba el·líptica i per tant no formen grup, és a dir, quan $4a^3+27b^2=0$. En la resta de casos, la criptografia de corbes el·líptiques és molt segura.

2.6 Criptografia quàntica

2.6.1 Història

Hi ha diversos mètodes criptogràfics basats en la física quàntica. El més conegut, explicat a continuació, va ser elaborat per Charles Bennett i Gilles Brassard, el 1984 (per això se l'anomena BB84). La criptografia quàntica és un mètode molt recent, que tot just està en fase experimental.

La teoria de la física quàntica va començar el 1900 quan Max Planck, un físic alemany, va dir que l'energia estava quantitzada, és a dir, agrupada en blocs indivisibles. Aquests blocs serien anomenats "fotons" per Gilbert N. Lewisk, el 1926. El 1905 Albert Einstein va explicar l'efecte fotoelèctric utilitzant un postulat sobre el qual tota la radiació electromagnètica pot ser dividia en un nombre finit de "quants d'energia", és a dir, blocs indivisibles, localitzats en punts de l'espai. La quantització va servir a Niels Bohr per poder explicar les línies espectrals de l'hidrogen, el 1913. Finalment, el físic francès Louis-Victor de Broglie va presentar la seva teoria d'ones de matèria, en la qual una partícula pot actuar com una ona i una ona pot actuar com una partícula.

2.6.2 Mètode

2.6.2.1 Idea utilitzada

Aquest mètode es basa en l'atzar. És impossible estar segur de la polarització que tenia un fotó abans de mesurar-lo basant-se en el resultat del mesurament, ja que si no es mesura en la base correcta el resultat és completament aleatori. Per tal que no es pugui desxifrar el missatge basant-se amb claus de missatges anteriors, trobant patrons, s'utilitzen claus d'un sol ús.

2.6.2.2 Fonaments de física quàntica

La polarització és una propietat de les ones electromagnètiques transversals, per exemple la llum, que descriu l'orientació de les seves oscil·lacions en el camp electromagnètic. Pot ser lineal, si el camp està orientat en només una direcció, o circular o el·líptic, si la direcció del camp canvia a mesura que l'ona es desplaça.

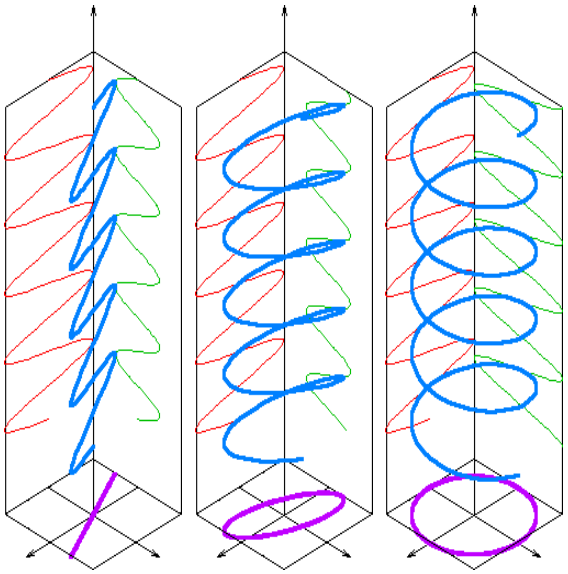


Fig. 2.6.2.2.1. Gràfic on es mostra com evoluciona la polarització d'una ona transversal. La de l'esquerra pertany a una polarització lineal, la del mig a una polarització el·líptica i la de la dreta a una polarització circular. Imatges obtingudes, respectivament, de:
http://upload.wikimedia.org/wikipedia/commons/2/2e/Linear_polarization_schematic.png
http://upload.wikimedia.org/wikipedia/commons/6/6a/Elliptical_polarization_schematic.png
http://upload.wikimedia.org/wikipedia/commons/6/67/Circular_polarization_schematic.png

Cada fotó té una polarització concreta, però un feix de llum no sempre està polaritzat. Això passa quan els fotons que formen el feix de llum no tenen la mateixa polarització.

Un polaritzador és un filtre que permet que passin només els fotons que tenen una determinada polarització, i evita que passin els que tenen la polarització perpendicular.

La intensitat inicial i la final (la suma de la intensitat reflectida i la transmesa) ha de ser la mateixa, ja que no apareixen ni desapareixen fotons. Per tant, $I=I_R+I_T$, on I és la intensitat inicial, I_R és la intensitat reflectida, és a dir, que no passa pel polaritzador, i I_T és la polarització transmesa, és a dir, que passa a través del polaritzador. La intensitat transmesa i la reflectida depenen de l'angle. Quan $\alpha=0$, tota la intensitat inicial es transmet, mentre que quan $\alpha=\pi/2$ radians o $\alpha=90^o$ tota la intensitat inicial es reflecteix. Es pot deduir que $I_R=sin^2\alpha$ i $I_T=cos^2\alpha$.

Si tenim un feix de llum sense polaritzar i hi posem un polaritzador, minvarà la quantitat de llum i la llum que passi a través del polaritzador s'orientarà segons la direcció del polaritzador. Si girem el polaritzador, la llum que passarà serà la mateixa, ja que aproximadament n'hi haurà la mateixa quantitat amb cada polarització possible, de manera que no importa com es posi el polaritzador.

Si tenim llum polaritzada i hi col·loquem un polaritzador amb la mateixa direcció, passarà tota la llum, ja que $\alpha=0$ (veure Fig. 2.6.2.2.2.). Si anem girant el polaritzador, cada vegada minvarà més la quantitat de llum. Quan $\alpha=\pi/4$ radians, és a dir, $\alpha=45^o$, la quantitat de llum que passarà pel polaritzador serà la meitat (veure Fig. 2.6.2.2.3.), ja que $\cos^2(\pi/4)=1/2$ i la quantitat de llum que es reflectirà també serà la meitat. Quan $\alpha=\pi/2$ rad tota la llum serà reflectida i, per tant, no passarà gens de llum pel segon polaritzador (veure Fig. 2.6.2.2.4).

Què passarà, si introduïm un altre polaritzador entremig del feix de llum i del polaritzador, formant un angle $\alpha=\pi/4$ rad, amb la polarització del feix de llum i amb el polaritzador? El més habitual seria pensar que, si amb l'orientació del polaritzador anterior no passa llum, encara que introduïm polaritzadors al mig, continuarà sense passar-ne. Però no és així. Imaginem que tenim el feix de llum polaritzat horitzontalment. Quan arribi al primer polaritzador, que acabem de col·locar, passarà la meitat de la llum, ja que $\alpha=\pi/4$ rad, i quedarà polaritzada amb la mateixa direcció que el polaritzador, és a dir, amb un angle $\alpha=\pi/4$ rad. Seguidament, aquest feix de llum passa per l'altre polaritzador, el qual està orientat amb un angle $\alpha=\pi/4$ rad respecte la polarització actual del feix de llum, per tant passarà la meitat del feix de llum actual, i quedarà polaritzat verticalment, és a dir, amb la direcció de l'últim polaritzador. Per tant, encara que inicialment costa de creure, una quarta part de la llum inicial passarà a través de l'últim polaritzador! (veure Fig. 2.6.2.2.5.)

Fins ara s'ha explicat la polarització de la llum però, què passa si s'analitzen els fotons individualment? Evidentment no passarà només una part del fotó, ja que són indivisibles. La intensitat transmesa i la intensitat reflectida seran la probabilitat que el fotó passi a través del polaritzador o no passi, respectivament. Per tant, si volem fer passar un fotó amb polarització horitzontal a través d'un polaritzador horitzontal, hi ha un 100% de probabilitats que el fotó passi, si el volem fer passar a través d'un polaritzador amb un angle $\alpha=\pi/4$ rad hi ha un 50% de probabilitats que passi i un 50% que no passi, és a dir, és completament aleatori, i si el volem fer

passar a través d'un polaritzador vertical hi haurà un 0% de probabilitats que passi, és a dir, no passarà mai (veure Fig. 2.6.2.2.2., 2.6.2.2.3., 2.6.2.2.4. i 2.6.2.2.5.).

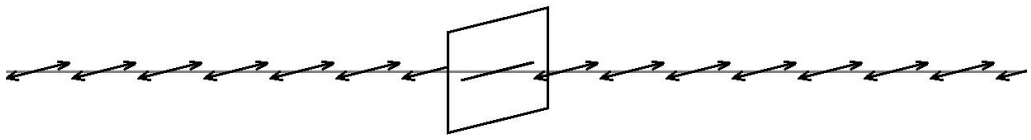


Fig. 2.6.2.2.2. Esquema on es mostra llum polaritzada horitzontalment passant per un polaritzador horitzontal. Passen tots els fotons.

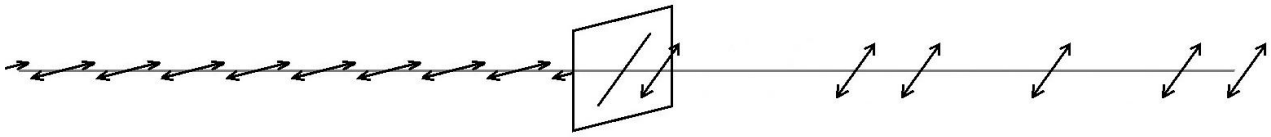


Fig. 2.6.2.2.3. Esquema on es mostra llum polaritzada horitzontalment passant per un polaritzador amb un angle de $\pi/4$ rad. Passen aproximadament la meitat dels fotons.

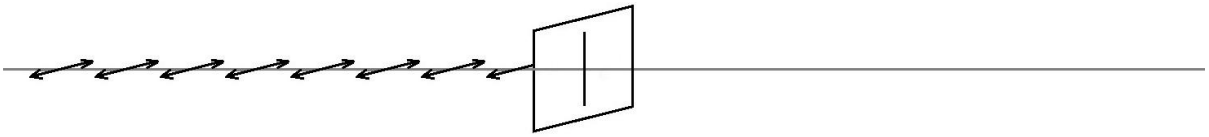


Fig. 2.6.2.2.4. Esquema on es mostra llum polaritzada horitzontalment passant per un polaritzador vertical. No passa cap fotó.

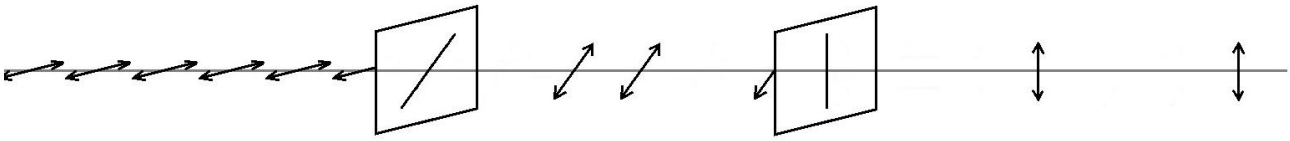


Fig. 2.6.2.2.5. Esquema on es mostra llum polaritzada horitzontalment passant per un polaritzador amb un angle de $\pi/4$ rad i seguidament per un de vertical. Passa un quart dels fotons, aproximadament.

Cal diferenciar entre l'aleatorietat que provoca un fotó o l'aleatorietat quan tirem una moneda per veure si surt cara o creu, o quan tirem un dau. Amb una moneda o un dau, si reproduíssim exactament el mateix procés, és a dir, tirar-ho des de la mateixa posició, des de la mateixa alçada, amb la mateixa força, amb el mateix angle, etc. sortiria exactament el mateix resultat. L'aleatorietat en aquest cas es basa en la dificultat de reproduir exactament les mateixes condicions. En el cas de la física quàntica, realment és aleatori. Si un fotó, la polarització del qual forma un angle diferent de 0 o 90^{o} amb un polaritzador, és impossible determinar amb exactitud si el fotó passarà o no a través del polaritzador. Einstein no creia que fos possible aquesta aleatorietat, i d'aquí ve la seva famosa frase "Déu no juga als daus".

La polarització, a part de ser utilitzada en la criptografia quàntica, també s'utilitza en les pel·lícules en 3 dimensions, on els vidres de les ulleres que s'utilitzen estan polaritzats de manera que amb un ull només es veuen unes imatges concretes i amb l'altre ull unes altres, per tal que l'observador creï, a la seva ment, una imatge en tres dimensions. La polarització s'utilitza també en fotografia. Per exemple per contrastar el cel i els núvols, o per eliminar reflexes en superfícies llises, vidres, superfícies d'aigua, etc.

En l'explicació del funcionament de la criptografia quàntica, quan es parla de bases + o × es refereix a utilitzar un polaritzador horitzontal o amb un angle $\alpha=\pi/4$ rad, respectivament. Les

diferents polaritzacions es simbolitzen amb ↔ , ↕, ↗ o ↘, que simbolitzen els angles, respecte l'horitzontal, 0, π/2, π/4 i 3π/4 radians, respectivament. Si un fotó passa pel polaritzador el bit corresponent és 0, sinó és 1. És a dir, tal com s'explicarà a continuació, si s'utilitza la base + i el fotó passa significarà que tenim el fotó amb la polarització ↔ , si no passa significarà que tenim el fotó amb la polarització ↕ i, si s'utilitza la base × i el fotó passa significarà que tenim el fotó amb la polarització ↗ i si no passa significarà que tenim el fotó amb la polarització ↘.

2.6.2.3 Creació de les claus

En general, els mètodes criptogràfics actuen de la mateixa manera si hi ha un espia o si no n'hi ha cap. Amb la criptografia quàntica, com s'ha comentat abans, es basa en la impossibilitat de saber la polarització d'un fotó abans de mesurar-lo, ja que amb el mesurament pot canviar. Si l'espia mesura el fotó, abans que arribi al receptor, pot ser que canviï informació sobre la clau. Per aquest motiu primer s'explicarà què passa si no hi ha l'espia i després s'introduirà l'espia per veure com pot canviar la clau, i la informació que pot aconseguir.

Sense tenir en compte l'espia

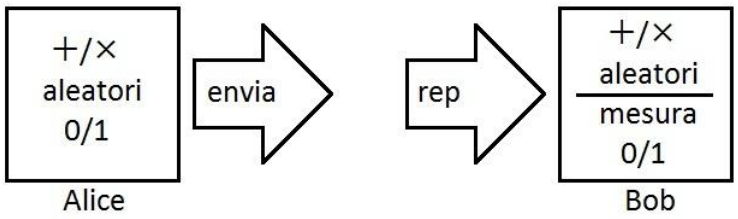


Fig. 2.6.2.3.1. Esquema per il·lustrar el mètode utilitzat en la criptografia quàntica per crear la clau, sense la presència de l'espia.

L'Alice envia un fotó a en Bob, amb una polarització determinada aleatòriament per un bit (0 o 1) i per una base (+ o ×).

	0	1
+	↔	↕
×	↗	↘

Fig. 2.6.2.3.2. Taula on es mostra la direcció de la polarització del fotó segons les bases utilitzades i el bit triat.

En Bob, quan rep el fotó el mesura amb una de les dues bases aleatòriament, ja que no sap en quina base l'ha enviat l'Alice, i si l'Alice li digués, un espia podria interceptar la clau fàcilment.

Si ho mesura amb la mateixa base que l'Alice, el bit rebut serà el mateix que l'enviat; en cas contrari, com s'ha explicat anteriorment, serà completament aleatori: hi haurà un 50% de possibilitats de rebre el bit 0 i el 50% de rebre el bit 1.

Alice envia			Bob mesura			Probabilitat
+	0	→	+	0		100 %
				1		0 %
			×	0		50 %
				1		50 %
	1	→	+	0		0 %
				1		100 %
			×	0		50 %
				1		50 %

×	0	→	+	0		50 %
				1		50 %
			×	0		100 %
				1		0 %
	1	→	+	0		50 %
				1		50 %
			×	0		0 %
				1		100 %

En la taula anterior es mostra la probabilitat que en Bob mesuri una polarització determinada depenent de la polarització que li ha enviat l'Alice.

