Treball final del grau de Matemàtiques

Transmissió segura d'informació i distribució quàntica de claus

Erik Martori López

Director: Dr. Artur Travesa
Departament de Matemàtiques i Informàtica
Barcelona, 17 de gener de 2018

Abstract

Security on digital communications is a recurrent issue nowadays due to the amount of sensitive information that is exchanged and the fact that we are getting more and more connected with our surroundings. Throughout this essay, we use Shannon's theory to pull off a study on security from a mathematical point of view with the aim of finding a method which allows the safe exchange of information along insecure communication channels.

Resum

La seguretat en les comunicacions digitals és un tema molt important en l'actualitat degut a la quantitat d'informació sensible que s'intercanvia i al fet que cada cop estem més connectats amb el que ens envolta. En aquest treball, ens basem en la teoria de Shannon per estudiar el problema de la seguretat des d'un punt de vista matemàtic amb la finalitat de trobar una manera que permeti l'intercanvi segur informació a través de canals insegurs de comunicació.

Agraïments

Vull agrair al Dr. Artur Travesa per haver-me guiat en aquest Treball de Fi de Grau tot aportant noves idees, diferents punts de vista i proporcionant fonts d'informació molt útils que m'han permès aprendre molts nous conceptes al llarg de la realització d'aquest treball. També voldria fer menció als meus pares i a la meva noia que, tot i no estar molt familiaritzats amb aquesta branca de les matemàtiques, han sigut sempre un punt de suport clau per a mi.

Índex

Introducció

L'objectiu fonamental de la criptografia és permetre que dos dispositius, que anomenarem emissor i receptor, es comuniquin a través d'un canal de comunicació de manera que cap tercer no pugui entendre el missatge que s'estan transmetent. La informació que l'emissor li vol enviar al receptor, que anomenarem *text pla*, serà tractada com una cadena de bits ja que així és com funcionen les comunicacions digitals avui dia. Per tal de transmetre la informació, l'emissor encripta el text pla amb una determinada *clau*, obtenint així un *text xifrat*, que enviarà a través del canal de comunicació. El receptor, per altra banda, sap amb antel·lació quina és la clau de desxifratge (que pot ser la mateixa que la de xifratge o no) i per tant pot reconstruir el text pla a partir del xifrat; és a dir, desxifrar el missatge.

En molts casos, és de vital importància que la informació intercanviada entre emissor i receptor sigui inaccessible per a qualsevol tercer que pugui estar interessat en ella. Malauradament, els canals de comunicació actuals no proporcionen una manera de transmetre informació de forma segura i per això és important xifrar el missatge per tal que, si un tercer l'intercepta, no sigui capaç de reconstruir el missatge pla original. A més, és important també trobar una manera per a què l'emissor i el receptor es posin d'acord en la clau (o les claus) a emprar sense que ningú més tingui aquesta informació.

La finalitat d'aquest projecte és fer un repàs dels protocols actuals de transmissió d'informació i arribar a trobar un mètode que permeti la comunicació entre dos interlocutors de forma segura. Es vol donar una visió global d'aquests mètodes i una descripció des del punt de vista matemàtic dels seus punts clau però sense entrar-hi en detalls massa tècnics.

En quant a l'estructura de la memòria, definim en primer lloc la teoria de la comunicació tal com la va explicar Claude Shannon a mitjans del segle passat i introduïm el concepte de criptosistema tot donant-ne els exemples més representatius. A continuació, expliquem quins són alguns dels mètodes de xifratge que es fan servir en l'actualitat i com sorgeix la necessitat de generar nombres de forma aleatòria per tal de garantir la seguretat en la transmissió del missatge. Posteriorment, discutim quins són alguns dels procediments emprats avui dia per tal d'acordar la clau a emprar entre els dos interlocutors i els defectes que presenten. Finalment, introduïm la distribució quàntica de claus com a alternativa per acordar la clau a emprar entre els dos interlocutors i expliquem com aquest protocol de comunicació salva els problemes que tenen els mètodes convencionals de predistribució de clau.

1 Teoria de Shannon

En Claude Elwood Shannon, matemàtic dels Estats Units, va publicar a mitjans del segle XX una teoria matemàtica de la informació [1]. Aquest article pioner va representar un punt d'inflexió en l'estudi matemàtic de la criptografia. En aquest capítol n'exposem els seus punts claus.

1.1 Conceptes bàsics

En el món de les comunicacions digitals la informació s'acostuma a enviar en forma de cadenes de bits així que sembla raonable tractar els missatges d'aquesta manera. En la pràctica, els missatges no són arbitràriament llargs i sovint es trenquen en unitats de missatge de longituds fixades. Per tant, podem considerar que el conjunt de missatges és finit.

Definició 1.1. *Un **criptosistema** és una quíntupla* $(\mathcal{P}, \mathcal{C}, \mathcal{K}, \mathcal{E}, \mathcal{D})$ *que satisfà les condicions següents:*

- $\mathcal{P}$ *és un conjunt finit, anomenat de missatges plans o, també, unitats de missatge pla.*
- $\mathcal{C}$ *és un conjunt finit, anomenat de missatges xifrats o, també, unitats de missatge xifrat.*
- $\mathcal{K}$ *és un conjunt finit, anomenat conjunt de claus.*
- $\mathcal{E} = \{e_K\}_{K\in\mathcal{K}}$, $\mathcal{D} = \{d_K\}_{K\in\mathcal{K}}$ *són dues famílies de funcions,* $e_K : \mathcal{P} \to \mathcal{C}$, $d_K : \mathcal{C} \to \mathcal{P}$, $K \in \mathcal{K}$, *tals que* $\forall x \in \mathcal{P}$, $d_K(e_K(x)) = x$. *S'anomenen les funcions de xifratge,* e_K, *i de desxifratge,* d_K, *associades a la clau* K.

Per tal de comunicar-se entre ells, l'emissor i el receptor faran servir el **protocol** següent.

1. En primer lloc, es posen d'acord en una clau $K \in \mathcal{K}$. Això implica l'elecció de la parella $\{e_K, d_K\}$.
2. Ara, suposem que l'emissor vol comunicar-se amb el receptor a través d'un canal insegur. Sigui $x = x_1x_2\cdots x_n$, per a algun $n \geq 1$ el missatge que es vol transmetre, on cada unitat de missatge del text pla $x_i \in \mathcal{P}$, $1 \leq i \leq n$.
3. Cada x_i s'encripta fent servir la funció de xifratge $e_K \in \mathcal{K}$ especificada per la clau escollida K. L'emissor computa $y_i = e_K(x_i)$ per a $1 \leq i \leq n$ i envia el text xifrat resultant a través del canal de comunicació de manera que es transmet el missatge xifrat $y = y_1y_2\cdots y_n$.
4. Quan el receptor rep el missatge xifrat y, el desxifra fent servir $d_K \in \mathcal{D}$, també especificat per la clau K, obtenint així el text original $x = x_1x_2\cdots x_n$.

Corol·lari 1.2. *A partir de les definicions anteriors podem treure les conclusions següents:*

- $\forall K \in \mathcal{K}$, e_K *ha de ser una funció injectiva i* d_K *una funció exhaustiva ja que la composició* $d_K \circ e_K$ *és la identitat.*
- *En el cas que* $\mathcal{P} = \mathcal{C}$, *cada funció de xifratge és una permutació.* □

Exemple 1.3. Criptosistemes com Cèsar, Vigenère, de tipus Hill, de permutació o de substitució, són sovint utilitzats com a entreteniment en diaris o revistes d'abast general. Altres, molt més elaborats, com DES o AES, s'empren en comunicacions digitals.

A continuació, definim un criptosistema que serà molt important en aquest tractat ja que és l'únic per al qual s'ha demostrat a dia d'avui que té la propietat de secret perfecte, que explicarem més endavant; és el *criptosistema de Vernam* o *llibreta d'un sol ús*. Sigui n la llargada del missatge que es vol transmetre; definim els conjunts

$$\mathcal{P} = \mathcal{C} = \mathcal{K} = (\mathbb{Z}/2\mathbb{Z})^n .$$

Siguin x un element de $\mathcal{P}$, $x = x_1 \cdots x_n$, $x_i \in \mathbb{Z}/2\mathbb{Z}$, $\forall i = 1, \ldots, n$ i K un element de $\mathcal{K}$, $K = k_1 \cdots k_n$, $k_i \in \mathbb{Z}/2\mathbb{Z}$, $\forall i = 1, \ldots, n$. Definim

$$e_K(x) = (x_1 + k_1 \mod 2)(x_2 + k_2 \mod 2) \cdots (x_n + k_n \mod 2) \in \mathcal{C}.$$

Anàlogament, sigui y un element de $\mathcal{C}$, $y = y_1 \cdots y_n$, $y_i \in \mathbb{Z}/2\mathbb{Z}$, $\forall i = 1, \ldots, n$. Definim

$$d_K(y) = (y_1 + k_1 \mod 2)(y_2 + k_2 \mod 2) \cdots (y_n + k_n \mod 2) \in \mathcal{P}.$$

Veiem que, efectivament, la composició $e_K(d_K(x)) = x$ ja que si $z \in \mathbb{Z}/2\mathbb{Z}$, $z \equiv 0 \mod 2$ o bé $z \equiv 1 \mod 2$; en qualsevol cas, $z + z \equiv 0 \mod 2$.□

1.2 Secret perfecte

Tot i haver-hi definicions precises de conceptes diferents de seguretat, ens limitarem a tractar la seguretat de manera informal. Entendrem per un criptosistema *computacionalment segur* aquell que per poder extreure el text pla a partir del xifrat, sense el coneixement de la clau, requereix d'una quantitat de recursos que la tecnologia actual no pot proporcionar o bé una quantitat de temps després del qual la informació desxifrada ja hauria perdut el seu valor. Anàlogament, entendrem per un criptosistema *incondicionalment segur* aquell que ni tan sols amb una quantitat il·limitada de temps i de recursos permetria obtenir el missatge pla a partir del xifrat sense el coneixement previ de la clau.

Donada una llargada n, tractarem els elements dels conjunts finits $\mathcal{P}$, $\mathcal{C}$ i $\mathcal{K}$ com elements d'una determinada distribució discreta de probabilitat. Això ens permetrà donar la definició d'un dels conceptes més importants del treball: el secret perfecte.