A la taula següent es mostra un exemple del mètode explicat anteriorment:

Alice (envia)	base	+	×	+	×	×	+	+	+	×	×	+	×
	bit	0	0	1	1	1	1	0	0	1	0	0	0
	polarització	↔	↗	↕	↘	↘	↕	↔	↔	↘	↗	↔	↗
Bob (mesura)	base	×	+	+	+	×	+	+	×	×	+	×	×
	possibles bits	0/1	0/1	1	0/1	1	1	0	0/1	1	0/1	0/1	0
	bit	1	0	1	0	1	1	0	0	1	1	1	0
	polarització	↘	↔	↕	↔	↘	↕	↔	↗	↘	↕	↘	↗

Com que els bits aleatoris no ens interessen per la clau, ja que no ens aporten informació perquè no podem saber si són correctes o no, un cop finalitzat l'enviament i el mesurament de fotons, l'Alice i en Bob comparen les bases que han utilitzat, i eliminen tots els bits mesurats en bases diferents (marcats en vermell), aprofitant només els mesurats amb la mateixa base (marcats en verd). Per tant la seqüència de bits utilitzada per la clau en aquest cas serà 111010.

<u>Tenint en compte l'espia</u>

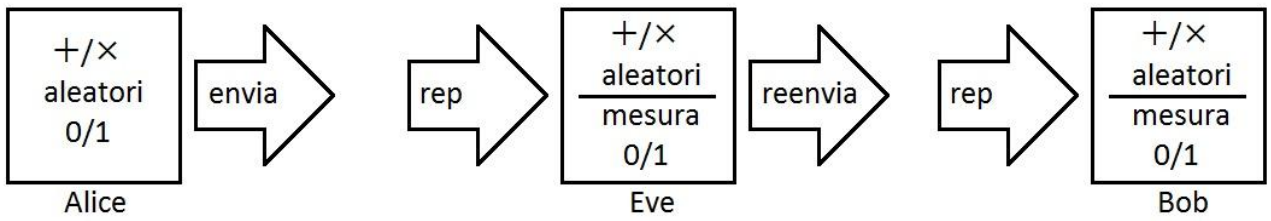


Fig. 2.6.2.3.3. Esquema per il·lustrar el mètode utilitzat en la criptografia quàntica per crear la clau, tenint en compte la presència de l'espia.

Suposem que ara hi ha un espia, l'Eve, que mesura els fotons enviats per l'Alice i els reenvia a en Bob (si no els reenvia és inútil que els mesuri, ja que no es crearà cap clau entre l'Alice i en Bob). L'Eve, igual que l'Alice i en Bob, utilitza les bases aleatòriament, ja que no sap quines bases utilitza l'Alice per enviar cadascun dels fotons. Seguidament envia, a en Bob, un fotó amb el bit que ha rebut amb les bases que ella ha mesurat. Si l'Eve utilitza la mateixa base que l'Alice i en Bob, aleshores no es detectarà cap incoherència. Si l'Eve utilitza una base diferent que l'Alice i en Bob, aleshores hi haurà, de mitjana, un 50% d'error. Per tant, si l'Eve intercepta la clau, l'Alice i en Bob podran observar, de mitjana, un 25% d'error, ja que aproximadament la meitat de les vegades utilitzarà la mateixa base que l'Alice i en Bob, i l'altra meitat de vegades utilitzarà la base diferent.

A la taula següent es mostra el bit que rebrà en Bob segons el que hagi enviat l'Alice i el que hagi interceptat l'Eve. Només tindrem en compte els casos en els quals en Bob i l'Alice utilitzen les mateixes bases, ja que sinó els descarten automàticament.

Alice envia			Eve mesura i reenvia		Probabilitat (Eve)		Bob mesura		Probabilitat (Bob)		Probabilitat (total)
+	0	→	+	0	100 %	→	+	0	100 %		100 %
								1	0 %		0 %
				1	0 %	→	+	0	0 %		0 %
								1	100 %		0 %
			×	0	50 %	→	+	0	50 %		25 %
								1	50 %		25 %
				1	50 %	→	+	0	50 %		25 %
								1	50 %		25 %
	1	→	+	0	0 %	→	+	0	100 %		0 %
								1	0 %		0 %
				1	100 %	→	+	0	0 %		0 %
								1	100 %		100 %
			×	0	50 %	→	+	0	50 %		25 %
								1	50 %		25 %
				1	50 %	→	+	0	50 %		25 %
								1	50 %		25 %
×	0	→	+	0	50 %	→	×	0	50 %		25 %
								1	50 %		25 %
				1	50 %	→	×	0	50 %		25 %
								1	50 %		25 %
			×	0	100 %	→	×	0	100 %		100 %
								1	0 %		0 %
				1	0 %	→	×	0	0 %		0 %
								1	100 %		0 %
	1	→	+	0	50 %	→	×	0	50 %		25 %
								1	50 %		25 %
				1	50 %	→	×	0	50 %		25 %
								1	50 %		25 %
			×	0	0 %	→	×	0	100 %		0 %
								1	0 %		0 %
				1	100 %	→	×	0	0 %		0 %
								1	100 %		100 %

Les caselles marcades en verd són les situacions en les quals és l'única opció possible si es mesura la polarització rebuda en la base indicada. Les caselles marcades en vermell són les situacions impossibles.

Quan l'Alice i en Bob tenen la clau, per comprovar que no hi ha errors, poden comparar alguns dígits. Un mètode per comprovar-ho és el següent, en el qual s'utilitzarà el símbol $\oplus$ per indicar suma en mòdul 2, és a dir $a \oplus b = a + b \ (mod\ 2)$ (veure exemples a l'apartat 2.6.2.4 Encriptar). L'Alice agafa els seus dos primers bits (a_1 i a_2) i els suma en mòdul 2, és a dir, calcula $a_1 \oplus a_2$. En Bob fa el mateix amb els seus dos primers bits (b_1 i b_2), és a dir, calcula $b_1 \oplus b_2$. Seguidament comparen els resultats. Si $a_1 \oplus a_2 \neq b_1 \oplus b_2$, aleshores l'Alice i en Bob eliminen els dos bits. Si

$a_1 \oplus a_2 = b_1 \oplus b_2$, aleshores guarden únicament el primer bit, és a dir a_1 i b_1, ja que l'Eve sabrà si a_2 i b_2 són iguals o diferents d'a_1 i b_1.

En el cas anterior quedaran només bits correctes, a no ser que els dos bits que sumem siguin incorrectes, però és poc probable, tot i que no impossible. Aquest procés es pot realitzar uns quants cops, ja que cada vegada es crearà una clau més segura, però també més curta.

Si detecten molts errors significa que l'Eve ha estat espiant, i que potser té més informació ella que en Bob. En aquest cas l'Alice i en Bob descarten la clau i en creen una altra.

Si detecten pocs errors o cap, significa que l'Eve no ha estat espiant, o almenys si ho ha fet no tindrà més informació que en Bob. En aquest cas l'Alice i en Bob poden dur a terme processos per tal d'aconseguir que l'Eve tingui cada vegada menys informació. El preu que han de pagar, però, és que com més segura és la clau més curta queda, ja que per fer més segura la clau, hem de prescindir de molts bits. Si la clau queda molt curta potser cal buscar-ne una de nova.

Quan l'Alice i en Bob estan convençuts que tenen els bits iguals, per obtenir una clau més segura, agafen els bits de dos en dos i els sumen, però sense intercanviar-se cap informació. L'Eve, si sap els dos bits que formen una parella, podrà saber el bit que formaran, però si només en sap un, o no en sap cap, perdrà tota la informació que tingui sobre el bit format per la parella. Aquest procés també es pot realitzar repetidament, per assegurar que l'Eve es queda sense informació o, almenys amb molt poca, però amb l'inconvenient que la clau és cada vegada més curta.

2.6.2.4 Encriptar

S'utilitzarà, igual que abans, el símbol $\oplus$ per indicar suma en mòdul 2, és a dir $a \oplus b = a + b \ (mod\ 2)$. Per tant:

$0 \oplus 0 = 0$ $\qquad$ $1 \oplus 0 = 1$

$0 \oplus 1 = 1$ $\qquad$ $1 \oplus 1 = 0$

k serà la clau, que es crea mitjançant la polarització, com s'ha mostrat anteriorment.

M serà el missatge que es vol enviar. Ha d'estar escrit en sistema binari, és a dir, utilitzant només 0 i 1. Per passar d'un text a un missatge amb binari es pot fer:

- utilitzant algun codi conegut, per exemple l'ASCII però passant-lo a binari. És a dir, en l'ASCII a la lletra *a* li correspon el nombre 97, que en binari seria 01100001, a la lletra *b* li correspon el 98, que seria 01100010, etc.
- creant un codi propi, per exemple: a → 00000, b → 00001, c → 00010, … z → 11001.

e serà el missatge encriptat, que l'Alice enviarà a en Bob un cop hagin acordat la clau.

El missatge encriptat es calcula de la següent manera: $e = M \oplus k$

2.6.2.5 Desencriptar

Per desencriptar es fa d'una manera semblant a la d'encriptar.

Igual que abans, *k* serà la clau i *e* serà el missatge encriptat. El missatge desencriptat, que és el missatge que l'Alice li vol enviar, l'anomenarem *d*. És evident que s'ha de complir que *d=M*.

Per desxifrar el missatge, hem de sumar, en mòdul 2, la clau al missatge encriptat, ja que:

$$d = k \oplus e = k \oplus k \oplus M = 2k \oplus M = M$$

2.6.2.6 Exemple

L'Alice vol enviar el missatge "photon"[13] ("fotó" en anglès) a en Bob. Primer han d'acordar la clau, de la manera explicada anteriorment. És a dir, l'Alice enviarà fotons a en Bob, el qual els mesurarà, després que alguns dels fotons hagi estat mesurat per l'Eve, també. Seguidament en Bob i l'Alice aplicaran algun mètode per assegurar que la clau és correcta i per fer-la més segura. Finalment l'Alice passarà el missatge a un codi binari, el xifrarà i l'enviarà a en Bob, el qual el desxifrarà.

Seguidament es mostra una taula, on s'indica els fotons que envia l'Alice, segons el bit i la base que utilitza, el que rep l'Eve, els cops que espia, i el que rep en Bob. Només es mostraran una petita quantitat dels bits, perquè es pugui veure com funciona, ja que mostrar-los tots es faria molt llarg i repetitiu.

Alice	+	+	+	+	×	×	+	×	+	×	×	×	+	×	×	+	+	+	×	×
	1	0	1	0	1	1	0	0	0	0	1	1	1	0	0	1	1	1	1	1
	↕	↔	↕	↔	↘	↘	↔	↗	↔	↗	↘	↘	↕	↗	↗	↕	↕	↕	↘	↘
Eve	×					+		×			+		×			×		+		+
	0					1		0			0		1			1		1		0
	↗					↕		↗			↔		↘			↘		↕		↔
Bob	+	×	×	+	×	+	+	×	×	+	×	+	×	×	×	+	×	+	×	×
	0	1	0	0	1	1	0	0	1	0	0	1	1	0	0	1	1	1	1	1
	↔	↘	↗	↔	↘	↕	↔	↗	↘	↔	↗	↕	↘	↗	↗	↕	↘	↕	↘	↘
Clau Alice	1			0	1		0	0			1			0	0	1		1	1	1
Clau Eve								0										1		
Clau Bob	0			0	1		0	0			0			0	0	1		1	1	1

Seguidament, l'Alice i en Bob intentaran eliminar errors en les seves claus, fent el procediment explicat anteriorment, en el qual sumen els bits per parelles, en mòdul 2, i, si coincideixen, mantenen el primer dels dos bits i, en cas contrari, els eliminen tots dos.

Alice	Inicial	1	0	1	0	0	1	0	0	1	1	1	1		
	Suma	1		1		1		0		0		0			
	Clau			1				0		1		1			
Bob	Inicial	0	0	1	0	0	0	0	0	1	1	1	1		
	Suma	0		1		0		0		0		0			
	Clau			1				0		1		1			
Eve	Inicial					0					1				
	Clau									1					

[13] S'ha escollit aquest missatge en lloc de l'utilitzat en la resta de casos perquè el missatge "aquest es el missatge" és molt llarg, i es necessitaria una clau molt llarga.

Per tant, de moment la clau obtinguda és 1011, però en aquesta clau, l'Eve té informació sobre una quarta part dels bits. Ara, per fer-la més segura, aconseguint que l'Eve tingui menys informació, poden sumar els bits de la clau de dos en dos, en mòdul 2. És a dir:

Alice i Bob	Clau inicial	1	0	1	1
	Clau final	1		0	
Eve	Clau inicial			1	
	Clau final				

Per tant, la clau final obtinguda per l'Alice i en Bob serà 10. L'Eve, ara, no té gens d'informació sobre la clau que comparteixen l'Alice i en Bob. Les dues últimes operacions, és a dir, comprovar que la clau és igual per l'emissor i el receptor i fer-la més segura, es poden repetir tantes vegades com es vulgui, per aconseguir millors claus. El problema, però, és que en cada operació la clau s'escurça.

De la mateixa manera es poden crear els bits que els falten per aconseguir una clau suficientment llarga. Suposem que la clau és la següent: 10100101111011011000101111111101111101

Seguidament, l'Alice substitueix el missatge "photon" per un codi en binari. Per exemple, utilitzarà el següent:

Text	Decimal	Binari
a	00	00000
b	01	00001
c	02	00010
d	03	00011
e	04	00100
f	05	00101
g	06	00110

Text	Decimal	Binari
h	07	00111
i	08	01000
j	09	01001
k	10	01010
l	11	01011
m	12	01100
n	13	01101

Text	Decimal	Binari
o	14	01110
p	15	01111
q	16	10000
r	17	10001
s	18	10010
t	19	10011

Text	Decimal	Binari
u	20	10100
v	21	10101
w	22	10110
x	23	10111
y	24	11000
z	25	11001

p → 01111; h → 00111; o → 01110; etc.
Per tant, el missatge substituït serà: "01111001110111010011011100 1101"

Llavors s'agafen els dígits necessaris de la clau, és a dir, en aquest cas 30, i es sumen al missatge, en mòdul 2.

Missatge	0	1	1	1	1	0	0	1	1	1	0	1	1	1	0
Clau	1	0	1	0	0	1	0	1	1	1	1	0	1	1	0
Missatge xifrat	1	1	0	1	1	1	0	0	0	0	1	1	0	0	0

Missatge	1	0	0	1	1	0	1	1	1	0	0	1	1	0	1
Clau	1	1	0	0	0	1	0	1	1	1	1	1	1	1	1
Missatge xifrat	0	1	0	1	1	1	1	0	0	1	1	0	0	1	0

Per tant, el missatge xifrat serà "11011 10000 11000 01011 11001 10010".

L'Alice envia el missatge xifrat a en Bob, el qual haurà de sumar la clau i el missatge xifrat per obtenir el missatge sense xifrar. Finalment haurà de substituir cada grup de 5 nombres per la lletra que representen.

Missatge xifrat	1	1	0	1	1	1	0	0	0	0	1	1	0	0	0
Clau	1	0	1	0	0	1	0	1	1	1	1	0	1	1	0
Missatge	0	1	1	1	1	0	0	1	1	1	0	1	1	1	0
Missatge xifrat	0	1	0	1	1	1	1	0	0	1	1	0	0	1	0
Clau	1	1	0	0	0	1	0	1	1	1	1	1	1	1	1
Missatge	1	0	0	1	1	0	1	1	1	0	0	1	1	0	1

Per tant, en Bob, fent les substitucions 01111 → p; 00111 → h; 01110 → o; etc. obtindrà el missatge desencriptat "photon".

2.6.3 **Avantatges i inconvenients**

Potser en un futur, els ordinadors quàntics aconseguiran desxifrar missatges encriptats utilitzant mètodes anteriors, en els quals només es necessita temps per trobar-ne les claus. Aquest mètode, en canvi, no pot ser atacat de cap manera, ja que no hi ha hi ha manera de violar la mecànica quàntica.

Per contra, tenim el problema que és difícil aconseguir fotons individuals, per tal de poder-los enviar i realitzar tot el procés de creació de la clau.

A més, la teoria de la criptografia quàntica és impecable, però la pràctica és més complicada. Bennett, el 1989, després de més d'un any de treball, va aconseguir posar a la pràctica el mètode, utilitzant dos ordinadors, separats per 32 centímetres. El 1995, uns investigadors de Ginebra van aconseguir arribar a 23 km, utilitzant un cable de fibra òptica. Finalment, el 2006, un equip del Laboratori Nacional de Los Álamos, d'Estats Units, va aconseguir arribar a 107 km utilitzant, també, fibra òptica. Per tant, la distància és un problema, ja que no es pot utilitzar per enviar missatges a llocs llunyans.

Si volem utilitzar els satèl·lits artificials, com en la telefonia, per exemple, caldrà trobar la manera d'enviar aquests fotons d'anada i tornada als satèl·lits (a uns 300 km per damunt de la superfície terrestre) de forma segura, tenint en compte les següents dificultats:

- Els fotons, de forma individual, s'han de dirigir amb precisió a l'objectiu.
- La velocitat dels fotons depèn del medi, i l'atmosfera experimenta molts canvis en les seves diverses capes i provoca refracció.
- L'ús massiu d'aquesta tecnologia podria provocar interferències entre els diferents emissors, sense comptar les interferències causades en l'espionatge.

3 Usos de la criptografia

Actualment la criptografia és utilitzada amb diverses finalitats:

- Confidencialitat: L'Alice vol enviar un missatge a en Bob, però ningú més pot saber què diu al missatge. S'ha vist que en un missatge xifrat només pot desxifrar el missatge el receptor, per tant qualsevol persona aliena no el podrà llegir.

- Integritat: L'Alice vol enviar un missatge a en Bob, i no és important si algú més el llegeix, però sí que ho és que el missatge no sigui modificat. Si no arriba el missatge original íntegre, quan en Bob el desxifri li sortirà un missatge totalment diferent, i molt probablement sense sentit, ja que per xifrar els missatge no es xifra lletra per lletra, sinó que s'agafen un conjunt de caràcters i per tant, si el missatge xifrat es modifica pot donar lloc a un missatge completament diferent.

- Autentificació: L'Alice vol enviar un missatge a en Bob, però ha de demostrar que és ella qui l'envia. Llavors, a part de xifrar el missatge amb la clau pública d'en Bob també el "xifrarà" amb la seva clau privada. En Bob el desxifrarà primerament amb la clau pública de l'Alice i seguidament amb la seva clau privada. Obtindrà el missatge desxifrat si i només si la clau que ha fet servir l'Alice per xifrar era la seva clau privada, que només coneix ella, la qual cosa significa que ha estat ella qui ha enviat el missatge.

- No repudiació: L'Alice vol enviar un missatge a en Bob i vol que quedi constància que en Bob ha rebut aquell missatge.

La primera d'aquestes finalitats, és a dir, la confidencialitat, és vàlida tant per xifrats simètrics com per asimètrics, mentre que les tres últimes, és a dir, la integritat, l'autentificació i la no repudiació només és vàlida per xifrats asimètrics, ja que es duen a terme amb la firma digital, on l'emissor, per firmar el missatge, ha d'utilitzar la seva clau privada.

Tal com s'ha comentat, els xifrats asimètrics, com el mètode RSA, ElGamal, o les corbes el·líptiques, s'utilitzen per intercanviar claus i en les firmes, però habitualment no s'utilitzen per enviar grans blocs d'informació, la qual cosa s'acostuma a fer amb xifrats simètrics.

La criptografia s'utilitza en operacions bancàries, identificació de persones, en l'intercanvi de documents entre governs i departaments de governs, documents comercials confidencials o secrets entre empreses, etc.

Tot i que es recomana utilitzar la criptografia de corbes el·líptiques com a xifrat asimètric, normalment s'utilitza el RSA.

El mètode RSA és molt utilitzat en la firma electrònica de documents en l'àmbit de l'administració pública (Hisenda, Seguretat Social, policia, jutjats, etc.) o privats (actes notarials, contractes, etc.) i en el xip del DNI. També és utilitzat per intercanviar, de forma segura, claus per un xifrat simètric a internet, per exemple quan hem d'entrar una contrasenya (quan es volen fer operacions bancàries per internet, es vol mirar el correu electrònic, etc.). Quan ja s'han distribuït les claus, aleshores s'encripten els missatges amb AES.

La criptografia de corbes el·líptiques és utilitzada, per exemple, en els passaports alemanys.

Com s'ha comentat anteriorment, actualment no es pot fer gaire ús de la criptografia quàntica degut a la distància. De moment, aquest mètode no és gaire útil per la comunicació, tot i que de moment es pot utilitzar en distàncies curtes, per exemple edificis governamentals, seus d'empreses, àmbits geogràfics petits, etc.

4 Conclusions

Actualment la criptografia és molt important, ja que es fa servir contínuament, tant per enviar informació confidencial com per demostrar que ha estat una persona concreta qui ha enviat el missatge, assegurar-se que no es modifica el contingut del missatge, etc. Cada minut milions d'operacions s'han de mantenir en secret, per exemple cada vegada que mirem el correu electrònic, quan comprem per internet, quan utilitzem targetes de crèdit o de dèbit, en la telefonia mòbil, etc. En tot moment estem enviant i rebent informació xifrada, encara que no en som conscients.

Normalment no s'utilitza un sol mètode, sinó que es combinen mètodes simètrics i asimètrics per tal de millorar-ne l'eficàcia, és a dir, poder distribuir les claus secretament, però poder enviar fàcilment grans informacions sense necessitat de càlculs extremadament llargs i complicats.

Degut a la gran capacitat de computació dels ordinadors i els coneixements matemàtics, els diferents mètodes criptogràfics, que abans podien durar segles, actualment amb poques dècades poden quedar desfasats, obsolets i inútils, per tant han d'anar evolucionant. De moment els mètodes actuals semblen segurs, però també l'Enigma semblava indesxifrable a la seva època. És probable que d'aquí a poc temps, en qüestió de poques dècades, ja no siguin bons mètodes, degut a l'evolució de la tecnologia de la informàtica, i es necessitin claus molt més llargues per aconseguir xifrats segurs o la invenció de nous mètodes més eficaços. Els mètodes RSA, elGamal i la criptografia de corbes el·líptiques es basen en problemes difícils de resoldre, però no està demostrat que siguin impossibles, ni que no existeixi una manera senzilla de resoldre'ls. Per tant, en un futur és possible que es trobin solucions als problemes en els quals es basen aquests mètodes i deixin de ser segurs. La criptografia quàntica, en canvi, es basa en lleis de la física, per tant encara que es facin nous descobriments en el camp de la física quàntica és impossible que una persona aliena pugui interceptar una clau sense ser detectada. Per contra, la criptografia quàntica només és útil per la confidencialitat, però no pels altres usos de la criptografia, és a dir, per la integritat, l'autentificació i la no repudiació, ja que es tracta d'un xifrat simètric.

Cada vegada és més difícil trobar nous mètodes criptogràfics que siguin segurs, relativament ràpids de computar i que funcionin. Si en un futur pròxim es construeixen ordinadors quàntics, probablement molts dels mètodes com el RSA, elGamal i les corbes el·líptiques, que actualment són molt útils i segurs, deixaran de funcionar, ja que amb un temps molt breu es podran provar milions de combinacions i serà molt fàcil atacar-los. Si els matemàtics aconsegueixen trobar la manera per facilitar algunes operacions, com per exemple, la descomposició de nombres o la resolució de logaritmes discrets, alguns mètodes de criptografia esdevindran molt poc segurs.

Crec que s'hauria d'utilitzar més la criptografia de corbes el·líptiques, tal com recomanen els experts, ja que no es coneixen mètodes per atacar-lo, a part de la força bruta, i per tant les claus necessàries són molt més curtes i no es necessita tant temps de computació. El problema és que fer el canvi d'un sistema a un altre té una certa complexitat.

També opino que, si en un futur s'aconsegueixen construir ordinadors quàntics, la criptografia quàntica serà la més utilitzada per enviar missatges confidencials, ja que sense la clau és

completament impossible, encara que es posseeixin ordinadors molt potents, deduir el que diu el missatge, ja que no es poden trobar patrons en la clau perquè és d'un sol ús. El problema és que s'ha de trobar un mètode per poder enviar fotons, de tal manera que es puguin enviar fotons a grans distàncies, que la seva polarització no canviï al llarg del recorregut, i que els diferents fotons procedents de diferents claus no interfereixin entre ells. A més, la criptografia quàntica només servirà per enviar missatges, però no per firmar-los, és a dir, poder demostrar que ha estat una persona concreta qui ha enviat un missatge, per exemple. És a dir, caldrà trobar alguna manera per poder fer tot això que, tot i l'existència d'ordinadors quàntics, es puguin enviar missatges firmats amb tota seguretat. Per tant, crec que encara queda molt per estudiar i descobrir en aquest camp.

La seguretat d'un sistema criptogràfic no es limita només al moment de enviar i rebre el missatge. Hi ha informacions que és necessari que estiguin protegides durant llargs períodes de temps, fins i tot dècades. Els mètodes criptogràfics emprats i les longituds de les claus, han de protegir aquestes informacions durant tot aquest temps, malgrat que les millors tecnologies dels ordinador i dels mètodes de xifrat facin progressos importants, i de moment imprevisibles, durant els propers anys.

Tot i que hi ha força informació que l'he tret de conferències, cursos i altres activitats, també hi ha hagut una part, sobretot amb la criptografia de corbes el·líptiques, que no en tenia cap coneixement i tampoc sabia gaire a on trobar informació, i que ho he hagut de buscar tot per internet, intentant entendre i estudiant el que trobava. A més m'ha estat molt difícil trobar informació suficientment detallada però senzilla alhora, que es pogués entendre bé sense tenir-ne massa coneixements. En aquests casos m'han estat molt útils els aclariments per part d'experts.

Aquest treball m'ha estat molt útil per comprendre molt millor en què es basa la criptografia, quins usos se'n fa, quins són els mètodes criptogràfics més importants de l'actualitat i quin pot ser el futur de la criptografia, entre d'altres coses. També m'ha servit per veure aplicacions en la vida quotidiana de teoremes i conceptes matemàtics, a part d'aprendre a utilitzar-los.

5 Fonts d'informació

5.1 Bibliografia

DE GUZMÁN, Miguel. ***Aventuras matemáticas. Una ventana hacia el caos y otros episodios***. Madrid: Pirámide 2006.

DU SAUTOY, Marcus. ***La música de los números primos***. Barcelona: Acantilado, 2007.

GÓMEZ, Joan. ***Matemáticos, espías y piratas informáticos. Codificación y criptografía***. Espanya: RBA, 2010.

GRACIÁN, Enrique. ***Los números primos. Un largo camino al infinito***. Espanya: RBA, 2010.

HAWKING, S.; MLODINOW, L. ***Brevíssima història del temps***. Barcelona: Columna, 2005.

M. LEDERMAN, Leon; T. HILL, Christopher. ***La simetría y la belleza del universo***. Barcelona: Metatemas, 2006.

PLA BRUNET, Joaquim. ***10 impactos de la ciencia del siglo XX***. Madrid: FCE España, 2003.

SCARANI, Valerio. ***Six Quantum Pieces. A First Course in Quantum Physics***. Singapore: World Scientific, 2010.

SINGH, Simon. ***El enigma de Fermat***. Barcelona: Booket, 2006.

VIOLANT, A. ***El enigma de Fermat. Tres siglos de desafío a la matemàtica***. Espanya: RBA, 2010.

RECIO, Tomás. "**La Columna de Matemática Computacional**". *La Gaceta de la Real Sociedad Matemática Española*, vol.13, núm. 2 (any 2010), pàgs. 317-336.

5.2 Recursos electrònics

Perimeter Institute for Theorical Physics. Conferència "Quantum Cryptography: A Tale of Secrets Hidden and Revealed Through the Laws of Physics", a càrrec de Daniel Gottesman; https://www.perimeterinstitute.ca/index.php?option=com_content&task=view&id=551&Itemid=568&lecture_id=4449 [Consulta: 22 d'agost de 2011]

Institute for Quantum Computing. "Faculty & Research. Quantum Cryptography"; http://iqc.uwaterloo.ca/faculty-research/quantum-cryptography [Consulta: 22 d'agost de 2011]

Universitat de Barcelona. "Òptica Electromagnètica"; http://ocw.ub.edu/fisica/optica/apunts/Capitol-02-Optica-electromagnetica.pdf [Consulta: 14 d'agost de 2011]

Wikipedia. "Polarització Electromagnètica"; http://ca.wikipedia.org/wiki/Polaritzaci%C3%B3_electromagn%C3%A8tica [Consulta: 14 d'agost de 2011]

Wikipedia. "Polarization (waves)"; http://en.wikipedia.org/wiki/Polarization_(waves) [Consulta: 14 d'agost de 2011]

Wikipedia. “Photon Polarization”; http://en.wikipedia.org/wiki/Photon_polarization [Consulta: 14 d’agost de 2011]

Wikipedia. “BB84”; http://en.wikipedia.org/wiki/BB84 [Consulta: 18 d’agost de 2011]

Wikipedia. “Història de la mecànica quàntica”; http://ca.wikipedia.org/wiki/Hist%C3%B2ria_de_la_mec%C3%A0nica_qu%C3%A0ntica [Consulta: 08 de setembre de 2011]

Biblioteca virtual de la UPC. “La Cambra Negra. Freqüència de lletres”; http://bibliotecnica.upc.es/cambranegra/frequencyanalysis.html [Consulta: 18 d’agost de 2011]

Simon Singh. “The Black Chamber. Letter frequencies”; http://www.simonsingh.net/The_Black_Chamber/frequencyanalysis.html [Consulta: 18 d’agost de 2011]

Wikipedia. “Cifrado ElGamal”; http://es.wikipedia.org/wiki/Cifrado_ElGamal [Consulta: 7 de setembre de 2011]

Ius Mentis. “The ElGamal public key sistem”; http://www.iusmentis.com/technology/encryption/elgamal/ [Consulta: 7 de setembre de 2011]

Certicom. “ECC Tutorial”; http://www.certicom.com/index.php/ecc-tutorial [Consulta: 2 de desembre de 2011]

Ius Mentis. “Elliptic Curve Cryptography”; http://www.iusmentis.com/technology/encryption/elliptic-curves/ [Consulta: 7 de setembre de 2011]

Search Security. “elliptical curve cryptography (ECC)”; http://searchsecurity.techtarget.com/definition/elliptical-curve-cryptography [Consulta: 3 de setembre de 2011]

Wikipedia. “Elliptic curve cryptography”; http://en.wikipedia.org/wiki/Elliptic_curve_cryptography [Consulta: 2 de desembre de 2011]

Wikipedia. “Elliptic curve Diffie-Hellman”; http://en.wikipedia.org/wiki/Elliptic_curve_Diffie%E2%80%93Hellman [Consulta: 2 de desembre de 2011]

Universidad Autónoma de Madrid. “Estalmat. El sistema RSA”; http://www.uam.es/proyectosinv/estalmat/Estalmat/susipablo02.pdf [Consulta: 22 d’agost de 2011]

Wikipedia. “RSA”; http://en.wikipedia.org/wiki/RSA [Consulta: 14 d’agost de 2011]

Wikipedia. “RSA”; http://es.wikipedia.org/wiki/Claves_RSA [Consulta: 14 d’agost de 2011]

Wikipedia. “Advanced Encryption Standard”; http://es.wikipedia.org/wiki/Advanced_Encryption_Standard [Consulta: 2 de desembre de 2011]

Wikipedia. “DES”; http://ca.wikipedia.org/wiki/DES [Consulta: 24 de desembre de 2011]

JAREÑO, J. “Criptografia”; http://www.xtec.cat/~jjareno/activitats/criptologia/intro.htm [Consulta: 10 de juliol de 2011]

El paraíso de las matemáticas. “Criptotaller”; http://www.matematicas.net/paraiso/cripto.php?id=cripto [Consulta: 14 d’agost de 2011]

Simon Singh. “Cryptography”; http://www.simonsingh.net/cryptography/ [Consulta: 18 d’agost de 2011]

WolframAlpha. “Computational knowledge engine”; http://www.wolframalpha.com/ [Consulta: 22 d’agost de 2011]

5.3 Altres

Llibre de Sessions de preparació per a l’Olimpíada Matemàtica. Es pot descarregar gratuïtament a: Societat Catalana de Matemàtiques. Publicacions Electròniques; http://scm.iec.cat/redir.asp?direc=Publicacions/pubs.asp&imag=societat [Consulta: 22 d’agost de 2011]

Recull d’articles científics realitzats per participants del Programa Joves i Ciència de Caixa Catalunya. Articles 2009. Caixa Catalunya Obra Social.