Definició 1.4. *Suposem que X i Y són variables aleatòries en un espai de probabilitat finit. Denotem la probabilitat que X prengui el valor x com $p(x)$ i la probabilitat que Y prengui el valor y com $p(y)$. La probabilitat conjunta $p(x, y)$ és la probabilitat que X prengui el valor x i Y el valor y alhora. A més, definim la probabilitat condicionada $p(x|y)$ com la probabilitat que X prengui el valor x sabent que Y pren el valor y.*
Diem que les dues variables són independents si $p(x, y) = p(x)p(y)$ per a qualssevol possibles x, y.

La probabilitat conjunta es pot relacionar amb la condicionada de la manera següent

$$p(x, y) = p(x|y)p(y).$$

Si intercanviem x i y, trobem que

$$p(y, x) = p(x, y) = p(y|x)p(x).$$

Igualant aquestes dues expressions obtenim un corol·lari del *Teorema de Bayes*.

Corol·lari 1.5. *Siguin x i y successos qualsevols definits sobre una variable aleatòria, aleshores*

$$p(x|y)p(y) = p(x)p(y|x).$$

A més, si $p(y) > 0$,

$$p(x|y) = \frac{p(x)p(y|x)}{p(y)}.\square$$

Tornem a la criptografia i suposem que hi ha una distribució de probabilitat en l'espai $\mathcal{P}$ de manera que $p_{\mathcal{P}}(x)$ és la probabilitat que l'element escollit sigui x. Anàlogament, Sigui $p_{\mathcal{K}}(K)$ la probabilitat que K sigui la clau escollida en l'espai $\mathcal{K}$. Assumim a més, que aquestes dues distribucions són independents; aquesta suposició és raonable ja que sovint la clau s'escull abans de saber quin missatge pla s'enviarà i el missatge pla no depèn de la clau escollida.

Les distribucions $p_{\mathcal{P}}(x)$ i $p_{\mathcal{K}}(K)$ determinen una distribució de probabilitat en $\mathcal{C}$ que anomenarem $p_{\mathcal{C}}(y)$ que es pot calcular com segueix. En primer lloc, considerem el conjunt dels possibles missatges xifrats si K és la clau escollida com

$$C(K) = \{e_K(x) : x \in \mathcal{P}\};$$

aleshores, la probabilitat que el missatge xifrat sigui y vindrà donada per

$$p_{\mathcal{C}}(y) := \sum_{\{K:y\in C(K)\}} p_{\mathcal{K}}(K)p_{\mathcal{P}}(d_K(y)).$$

A més, podem obtenir fàcilment una expressió per a la probabilitat condicionada $p_{\mathcal{P}}(y|x)$, és a dir, la probabilitat que y sigui el missatge xifrat sabent que x és el missatge pla. Obtenim que

$$p_{\mathcal{C}}(y|x) = \sum_{\{K|x=d_{\mathcal{K}}(y)\}} p_{\mathcal{K}}(K).$$

Finalment, amb l'ajut del *Teorema de Bayes* podem deduir quina és la probabilitat que el missatge pla sigui x si el missatge xifrat és y.

$$p_{\mathcal{P}}(x|y) = \frac{p_{\mathcal{P}}(x) \sum_{\{K|x=d_{\mathcal{K}}(y)\}} p_{\mathcal{K}}(K)}{\sum_{\{K:y\in C(K)\}} p_{\mathcal{K}}(K) p_{\mathcal{P}}(d_{\mathcal{K}}(y))}.$$

Aquests resultats els podem resumir en el lema següent que farem servir més endavant per demostrar la propietat de secret perfecte del Xifrat de Vernam.

Lema 1.6. *Les distribucions $p_{\mathcal{P}}(x)$ i $p_{\mathcal{K}}(K)$ determinen una distribució de probabilitat en $\mathcal{C}$ que anomenarem $p_{\mathcal{C}}(y)$ i se satisfà que*

$$p_{\mathcal{C}}(y) = \sum_{\{K:y\in C(K)\}} p_{\mathcal{K}}(K) p_{\mathcal{P}}(d_K(y)),$$

$$p_{\mathcal{C}}(y|x) = \sum_{\{K|x=d_{\mathcal{K}}(y)\}} p_{\mathcal{K}}(K),$$

$$p_{\mathcal{P}}(x|y) = \frac{p_{\mathcal{P}}(x) \sum_{\{K|x=d_{\mathcal{K}}(y)\}} p_{\mathcal{K}}(K)}{\sum_{\{K:y\in C(K)\}} p_{\mathcal{K}}(K) p_{\mathcal{P}}(d_{\mathcal{K}}(y))}.$$

Definició 1.7. *Un criptosistema té la propietat de* ***secret perfecte*** *si $p_{\mathcal{P}}(x|y) = p_{\mathcal{P}}(x)$ $\forall x \in \mathcal{P}$, $\forall y \in \mathcal{C}$.*

Proposició 1.8. *Si un criptosistema té la propietat de secret perfecte, aleshores $|\mathcal{K}| \geq |\mathcal{C}'| \geq |\mathcal{P}|$, on $\mathcal{C}'$ és el conjunt dels $y \in \mathcal{C}$ tals que $p_{\mathcal{C}}(y) > 0$.*

Fixem-nos que la condició $p_{\mathcal{P}}(x|y) = p_{\mathcal{P}}(x)$ és equivalent a $p_{\mathcal{C}}(y|x) = p_{\mathcal{C}}(y)$ $\forall x \in \mathcal{P}$, $\forall y \in \mathcal{C}$, pel corol·lari 1.5. Fixat un $x \in \mathcal{P}$, $\forall y \in \mathcal{C}'$ tenim $p_{\mathcal{C}'}(y|x) = p_{\mathcal{C}'}(y) > 0$ i per tant per a cada $y \in \mathcal{C}'$ ha d'haver-hi com a mínim una clau K tal que $e_K(x) = y$. D'aquí deduïm que $|\mathcal{K}| \geq |\mathcal{C}'|$. A més, com que cada funció d'encriptació és injectiva, s'ha de satisfer que $|\mathcal{C}'| \geq |\mathcal{P}|$. En conclusió, $|\mathcal{K}| \geq |\mathcal{C}'| \geq |\mathcal{P}|$. □

1.3 Entropia

Definició 1.9. *Suposem que X és una variable aleatòria que pot prendre un conjunt finit de valors $\{x_1, \ldots, x_n\}$ amb una distribució de probabilitat $p(X)$ de tal manera que $p_i = P(X = x_i)$ $\forall i = 1, \ldots, n$. Definim l'****entropia*** *d'aquesta distribució de probabilitat com*

$$H(X) := -\sum_{i=1}^{n} p_i \log_2 p_i.$$

Aquesta quantitat ens ajudarà a saber com de fàcil un criptoanalista serà capaç d'extreure el text pla a través del xifrat amb temps suficient. L'entropia pot ser entesa com una mesura de la informació. Considerem el següent exemple.

Exemple 1.10. Si llancem una moneda, podem suposar que la $p(X = cara) = p(X = creu) = \frac{1}{2}$. Sembla raonable afirmar que l'entropia o la informació d'aquesta distribució es pot englobar en un sol bit de manera que $cara = 1$ i $creu = 0$.

Si ara considerem una variable aleatòria X que pot prendre els valors $\{x_1, x_2, x_3\}$ amb probabilitat $p(X = x_1) = p(X = x_2) = \frac{1}{4}$ i $p(X = x_3) = \frac{1}{2}$, una manera de codificar la informació és la següent. Assignem $x_3 = 0$, $x_1 = 10$ i $x_2 = 11$. Per tant el nombre mitjà de bits per a fer la codificació és de

$$\frac{1}{2} \times 1 + \frac{1}{4} \times 2 + \frac{1}{4} \times 2 = \frac{3}{2}.$$

També podríem haver codificat la informació com $x_3 = 10$, $x_1 = 11$ i $x_2 = 0$ i aleshores el nombre mitjà de bits seria $\frac{7}{4}$. Notem que ara cal una quantitat mitjana de bits superior.

En general, si tenim una variable aleatòria X que pot prendre valors x_i, $1 \leq i \leq n$ amb una probabilitat $P(X = x_i) = p_i$, sempre podrem codificar els possibles x_i en cadenes de 0 i 1 i obtenir el menor nombre mitjà de bits possibles fent servir l'*algoritme de Huffman* [3]. Com que no el farem servir, no en donarem més detalls.

Observació 1.11. Si un succés ocorre amb probabilitat 2^{-n}, pot ser codificat mitjançant l'algoritme de Huffman en una cadena d'n bits. Fent un canvi de variable, si el succés ocorre amb probabilitat p podrà ser codificat amb una cadena d'aproximadament $-log_2(p)$ bits. Si fem la mitjana ponderada d'aquestes quantitats per la probabilitat que ocorren, recuperem la definició 1.9 del concepte d'entropia.

Definició 1.12. *L'entropia conjunta de dues variables aleatòries X i Y amb possibles valors $X \in \{x_1, ...x_m\}$ i $Y \in \{y_1, ...y_n\}$ es defineix com*

$$H(X, Y) := -\sum_{i=1}^{m} \sum_{j=1}^{n} r_{ij} log_2(p_i q_j),$$

on $r_{ij} := P(X = x_i, Y = y_j)$, $p_i := P(X = x_i)$ i $q_j := P(Y = y_j)$.

Anàlogament, definim l'entropia condicionada de X en Y com

$$H(X|Y) = \sum_{i=1}^{m} \sum_{j=1}^{n} r_{ij} log_2(p(x_i|y_j)).$$

Si X és una variable aleatòria amb distribució de probabilitat $p_1, \ldots, p_n$ on $p_i > 0$ $\forall i = 1, \ldots, n$; la seva entropia satisfarà les propietats següents:

1. $H(X) \leq log_2(n)$ i la igualtat es donarà només quan $p_i = 1/n$, $\forall i = 1, \ldots, n$.

2. Si Y és una altra variable aleatòria, aleshores $H(X,Y) \leq H(X) + H(Y)$ i seran iguals si i només si X i Y són independents.

3. $H(X,Y) = H(Y) + H(X|Y)$.

4. $H(X|Y) \leq H(X)$ i seran iguals si i només si són independents.

Aquestes propietats són demostrables amb l'ajut de la *desigualtat de Jensen*. Sigui $\phi : U \subset \mathbb{R} \longrightarrow \mathbb{R}$ una funció convexa, $\{x_1, ..., x_n\}$ un conjunt de punts de U i $\{a_1, ..., a_n\}$ un conjunt de nombres reals positius, anomenats pesos, aleshores,

$$\phi\left(\frac{\sum a_i x_i}{\sum a_i}\right) \leq \frac{\sum a_i \phi(x_i)}{\sum a_i}.$$

Recordem que en els conjunts $\mathcal{P}$, $\mathcal{C}$ i $\mathcal{K}$ hi ha distribucions discretes de probabilitat $P_{\mathcal{P}}$, $P_{\mathcal{C}}$, $P_{\mathcal{K}}$, de manera que podem considerar-los com variables aleatòries. Això ens permetrà parlar de la *probabiltat que una clau sigui* K o de la *probabilitat que el missatge pla sigui* x.

La quantitat $H(\mathcal{K}|\mathcal{C})$ és important perquè ens dóna una idea de quanta informació de la clau ens revel·la el missatge xifrat. Es pot calcular de la manera següent.

Teorema 1.13. *Sigui* $(\mathcal{P}, \mathcal{C}, \mathcal{K}, \mathcal{E}, \mathcal{D})$ *un criptosistema; aleshores*

$$H(\mathcal{K}|\mathcal{C}) = H(\mathcal{K}) + H(\mathcal{P}) - H(\mathcal{C}).$$

En primer lloc, observem que, per la propietat 3, $H(\mathcal{K}, \mathcal{P}, \mathcal{C}) = H(\mathcal{C}|\mathcal{K}, \mathcal{P}) + H(\mathcal{K}, \mathcal{P})$. A més, donades la clau K, e_K, d_K i el missatge pla, el missatge xifrat queda determinat de forma unívoca; se satisfà que $H(\mathcal{C}|\mathcal{K}, \mathcal{P}) = 0$. Per tant, $H(\mathcal{K}, \mathcal{P}, \mathcal{C}) = H(\mathcal{K}, \mathcal{P}) = H(\mathcal{K}) + H(\mathcal{P})$ per la propietat 2 ja que són variables independents.

Fent un raonament similar, ara $H(\mathcal{K}, \mathcal{P}, \mathcal{C}) = H(\mathcal{P}|\mathcal{K}, \mathcal{C}) + H(\mathcal{K}) + H(\mathcal{C})$. De nou, el missatge pla queda unívocament determinat pel text xifrat i la clau i per tant $H(\mathcal{P}|\mathcal{K}, \mathcal{C}) = 0$. Fent servir de nou la propietat 3 i els resultats anteriors,

$$H(\mathcal{K}|\mathcal{C}) = H(\mathcal{K}, \mathcal{C}) - H(\mathcal{C}) = H(\mathcal{K}, \mathcal{P}, \mathcal{C}) - H(\mathcal{C}) = H(\mathcal{K}) + H(\mathcal{P}) - H(\mathcal{C}).\square$$

1.4 Entropia d'un llenguatge

En aquest apartat, considerarem els criptosistemes on el conjunt de missatges plans i el conjunt de missatges xifrats són l'alfabet d'un cert idioma i les funcions d'encriptació mantenen les freqüències dels caràcters en fer l'encriptació; és a dir, si la freqüència d'un caràcter x en el missatge pla és f, aleshores la freqüència del caràcter $e_{\mathcal{K}}(x)$ és f en el missatge xifrat. Exemples d'aquests tipus de criptosistemes serien l'afí, el de substitució o el Cèsar.

Ens interessarem en saber si un tercer que només tingui accés al missatge xifrat podrà retrobar el missatge pla amb facilitat. En un primer intent, descartarà les

claus que donin lloc a missatges plans que no tinguin significat en l'idioma corresponent i reduirà l'estudi a les que donin lloc a missatges amb sentit; a aquestes últimes, excepte a la bona, les anomenarem el conjunt de **claus falses**.

Exemple 1.14. Suposem que l'emissor vol dir-li HOLA al receptor i, després de xifrar el missatge, envia el missatge xifrat HWQS a través del canal. Un tercer ho veu, i després de provar totes les claus i de llegir els corresponents missatges plans, els únics que són paraules amb sentit són HOLA o ADEU però no sap quin dels dos és el missatge enviat. La clau que dóna la paraula ADEU serà doncs una clau falsa perquè és una clau que el portaria a una paraula equivocada.

La nostra finalitat és ara trobar una cota del nombre esperat de claus falses ja que quan aquest nombre sigui 0, el tercer haurà trobat la clau adequada i per tant el missatge correcte.

En primer lloc, definim el que entenem per **entropia per lletra d'un llenguatge** L, H_L. És una mesura de la informació mitjana per lletra en un text del llenguatge amb sentit. Com a primera aproximació podríem prendre $H_L \approx H(P)$ però també hem de tenir en compte que hi ha parelles de lletres que són més freqüents que d'altres (com per exemple la lletra Q que només pot anar acompanyada de U llevat dièresi). Per a una aproximació de segon ordre, hauríem de calcular la freqüència de tots els digrames i dividir per 2. En general, definim P^n com la variable aleatòria que té per distribució de probabilitat aquella que té en compte tots els n-grames de text. Sembla natural doncs fer les següents definicions.

Definició 1.15. *Si L és un llenguatge natural, definim l'**entropia de** L com*

$$H_L = \lim_{n\to\infty} \frac{H(P^n)}{n}.$$

En la pràctica, no és fàcil estimar una funció que doni l'entropia de cada conjunt de possibles n-grames. Per fer el càlcul de $H(P^n)$ s'acostuma a tabular la probabilitat de cada paraula en l'idioma corresponent i fer el càlcul

$$H(P^n) \approx \sum_{n=1}^{n_{lim}} p_i log_2(p_i)$$

per a n prou gran on n_{lim} és el nombre de paraules que es tenen en compte. Per a l'anglès, una possible estimació s'obté de considerar les 8700 paraules més usades (*the*, *of* , ...). Finalment, per trobar H_L es divideix el resultat anterior pel nombre mitjà de lletres per paraula [2].

Definició 1.16. *Definim la **redundància de** L com*

$$R_L = 1 - \frac{H_L}{log_2|\mathcal{P}|}.$$

Cal remarcar que un llenguatge aleatori tindria una entropia de $log_2|\mathcal{P}|$ i per això la quantitat R_L mesura la fracció de caràcters en excès.

De fet, la freqüència de les lletres en un text depèn de molts factors: l'idioma, el tipus de text (matemàtic, novel·la amorosa, jurídic...), la persona en què es narren els fets (primera, narrador omniscent...), etc. Un exemple d'una taula que proporciona un model de freqüències de les lletres en anglès és la següent.

e	t	a	o	i	n	s	h	r	d	l	c	u
12.4	9.1	8.2	7.5	7.0	6.8	6.3	6.1	6.0	4.3	4.0	2.8	2.8

m	w	f	g	y	p	b	v	k	j	x	q	z
2.4	2.4	2.2	2.0	2.0	1.9	1.5	0.9	0.8	0.2	0.2	0.1	0.1

Taula 2: Taula de les freqüències de les lletres de l'anglès extreta del *Concis Oxford Diccionary*.

En aquesta taula només es té en compte l'arrel de la paraula i no els seus derivats. No és, per tant, una taula de freqüències de textos escrits però ens dóna una idea de quines són les lletres més utilitzades en l'anglès. Emprant-la obtenim una primera estimació de $H_L \approx H(P) \approx 4.176$. A continuació, hauríem de tenir en compte els bigrames, trigrames, i n-grames d'ordre superior per obtenir un valor més precís. De fet, el mateix Shannon va aconseguir acotar el valor de H_L entre $1.0 \leq H_L \leq 1.5$ [1].

Si prenem $H_L = 1.25$, aleshores obtenim una *redundància* en l'anglès de $R_L = 0.75$. Això no vol dir que si traiem tres de cada quatre lletres d'un text en anglès seguirem sent capaços d'entendre'l sinò que és possible trobar una codificació de Huffman de n-grames que, per a n prou gran, seria capaç de comprimir el text a un quart de la seva llargària.

1.5 Acotació de claus falses i distància a la unicitat

Sigui n el nombre de missatges plans que conté la comunicació i donades les distribucions de probabilitat de $\mathcal{P}^n$ i $\mathcal{K}$, podem definir la distribució de probabilitat induïda en $\mathcal{C}^n$, el conjunt de n-grames de text xifrat. Donat $y \in \mathcal{C}^n$, definim

$$K(y) = \{K \in \mathcal{K} : \exists x \in \mathcal{P}^n | \mathrm{p}_{\mathcal{P}^n}(x) > 0, e_K(x) = y\}.$$

$K(y)$ és doncs el conjunt de claus que donen lloc a un text pla amb sentit sabent que y és el text xifrat. El cardinal de claus falses serà doncs $|K(y)| - 1$. Calculem el nombre mitjà de claus falses $\overline{s_n}$ de tots els possibles textos xifrats de llargària n.

$$\overline{s_n} = \sum_{y \in \mathcal{C}^n} p(y)(|K(y)| - 1) = \sum_{y \in \mathcal{C}^n} p(y)|K(y)| - \sum_{y \in \mathcal{C}^n} p(y) = \sum_{y \in \mathcal{C}^n} p(y)|K(y)| - 1.$$

Recordem que pel Teorema 1.13,

$$H(K|C^n) = H(K) + H(P^n) - H(C^n).$$

Si ara considerem n prou gran, podem estimar

$$H(P^n) \approx nH_L = n(1 - R_L)log_2|\mathcal{P}|.$$

A més, $H(C^n) \leq n\, log_2|\mathcal{C}|$. Si fem servir la mateixa codificació tant per al text pla com per al xifrat, és a dir, $|\mathcal{C}| = |\mathcal{P}|$,

$$H(K|C^n) \geq H(K) - nR_L log_2|\mathcal{P}|.$$

Ara relacionem aquesta quantitat amb el nombre de *claus falses*.

$$H(K|C^n) = \sum_{y \in \mathcal{C}^n} p(y)H(K|y) \leq \sum_{y \in \mathcal{C}^n} p(y)log_2|K(y)| \leq$$
$$\leq log_2 \sum_{y \in \mathcal{C}^n} p(y)|K(y)| = log_2(\overline{s_n} + 1),$$

on hem fet servir les propietats de l'entropia enunciades anteriorment i la *desigualtat de Jensen* en $f(x) = log_2(x)$. Ajuntant els dos resultats, obtenim que

$$log_2(\overline{s_n} + 1) \geq H(K) - nR_L log_2|\mathcal{P}|.$$

Això ens porta al següent teorema.