International Summer School for Young Physicists (ISSYP), al Perimeter Institute for Theorical Physics. Conferència a càrrec de Ashwin Nayak, el dia 3 d’agost de 2011.

Visita al Institute for Quantum Computing (IQC), durant l’estada a l’International Summer School for Young Physicists, el dia 27 de juliol de 2011.

Apunts i coneixements adquirits a l’International Summer School for Young Physicists, dut a terme del 21 de juliol al 6 d’agost.

Apunts i coneixements adquirits al curs d’introducció a la criptografia quàntica, a l’Institut de Ciències Fotòniques (ICFO), a càrrec de Piotr Migdal, dut a terme 21 de juny al 18 de juliol.

Apunts de les classes de preparació per les olimpíades matemàtiques, a la Universitat de Girona, durant els cursos 2009-2010 i 2010-2011.

Versió del llibre: SINGH, Simon. *The Code Book*, en CD-ROM. Es pot descarregar gratuïtament a: Simon Singh. “Crypto CD-ROM”; http://www.simonsingh.net/cryptography/crypto-cd-rom/ [Consulta 23 d’agost de 2011]

HANKERSON, Darrel; MENEZES, Alfred; VANSTONE, Scott. “Guide to Elliptic Curve Cryptography”. Es pot descarregar gratuïtament a: http://kolhoz.tiera.ru/Cs_Computer%20science/CsCr_Cryptography/Hankerson,%20Menezes,%20Vanstone.%20Guide%20to%20elliptic%20curve%20cryptography%20(Springer,%202004)(ISBN%20038795273X)(332s)_CsCr_.pdf [Consulta: 7 de setembre de 2011]

6 Agraïments

Vull mostrar el meu agraïment a totes les persones que han contribuït d'alguna manera o altra a la realització d'aquest treball. Per la rellevància de les seves aportacions, a continuació esmento algunes d'aquestes persones:

a la professora Francesca Masnou per haver acceptat ser la meva tutora en aquest treball, ajudar-me en tot el que he necessitat i, sobretot, per la confiança que ha dipositat en mi;

a tothom que fa possible les classes de preparació per a les olimpíades matemàtiques, especialment els Srs. Josep Grané i José Luis Díaz-Barrero, professors de la UPC, en les quals, entre d'altres coses he adquirit coneixements sobre aspectes fonamentals per entendre el funcionament d'alguns dels sistemes actuals;

al Sr. Jordi Quer, professor de la UPC, per haver-me assessorat en el treball i pel temps que ha dedicat a explicar-me conceptes matemàtics relacionats amb les corbes el·líptiques i la seva aplicació a la criptografia;

al Sr. Piotr Migdal, investigador a l'ICFO, per haver-me ensenyat el funcionament de la criptografia quàntica l'estiu passat;

al PI, Perimeter Institute for Theorical Physics, i al seu personal, per haver-me acceptat al programa ISSYP, International Summer School for Young Physicists, on, entre d'altres coses, he aprofundit en el coneixement de la física quàntica i de la criptografia quàntica, i que m'ha permès visitar l'IQC, Institute for Quantum Computing, on també he aprofundit en el coneixement d'aquests temes;

al programa Joves i Ciència, de CatalunyaCaixa, especialment a les Sres. Maria Calsamiglia i Eva Calvés, per haver-me ofert la plaça a l'ICFO i facilitar-me l'accés al ISSYP;

i, finalment, a la família, especialment els pares, pel suport i l'interès que han mostrat.

7 Annexos

7.1 Annex A: Esteganografia

Com s'ha comentat abans, l'esteganografia consisteix en amagar els missatges, de tal manera que sigui difícil interceptar-los. Però, si s'intercepta un missatge, el pot llegir qualsevol, ja que no està encriptat.

Hi ha molts mètodes d'esteganografia. Per exemple, a l'antiguitat, gravaven missatges en tauletes de fusta i seguidament les recobrien amb cera, per tal que no es veiés el missatge. Quan arribava a la destinació correcta, com que el receptor sabia on estava amagat, treia la cera i llegia el missatge.

Un altre mètode de l'antiguitat, però que no servia per missatges urgents, ja que necessitava més temps, consistia en rapar els cabells d'algú. Seguidament li escrivien el missatge al cap i esperaven que li creixessin suficientment els cabells com perquè no es veiés el missatge. Quan ja els portava prou llargs se n'anava amb el receptor, el qual el rapava un altre cop per poder llegir el missatge.

També, hi havia mètodes que consistien en utilitzar tintes invisibles, que quan s'assecaven no es veien, i per llegir el missatge s'havia d'escalfar, o posar-lo en remull en alguna substància concreta, etc.

Amb l'existència de diaris i periòdics, s'agafava un punxó, o algun altre eina per fer petits forats i es feien forats a sota de cadascuna de les lletres que formaven el missatge amagat. El receptor llegia únicament les lletres marcades per llegir el missatge.

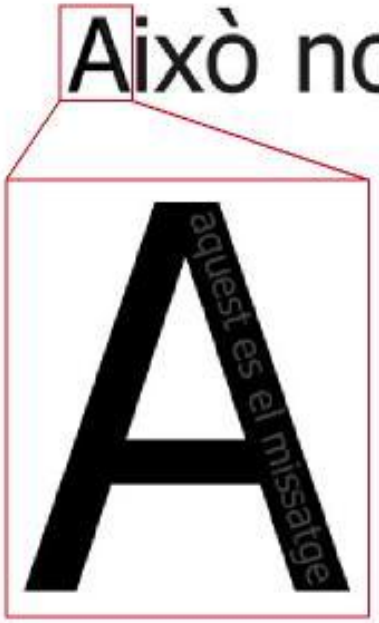
Altres mètodes són els acròstics, és a dir, textos en vers on les lletres d'una posició concreta formen una paraula o un missatge.

Una altra manera d'amagar missatges consisteix en escriure'ls molt petits en un fragment de text, per exemple en el punt d'una "i", o en una "l", etc. o en un petit fragment d'una fotografia. El receptor sabia exactament on era el missatge i per tant el podia trobar fàcilment i llegir-lo. Qualsevol persona aliena hagués pensat que el text o la fotografia que l'emissor enviava era completament innocent.

Actualment, amb la digitalització d'imatges, es poden manipular, de manera que a cada píxel es modifica o no si el missatge, en sistema binari, conté un 1 o un 0, respectivament.

Seguidament es mostren alguns exemples d'esteganografia. Primerament, un text on hi ha un missatge amagat. Després un tros de diari, on hi ha marcades, amb un forat a sota, unes lletres, i si es llegeixen aquestes lletres hi ha el missatge "aquest es el missatge". Finalment una foto on s'hi amaguen alguns missatges.

Això no és el missatge



LLIBRES

La RAE edita els «números u» de la literatura clàssica

La col·lecció, de 111 títols, inclou des de 'Mio Cid' fins a 'Los pazos de Ulloa'

Cada any es publicaran vuit llibres, que tindran presència a internet

OLGA PEREDA
MADRID

Hi ha veus que anuncien la mort del paper, però els llibres són una institució «prou poderosa» per sobreviure. Amb aquesta declaració d'intencions, la Real Academia Española (RAE) acaba d'editar la Biblioteca Clásica, una col·lecció de «números u» de la literatura espanyola i hispanoamericana fins a finals del segle XIX. Els seus responsables ofereixen al lector la possibilitat de redescobrir títols imprescindibles, com *La Celestina*, *Novelas ejemplares*, *Miau* i *Los pazos de Ulloa*. Hi haurà fins

«¿Té sentit avui dia una biblioteca clàssica en paper, un projecte que durarà 14 o 15 anys?», va preguntar ahir, durant la presentació de la col·lecció, el secretari de la RAE, Darío Villaneuva. «Sí, sí que en

Hi ha veus que anuncien la mort del paper, però els llibres són una institució «prou poderosa» per sobreviure. Amb aquesta declaració d'intencions, la Real Academia Española (RAE) acaba d'editar la Biblioteca Clásica, una col·lecció de «números u» de la literatura espanyola i hispanoamericana fins a finals del segle XIX. Els seus responsables ofereixen al lector la possibilitat de


NEWTON
aquest es el
missatge
NEWTON
NEWTON
NEWTON

7.2 Annex B: Història de la criptografia

7.2.1 Railfence

Es tracta d'un mètode basat en la transposició. Consisteix en agafar el text i separar-lo en diferents línies, segons la clau, és a dir, si la clau és 3, separar-lo en 3 línies. Les lletres que ocupen una posició de la forma 3k+1, on k és un nombre enter no negatiu, van a la primera línia, les que ocupen una posició de la forma 3k+2 van a la segona línia i les que ocupen una posició de la forma 3k, on k és un nombre enter positiu, van a la tercera. Finalment s'escriuen primer totes les lletres de la primera fila, llavors totes les de la segona i finalment totes les de la tercera. Per exemple:

Missatge: "aquest es el missatge"
Clau: 3

a				e				e				l				s				t	
	q				s				s				m				s				g
			u				t				e				i				a				e

Per tant, el missatge encriptat serà: aeelstqssmsguteiae"

Per desxifrar el missatge només s'ha de separar el text encriptat en la quantitat de blocs que sigui necessari, segons la clau, i es llegeixen primer la primera lletra de cadascun dels blocs, després la segona lletra, etc. En aquest cas hi ha 18 lletres al missatge i la clau és 3, per tant hi ha 3 blocs de 6 lletres cadascun.

Per tant, el missatge descodificat serà "aquesteselmissatge", i, fent les separacions adequades, s'obté "aquest es el missatge".

7.2.2 "Scytale" romana

És un mètode del segle V a.C. que es basa en la transposició. Consistia en un cilindre o un prisma de fusta, on se li enrotllava un papir o una cinta de cuir[14]. Seguidament s'escrivia el missatge horitzontalment i finalment es desenrotllava el papir o la cinta. El missatge xifrat quedava escrit verticalment a la cinta de cuir o al papir. Per desxifrar-lo, l'únic que calia fer era enrotllar-lo en un cilindre del mateix diàmetre que l'utilitzat al xifrar el missatge.

Fig. 7.2.2.1. Dibuix d'una "scytale". Aquí es pot veure com el paper queda enrotllat al voltant del cilindre i com s'ha escrit el missatge ("kill king tomorrow midnight"). Al desenrotllar el paper, el missatge seria "ktmioilmdlonkriirgnohgwt". Imatge extreta de http://www.ecriture-art.com/images/scytale1.gif

[14] Si actualment s'utilitza aquest mètode es fa amb paper, en lloc de papir o cinta de cuir, però en aquella època encara no s'havia inventat.

Per exemple:

Missatge: “aquest es el missatge”
Per encriptar-lo, escrivim el missatge, sense espais, en la graella, és a dir:

a	q	u
e	s	t
e	s	e
l	m	i
s	s	a
t	g	e

En aquest cas, el cilindre tindria gruix 6 (l’altura de la graella). El paper enrotllat, un cop el desenrotlléssim, quedaria com el de la dreta.
Missatge codificat: “aeelstqssmsguteiae”
El receptor del missatge, si sap el diàmetre del cilindre, en aquest cas 6, podrà desencriptar el missatge, enrotllant-lo en un cilindre del mateix gruix.
Missatge descodificat: “aquesteselmissatge”, per tant, fent les separacions adequades s’obté “aquest es el missatge”

a
e
e
l
s
t
q
s
s
m
s
g
u
t
e
i
a
e

Aquest mètode es pot descodificar fàcilment sense saber la clau, provant amb cilindres de mides diferents.

Es pot veure fàcilment que el Railfence i la “Scytale” romana són molt semblants. El procediment és una mica diferent, però s’arriba al mateix resultat.

7.2.3 **Quadrat llatí**

El quadrat llatí, també basat en la transposició, no és un mètode criptogràfic, sinó un missatge concret que representava el cristianisme, i que consisteix en el quadrat següent:

R	O	T	A	S
O	P	E	R	A
T	E	N	E	T
A	R	E	P	O
S	A	T	O	R

El text “rotas opera tenet arepo sator” significa “el que guia l’arada que sembra la llavor”. Canviant la posició de les lletres del text, és a dir, transposant-les, s’obté el següent:

P
A
A T O
T
E
R
P A T E R N O S T E R
O
S
O T A
E
R

"Paternoster" significa "Pare nostre" i està en forma de creu, que és un símbol del cristianisme. Les As i les Os signifiquen Alfa i Omega, és a dir, el principi i el final, que també té un significat en el cristianisme.

7.2.4 **Xifrat de Cèsar**

Un mètodes per substitució molt senzill és el que es feia a l'època de Juli Cèsar, que consistia en desplaçar l'alfabet, per exemple:

Text	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
Codi	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

Vist d'una forma més matemàtica podem substituir ordenadament cadascuna de les lletres per un nombre, és a dir a → 00, b → 01, c → 02, d → 03, … , z → 25. Seguidament hi sumem la clau, que seran els llocs que s'ha desplaçat l'alfabet, és a dir codi=text+clau. En l'exemple anterior és 3. Per tant, en aquest cas, *a+clau=00+3=03=d*, *b+clau=04=e*, *c+clau=05=f*, etc. En les últimes xifres, quan hi sumem la clau ens quedarà un nombre que no correspondrà a cap lletra, per exemple, quan la clau és 3, *z+clau=25+3=28*. Aleshores el que fem és restar 26, és a dir, el nombre de lletres que tenim a l'alfabet, per obtenir una lletra al codi. Per tant, en aquest cas, a la z li correspondrà la c.

En total hi ha 25 possibles claus, ja que podem començar l'alfabet del codi en 26 posicions diferents, és a dir, podem començar en cadascuna de les lletres, però si comencem a la lletra *a* no estem creant cap codi, ja que a cada lletra li correspon ella mateixa.

L'emissor i el receptor han d'acordar la clau, que consisteix en un nombre, generalment entre 1 i 25. Per enviar el missatge, l'emissor assigna, a cada lletra del seu missatge, la lletra que li correspon del codi. Per exemple:

Missatge: "aquest es el missatge"
a → d; q → t; u → x; etc.
Missatge codificat: "dtxhvw hv ho plvvdwjh"
El receptor del missatge, si sap el codi podrà desxifrar fàcilment el missatge invertint el procés.
d → a; t → q; x → u; etc.
Missatge descodificat: "aquest es el missatge"

7.2.4.1 Roda de Cèsar

Un sistema millorat del xifrat de Cèsar és la roda de Cèsar. Aquest mètode fa més còmode l'escriptura i la lectura de missatges escrits en aquest tipus de xifrat. Consisteix en dues rodes, de diferent mida, centrades en el mateix punt, les quals poden girar una respecte l'altra. Al voltant de cadascuna de les rodes hi ha les lletres de l'alfabet. La roda gran conté les lletres del text sense xifrar, mentre que la roda petita conté les lletres del text xifrat. Segons la clau que utilitzin l'emissor i el receptor, es fan girar les

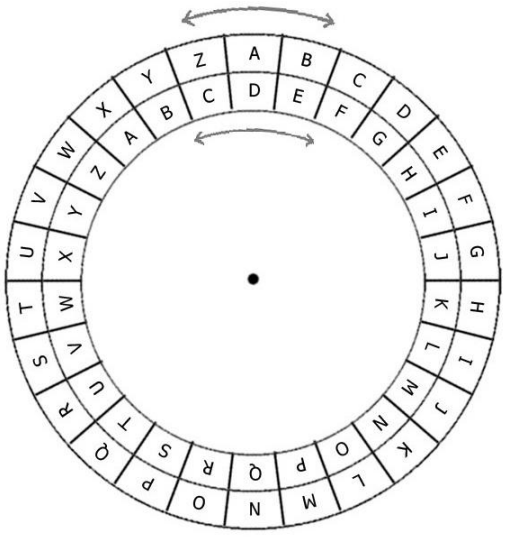


Fig. 7.2.4.1.1. Esquema de la roda de Cèsar

rodes per tal que coincideixin les lletres del text sense xifrar i el text xifrat, és a dir, si la clau és 3, la lletra *a* de la roda gran ha de coincidir amb la *d* de la roda petita, i llavors la *b* de la roda gran coincidirà amb la *e* de la roda petita, etc.

7.2.5 **Xifrat de Kama-sutra**

Aquest mètode, utilitzat al segle IV a.C. consisteix fer parelles de lletres. Per exemple:

a	b	c	e	f	g	h	i	j	m	n	r	w
d	u	z	l	q	k	t	s	p	v	o	x	y

Al crear el codi, la primera lletra que agafem la podem aparellar amb 25 lletres diferents. La segona que agafem, com que ja n'haurem utilitzat dues, només la podrem aparellar amb 23 lletres diferents. La tercera, pel mateix motiu, només la podrem aparellar amb les 21 lletres restants. Per tant, hi ha $25 \cdot 23 \cdot 21 \cdot \ldots \cdot 5 \cdot 3 \cdot 1 = 7.905.853.580.625$ possibles claus.

Primerament l'emissor i el receptor han d'acordar la clau, que consisteix en les 13 parelles de lletres. Seguidament, l'emissor, igual que en l'apartat anterior, substitueix cada lletra del missatge per la que li correspon de la clau. Per exemple:

Missatge:
a → d; q → f; u → b; etc.
Missatge codificat: "dfblih li le vsiidhkl"
El receptor del missatge, si sap el codi podrà desxifrar fàcilment el missatge invertint el procés.
d → a; f → q; b → u; etc.
Missatge descodificat: "aquest es el missatge"

7.2.6 **Xifrat de Pigpen**

Aquest mètode consisteix en el següent codi:

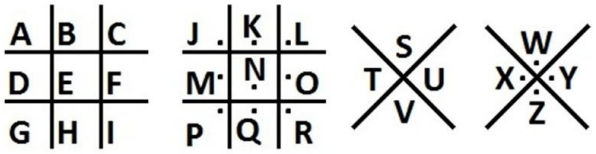


Fig. 7.2.6.1. Clau per xifrar i desxifrar missatges utilitzant el xifrat de Pigpen

Per escriure el missatge xifrat es copia el tros del dibuix, és a dir els segments i punts, on apareix la lletra, per exemple:

Missatge:

a → ; q →  ; u →  ; etc.

Missatge codificat:

El receptor del missatge, si sap el codi podrà desxifrar fàcilment el missatge invertint el procés.

 → a; → q;  → u; etc.

Missatge descodificat: “aquest es el missatge”

Hi ha altres codis que també es basen en substituir cada lletra per un símbol o un dibuix, per exemple homenets en diferents posicions, fruites, animals, símbols diversos, etc. S’utilitzen variacions del xifrat de Pigpen en jocs d’entreteniment o passatemps.

7.2.7 **Xifrat d’Atbash**

El mètode d’Atbash consisteix a copiar l’alfabet al revés, a la clau, és a dir:

Text	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
Codi	z	y	x	w	v	u	t	s	r	q	p	o	n	m	l	k	j	i	h	g	f	e	d	c	b	a

Aquest xifrat només té una clau possible, per tant, l’emissor i el receptor, a l’hora d’enviar el missatge utilitzant aquest xifrat, només necessiten acordar que utilitzaran el mètode d’Atbash, sense necessitat d’haver d’acordar cap clau concreta. Per enviar el missatge, igual que en els mètodes anteriors, es substitueix cada lletra per la seva corresponent del codi, per exemple:

Missatge: “aquest es el missatge”
a → z; q → j; u → f; etc.
Missatge codificat: “zjfvhg vh vo nrhhzgtv”
El receptor del missatge, si sap el tipus de xifrat podrà desxifrar fàcilment el missatge invertint el procés.
z → a; j → q; f → u; etc.
Missatge descodificat: “aquest es el missatge”

7.2.8 **Xifrat afí**

Anteriorment s’ha mostrat que una manera de codificar missatges és sumant una clau a cadascuna de les lletres[15]. El mètode del xifrat afí és semblant al de Cèsar, amb la diferència que, l’afí, abans de sumar una quantitat determinada, multiplica la lletra, és a dir, el nombre que representa la lletra, per una altra quantitat determinada. Per tant, la clau consta de dos nombres. El de la multiplicació ha de ser un nombre tal que no tingui divisors comuns amb el nombre de lletres, és a dir, 26, ja que sinó hi hauria diferents lletres el codi de les quals seria el mateix. El de la suma ha de ser un nombre entre 0 i 25, ja que, tal com es veurà més tard, és el mateix sumar *k* o sumar *k+26a*, on k seria la clau i *a* és qualsevol nombre enter. Finalment, s’aplica aritmètica modular[16], en mòdul 26, per tal que el nombre final sigui entre 0 i 25, ambdós inclosos, ja que així a cada lletra n’hi correspon una de l’alfabet.

Per exemple:
Clau de la multiplicació = 3
Clau de la suma = 5

[15] Veure 7.2.4 Xifrat de Cèsar

[16] Per més informació consultar 2.3.2.2 Fonaments matemàtics del mètode RSA.

Lletra	a	b	c	d	e	f	g	h	i	j	k	l	m
Núm. lletra	00	01	02	03	04	05	06	07	08	09	10	11	12
Multiplicació	00	03	06	09	12	15	18	21	24	27	30	33	36
Suma	05	08	11	14	17	20	23	26	29	32	35	38	41
Mòdul 26	05	08	11	14	17	20	23	00	03	06	09	12	15
Codi	f	i	l	o	r	u	x	a	d	g	j	m	p

Lletra	n	o	p	q	r	s	t	u	v	w	x	y	z
Núm. Lletra	13	14	15	16	17	18	19	20	21	22	23	24	25
Multiplicació	39	42	45	48	51	54	57	60	63	66	69	72	75
Suma	44	47	50	53	56	59	62	65	68	71	74	77	80
Mòdul 26	18	21	24	01	04	07	10	13	16	19	22	25	02
Codi	s	v	y	b	e	h	k	n	q	t	w	z	c

Missatge: “aquest es el missatge”
a → f; q → b; u → n; etc.
Missatge codificat: “fbnrhk rh rm pdhhfkxr”
L’emissor envia el missatge al receptor, el qual, si sap el codi podrà desxifrar fàcilment el missatge invertint el procés.
f → a; b → q; n → u; etc.
Missatge descodificat: “aquest es el missatge”

7.2.9 **Xifrat monoalfabètic general**

Tots els mètodes de substitució anteriors, exceptuant el xifrat de Pigpen, es poden incloure a aquest apartat. En el xifrat monoalfabètic general a cada lletra n’hi correspon una altra qualsevol.

Per exemple:

Text	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
Codi	q	p	a	f	w	o	n	j	r	x	h	c	m	y	v	i	d	t	g	k	u	b	s	z	e	l

En aquest exemple, creat aleatòriament, hi ha lletres (la *m* i la *u*) el codi de les quals és la mateixa lletra. Això és possible sempre i quan no n’hi hagi moltes, ja que llavors la major part del missatge seria fàcil de llegir sense necessitat del codi i, per tant, no seria segur.

L’emissor vol enviar el missatge: “aquest es el missatge”
a → q; q → d; u → u; etc.
Missatge codificat: “qduwgk wg wc mrggqknw”
El receptor del missatge, si sap el codi podrà desxifrar fàcilment el missatge invertint el procés.
q → a; d → q; u → u; etc.
Missatge descodificat: “aquest es el missatge”

En el xifrat monoalfabètic general hi ha molts codis possibles. La lletra *a* pot anar amb totes 26 lletres; la lletra *b* pot anar amb totes exceptuant la que va amb la lletra *a*, és a dir, pot anar amb 25; la lletra *c* pot anar amb totes excepte les que van amb la *a* i la *b*, és a dir 24, etc. Per tant, en

total hi ha 26·25·24·…·3·2·1 possibles codis, és a dir 26! (on el signe "!" indica factorial). Per tant, hi ha 403.291.461.126.605.635.584.000.000 possibles codis ≈ $4 \cdot 10^{26}$ possibles claus.

Per tant, com podem atacar, és a dir, desxifrar sense saber la clau, un missatge en el qual han utilitzat un xifrat monoalfabètic general? Els mètodes més habituals són buscar lletres repetides, com "ss", "rr" en el cas del català, o buscar apòstrofs, en cas que s'escrigui utilitzant els signes de puntuació convencionals, ja que en català hi ha algunes lletres que no les trobarem davant d'un apòstrof. També, un mètode molt habitual per atacar-lo és mirant la freqüència de cadascuna de les lletres, o de grups de lletres, i consultar taules on es mostra el percentatge de vegades que surt cadascuna de les lletres segons l'idioma. Cada idioma té unes freqüències diferents, i en un mateix idioma la freqüència canvia una mica segons el text que s'agafi.

Per exemple, en el cas del català, la freqüència mitjana seria[17]:

Lletra	A	B	C	Ç	D	E	F	G	H	I	J	K	L	M
%	12,55	1,32	3,60	1,06	3,94	13,89	1,00	1,28	0,72	6,99	0,30	0,00	7,74	3,16

Lletra	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
%	6,40	6,58	2,39	1,2	5,99	7,43	5,44	4,84	1,25	0,01	0,45	0,35	0,05

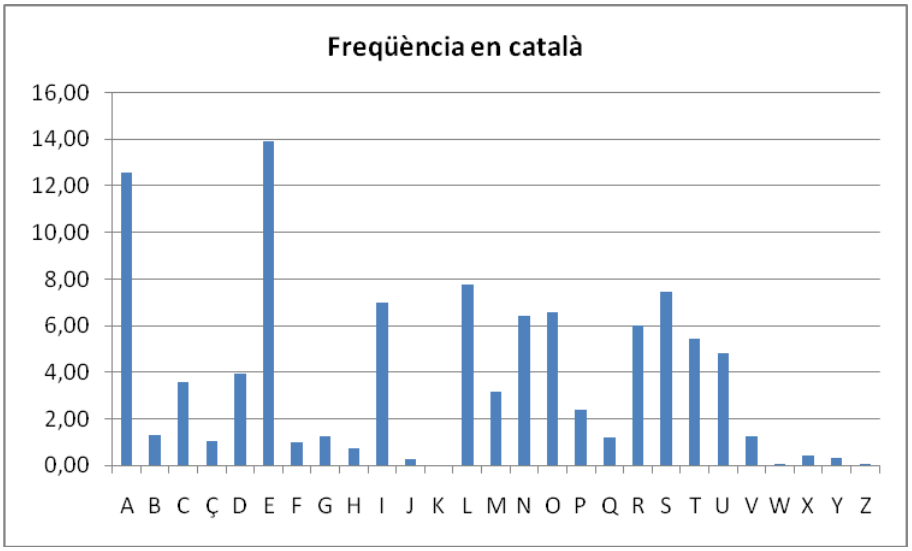


Fig. 7.2.9.1. Gràfic on es mostra la freqüència de cadascuna de les lletres en un text en català.

En un text xifrat en català, probablement les lletres que apareguin més correspondran a la lletra *a* o a la lletra *e*.

En canvi, en anglès la freqüència de les lletres és la següent[18]:

Lletra	A	B	C	D	E	F	G	H	I	J	K	L	M
%	8,2	1,5	2,8	4,3	12,7	2,2	2,0	6,1	7,0	0,2	0,8	4,0	2,4

[17] Informació extreta de http://bibliotecnica.upc.es/cambranegra/frequencyanalysis.htm l [Consulta 18 d'agost de 2011]

[18] Informació extreta de http://www.simonsingh.net/The_Black_Chamber/frequencyanalysis.html [Consulta: 18 d'agost de 2011]

Lletra	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
%	6,7	7,5	1,9	0,1	6,0	6,3	9,1	2,8	1,0	2,4	0,2	2,0	0,1

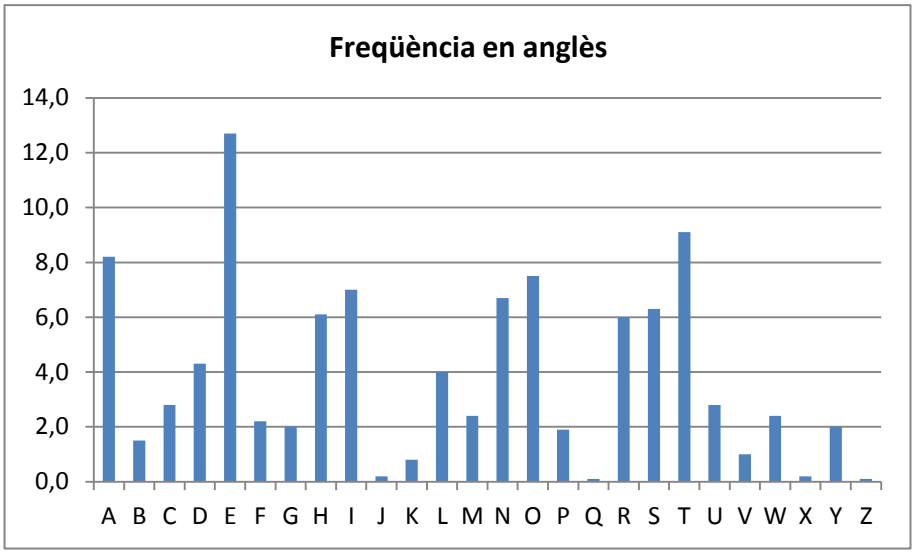


Fig. 7.2.9.2.. Gràfic on es mostra la freqüència de cadascuna de les lletres en un text en anglès.

En un text xifrat en anglès, la lletra que aparegui més probablement correspondrà a la lletra *e*.

Els missatges llargs són més fàcils de desxifrar que els curts, ja que hi pots trobar més informació, és a dir, hi ha més possibilitat de trobar-hi característiques, com buscar apòstrofs o lletres repetides, i la freqüència de les lletres s'assembla més a les de les taules.

7.2.10 Xifrat de Vigenère

Després de trobar la manera d'atacar els xifrats anteriors, evidentment ja no eren segurs. A finals del segle XVI, el francès Blaise de Vigenère va inventar aquest xifrat després d'examinar amb detall les idees dels italians Leon Alberti i Giovanni Porta i l'alemany Johannes Trithemius, que havien treballat per trobar un mètode criptogràfic segur.

El xifrat de Vigenère es basa en substituir utilitzant un codi diferent depenent de la posició de la lletra. És a dir, si hi ha n codis, les lletres de la forma 1+kn, on k és un enter no negatiu qualsevol, utilitzaran el primer codi; les lletres de la forma 2+kn utilitzaran el segon codi, etc. Per recordar els codis s'utilitza una clau, que és una paraula o un conjunt de lletres.

Vigenère va crear la taula següent:

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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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

Llavors es tria una paraula que servirà com a clau, per exemple “hola”. Les lletres de la primera fila, que estan en negreta, són les que corresponen al text sense xifrar. La primera columna, també en negreta, corresponen a les lletres de la paraula clau. En blau hi ha marcats els codis que es faran servir per un missatge en el qual la clau sigui “hola”. La primera lletra del missatge es xifra amb el codi de la fila on la primera casella és “h”, la segona lletra amb el codi de la fila on la primera casella és “o”, i així successivament. Quan s’acaba la paraula es torna a començar.