Teorema 1.17. *Sigui* $(\mathcal{P}, \mathcal{C}, \mathcal{K}, \mathcal{E}, \mathcal{D})$ *un criptosistema tal que* $|\mathcal{C}| = |\mathcal{P}|$ *i on les claus s'escullen equiprobablement* $(p_{\mathcal{K}}(K) = 1/|\mathcal{K}|)\ \forall K \in \mathcal{K}$. *Aleshores, donat un text xifrat de longitud n, amb n prou gran, el nombre esperat de claus falses satisfà que*

$$\overline{s_n} \geq \frac{|\mathcal{K}|}{|\mathcal{P}|^{nR_L}} - 1.\square$$

Fem notar que, a mesura que n augmenta, aquesta quantitat tendeix ràpidament a 0, com és d'esperar. També cal remarcar que aquesta aproximació pot no ser bona per a valors petits de n ja que $H(P^n)/n$ podria no ser un bon estimador de H_L.

Si ara el que volem és saber quants caràcters necessitem per tal de reduir el nombre de claus falses a 0, només cal imposar $\overline{s_n} = 0$ i aïllar n,

$$n_0 \approx \frac{log_2|\mathcal{K}|}{R_L log_2|\mathcal{P}|}.$$

Aquest valor es coneix com **distància a la unicitat**. Com a exemple, si prenem $\mathbb{Z}/26\mathbb{Z} = \mathcal{P} = \mathcal{C}$ com a conjunt de textos plans i xifrats i considerem el *xifrat de*

permutacions, on cada lletra és enviada mitjançant una bijecció a una altra, donant lloc a 26! possibilitats, juntament amb $R_L = 0.75$, obtenim el següent resultat.

$$n_0 \approx \frac{88.4}{0.75 \times 4.7} \approx 25.$$

Això vol dir que donat un text xifrat de longitud mínima 25 caràcters, normalment es pot aconseguir desencriptar de forma única. Diem *normalment* perquè hem treballat amb el nombre mitjà de claus falses i hem fet l'aproximació $H(P^n)/n \approx H_L$. És per aquest motiu que el xifrat de permutacions s'utilitza com a entreteniment en diaris o revistes de caire general.

2 Mètodes d'encriptació més coneguts

Després de definir algunes de les idees que va aportar Shannon a la teoria de la informació, passem a explicar els algoritmes més emprats per tal d'encriptar els missatges. L'Institut Nacional d'Estàndards i Tecnologia (NIST)[1] conté alguns dels protocols estàndards que es fan servir actualment per a la encriptació de missatges.

Recordem que tractem els missatges com successions de bits ja que és així com es fan les comunicacions digitals avui dia. Per tal d'escriure un missatge en forma de cadena de bits, hi ha moltes codificacions possibles però, per raons de simplicitat, suposarem que fem servir els 128 caràcters imprimibles de la codificació ASCII. A més, el missatge s'acostuma a enviar envoltat de soroll o bits aleatoris per tal de complicar encara més la tasca de desxifratge per part d'un tercer. Aquest és un dels motius que justifica la necessitat de generar nombres de forma aleatòria que explicarem més endavant.

Els mètodes d'encriptació es poden dividir en simètrics i asimètrics. Els primers permeten obtenir fàcilment la clau de desencriptació a partir de la d'encriptació mentre que en els segons hi ha una dificultat considerable en aconseguir aquesta segona clau. Actualment, hi ha moltes maneres força segures d'encriptar missatges, com el DES, el RSA, el Merkle-Hellman Knapsack, el McEliece, ElGamal, el Chor-Rivest, etc. En aquesta secció, farem una descripció breu del **DES** (*Data Encryption Standard*), del **RSA** (inicials dels seus creadors, Rivest, Shamir i Adleman) i del **xifrat de Vernam**, demostrant que aquest últim té la propietat de secret perfecte.

2.1 Data Encryption Standard (DES)

El 15 de maig del 1973, el NIST va publicar el primer esboç del DES, que seria una modificació del LUCIFER, un sistema emprat anteriorment. Aquest algoritme va ser desenvolupat a l'IBM i va ser publicat el 17 de març del 1975 al Registre Federal. Després de molta discussió, va ser adoptat com a sistema d'encriptació per a aplicacions 'no classificades'. Per trobar una descripció completa de l'estàndard del DES, cal recórrer al FIBS [6].

2.1.1 L'algoritme

A continuació donarem una descripció de l'algoritme però sense entrar en detalls massa tècnics. El criptosistema DES està format pels conjunts següents:

$$\mathcal{P} = (\mathbb{Z}/2\mathbb{Z})^{64}, \quad \mathcal{K} = (\mathbb{Z}/2\mathbb{Z})^{56}, \quad \mathcal{C} = (\mathbb{Z}/2\mathbb{Z})^{64}.$$

De fet, cada clau consta de 56 bits efectius i 8 bits més de paritat. A continuació definim la funció $e_K : (\mathbb{Z}/2\mathbb{Z})^{64} \longrightarrow (\mathbb{Z}/2\mathbb{Z})^{64}$.

[1] https://csrc.nist.gov/

1. Donat un missatge pla x, es permuten els seus bits seguint una permutació IP i s'obté un nou missatge x_0. Escriurem $x_0 = IP(x) = L_0R_0$, on L_0 comprèn els primers 32 bits i R_0 els 32 restants.

2. Es fan 16 iteracions d'una determinada funció i es computa L_iR_i de la manera següent. $\forall 1 \leq i \leq 16$,
$$L_i = R_{i-1},$$
$$R_i = L_{i-1} \oplus f(R_{i-1}, K_i).$$
El símbol $\oplus$ indica la suma mitjançant una operació XOR i la funció f serà definida més endavant. Els K_i són permutacions de 48 bits que depenen de la clau inicial K.

3. S'aplica la permutació inversa IP^{-1} a $R_{16}L_{16}$ i s'obté el missatge xifrat y.

La funció f pren com a primer argument una cadena de 32 bits ($A := R_{i-1}$) i com a segon, una cadena de 48 bits ($B := K_i$) per cada i. A partir d'aquests, produeix una nova cadena de 32 bits mitjançant els passos següents:

1- El primer argument s'expandeix a una cadena de 48 bits seguint una *funció d'expansió* E. $E(A)$ consisteix de 32 bits del primer argument, permutats d'alguna manera, i 16 bits més que són repetits dels anteriors.

2- Es computa $E(A) \oplus B$ i s'escriu el resultat com a concatenació de vuit cadenes de 6 bits $B = B_1B_2 \cdots B_8$.

3- El següent pas requereix 8 **capses S** $S_1, \ldots, S_8$. Cada S_i es una matriu fixada 4×16 formada per enters entre 0 i 15. Es calcula C_j en funció de S_j i B_j i s'obté una nova cadena $C = C_1 \cdots C_8$.

4- Per acabar, es permuta la cadena C seguint una permutació fixada P. El resultat és el que es defineix com $f(A, B)$.

Finalment, el procés de desxifratge d_K fa servir el mateix algoritme però les subclaus K_i s'agafen de manera inversa.

2.1.2 Seguretat

Quan el DES va ser proposat com un estàndard, va haver-hi molta controvèrsia. En primer lloc, tots els càlculs que es duen a terme són lineals a excepció dels que tenen a veure amb les capses S i aquests càlculs són vitals per a la seguretat de l'algoritme. És cert que hi ha una sèrie de propietats que les capses S han de satisfer però no se sap exactament com el NIST va dissenyar aquestes capses i això no va fer més que augmentar les sospites de què hi hagués *trapes* o maneres de trencar aquest sistema.

Conspiracions a part, el punt més feble del DES és que l'espai de claus té 2^{56} elements, molt petit donada la capacitat de la tecnologia actual. De fet, moltes

màquines han sigut especialment dissenyades per trobar la clau de l'algoritme un cop conegut tant el text xifrat com el text pla, fet que permetria el desxifratge de més textos que fossin encriptats amb aquesta mateixa clau.

Més concretament, Michael Wiener va detallar l'any 93 com s'hauria de fer tal màquina per trencar l'algoritme: contindria xips capaços de fer 16 proves simultàniament amb un preu 10.50$ per xip. D'aquesta manera, amb 100.000$ podríem trobar la clau en 1.5 dies de mitjana i amb 1.000.000$ es podria arribar a reduir a 3.5 hores. Per tal d'evitar-ho, s'acostuma a fer servir en comunicacions més segures el **TripleDES** que no és més que el mateix algoritme aplicat tres cops. Això permet engrandir l'espai de claus a $(\mathbb{Z}/2\mathbb{Z})^{168}$ si s'escullen tres claus independents per a cada pas de l'algoritme. Si enlloc de 16 rondes d'encriptació féssim servir un nombre menor, el missatge pla podria ser extret en qüestió d'hores pel mètode de la *criptoanàlisi diferencial* [7] en un ordinador qualsevol.

2.2 RSA

En el criptosistema anterior, l'emissor i el receptor es posen d'acord en una clau K que permet definir una forma d'encriptació e_K i una de desencriptació d_K. Normalment, un cop coneguda e_K és fàcil determinar d_K de manera que l'exposició d'una de les dues fa que el sistema sigui insegur. Aquest tipus de criptosistema s'anomena de **clau privada**. Aquesta mena de comunicació requereix que els dos interlocutors hagin de posar-se d'acord en la clau K mitjançant un canal segur però això, en la pràctica, pot no ser senzill.

La idea darrere dels criptosistemes de **clau pública** és trobar la forma de fer que, coneguda e_K, sigui pràcticament impossible determinar d_K. Així doncs, si el receptor fa pública la forma e_K i l'emissor la fa servir, com que el receptor serà l'únic que podrà saber d_K, només ell podrà desencriptar el missatge.

Els pioners en aquest tipus de criptosistemes van ser *Diffie* i *Hellman* l'any 1976 i el primer sistema de clau pública es va realitzar un any després per *Rivest*, *Shamir* i *Adelman*; el RSA, que explicarem a continuació.