Com que a la clau hi ha la lletra *a*, quan es xifrin les lletres que han d’utilitzar aquest codi, la lletra del missatge xifrat serà la mateixa que la lletra del missatge sense xifrar.

Text	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
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
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
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
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

Per exemple, l’emissor vol enviar, utilitzant la clau anterior, el següent missatge: “aquest es el missatge”
a (codi “h”) → h; q (codi “o”) → e; u (codi “l”) → f; e (codi “a”) → e; s (codi “h”) → z; etc.
Missatge codificat: “hefezh ps lz xizgltns”
El receptor del missatge, si sap el codi podrà desxifrar fàcilment el missatge invertint el procés.
h (codi “h”) → a; e (codi “o”) → q; f (codi “l”) → u; e (codi “a”) → e; z (codi “h”) → s; etc.
Missatge descodificat: “aquest es el missatge”

Per atacar aquest xifrat no es pot utilitzar l’anàlisi de freqüències, ja que no sabem quina llargada té la clau, i cada lletra de la clau crearà unes freqüències de lletres diferents, ja que són codis diferents.

El 1854, Charles Baggage va aconseguir atacar-lo. Va veure que, en missatges molt llargs, es poden trobar repeticions, ja que hi ha paraules que apareixen més sovint, i per tant és probable que en més d’un lloc coincideixin amb les mateixes claus. Per tant es poden trobar seqüències de lletres

que apareguin més d'un cop al text xifrat i, a partir d'aquí, deduir quantes claus hi ha. Un cop se n'han deduït la quantitat, per anàlisi de freqüències es poden trobar cadascun dels codis.

7.2.11 Xifrat de Playfair

El mètode de Playfair va ser popularitzat per Lyon Playfair, tot i que va ser inventat per Charles Wheatstone. Consistia en una clau, que era una paraula o una seqüència de lletres, que s'escrivia en una graella, sense repetir cap lletra. Seguidament s'escrivien les altres lletres de l'alfabet, també sense repetir-ne. Per exemple:

Clau: "hola"

h	o	l	a	b
c	d	e	f	g
i	j	k/w	m	n
p	q	r	s	t
u	v	x	y	z

La lletra k i la w es posen en una mateixa casella perquè tenim 26 lletres i només 25 cel·les, i són les dues lletres de l'alfabet menys utilitzades, en català.

Seguidament, per xifrar el missatge, es separen les lletres de dues en dues, és a dir:

Missatge: "aquest es el missatge"
Separació: "aq ue st es el mi ss at ge"
En un mateix grup de lletres no pot haver-hi les dues lletres iguals. En cas que passi, s'afegeix una lletra per tal de separar-les, per exemple una k. Si hi ha un nombre senar de lletres, la última lletra quedarà sola, per tant també s'hi afegeix una lletra. També afegirem la k. Per tant, quedarà:
"aq ue st es el mi sk sa tg ek"
Després, per encriptar el missatge es du a terme el següent procés:

- Si les dues lletres d'un mateix grup estan a la mateixa fila, es substitueixen les lletres per les que tenen immediatament a la dreta, respectivament. Si una de les lletres està a l'última columna, s'escriu la de la primera. Per exemple, a l'encriptar "st" s'obtindria "tp".
- Si les dues lletres d'un mateix grup estan a la mateixa columna, es substitueixen les lletres per les que tenen immediatament a sota, respectivament. Si una de les lletres està a l'última fila, s'escriu la de la primera. Per exemple, a l'encriptar "el" s'obtindria "ke" o "we".
- Si no compleix cap dels requisits anteriors, aleshores s'escull la primera lletra, es va seguint la fila fins a localitzar la columna on hi ha la segona lletra i s'escriu la lletra que correspon a la fila de la primera i la columna de la segona. Seguidament es fa al revés, és a dir, s'escull la segona lletra, es va seguint la fila fins a localitzar la columna on hi ha la segona lletra i s'escriu la lletra que correspon a la fila de la segona lletra i la columna de la primera. Per exemple, a l'encriptar "aq" s'obtindria "os".

Per tant, aq → os; ue → xc; st → tp; etc.
Missatge codificat: "osxctpfrkenjrmyfznwr"

Per desencriptar-lo, el receptor ha de saber la clau i crear una taula com l'anterior. També ha de separar les lletres del missatge de dues en dues, és a dir "os xc tp fr ke nj rm yf zn wr". Per desxifrar el missatge, el receptor du a terme el següent procés:

- Si les dues lletres estan en una mateixa fila o en una mateixa columna, s'escullen les lletres que es troben immediatament a l'esquerra o a sobre, respectivament, és a dir, s'inverteix el procés anterior.
- En cas contrari, escull la primera lletra, va seguint la fila fins a localitzar la columna on hi ha la segona lletra i escriu la lletra que correspon a la fila de la primera lletra i la columna de la segona. Seguidament fa al revés, és a dir, va seguint la fila on està la segona lletra fins a trobar la columna on està la primera, i escriu la lletra que correspon a la fila on està la segona lletra i la columna de la primera. És a dir, realitza el mateix procés que realitzava l'emissor quan les dues lletres no es trobaven ni a la mateixa fila ni a la mateixa columna.

Per tant, os → aq; xc → ue; tp → st; etc.
És a dir, el missatge queda així: "aquesteselmisksatgek".
Finalment separem les paraules i traiem les "k" que sobren. Ens quedarà el següent missatge descodificat: "aquest es el missatge"

7.2.12 **Xifrat homofònic**

Per evitar el problema de l'atac comparant les freqüències de cadascuna de les lletres, es va crear un altre mètode, que consistia en tenir més d'un codi per cada lletra, depenent de la freqüència amb què sortien. És a dir, les lletres que surten amb més freqüència tindrien més codis i les que són menys freqüents en tindrien menys. Per exemple:

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
10	48	07	14	00	75	82	67	37	17	12	04	35	28	20	74	11	01	02	08	41	30	51	13	22	16
18		27	33	15				43			23	57	61	39	78		45	03	09	42					
21		72	53	19				59			24	85	66	58			49	05	46	29					
34			84	31				62			25		70	89			56	06	79	63					
38				36				64			26		71	91			60	32	90	93					
44				40				65			55		94	97			73	54							
52				47				76			81							69							
77				50							99														
87				68																					
88				80																					
95				83																					
96				86																					
				92																					
				98																					

Per xifrar un missatge es pot fer servir qualsevol dels codis d'una mateixa lletra, és a dir, per exemple, per xifrar la lletra d podem posar aleatòriament 14, 33, 53 o 84.

Missatge: "aquest es el missatge"
a → 77; q → 11; u → 42; etc.
Missatge codificat: "771142920508 1932 9204 8537690696908231"
El receptor del missatge, si sap el codi podrà desxifrar fàcilment el missatge separant els nombres de dos en dos i invertint el procés.

77 → a; 11 → q; 42 → u; etc.
Missatge descodificat: “aquest es el missatge”

Si s’utilitzen 100 codis i es reparteixen fixant-se en les freqüències de lletres, cada codi apareixerà, aproximadament, un 1% de les vegades. Per tant, l’anàlisi de freqüències serà completament inútil.

7.2.13 Xifrat del llibre

S’escull un fragment d’un text o d’un llibre, que tant l’emissor com el receptor saben, i es numeren les lletres amb l’ordre que surten. Per exemple, utilitzarem el text següent[19]:

> *“El desafío de las ecuaciones elípticas, al igual que en el último teorema de Fermat, es descubrir si tienen soluciones con números enteros y, en tal caso, cuántas.”*

Per tant, per xifrar el missatge “aquest és el missatge” utilitzarem:

A	006, 013, 018, 032, 034, 039, 060, 067, 119, 122, 127, 130
E	001, 004, 011, 015, 023, 025, 042, 044, 046, 055, 058, 062, 064, 069, 072, 084, 086, 096, 104, 108, 111, 116
G	037
I	008, 020, 027, 030, 036, 051, 078, 081, 083, 093
L	002, 012, 026, 035, 040, 047, 049, 090, 120
M	052, 059, 066, 103
Q	041
S	005, 014, 024, 033, 070, 073, 080, 088, 097, 107, 114, 123, 131
T	029, 050, 054, 068, 082, 110, 118, 129
U	017, 038, 042, 048, 075, 091, 102, 126

a → 039; q → 041; u → 126; etc.
Missatge codificat: “039041126069005054 064024 055012 066020070033032118037064”
El receptor del missatge, separa el codi amb grups de 3 nombres i, si sap el text del qual s’han extret les lletres, podrà desxifrar fàcilment el missatge invertint el procés.
039 → a; 041 → q; 126 → u; etc.
Missatge descodificat “aquest es el missatge”

7.2.14 Llibre de codis

Aquest mètode consisteix en assignar un conjunt de lletres i números a cada paraula, com si es tractés d’un nou idioma. Cada usuari té un llibre, com si fos un diccionari traductor, on hi ha l’idioma que coneixen l’emissor i el receptor i l’idioma que utilitzen per comunicar-se. Per exemple, la paraula “missatge” podria ser “G7aMr7g”. Normalment, quan s’utilitzava aquest mètode, no es canviava gairebé mai de clau, ja que no era fàcil ni econòmic fer tots els llibres amb els codis i distribuir-los.

[19] Text extret del llibre: SINGH, Simon. *El enigma de Fermat*. pàg. 172.

Normalment les paraules codificades estaven ordenades alfabèticament igual que les paraules sense codificar. Per tant, si l'enemic o la persona aliena descobria alguna paraula, llavors podien deduir-ne alguna altra a partir d'aquesta.

7.2.15 Codi ADFGVX

Aquest mètode utilitza tant la substitució com la transposició. Primer es crea una taula, on hi ha les lletres i els números, posats aleatòriament, però de manera que tant l'emissor com el receptor sàpiguen com estan posats. A la primera fila i a la primera columna s'escriuen les lletres A, D, F, G, V i X. Per exemple:

	A	D	F	G	V	X
A	u	g	2	v	x	i
D	a	9	m	z	r	q
F	y	t	p	d	8	e
G	o	k	h	f	j	1
V	6	4	s	3	0	7
X	w	c	n	l	b	5

Per xifrar una lletra s'apunten primer la lletra de la fila i seguidament la lletra de la columna. És a dir, per mesurar el missatge "aquest es el missatge" farem el següent:
a → DA; q → DX; u → AA; etc.
Missatge substituït: "DADXAAFXVFFD FXVF FXXG DFAXVFVFDAFDAGFX"

Seguidament es tria una clau, per exemple "hola", i es fa una taula en la qual la primera fila sigui la clau, i a les altres files s'hi escriu el missatge substituït, una lletra a cada columna, tal com es veu a continuació, i llavors s'ordenen les columnes per ordre alfabètic de les lletres de la clau, és a dir:

h	o	l	a
D	A	D	X
A	A	F	X
V	F	F	D
F	X	V	F
F	X	X	G
D	F	A	X
V	F	V	F
D	A	F	D
A	G	F	X

a	h	l	o
X	D	D	A
X	A	F	A
D	V	F	F
F	F	V	X
G	F	X	X
X	D	A	F
F	V	V	F
D	D	F	A
X	A	F	G

Fig. 7.2.15.1 A la taula de l'esquerra es mostra com s'ordenen les lletres del missatge substituït, quan la clau no està ordenada alfabèticament. A la taula de la dreta es mostra com queden ordenades les lletres del missatge substituït un cop s'ordenen les lletres de la clau.

Seguidament s'agafen les lletres de les columnes, de dalt cap a baix, i des de la primera fins a l'última, és a dir:

Missatge codificat: "XXDFGXFDXDAVFFDVDADFFVXAVFFAAFXXFFAG"

Per descodificar-lo, el receptor inverteix el procés, és a dir, primer ho separa en 4 columnes, ja que són la quantitat de lletres de la clau, després ordena les lletres de la clau i finalment agafa les lletres per parelles per trobar la lletra que representen al quadre. Després de realitzar això, el

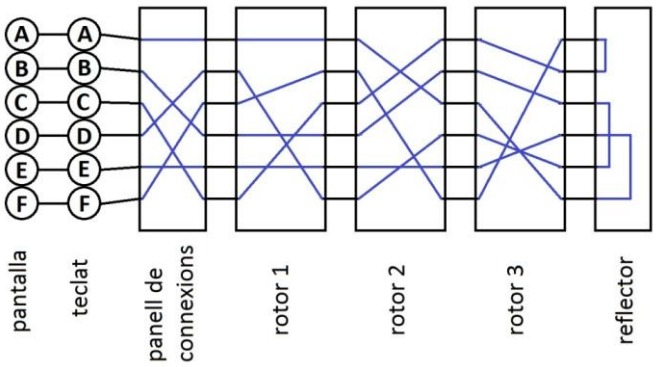
receptor obtindrà el missatge descodificat “aquesteselmissatge”, que fàcilment podrà separar en les paraules que el componen, obtenint “aquest es el missatge”.

Per què s’utilitzen les lletres ADFGVX, en lloc de fer servir, per exemple, ABCDEF? Normalment els missatges s’enviaven utilitzant el codi Morse, que consisteix en sèries de marques curtes i llargues, simbolitzades per “.” i “_”. S’utilitzaven aquestes lletres ja que eren força diferents, per tant minimitzava el risc d’errors durant la transmissió.

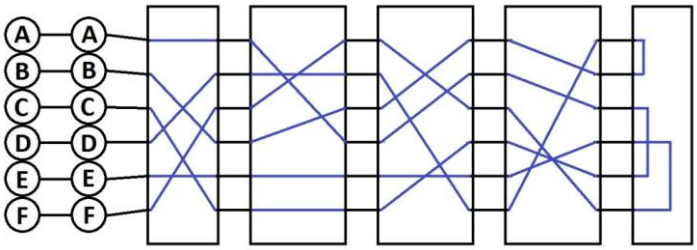
7.2.16 **Enigma**

Durant la Segona Guerra Mundial, els alemanys van inventar una màquina per encriptar missatges, la qual consistia en un gran nombre de codis, de tal manera que semblava impossible d’atacar. La màquina Enigma ser inventada per Arthur Scherbius, l’any 1918.

Consistia en un teclat amb tot l’abecedari i una pantalla on hi havia totes les lletres de l’abecedari, de les quals se n’il·luminava una quan es pitjava una lletra diferent del teclat. Quan es teclejava una lletra dues vegades seguides no s’il·luminava la mateixa lletra, ja que les claus canviaven a cada tecla. A l’interior de la màquina hi havia uns rotors, que connectaven una posició amb una altra, per tal de crear les diferents claus. Després de teclejar una lletra, el primer rotor canviava de posició. Quan passava per un punt concret, el segon rotor canviava de posició. El primer rotor anava donant voltes i, cada cop que passava per aquell punt el segon rotor canviava. Finalment, quan el segon rotor passava per un punt concret, el tercer rotor canviava de posició. La quantitat de rotors variava segons la màquina Enigma que s’utilitzava. També hi havia un panell de connexions, situat entre el teclat i els rotors, el qual intercanviava algunes lletres, per parelles. Finalment, hi havia un reflector, que connectava les sortides de dues en dues, per tal que es codifiqués i es descodifiqués de la mateixa manera si la clau era la mateixa. Seguidament es mostra un exemple, d’una Enigma de només 6 lletres (A, B, C, D, E i F). Les enigmes reals eren de 26, però seria més complicat d’entendre.



Per exemple, si es tecleja la lletra A s’obté la E, i si es tecleja la E s’obté la A; si es tecleja la B s’obté la D, i si es tecleja la D s’obté la B; etc. Quan s’hagi teclejat una lletra, el rotor 1 baixarà una posició i quedarà de la següent manera:



Si ara es tecleja una A no s'obtindrà una E com abans, sinó que s'obtindrà una C. Amb la resta de lletres tampoc s'obtindrà la que s'obtenia en l'anterior cas. Quan el primer rotor passi per un punt concret, el rotor 2 es mourà una posició. Llavors es continuarà movent el rotor 1, fins a donar una altra volta.