La propietat que ha de satisfer e_K per garantir una bona seguretat és que sigui *unidireccional*, és a dir, que sigui fàcil d'aplicar però difícil d'invertir (és a dir, que d_K sigui difícil de trobar). A més, tampoc ha de ser computacionalment difícil de calcular perquè el receptor voldrà desxifrar el missatge ràpidament així que cal que tingui alguna mena de trapa. Abans de descriure l'algoritme, recordem el resultat següent.

Teorema 2.1. (Teorema xinès del residu). *Siguin $m_1, \ldots, m_r$ enters positius coprimers dos a dos i $a_1, \ldots, a_r$ enters qualssevol. Aleshores, el sistema de r congruències $x \equiv a_i \ mod\ m_i$, on $1 \leq i \leq r$, té solució única mòdul $M = m_1 \times \cdots \times m_r$ donada per*

$$x = \sum_{i=1}^{r} a_i M_i y_i \ \ mod \ \ M,$$

on $M_i = M/m_i$ i $y_i = M_i^{-1} \ mod\ m_i$ per a cada $1 \leq i \leq r$.$\square$

2.3 L'algoritme RSA

Ara estem en millors condicions de definir l'algoritme que implementa el RSA. Siguin n, m_1, $m_2 \in \mathbb{N}$ tals que $m_1 < n < m_2$, definim els conjunts següents:

$$\begin{aligned}\mathcal{P} &= \{x \in \mathbb{N} : 0 \leq x < 2^{m_1}\},\\ \mathcal{C} &= \{x \in \mathbb{N} : 0 \leq x < 2^{m_2}\},\\ \mathcal{K} = \{(n,a,b) : n = pq,\ \ &p,q\ primers,\ \ p \neq q,\ \ 2^{m_1} < n < 2^{m_2},\\ &ab \equiv 1\ \ (mod\ mcm(p-1,q-1))\}.\end{aligned}$$

Si ara considerem $K = K(n,a,b) \in \mathcal{K}$, $x \in \mathcal{P}$ i $y \in \mathcal{C}$, es defineixen les formes

$$e_K : \mathcal{P} \xhookrightarrow{i_{\mathcal{P}}} \mathbb{Z}/n\mathbb{Z} \xrightarrow{\widehat{e_K}} \mathbb{Z}/n\mathbb{Z} \xhookrightarrow{i_{\mathcal{C}}} \mathcal{C},$$

on $i_{\mathcal{P}}$ és la reducció d'un element $x \in \mathcal{P}$ en $\mathbb{Z}/n\mathbb{Z}$, $i_{\mathcal{C}}$ és la inclusió d'un element de $\mathbb{Z}/n\mathbb{Z}$ en $\mathcal{C}$ que s'obté en prendre com a conjunt de representants de $\mathbb{Z}/n\mathbb{Z}$ el conjunt $\{x \in \mathbb{N} : 0 \leq x \leq n\}$, i

$$\widehat{e_K}(x) = x^b \mod n.$$

Anàlogament,

$$d_K : \mathcal{C} \xrightarrow{\pi_{\mathcal{C}}} \mathbb{Z}/n\mathbb{Z} \xrightarrow{\widehat{d_K}} \mathbb{Z}/n\mathbb{Z} \xrightarrow{\pi_{\mathcal{P}}} \mathcal{P}$$

on $\pi_{\mathcal{C}}$ és la projecció d'un element $y \in \mathcal{C}$ en $\mathbb{Z}/n\mathbb{Z}$ (reducció mòdul n); $\pi_{\mathcal{P}}$ és l'aplicació que s'obté en prendre representats de $\mathbb{Z}/n\mathbb{Z}$ en el conjunt definit com $\{x \in \mathbb{N} : 0 \leq x \leq n\}$ i reduir mòdul 2^{m_2}, i

$$\widehat{d_K}(y) = y^a \mod n.$$

Els valors n i b són públics mentre que p, q i a són secrets. A continuació, demostrem que, efectivament, $(\pi_{\mathcal{P}} \circ \widehat{d_K} \circ \pi_{\mathcal{C}} \circ i_{\mathcal{C}} \circ \widehat{e_K} \circ i_{\mathcal{P}})(x) = x\ \forall x \in \mathcal{P}$.

En primer lloc, notem que si s'inclou un element $x \in \mathbb{Z}/n\mathbb{Z}$ en $\mathcal{C}$ mitjançant $i_{\mathcal{C}}$ i posteriorment es projecta de nou en $\mathbb{Z}/n\mathbb{Z}$ mitjançant $\pi_{\mathcal{C}}$, es retrobarà el mateix x ja que $n < m_2$. Això implica que $\pi_{\mathcal{C}}(i_{\mathcal{C}}(x)) = x$.

Anàlogament, incloure un element $x \in \mathcal{P}$ en $\mathbb{Z}/n\mathbb{Z}$ mitjançant $i_{\mathcal{P}}$ i posteriorment projectar-lo en $\mathcal{P}$ fent servir $\pi_{\mathcal{P}}$ torna a donar a la identitat perquè $m_1 < n$. Això implica que $\pi_{\mathcal{P}}(i_{\mathcal{P}}(x)) = x$.

Si demostrarem que $\widehat{d_K}(\widehat{e_K}(x)) = x$, fent servir els resultats anteriors podrem provar que, per composició, $d_K(e_K)(x) = x$.

Per hipòtesi, sabem que $ab \equiv 1\ mod(mcm(p-1,q-1))$, això implica que

$$\begin{cases} ab = \mu(p-1)+1 \\ ab = \lambda(q-1)+1 \end{cases}$$

per a alguns μ, $\lambda \in \mathbb{N}$.

Ara, si $x \in \mathbb{Z}/n\mathbb{Z}$ i fent servir el *petit teorema de Fermat* tenim que

$$x \equiv 0 \mod p \Longrightarrow x^{ab} \equiv 0 \mod p \Longrightarrow x^{ab} \equiv 0 \equiv x \mod p$$

i si

$$x \not\equiv 0 \mod p \Longrightarrow x^{p-1} \equiv 1 \mod p \Longrightarrow x^{ab} = x^{\mu(p-1)+1} = (x^{p-1})^{\mu} \cdot x \equiv x \mod p.$$

Anàlogament per a q. Ajuntant els dos resultats i emprant el teorema xinès del residu, deduïm que, en qualsevol cas,

$$x^{ab} \equiv x \mod pq \Longrightarrow x^{ab} \equiv x \mod n. \square$$

Cal remarcar el fet què, fixat un n i una clau K, qualsevol missatge $x \in \mathcal{P}$ pot ser xifrat de forma unívoca mitjançant l'aplicació e_K i posteriorment desxifrat amb d_K. Notem, però, que els missatges xifrats 1 i $n+1$, de $\mathcal{C}$, satisfaran que $d_K(1) = d_K(n+1)$, però $n+1$ no podrà ser mai un missatge xifrat perquè és major que n i per tant no es pot obtenir a partir d'una inclusió de $\mathbb{Z}/n\mathbb{Z}$ en $\mathcal{C}$.

En les comunicacions actuals, s'acostuma a agafar claus de 1024, 2048 o fins i tot 4096 bits. Per aquest motiu, els nombres m_1 i m_2 es prenen normalment d'aquest ordre si es vol tenir un nivell raonable de seguretat.

2.3.1 Exponenciació binària

Per tal de fer servir aquestes formes d'encriptació amb un cert grau de seguretat computacional, cal un mètode que permeti elevar un nombre molt gran a un altre també molt alt de forma eficient i ràpida. Un d'aquests mètodes és l'anomenat exponenciació binària.

Suposem que volem calcular $a^b \mod c$ amb a, b, $c \in \mathbb{N}$ i tal que $b = (b_n b_{n-1} \cdots b_0)_2$ és la seva representació binària amb b_n el primer digit de valor 1. Comencem amb $x_n = a$ i per cada b_i, amb $i = n-1, n-2, \ldots, 0$, calculem

$$y_i = x_{i+1}^2, \quad \begin{cases} x_i = y_i \mod c & si \ \ b_i = 0 \\ x_i = a \cdot y_i \mod c & si \ \ b_i = 1 \end{cases}$$

Es pot veure que $a^b \mod c = x_0$. Efectivament,

$$a^b = a^{\sum_i b_i 2^i} = a^{b_0}\left[a^{b_1}\left[a^{b_2}...[a^{b_n}]^2...\right]^2\right]^2. \square$$

Començant per $a^{b_n} = a = x_n$ l'algoritme segueix la descomposició anterior en producte de potències. Aquest algoritme redueix el nombre d'operacions de b multiplicacions a un màxim de $2log_2(b)$ multiplicacions i $log_2(b)$ divisions en el pitjor dels casos (quan tots els $b_i = 1$).

Exemple 2.2. Suposem que volem calcular $122^{273} \mod 62$. Tot i no ser un nombre excessivament gran, fer un càlcul amb el mètode convencional d'aquest valor necessitaria de 273 multiplicacions. Pel mètode descrit anteriorment, calculem $273 = (100010001)_2$ i per tant, amb $x_8 = 122$,

$$\begin{cases} y_7 = 14884 & x_7 = 14884 \mod 62 \equiv 4 \\ y_6 = 16 & x_6 = 16 \mod 62 \equiv 16 \\ y_5 = 256 & x_5 = 256 \mod 62 \equiv 8 \\ y_4 = 64 & x_4 = 64 \cdot 122 \mod 62 \equiv 58 \\ y_3 = 3364 & x_3 = 3364 \mod 62 \equiv 16 \\ y_2 = 256 & x_2 = 256 \mod 62 \equiv 8 \\ y_1 = 64 & x_1 = 64 \mod 62 \equiv 2 \\ y_0 = 4 & x_0 = 4 \cdot 122 \mod 62 \equiv 54. \end{cases}$$

Per tant, $122^{273} \mod 62 \equiv 54$ després de fer només 18 operacions en total.

2.3.2 Seguretat

La seguretat del criptosistema RSA rau en la dificultat en descompondre n com a producte de p i q i per això és de vital importància agafar aquests dos nombres suficientment grans. Un cop feta aquesta descomposició, es podria calcular $mcm[(p-1),(q-1)]$ i finalment trobar el valor a amb l'*algoritme d'Euclides*. La descomposició d'un enter molt gran en dos factors primers és una operació que pot ser computacionalment molt complicada i per garantir una bona seguretat els algoritmes actuals empren normalment un n de 4096 bits.

Per construir primers molt grans es pot agafar un nombre primer conegut m i un altre nombre no primer de descomposició factorial coneguda k i es comprova si el nombre $2mk + 1$ és primer amb certificats o tests de primeritat. Si no ho és, anem variant k fins que ho sigui. Una descripció més detallada del mètode i la seva prova de funcionament es pot trobar a [8].

2.4 Xifrat de Vernam

Com hem comentat anteriorment, aquest és l'únic mètode de xifratge útil per al qual s'ha demostrat, a dia d'avui, que té la propietat de secret perfecte. Funciona de la manera següent.

Sigui n la llargada del missatge que es vol transmetre i prenem $\mathcal{P} = \mathcal{C} = \mathcal{K} = (\mathbb{Z}/2\mathbb{Z})^n$. Sigui $x = x_1 \dots x_n$ el missatge que es vol transmetre, on cada $x_i \in \{0,1\}$, $1 \leq i \leq n$, i $K = K_1 \dots K_n$ la clau escollida, on $K_i \in \{0,1\}$, $1 \leq i \leq n$ aleshores,

$$e_K(x) = (x_1 + K_1, \ldots, x_n + K_n) \ mod\, 2.$$

Si $y = y_1 \ldots y_n$ és el text xifrat, aleshores

$$d_K(y) = (y_1 + K_1, \ldots, y_n + K_n) \ mod\, 2.$$

Exemple 2.3. Imaginem que volem encriptar la paraula *Llibre* amb la clau *cADIra*. Per fer-ho, escrivim les dues paraules en la seva codificació ASCII i apliquem l'algoritme anterior.

	01001100	01101100	01101001	01100010	01110010	01100011
+	01100011	01000001	01000100	01001001	01110010	01100001
	00101111	00101101	00101101	00101011	00000000	00000010

Obtenim així el text xifrat $y = / - - + 0\ 2$. Per retrobar el text pla original només caldria sumar-li de nou la clau K.

Aquest xifrat tan senzill és l'únic que s'ha demostrat ser secret perfecte si la clau és escollida de forma aleatòria. La demostració ve a continuació i es deu a Claude Shannon entre els anys 1940 i 1945.

Teorema 2.4. *Sigui* $(\mathcal{P}, \mathcal{C}, \mathcal{K}, \mathcal{E}, \mathcal{D})$ *un criptosistema on* $|\mathcal{K}| = |\mathcal{C}| = |\mathcal{P}|$. *Aleshores el criptosistema és de secret perfecte si i només si cada clau és emprada amb la mateixa probabilitat* $1/|\mathcal{K}|$ *i si per a cada* $x \in \mathcal{P}$ *i per a cada* $y \in \mathcal{C}$ *hi ha una única clau* K *tal que* $e_K(x) = y$.

Demostració:

$\Rightarrow$ Suposem que el criptosistema té la propietat de secret perfecte. Com hem vist en la proposició 1.8, per a cada $x \in \mathcal{P}$ i $y \in \mathcal{C}$ hi ha com a mínim una clau K tal que $e_K(x) = y$ així que

$$|\mathcal{C}| = |\{e_K(x) : K \in \mathcal{K}\}| \leq |\mathcal{K}|.$$

Però estem assumint $|\mathcal{C}| = |\mathcal{K}|$ i per tant s'ha de satisfer que

$$|\{e_K(x) : K \in \mathcal{K}\}| = |\mathcal{K}|.$$

Aleshores no existeixen dues claus diferents K_1 i K_2 tals que $e_{K_1}(x) = e_{K_2}(x) = y$. En definitiva, per cada $x \in \mathcal{P}$ i per cada $y \in \mathcal{C}$ hi ha una única clau K tal que $e_K(x) = y$.

Ara, denotem $n = |\mathcal{K}|$ i $\mathcal{P} = \{x_i : 1 \leq i \leq n\}$. Fixat un $y \in \mathcal{C}$, anomenem les claus $K_1 \ldots K_n$ de manera que $e_{K_i}(x_i) = y$. Emprant el Teorema de Bayes,

$$p_{\mathcal{P}}(x_i|y) = \frac{p_{\mathcal{C}}(y|x_i)p_{\mathcal{P}}(x_i)}{p_{\mathcal{C}}(y)} = \frac{p_{\mathcal{K}}(K_i)p_{\mathcal{P}}(x_i)}{p_{\mathcal{C}}(y)}.$$

Si ara recordem la condició de secret perfecte, $p_{\mathcal{P}}(x_i|y) = p_{\mathcal{P}}(x_i)$, s'ha de satisfer que $p_{\mathcal{K}}(K_i) = p_{\mathcal{C}}(y)$ per cada $1 \leq i \leq n$ de manera que cada clau és equiprobable i aquesta probabilitat és, efectivament, $1/|\mathcal{K}|$.

$\Leftarrow$ Ara, suposem que cada clau s'empra equiprobablement i que per a cada $x \in \mathcal{P}$ i per a cada $y \in \mathcal{C}$ hi ha una única clau K tal que $e_K(x) = y$. Recordem que $e_K(x) = y + K \mod 2$ i que $\mathcal{C} = \mathcal{P} = \mathcal{K} = (\mathbb{Z}/2\mathbb{Z})^n$. Aleshores si $y \in \mathcal{C}$, pel lema 1.6,

$$\begin{aligned} p_{\mathcal{C}}(y) &= \sum_{K \in \mathcal{K}} p_{\mathcal{K}}(K) p_{\mathcal{P}}(d_K(y)) \\ &= \sum_{K \in \mathcal{K}} \frac{1}{|\mathcal{K}|} p_{\mathcal{P}}(y - K) \\ &= \frac{1}{|\mathcal{K}|} \sum_{K \in \mathcal{K}} p_{\mathcal{P}}(y - K). \end{aligned}$$

Ara, fixada la y, els possibles valors $y - K \mod 2$ per a totes les K que podem emprar coincideix amb tots els possibles missatges xifrats y (que coincideix amb tots els missatges plans possibles i amb totes les claus possibles). De manera que

$$\sum_{K \in \mathcal{K}} p_{\mathcal{P}}(y - K) = \sum_{y \in (\mathbb{Z}/2\mathbb{Z})^n} p_{\mathcal{P}}(y) = 1.$$

Per tant, $p_{\mathcal{C}}(y) = 1/|\mathcal{K}| \ \forall y \in \mathcal{C}$.

A més, com per a cada (x, y) l'única clau tal que $e_K(x) = y$ és $K = y - x \mod 2$, tenim que

$$p_{\mathcal{C}}(y|x) = p_{\mathcal{K}}(y - x \ \ mod\, 2) = \frac{1}{|\mathcal{K}|},$$

ja que cada clau és equiprobable per hipòtesi. Per tant, pel *Teorema de Bayes*,

$$p_{\mathcal{P}}(x|y) = \frac{p_{\mathcal{C}}(y|x) p_{\mathcal{P}}(x)}{p_{\mathcal{C}}(y)} = \frac{p_{\mathcal{P}}(x) \frac{1}{|\mathcal{K}|}}{\frac{1}{|\mathcal{K}|}} = p_{\mathcal{P}}(x). \square$$

Tal com volíem provar, si la clau és escollida aleatòriament, el xifrat de Vernam té la propietat de secret perfecte. És important fer ènfasi en què tenir la propietat de secret perfecte no implica que la comunicació sigui completament segura ja que, per exemple, sabent la clau prèviament la desencriptació del text seria trivial. A més, si es fer servir la mateixa clau per encriptar dos missatges diferents amb el xifrat de Vernam i coneguéssim un missatge pla i els altres dos xifrats, podríem retrobar el segon missatge pla sumant tots tres; és a dir,

$$(x_1 + K) + (x_2 + K) + x_1 \equiv x_2.$$

Per tant, és important que cada clau s'empri només una vegada per mantenir la seguretat en la comunicació. És per això que a aquest xifrat també se'l coneix com la *llibreta d'un sol ús*. L'inconvenient principal d'aquest xifrat és que la clau ha de tenir la mateixa llargada que el missatge que es vol transmetre.

Un punt molt important és el fet que la clau ha de ser aleatòria per tal de garantir la propietat de secret perfecte. Aquest motiu, juntament amb la pràctica comuna d'enviar soroll aleatori que envolti el missatge per tal de dificultar encara més la tasca de desxifratge, motiven la necessitat de generar nombres de forma aleatòria.

Ara apareixen dos nous problemes en l'horitzó que tractarem en les seccions següents; com generar nombres de forma aleatòria per tal de garantir la propietat de secret perfecte del xifrat de Vernam i com es posen d'acord els interlocutors en la clau que empraran per al xifratge a través d'un canal insegur de comunicació.

3 Aleatorietat

Amb tot el que hem vist fins ara, si aconseguim que els interlocutors es posin d'acord en una clau aleatòria i encriptin el missatge amb aquesta clau fent servir el xifrat de Vernam serà impossible, des del punt de vista matemàtic, que ningú pugui saber el contigut del missatge pla. Més endavant tractarem el problema de com es posen tots dos d'acord en utilitzar aquesta clau.

No és fàcil definir amb exactitud què és un nombre aleatori. De fet, al llarg de la història hi ha hagut molts intents de fer-ho i cap d'ells ha pogut proporcionar una definició d'aleatorietat que hagi posat d'acord a tota la comuntat científica. En aquesta secció donarem unes petites pinzellades d'alguns dels mètodes actuals per generar nombres de forma aleatòria i els tests que ens permeten determinar si aquests mètodes són prou fiables o no. En qualsevol cas, amb les tecnologies actuals es poden generar nombres de forma aleatòria amb facilitat i per tant aquest problema no és un punt crític dins el protocol de comunicació que volem establir.

3.1 Com generar nombres aleatoris

Tot i que hi ha molts algoritmes per fer-ho, tots es poden classificar en dos tipus; els *deterministes* i els *no deterministes*.

Els deterministes són aquells on el nombre resultant depèn d'una funció f i d'una condició inicial o *llavor* i per tant aquests no poden proporcionar nombres aleatoris ja que l'argument determina de forma única la funció. L'única manera de trobar nombres realment aleatoris és doncs a partir de mètodes no deterministes. Aquests s'obtenen a partir de mesures empíriques com llançar una moneda, un dau, el moviment del ratolí de l'ordinador, el soroll atmosfèric, etc. De fet, una de les millors formes és a partir de materials radioactius lligats a un comptador Geiger.