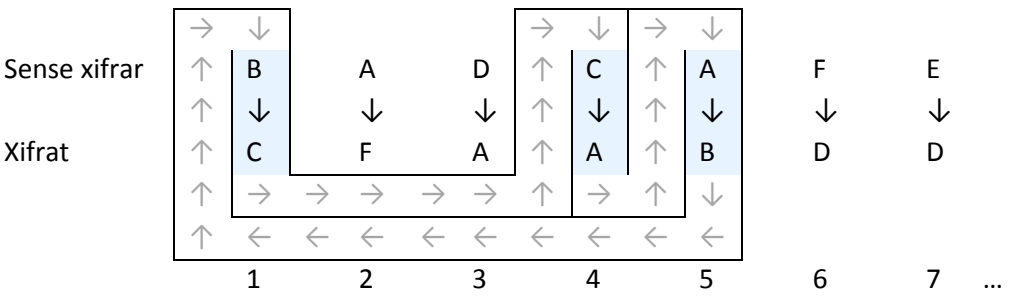
El xifrat depèn del panell de connexions, de la posició (1r, 2n o 3r rotor) i l'orientació inicial de cada rotor, del punt on cada rotor, excepte l'últim, fa moure el següent i del reflector.

Suposem que hi ha 5 possibles rotors, i se n'han de triar 3 per xifrar un missatge utilitzant l'Enigma. Per triar el primer rotor hi haurà 5 possibilitats, pel segon rotor n'hi haurà 4, ja que un rotor ja l'haurem utilitzat pel primer lloc. Pel tercer rotor hi haurà 3 possibilitats. Per tant, per triar els rotors tindrem $5 \cdot 4 \cdot 3 = 60$ possibilitats. En una màquina Enigma de 26 lletres, cada rotor es pot orientar de 26 maneres diferents, inicialment, per tant hi ha $26 \cdot 26 \cdot 26 = 26^3 = 17576$ possibilitats. Finalment, en els dos primers rotors, hi ha 26 possibles llocs en cadascun on faci moure el següent rotor, per tant $26 \cdot 26 = 26^2 = 676$ possibles llocs.

Per tant, tenint en compte només els rotors, ja hi ha $60 \cdot 17576 \cdot 676 = 712882560$ possibles configuracions inicials. Però en realitat n'hi ha més, perquè no hem tingut en compte les possibles connexions del panell, ni el reflector utilitzat. Per tant, per un espia és pràcticament impossible saber amb quina configuració s'ha començat a escriure el missatge.

A la Segona Guerra Mundial, moltes nacions, al veure la dificultat de desxifrar l'Enigma, ho van deixar córrer. Polònia, però, va seguir intentant atacar aquest xifrat. Finalment, els criptoanalistes polacs van aconseguir descodificar un missatge xifrat amb Enigma. Polònia va passar tot el que havien fet al govern Britànic, que va reunir matemàtics, científics, enginyers, jugadors d'escacs, i qualsevol que pogués ajudar a descodificar missatges al Bletchley Park.

Un defecte de l'Enigma és que una lletra no podia estar codificada com a ella mateixa. Allan Turing va fixar-se, que si es tenia un text xifrat i es sabia què deia el text sense xifrar, es podien trobar sèries. Per exemple, si en un lloc del text sense xifrar hi havia una B, que xifrada quedava una C, en un lloc del text sense xifrar hi havia una C que xifrada es transformava en una A i en un lloc del text sense hi havia una A que quan es xifrava es convertia en una B (veure l'exemple següent).



A partir d'aquestes sèries es podien descartar moltes posicions inicials, connectant tantes sèries de rotors amb els quals s'hagués escrit el missatge com lletres intervinguessin en aquest, és a dir, en aquest cas, connectar 3 sèries de rotors. Seguidament, es contaven les separacions que hi havia al missatge entre cadascuna de les lletres que formaven la sèrie, per tal de posar les sèries de rotors en les posicions relatives adequades, és a dir, si dues lletres estaven separades 3 llocs, la sèrie de rotors que representava l'última havia d'estar en la posició que estaria la primera després d'haver teclejat 3 lletres.

Si connectant les sèries de rotors i teclejant la primera lletra de la sèrie s'obtenia la mateixa lletra que s'havia teclejat i, a més a més, la primera sèrie de rotors la transformaven en la segona lletra de la sèrie, la segona sèrie de rotors la transformaven en la tercera lletra, etc., aleshores significava que era possible que en les lletres corresponents s'hagués utilitzat aquella configuració. En cas contrari, es podia descartar aquella configuració.

7.2.17 Altres xifrats de la Segona Guerra Mundial

Durant la Segona Guerra Mundial, a part de l'Enigma es van utilitzar altres mètodes per encriptar missatges.

Per exemple, els alemanys també feien servir la màquina Lorenz SZ40, que era semblant a l'Enigma, però més complicada. Per atacar-lo, van crear una màquina, Colossus, basada en un disseny d'un matemàtic de Bletchley, Max Newman, que va utilitzar idees de Turing. Colossus era ràpida i programable. Va ser el precursor dels ordinadors digitals moderns.

Altres mètodes van ser la màquina de xifrar Type X, utilitzada per l'armada britànica i les forces aèries, la màquina Purple, usada pels japonesos, i la màquina Sigaba, utilitzada pels militars americans.

Un altre mètode utilitzat pels americans era comunicar-se utilitzant nadius americans, que parlaven una llengua que sabien només ells, per tant l'enemic no els entenia. El problema, però, era que els nadius no tenien paraules per definir conceptes militars moderns. Per això van crear un codi, on cada tipus d'avió representava un ocell, els diferents tipus de vaixells i naus representaven animals marins, etc. Per exemple, els avions de combat eren anomenats colibrís, els avions per observar eren anomenats mussols, els vaixells destructors eren anomenats taurons, etc.

7.2.18 Altres mètodes moderns[20]

Després de l'Enigma van començar a aparèixer altres mètodes més moderns, com el DES (Data Encryption Standard) i variants d'aquest, per exemple el Triple DES. Més tard també es va desenvolupar el Rijndael, adoptat pel NIST amb el nom d'AES.

[20] Veure 2.1 DES i 2.2 AES.

7.3 Annex C: Demostracions i explicacions

7.3.1 Existeixen infinits nombres primers

Per demostrar que existeixen infinits nombres primers s'utilitzarà el mètode per reducció a l'absurd, que consisteix en suposar que l'enunciat no és cert i, d'alguna manera, arribar a una contradicció, la qual cosa significarà que la suposició que l'enunciat no era cert és falsa i, per tant, que l'enunciat és cert.

Suposem, doncs, que hi ha un nombre finit de primers, que anomenarem p_1, p_2, p_3, …, p_n. Els multipliquem tots i li sumem 1, és a dir realitzem l'operació següent: $p_1 \cdot p_2 \cdot \ldots \cdot p_n + 1$.

El nombre que obtenim, segons la suposició inicial no és primer, ja que no és cap dels anteriors, els quals eren tots els primers existents.

Però, alhora, aquest nombre no és divisible per cap dels primers anteriors, per tant no és divisible per cap primer, ja que hem suposat que eren tots els primers que existeixen. És a dir, que es tracta d'un altre nombre primer.

Arribem a una contradicció, per tant hem suposat un enunciat fals i això significa que el que volíem demostrar és cert, és a dir, existeixen infinits nombres primers.

7.3.2 Teorema del nombre primer

Sigui $\pi(x)$ el nombre de primers més petits o iguals que x. Es tracta d'una funció esglaonada, ja que si x és un primer, aleshores $\pi(x)=\pi(x-1)+1$, i si x no és primer, aleshores $\pi(x)=\pi(x-1)$, per tant va augmentant d'1 en 1. Per veure la densitat de primers, és interessant aproximar aquesta funció a una altra, que sigui més fàcil de calcular per valors alts. Una funció que està demostrat que és força aproximada és $\pi(x) \sim x/\ln(x)$.

7.3.3 Algoritme d'Euclides

$mcd(a, b) = mcd(b, r)$, on $a, b \in \mathbb{N}$, i r és el residu de la divisió d'aquests dos nombres.

$a=bq+r$, per tant, $r=a-bq$, on q és el quocient de la divisió de a entre b. Aleshores:

Si d és un divisor comú de a i b, és també un divisor de r, i per tant és divisor comú de b i r.
Si d és un divisor comú de b i r, també ho és de a i, per tant, és divisor comú de a i b.

Per tant, els divisors comuns de a i b són els mateixos que els divisors comuns de b i r.

Es tracta d'un mètode molt eficient per calcular el màxim comú divisor de dos nombres, ja que es pot fer en temps polinomial.

7.3.4 Identitat de Bézout

$\exists\, x,y \in \mathbb{Z}$ tals que $xa+yb=mcd(a,b)$, és a dir, donats dos nombres a i b existeixen uns nombres enters x i y tals que $xa+yb=mcd(a, b)$.

Donats dos nombres *a* i *b*, per exemple 4992 i 925, respectivament, apliquem l'algoritme d'Euclides. Primer escrivim $a=bq_1+r_1$, seguidament $b=r_1q_2+r_2$, llavors $r_1=r_2q_3+r_3$, etc. fins que el residu (r_n) sigui 0.

4992 = 925·5 + 367
925 = 367·2 + 191
367 = 191·1 + 176
191 = 176·1 + 15
176 = 15·11 + 11
15=11·1+4
11=4·2+3
*4=3·1+**1***
3=1·3+0

El penúltim residu, que està en negreta és el *mcd (a, b)*, és a dir, en aquest cas, *mcd (4992, 925)=1*. Seguidament volem escriure el *mcd (a, b)* com a suma dels nombres *a* i *b*, cadascun d'ells multiplicat per un altre nombre.

Primer de tot escriurem les operacions anteriors aïllant el residu en cada cas, és a dir:

Cas particular *a=4992, b=925*	Cas general amb 6 operacions	Cas general amb *n* operacions
$367=4992-925\cdot5$	$r_1=a-bq_1$	
$191=925-367\cdot2$	$r_2=b-r_1q_2$	
$176=367-191\cdot1$	$r_3=r_1-r_2q_3$	…
$15=191-176\cdot1$	$r_4=r_2-r_3q_4$	
$11=176-15\cdot11$	$r_5=r_3-r_4q_5$	
$4=15-11\cdot1$	$r_6=r_4-r_5q_6$	
$3=11-4\cdot2$	$r_7=r_5-r_6q_7$	$r_{n-2}=r_{n-4}-r_{n-3}q_{n-2}$
$1=4-3\cdot1$	$r_8=r_6-r_7q_8$	$r_{n-1}=r_{n-3}-r_{n-2}q_{n-1}$
$mcd\ (4992, 925)=1=4-3\cdot1$	$mcd\ (a, b)=r_9=r_7-r_8q_9$	$mcd\ (a, b)=r_n=r_{n-2}-r_{n-1}q_n$

Llavors es comença amb l'últim, que és el que conté el *mcd (a, b)*. Seguidament es substitueix r_8 (en el cas general r_{n-1}), utilitzant la penúltima operació. És a dir:

$1=5-4\cdot1=5-(9-5\cdot1)\cdot1$

Evidentment, en totes les operacions podem treure els 1 que multipliquen. Llavors es du a terme el següent procés: primer s'agrupen els nombres que siguin el residu r_{n-2}, és a dir, en aquest cas el 3; després es substitueix el residu r_{n-2} per l'operació núm. n-2, és a dir, l'antepenúltima. Finalment es realitza el mateix procés per r_{n-3}, r_{n-4}, i així successivament, fins a arribar a r_2 i r_1, quan s'obtindran, únicament, els nombres *a* i *b*, cadascun d'ells multiplicat per un nombre. Seguidament es mostra un exemple amb els nombres anteriors, per fer-ho més clar:

1 = 4-3 = 4-11+4·2 = 4·3-11 = (15-11)·3-11 = 15·3-11·4 = 15·3-(176-15·11)·4 = 15·3+15·44-176·4 = 15·47-176·4 = (191-176)·47-176·4 = 191·47-176·51 = 191·47-(367-191)·51 = 191·98-367·51 = (925-

367·2)·98-367·51 = 925·98-367·(51-2·98) = 925·98-367·247 = 925·98-(4992-925·5)·247 = 925·(98+5·247)-4992·247 = 1333·925-247·4992 = yb+xa = 1 = mcd (a, b)

x=-247; *y=1333*

Aquest mètode, igual que l'algoritme d'Euclides, és molt important perquè té una complexitat molt baixa, computacionalment, és a dir, és molt ràpid.

7.3.5 Petit Teorema de Fermat

Sigui *p* un nombre primer i *a* un nombre natural coprimer amb *p*, de manera que *a≠0*. Aleshores $a^{(p-1)} \equiv 1 \pmod p$.

Escrivim tots els nombres *1a, 2a, 3a, …, (p-1)a.* Cap d'aquests és divisible per *p*, ja que *a* no és divisible per *p* i els nombres entre *1* i *p-1* tampoc ho són, per tant, aquests nombres seran de la forma $ia=k_ip+r_i$, on r_i és el residu que donen al dividir-los per *p*, i $1 \leq r_i \leq p-1$ i $1 \leq i \leq p-1$.

Suposem que hi ha dos d'aquests nombres que donen el mateix residu al dividir-los per *p*, per tant $i \neq j$, tals que $r_i=r_j$. Llavors, $ia-k_ip=r_i=r_j=ja-k_ip$, per tant, $(i-j)a=(k_i-k_j)p$. Tots els *i* i *j* són $1 \leq i \leq p-1$ i $1 \leq j \leq p-1$, per tant *i-j* no és divisible entre *p*. Com que *a* és coprimer amb *p*, tampoc és divisible entre *p*. Per tant la suposició que existeixen dos residus iguals és falsa, la qual cosa significa que són tots diferents, per tant seran els nombres de l'*1* al *p-1*.

Seguidament es multipliquen totes les igualtats $ia=k_ip+r_i$:

$1 \cdot 2 \cdot 3 \cdot \ldots \cdot (p-1) \cdot a^{p-1} = k_1 \cdot k_2 \cdot \ldots \cdot k_{p-1} \cdot p^{p-1} + 1 \cdot 2 \cdot \ldots \cdot (p-1)$

$1 \cdot 2 \cdot \ldots \cdot (p-1) \cdot (a^{p-1}-1) = (k_1 \cdot k_2 \cdot \ldots \cdot k_{p-1} \cdot p^{p-2}) \cdot p$

Com que *p* no divideix a $1 \cdot 2 \cdot \ldots \cdot (p-1)$ és evident que ha de dividir a $a^{p-1}-1$, per tant, $a^{p-1}-1 \equiv 0 \pmod p$, d'on surt que $a^{p-1} \equiv 1 \pmod p$.

Es tracta d'un cas concret del teorema d'Euler, que anuncia que $a^{\varphi(n)} \equiv 1 \ (mod\ n)$, on $mcd\ (a, n) = 1$, i, en aquest cas *n* és primer.

7.3.6 Adaptació del Petit Teorema de Fermat

Siguin *p* i *q* dos nombres primers diferents, i *a* un nombre natural coprimer amb *pq*, de manera que $a \not\equiv 0 \ (mod\ pq)$. Aleshores $a^{(p-1)(q-1)} \equiv 1 \ (mod\ pq)$.

Escrivim tots els nombres *1a, 2a, 3a, …, (pq-1)a.* D'aquests traiem tots els divisibles entre *p* i tots els divisibles entre *q*, és a dir, traiem *pa, 2pa, 3pa, …, (q-1)pa* i *qa, 2qa, 3qa, …, (p-1)qa*. En total haurem tret *p+q-2* nombres, per tant, en quedaran *(p-1)(q-1)* que seran coprimers amb *pq*. Aquests nombres seran de la forma $ia=k_ipq+r_i$, on r_i és el residu que donen al dividir-los per *pq*, i $1 \leq r_i \leq pq-1$ i $1 \leq i \leq pq-1$.