Una altra possible aproximació són els **generadors de nombres pseudoaleatoris** ($pRNG$): fórmules deterministes amb certes propietats matemàtiques que donen nombres que semblen generats aleatòriament. Com a exemples no trivials, considerem el *Linear feedback shift register* ($LFSR$) i el $Blum - Blum - Shub$ amb la finalitat d'obtenir una seqüència aleatòria de nombres naturals.

Definició 3.1. *Sigui $n, m, c_0, \ldots, c_{N-1}$ elements de $\mathbb{N}$ i s una llavor $(s_0, ..., s_{N-1})$ amb $s_i \in \mathbb{N}\ \forall\ 1 \leq i \leq n$; aleshores, es defineix l'algoritme LFSR $\forall\ n+1 \geq N$ com*

$$s_{n+1} = c_0 s_n + c_1 s_{n-1} + ... + c_{N-1} s_{n-(N-1)} \mod m,\ 0 \leq s_{n+1} < m.$$

Definició 3.2. *Siguin p i q dos nombres primers grans tals que $p,\ q \equiv 3 \mod 4$ i definim $m = pq$. Sigui $s_0 \in \mathbb{N}$ la llavor, amb l'algoritme Blum-Blum-Shub es calculen els termes de la successió com*

$$s_{n+1} \equiv s_n^2 \mod m,\ 0 \leq s_{n+1} < m.$$

En qualsevol cas, hauríem de reduir mòdul 2 cada nombre obtingut i construir així la nostra seqüència de bits. Altres algoritmes més senzills s'engloben dins dels

anomenats *LCG's* (de l'anglès, *Linear Congruential Generators*) o altres, de més complicats, són per exemple el *Arc4Random* o el *PCG*.

3.2 Tests d'aleatorietat

En aquesta secció ens centrarem en els tests d'aleatorietat que tenen la finalitat de comprovar si una seqüència de bits generada per algun dels mètodes anteriors és "suficientment aleatòria". Principalment, es divideixen en dos tipus, els empírics i els teòrics. Els primers es duen a terme sobre una seqüència en sí i no requereixen coneixement del RNG que s'ha emprat per a la seva construcció. Els segons són tests *a priori* i prenen com a argument l'estructura del RNG que generarà la seqüència corresponent. Com que volem comprovar si una seqüència és aleatòria o no sense importar de quin generador provingui, ens centrarem en els tests empírics.

3.2.1 Test de freqüències

Si una cadena de n bits ha sigut generada aleatòriament, és d'esperar que contingui aproximadament el mateix nombre de 0 que d'1s. Per a aquest test només cal comparar les freqüències dels dos valors i veure si s'apropen al valor esperat $\frac{1}{2}$.

3.2.2 Test de sèries

Seguint la idea del test anterior, també és esperable que les parelles de nombres successius siguin independents i estiguin uniformement distribuides; és a dir, que la $P(0,0) = P(0,1) = P(1,0) = P(1,1) = \frac{1}{4}$ on $P(i,j)$ denota la probabilitat que el bit j aparegui just després del bit i. Anàlogament, aquest test es pot extendre a successions de 3, 4 o més elements per tal d'aconseguir una prova més robusta.

$$P(i_1, i_2, ...i_m) = \frac{1}{2^m} \quad \forall\, 2 \leq m \ll n, \;\; m \in \mathbb{N}.$$

Com hem dit anteriorment, per a aquest treball ens interessen els nombres aleatoris per assegurar la hipòtesi d'aleatorietat en la clau quan fem servir el xifrat de Vernam. Aquests algoritmes ens proporcionen una manera senzilla de generació de nombres pseudoaleatoris però tenen un punt dèbil. Conegut el tipus de generador pseudoaleatori emprat, es pot fer un atac per força bruta de les llavors per tal d'obtenir posteriorment tota la clau. D'aquesta manera l'espai de claus possibles es redueix a l'espai de llavors possibles per a aquest pRNG i això facilita la tasca d'interceptar la comunicació si aquest espai no és excessivament gran.

En qualsevol cas, podem aplicar els mètodes no deterministes per generar nombres aleatoris i per tant prendre com a vàlida la hipòtesi d'aleatorietat en el xifrat de Vernam.

4 Enviament de claus de forma segura

El fet que les tecnologies actuals ens permetin generar nombres aleatoris amb facilitat i fiabilitat mitjançant mètodes no deterministes ens permet prendre com a certa la propietat de secret perfecte del xifrat de Vernam. Ara ens centrarem en com els dos interlocutors es posen d'acord en la clau a emprar a través d'un canal insegur de comunicació. En primer lloc, estudiarem els mètodes convencionals de predistribució de clau i els problemes que presenten a nivell de seguretat. Posteriorment, definirem uns conceptes previs de mecànica quàntica i explicarem com la distribució quàntica de claus soluciona les debilitats en termes de seguretat dels mètodes anteriors.

4.1 Predistribució de clau convencional

La majoria dels mètodes convencionals de predistribució de clau proporcionen una seguretat relativament bona contra atacs de missatge xifrat. Aquests tipus d'atacs, anomenats també atacs passius, consisteixen en què un tercer té accés al missatge xifrat i, sabent el tipus de xifratge emprat, intenta retrobar el missatge pla original. Un altre tipus d'atac molt més perillós és l'anomenat *man-in-the-middle* que consisteix en un agent actiu que se situa entre l'emissor i el receptor i té la capacitat de rebre i modificar la informació que s'estan enviant i fins i tot de fer-se passar per un d'ells.

Malauradament, els mètodes de predistribució de clau que s'empren avui dia són vulnerables a aquest atac. Això se soluciona mitjançant l'ús de **certificats**, un conjunt d'informació que permet assegurar que el missatge és enviat per l'emissor i no per cap man-in-the-middle. A més, l'ús de signatures digitals també proporciona un esglaó més de seguretat però avui dia tant uns com altres poden arribar a ser falsificats i per tant caldrà anar un pas més enllà si volem estar segurs que ningú interceptarà la clau per fer el xifratge. Com a exemples de mètodes convencionals de predistribució de clau, considerarem l'*esquema de Blom* i el *Diffie-Hellman*.

4.1.1 Esquema de Blom

En aquest apartat, suposarem que tenim una xarxa insegura de n usuaris i confiarem en una *autoritat de confiança* (AC) responsable d'identificar els usuaris i escollir i transmetre claus de forma segura. Aquest mètode està inclòs dins del que s'anomena esquema de compartició de secrets. Consisteix en distribuir un secret entre un grup de participants de manera que cada un d'ells té un tros d'aquest secret. El secret podrà ser reconstruït si un nombre suficient de participants es posa d'acord i comparteixen la informació de què disposen entre ells. Fent un símil amb la geometria euclidiana, si el secret és un punt i cada participant coneix un pla que conté aquest punt i tal que els plans no són paral·lels dos a dos, tres participants que comparteixin el seu pla podran calcular la intersecció i per tant saber el secret. En particular, l'esquema de Blom va ser introduït per Rolf Blom a principis dels anys vuitanta.

Suposem doncs que es vol compartir un secret (o una clau) $K \in \mathbb{Z}/p\mathbb{Z}$ entre una xarxa insegura de n usuaris $\{U_1, \ldots, U_n\}$, on $p \geq n$ i p primer. Sigui $k-1$, $1 \leq k \leq n-2$, el nombre màxim d'usuaris que es poden ajuntar sense poder saber la clau; és a dir, si k agents compartissin la informació de què disposen, haurien de poder determinar la clau K, però aquesta tasca no hauria de ser possible només per a $k-1$ usuaris. L'esquema de compartició del secret funciona de la manera següent.

1. L'AC escull n elements diferents no nuls de $\mathbb{Z}/p\mathbb{Z}$ que denotarem $x_1, \ldots, x_n$, i els fa públics.
2. L'AC escull aleatòriament $k-1$ elements de $\mathbb{Z}/p\mathbb{Z}$ que denotarem $a_1, \ldots, a_k$. A més a més, denotem $a_0 = K$.
3. L'AC computa $y_i = a(x_i)$ per a $1 \leq i \leq n$, on
$$a(x) = \sum_{j=0}^{k-1} a_j x^j \mod p.$$
4. L'AC dóna a cada usuari U_i l'element y_i.

En resum, l'autoritat de confiança construeix un polinomi en $\mathbb{Z}/p\mathbb{Z}[x]$ de coeficients aleatoris i grau $k-1$ on la clau a compartir és el terme independent. Posteriorment, cada participant obté un punt d'aquest polinomi (x_i, y_i). Ara cal verificar dues proposicions.

Proposició 4.1. *Qualsevol conjunt de k usuaris és capaç de reconstruir el polinomi i calcular el valor de K.*

Efectivament, suposem sense perdre generalitat que els usuaris $\{U_1, ...U_k\}$ volen trobar el secret K. Cada participant d'aquest conjunt coneix el seu propi $a(x_i) = y_i$ i ajuntaran tots els seus punts per plantejar i resoldre el sistema d'equacions següent.

$$\left\{ \begin{array}{c} a_0 + a_1x_1 + a_2x_1^2 + ... + a_{k-1}x_1^{k-1} = y_1, \\ a_0 + a_1x_2 + a_2x_2^2 + ... + a_{k-1}x_2^{k-1} = y_2, \\ \vdots \\ a_0 + a_1x_k + a_2x_k^2 + ... + a_{k-1}x_k^{k-1} = y_k. \end{array} \right\}$$

Aquest sistema es pot escriure en forma matricial com

$$\begin{pmatrix} 1 & x_1 & x_1^2 & \ldots & x_1^{k-1} \\ 1 & x_2 & x_2^2 & \ldots & x_2^{k-1} \\ \vdots & \vdots & \vdots & \vdots & \vdots \\ 1 & x_k & x_k^2 & \ldots & x_k^{k-1} \end{pmatrix} \begin{pmatrix} a_0 \\ a_1 \\ \vdots \\ a_k \end{pmatrix} = \begin{pmatrix} y_0 \\ y_1 \\ \vdots \\ y_k \end{pmatrix}.$$

La matriu de coeficients és una matriu de Vandermonde i el seu determinant és per tant

$$\prod_{1\leq i<j\leq k}(x_i - x_j) \mod p.$$

Com que els punts són diferents i no nuls ja que així han estat escollits per l'AC i estem en $\mathbb{Z}/p\mathbb{Z}$, el producte d'elements no nuls és no nul i per tant aquest determinant és diferent de zero. Això implica que la solució a aquest sistema és única i per tant que el polinomi $a(x)$ es pot reconstruir a partir de la informació de què disposen els k usuaris. En particular, hauran calculat $a_0 = a(0) = K$. □