Suposem que hi ha dos d'aquests nombres que donen el mateix residu al dividir-los per *p*, per tant $i \neq j$, tals que $r_i=r_j$. Llavors, $ia-k_ipq=r_i=r_j=ja-k_ipq$, per tant, $(i-j)a=(k_i-k_j)pq$. *i-j* no divideix *pq* (pot dividir a *p* o a *q*, però no a tots dos alhora, ja que $1 \leq i \leq pq-1$ i $1 \leq j \leq pq-1$) i *a* tampoc divideix *pq*, ja que són

coprimers. Per tant la suposició que existeixen dos residus iguals és falsa, la qual cosa significa que són tots diferents, per tant seran els nombres de l'*1* al *pq-1*, però traient els múltiples de *p* o de *q*.

Seguidament es multipliquen totes les igualtats $ia=k_ip+r_i$ de la llista, és a dir, sense múltiples de *p* o de *q*:

$1\cdot2\cdot3\cdot\ldots\cdot(pq-1)\cdot a^{(p-1)(q-1)}=k_1\cdot k_2\cdot\ldots\cdot k_{pq-1}\cdot(pq)^{(p-1)(q-1)}+1\cdot2\cdot\ldots\cdot(pq-1)$

$1\cdot2\cdot\ldots\cdot(pq-1)\cdot(a^{(p-1)(q-1)}-1)=(k_1\cdot k_2\cdot\ldots\cdot k_{pq-1}\cdot(pq)^{(p-1)(q-1)-1})\cdot pq$

Com que *pq* és coprimer amb $1\cdot2\cdot\ldots\cdot(pq-1)$ és evident que ha de dividir a $a^{(p-1)(q-1)}-1$, per tant, $a^{(p-1)(q-1)}-1\equiv 0\ (mod\ pq)$, d'on surt que $a^{(p-1)(q-1)}\equiv 1\ (mod\ pq)$.

Es tracta, igual que el petit teorema de Fermat, d'un cas concret del teorema d'Euler, que anuncia que $a^{\varphi(n)}\equiv 1\ (mod\ n)$, on $mcd\ (a,n)=1$ i, en aquest cas $n=pq$, on p i q són dos nombres primers diferents.

7.3.7 **Definició de cos finit**

Grup abelià o commutatiu: grup que té la propietat commutativa, és a dir, que el resultat d'aplicar l'operació en dos elements del grup no depèn de l'ordre, per tant, donat un grup abelià $(G,\diamondsuit)$, aleshores, $a\diamondsuit b=b\diamondsuit a,\ \forall\ a,b\ \in\ G$.

Anell: conjunt amb dues operacions internes $(A,\perp,*)$ tal que $(A,\perp)$ és un grup abelià i * és associativa, té element neutre i és distributiva respecte $\perp$.

Cos: conjunt amb dues operacions internes $(A,\perp,*)$ tal que $(A,\perp,*)$ és un anell i tot element de A diferent de l'element neutre de $\perp$ té invers respecte de *.

Cos finit: cos amb un nombre finit d'elements.

7.4 Annex D: Fotons que s'han d'enviar per crear una clau quàntica

Suposem que l'Alice envia el fotó amb la base $+$. El resultat serà el mateix si l'Alice envia amb base $+$ o $\times$, per tant no cal fer els dos casos. La probabilitat que l'Eve estigui espiant l'anomenarem *p*.

Primer es calcularà la probabilitat que un fotó enviat per l'Alice formi part o no de la clau, en cas que en formi part si és correcta o no i, finalment, si l'Eve sap el bit o no.

Si l'Alice i en Bob no mesuren amb les mateixes bases, el bit serà eliminat, per tant ja no formarà part de la clau. Per tant, tal com es mostra a la taula següent, de mitjana la meitat de fotons formaran un bit, mentre que l'altra meitat no.

A		B		Bit	Probabilitat
$+$	→	$+$ 1/2	→	**Sí**	**1/2**
	→	$\times$ 1/2	→	**No**	**1/2**

Seguidament s'estudiarà la probabilitat que el bit sigui correcte i la probabilitat que l'Eve sàpiga el bit.

A		E			Igual A?		B		Igual E?		Correcte?	E sap?	Probabilitat
$+$	→	No 1-p		→			$+$ 1/2	→			Sí	**No**	**(1-p)/2**
	→	Sí p	$+$ 1/2	→	Sí	→	$+$ 1/2	→	Sí	→	Sí	**Sí**	**p/4**
			$\times$ 1/2	→	Sí 1/2	→	$+$ 1/2	→	Sí 1/2	→	Sí	**No**	**p/16**
								→	No 1/2	→	No	**No**	**p/16**
				→	No 1/2	→	$+$ 1/2	→	Sí 1/2	→	No	**No**	**p/16**
								→	No 1/2	→	Sí	**No**	**p/16**

Per tant, les probabilitats són les següents:

Sí clau → 1/2
- → correcta → 1/2-p/8
  - → Eve sap → p/4
  - → Eve no sap → 1/2-3p/8
- → incorrecta → p/8

No clau → 1/2

Aquí es pot veure que la meitat dels fotons que l'Alice enviï no serviran per fer la clau. Per tant, dels bits que formin la clau inicial, abans d'aplicar processos per comprovar-la i per fer-la més

segura, *p/2* seran correctes però coneguts per l'Eve, *1-3p/4* seran correctes i no coneguts per l'Eve i *p/4* seran incorrectes.

Seguidament, l'Alice i en Bob agrupen els bits per parelles, els sumen, en mòdul 2 i comparen els resultats, per detectar possibles errors. Si la suma en mòdul 2 és igual, guarden el primer dels dos bits, sinó els eliminen tots dos. Seguidament s'analitzaran les possibles parelles, i la probabilitat que hi ha que apareguin. Si els dos bits són incorrectes l'Alice i en Bob no ho notaran, ja que la suma en mòdul 2 serà igual pels dos.

1r bit	2n bit	Probabilitat	Correcte?	Eve sap?
Eve sap	Eve sap	$p^2/4$	Sí	Sí
	Eve no sap	$p/2-3p^2/8$	Sí	Sí
	Incorrecte	$p^2/8$	No	-
Eve no sap	Eve sap	$p/2-3p^2/8$	Sí	Sí
	Eve no sap	$1-3p/2+9p^2/16$	Sí	No
	Incorrecte	$p/4-3p^2/16$	No	-
Incorrecte	Eve sap	$p^2/8$	No	-
	Eve no sap	$p/4-3p^2/16$	No	-
	Incorrecte	$p^2/16$	Sí	No

De les sumes correctes es guarda només el primer, per tant la meitat dels que hem sumat. En les sumes incorrectes s'eliminen els dos bits. Per tant, el nombre esperat de bits que quedaran serà:

$$\frac{correctes}{2} + incorrectes \cdot 0 = \frac{correctes}{2} = \frac{1 - \frac{p}{2} + \frac{p^2}{8}}{2} = \frac{1}{2} - \frac{p}{4} + \frac{p^2}{16}$$

Dels bits que formin la clau després d'haver eliminat bits incorrectes, la probabilitat que l'Eve els sàpiga és de $p/2-p^2/4$. També, en les sumes correctes hi haurà algun bit incorrecte. La probabilitat de trobar-ne és de $p^2/32$. Per tant els bits correctes que l'Eve no sap seran $1/2-3p/4+9p^2/32$.

Total bits després del procés d'eliminació de bits incorrectes $\rightarrow \frac{1}{2} - \frac{p}{4} + \frac{p^2}{16}$

- → Correctes
  - → Eve sap → $\frac{p}{2} - \frac{p^2}{4}$
  - → Eve no sap → $\frac{1}{2} - \frac{3p}{4} + \frac{9p^2}{32}$
- → Incorrectes → $\frac{p^2}{32}$

Si es repetís aquest procés, cada vegada hi hauria menys errors a la clau, però, també, s'escurçaria més.

Finalment, l'Alice i en Bob volen aconseguir una clau més segura, i per això agafen els bits per parelles i els sumen, en mòdul 2. L'Eve, per saber el valor de la suma dels dos bits necessita saber-los tots dos. En cas contrari perd la informació que tenia. En aquesta operació la clau s'encongeix la meitat, per tant, el nombre esperat de bits que quedaran serà la meitat, és a dir, $1/4-p/8+p^2/32$.

1r bit	2n bit	Probabilitat	Correcte?	Eve sap?
Eve sap	Eve sap	$\frac{64p^2 - 64p^3 + 16p^4}{64 - 64p + 32p^2 - 8p^3 + p^4}$	Sí	Sí
	Eve no sap	$\frac{64p - 128p^2 + 84p^3 - 18p^4}{64 - 64p + 32p^2 - 8p^3 + p^4}$	Sí	No
	Incorrecte	$\frac{4p^3 - 2p^4}{64 - 64p + 32p^2 - 8p^3 + p^4}$	No	-
Eve no sap	Eve sap	$\frac{64p - 128p^2 + 84p^3 - 18p^4}{64 - 64p + 32p^2 - 8p^3 + p^4}$	Sí	No
	Eve no sap	$\frac{256 - 768p + 864p^2 - 432p^3 + 81p^4}{256 - 256p + 128p^2 - 32p^3 + 4p^4}$	Sí	No
	Incorrecte	$\frac{16p^2 - 24p^3 + 9p^4}{256 - 256p + 128p^2 - 32p^3 + 4p^4}$	No	-
Incorrecte	Eve sap	$\frac{4p^3 - 2p^4}{64 - 64p + 32p^2 - 8p^3 + p^4}$	No	-
	Eve no sap	$\frac{16p^2 - 24p^3 + 9p^4}{256 - 256p + 128p^2 - 32p^3 + 4p^4}$	No	-
	Incorrecte	$\frac{p^4}{256 - 256p + 128p^2 - 32p^3 + 4p^4}$	Sí	No

Per tant, la probabilitat que un bit de la clau inicial esdevingui un bit al final és de, és a dir, la meitat que els que quedaven abans de començar aquest últim procés, dels quals l'Eve en sap aproximadament $\frac{64p^2-64p^3+16p^4}{64-64p+32p^2-8p^3+p^4}$, *de mitjana* $\frac{16p^2-8p^3+p^4}{128-128p+64p^2-16p^3+2p^4}$ són incorrectes i la resta, és a dir, uns $\frac{128-128p-80p^2+120p^3-31p^4}{128-128p+64p^2-16p^3+2p^4}$ són correctes i no coneguts per l'Eve.

Total de bits de la clau final $\rightarrow \frac{1}{4} - \frac{p}{8} + \frac{p^2}{32}$

- → Correctes
  - → Eve sap → $\frac{64p^2 - 64p^3 + 16p^4}{64 - 64p + 32p^2 - 8p^3 + p^4}$
  - → Eve no sap → $\frac{128 - 128p - 80p^2 + 120p^3 - 31p^4}{128 - 128p + 64p^2 - 16p^3 + 2p^4}$
- → Incorrectes → $\frac{16p^2 - 8p^3 + p^4}{128 - 128p + 64p^2 - 16p^3 + 2p^4}$

Els bits correctes seran la suma dels que sap l'Eve i dels correctes que l'Eve no sap o, també, els bits totals menys els incorrectes, és a dir $\frac{128-128p+48p^2-8p^3+p^4}{128-128p+64p^2-16p^3+2p^4}$.

Aquest procés també es pot repetir, per fer més segura la clau, però cada vegada que es repeteix s'escurça.

Suposem que l'Eve espia la meitat de les vegades, per tant *p=1/2*. Aleshores, dels bits de la clau inicial se n'aprofitaran, aproximadament:

$$\frac{1}{4}-\frac{p}{8}+\frac{p^2}{32}=\frac{1}{4}-\frac{1}{16}+\frac{1}{128}=\frac{25}{128}\approx \mathbf{0,1953}$$

D'aquests, d'incorrectes n'hi haurà, de mitjana:

$$\frac{16p^2-8p^3+p^4}{128-128p+64p^2-16p^3+2p^4}=\frac{4-1+\frac{1}{16}}{128-64+16-2+\frac{2}{16}}=\frac{49}{1250}\approx \mathbf{0,0392}$$

Per tant, l'esperança que un bit sigui correcte, que serà de:

$$\frac{128-128p+48p^2-8p^3+p^4}{128-128p+64p^2-16p^3+2p^4}=\frac{128-64+12-1+\frac{1}{16}}{128-64+16-2+\frac{1}{8}}=\frac{1201}{1250}\approx \mathbf{0,9608}$$

Dels bits de la clau final, l'Eve en sabrà:

$$\frac{64p^2-64p^3+16p^4}{64-64p+32p^2-8p^3+p^4}=\frac{16-8+1}{64-32+8-1+\frac{1}{16}}=\frac{144}{625}\approx \mathbf{0,2304}$$

I els bits de la clau final correctes i no coneguts per l'Eve seran, aproximadament:

$$\frac{128-128p-80p^2+120p^3-31p^4}{128-128p+64p^2-16p^3+2p^4}=\frac{128-64-20+15-\frac{31}{16}}{128-64+16-2+\frac{1}{8}}=\frac{913}{1250}\approx \mathbf{0,7304}$$

Utilitzant el codi que s'ha usat anteriorment per passar les lletres a un codi binari, per cada lletra eren necessaris 5 bits. Per tant, per enviar la paraula "photon", eren necessària una clau de 30 bits. Com s'ha dit, dels bits de la clau inicial, és a dir, abans de fer comparacions o fer-la més segura, només uns 25/128 s'aprofiten per la clau final, és a dir, que per cada 128 bits de la clau inicial només n'obtindrem uns 25 per a la clau final. Per tant, per obtenir una clau de 30 bits, necessitarem, aproximadament, tenir una clau inicial d'uns 154 bits. Però no tots els fotons que s'envien formen part de la clau: només la meitat, de mitjana, serveixen. Per tant, per obtenir una clau de 30 bits, s'hauran d'enviar, aproximadament, 308 fotons.

Dels 30 bits, n'hi haurà, de mitjana, 1 d'incorrecte, i l'Eve en sabrà més o menys 7. La resta, és a dir, aproximadament 22, seran correctes i no coneguts per l'Eve.

Si en lloc d'enviar el missatge "photon" l'Alice volgués enviar el missatge "aquest es el missatge", com en la resta de casos, necessitaria una clau de 90 bits, ja que hi ha 18 lletres i per cada lletra necessitem 5 bits. Per tant, l'Alice necessitaria enviar uns 922 fotons, i de la clau final aproximadament 3 o 4 serien incorrectes, l'Eve en sabria, de mitjana 21 i la resta, és a dir, uns 65 o 66, serien correctes i no coneguts per l'Eve.

7.5 **Annex E: Complexitat**

La complexitat és molt important en la criptografia, ja que indica quants càlculs i, per tant, quant temps es necessita per resoldre un problema o un algoritme. Es calcula segons el nombre de xifres dels nombres d'entrada.

Un algoritme computacionalment fàcil és aquell que és ràpid, que es necessita poc temps per donar la sortida a partir dels valors d'entrada. Per exemple la multiplicació de dos nombres, tal com s'ensenya a l'escola, és bastant eficient, ja que no s'han de fer gaires operacions per obtenir el producte. Tot i així hi ha mètodes més eficients computacionalment, per calcular el producte de dos nombres.

Un algoritme computacionalment difícil és aquell que és ineficient, que s'han de fer moltes operacions abans de donar el resultat. Per exemple, per multiplicar dos nombres podríem agafar-ne un i sumar-lo a ell mateix tantes vegades com indiqués l'altre nombre, però si es fa amb nombres molt grans no s'acabaria mai. Un altre exemple és la descomposició d'un nombre en factors primers. El primer que se li acudiria a la majoria seria anar provant per tots els primers, començant pels més petits. Això necessita un temps exponencial, per tant no és gens eficient. A la pràctica es coneixen alguns algoritmes millors, però tampoc ho són suficientment com perquè es considerin eficients. El mateix passa amb el logaritme discret.

La complexitat d'un problema ve donada per la complexitat del millor algoritme per resoldre aquell problema. En el cas de la multiplicació, com que es coneixen algoritmes molt eficients, es tracta d'un problema computacionalment fàcil, mentre que la factorització és considerat un problema computacionalment difícil, encara que no està demostrat que ho sigui, ja que no es coneixen mètodes eficients.