Proposició 4.2. *Cap grup de $k-1$ usuaris pot saber, compartint només la informació de què disposen, la clau K.*

Demostració

Seguint la línea de la demostració anterior, ara els $k-1$ usuaris podran construir les $k-1$ equacions següents.

$$\left\{\begin{array}{c} a_0 + a_1x_1 + a_2x_1^2 + ... + a_{k-1}x_1^{k-1} = y_1, \\ a_0 + a_1x_2 + a_2x_2^2 + ... + a_{k-1}x_2^{k-1} = y_2, \\ \vdots \\ a_0 + a_1x_{k-1} + a_2x_{k-1}^2 + ... + a_{k-1}x_{k-1}^{k-1} = y_{k-1}. \end{array}\right\}$$

Ara, suposem que el secret K té el valor y_0 i , per tant, $K = a_0 = a(0)$. Afegim doncs l'equació

$$a_0 = y_0$$

al sistema anterior i retrobem un sistema de k equacions lineals i k incògnites. De nou, la matriu asociada al sistema és de Vandermonde i el determinant, pel mateix argument que abans, és no nul. Això implica que per a cada valor possible y_0 del secret K, hi ha un únic polinomi $a_{y_0}(x)$ tal que

$$y_i = a_{y_0}(x_i),$$

per a $1 \leq i \leq k-1$ i tal que

$$y_0 = a_{y_0}(0).$$

Per tant, qualsevol valor de $\mathbb{Z}/p\mathbb{Z}$ podria ser el secret que s'està compartint. Queda provat doncs que els $k-1$ usuaris no han obtingut cap informació sobre el secret □.

De fet, el sistema de Cramer de la demostració de 4.1 és equivalent a l'ús del mètode d'interpolació de Lagrange, que proporciona un polinomi de grau màxim $k-1$ si es disposa de k punts per on hi passa. D'aquesta manera, k usuaris poden reconstruir el polinomi $a(x)$ i calcular la clau $a(0)$.

Proposició 4.3. *Siguin $\{U_1, \ldots, U_k\}$ els usuaris que volen calcular el secret K de manera que cada usuari U_i disposa d'un punt (x_i, y_i) on $y_i = a(x_i)$ per $1 \leq i \leq n$, aleshores*

$$a(x) = \sum_{i=1}^{k} y_i \prod_{1 \leq j \leq k, j \neq i} \frac{x - x_j}{x_i - x_j}$$

i, a més,

$$K = a(0) = \sum_{i=1}^{k} y_i \prod_{1 \leq j \leq k, j \neq i} \frac{x_j}{x_j - x_i}.\square$$

4.1.2 Diffie-Hellman

A diferència de l'esquema de Blom, aquest esquema no entra dins de els mètodes de compartició de secrets ja que només permet l'acordament de la clau entre dos usuaris individuals. El mètode generalitzat de Diffie-Hellman considera un grup G escrit multiplicativament, un subgrup cíclic $F < G$ i dos usuaris U i V que volen posar-se d'acord en una clau $K_{U,V} \in F$. Per tal de fer-ho, es fa servir el protocol següent.

1. Es fa públic un generador $A \in F$ que s'emprarà com a element base per acordar la clau.
2. Posteriorment, U escull de forma privada un exponent natural α_U i V escull de forma privada un altre exponent natural α_V.
3. U envia l'element A^{α_U} a V i V envia l'element A^{α_V} a U.
4. U calcula $(A^{\alpha_V})^{\alpha_U}$ i V calcula $(A^{\alpha_U})^{\alpha_V}$ i aquest valor serà precisament la clau buscada. Efectivament, $(A^{\alpha_V})^{\alpha_U} = (A^{\alpha_U})^{\alpha_V} = K_{U,V}$.

El mètode original considera G com el grup $(\mathbb{Z}/p\mathbb{Z})^*$ dels elements invertibles de $(\mathbb{Z}/p\mathbb{Z})$ per a un primer p, gran. Suposem a partir d'ara que A és un element generador d'un subgrup $F :=< A >$ d'ordre gran i que tant A com p són de domini públic. Si U i V volen posar-se d'acord en una clau, faran servir el protocol següent.

1. U escull un valor $a_U \in \mathbb{N}$ i V escull un valor $a_V \in \mathbb{N}$ de forma secreta.
2. U calcula
$$b_U = A^{a_U} \ \ mod\, p$$
i li envia aquest valor a V per un canal públic.
3. V computa
$$K_{U,V} = A^{a_U a_V} \ \ mod\, p = b_U^{a_V} \ \ mod\, p$$
de manera que V ja té la clau.

4. V calcula
$$b_V = A^{a_V} \mod p$$
i li envia aquest valor a U per un canal públic.

5. V computa
$$K_{U,V} = A^{a_U a_V} \mod p = b_V^{a_U} \mod p$$
i obté també la clau desitjada.

A nivell d'atacs passius, la seguretat computacional d'aquest mètode queda determinada per la dificultat del problema del logaritme discret en el grup G. Per exemple si considerem el grup G com $(\mathbb{Z}/p\mathbb{Z}, +)$, la resolució d'aquest problema és trivial mentre que si fem servir el grup multiplicatiu $(\mathbb{Z}/p\mathbb{Z})^*$ per a p prou gran, la dificultat de resoldre l'equació $b = A^x \mod p$ augmenta considerablement. De fet, hi ha algoritmes que permeten resoldre el problema anterior en un temps proporcional a $\sqrt{p}$ (com *Baby-step, giant-step* o *Pohlig-Hellman*, per exemple) que és força millor que un atac per força bruta, que fa servir un temps proporcional a p.

Fem notar de nou que un dels contrapunts d'usar aquest algoritme és que si hi hagués un *man-in-the-middle* podria fer creure U i V que s'estan comunicant entre ells però en realitat cadascun podria estar compartint una clau diferent amb aquest tercer i per tant comunicant-se amb ell sense que ni U ni V ho sapigués.

4.2 Distribució quàntica de claus (QKD)

Aquest mètode alternatiu per a la distribució de clau es basa en l'enviament de fotons i la seva mesura posterior amb un polaritzador. A continuació repassarem uns quants conceptes sobre radiació electromagnètica i mecànica quàntica per tal d'acabar definint el protocol de comunicació i demostrar com és capaç de contrarestar tant els atacs passius com els actius. No es pretén donar una descripció detallada a nivell matemàtic dels conceptes de la mecànica quàntica involucrats en el protocol però explicarem els punts més importants.

El fotó és la partícula elemental d'espí 1 responsable de la interacció electromagnètica i l'encarregada de portar la radiació electromagnètica, abarcant totes les freqüències possibles des d'ones de radio fins als intensos raigs gamma. La freqüència no és un factor important en aquest protocol així que suposarem que es tracta de llum en el rang visible.

Suposant que el fotó es propaga en el buit en absència de càrregues i, considerant les *equacions de Maxwell*,

$$\vec{\nabla} \cdot \vec{E} = 0, \qquad \vec{\nabla} \cdot \vec{B} = 0,$$
$$\vec{\nabla} \times \vec{E} = -\frac{\partial \vec{B}}{\partial t}, \qquad \vec{\nabla} \times \vec{B} = \epsilon_0 \mu_0 \frac{\partial \vec{E}}{\partial t},$$

on $\vec{E}$ és el camp elèctric, $\vec{B}$ és el camp magnètic i ϵ_0 i μ_0 són la permeabilitat elèctrica i magnètica del buit, respectivament; el fotó es regeix per les equacions

$$\vec{E}(x,y,z,t) = \vec{E_0}\, cos(\vec{k}\cdot\vec{r} - wt + \phi),$$
$$\vec{B}(x,y,z,t) = \vec{B_0}\, cos(\vec{k}\cdot\vec{r} - wt),$$

on $\vec{k}$ és el vector d'ona, $\vec{r}$ el vector posició, w la freqüència angular i ϕ el desfasament entre les dues ones. En el nostre marc de treball, l'ona electromagnètica es propagarà al llarg de l'eix Z i ,per tant,

$$\vec{E}(z,t) = \vec{E_0}\, cos(k\cdot z - wt),$$
$$\vec{B}(z,t) = \vec{B_0}\, cos(k\cdot z - wt),$$

on per comoditat prenem $\phi = 0$. Recordem a més, que $|\vec{k}| = \frac{w}{c}$, on c és la velocitat de la llum, que és igual a $\frac{1}{\sqrt{\epsilon_0\mu_0}} \approx 3\cdot 10^8$ m/s.

Centrem-nos només en la part del camp elèctric perquè és la que mesurarem. Per fer la transmissió de fotons ens interessarà enviar la llum polaritzada linealment en una de les quatre direccions presentades a continuació. En mecànica quàntica, cadascuna d'aquestes direccions s'anomena estat i els representarem amb la notació de Dirac.

$$|0,+>:= E_0\, cos(k\cdot z - wt)\widehat{e_x}, \quad |1,+>:= E_0\, cos(k\cdot z - wt)\widehat{e_y},$$
$$|0,\times>:= E_0\, cos(k\cdot z - wt)\frac{\widehat{e_x}+\widehat{e_y}}{\sqrt{2}}, \quad |1,\times>:= E_0\, cos(k\cdot z - wt)\frac{\widehat{e_x}-\widehat{e_y}}{\sqrt{2}}.$$

De fet, el fotó podria oscil·lar al llarg de qualsevol direcció perpendicular a la direcció de propagació de l'ona així que aquests no són els únics estats possibles. Prenent coeficients en $\mathcal{B} = \{(z_1,z_2)\in\mathbb{C}\times\mathbb{C},\ |z_1|^2+|z_2|^2 = 1\}$, un estat qualsevol es podrà escriure tant com a combinació lineal de $\{|0,+>,|1,+>\}$ com de $\{|0,\times>,|1,\times>\}$ ja que aquests dos conjunts defineixen bases ortonormals + i $\times$, respectivament. Notem que els coeficients poden ser complexos; això només implica un desfasament entre els estats i no és important per al protocol de comunicació.

Exemple 4.4. Un possible estat d'un fotó seria

$$|\psi>= \frac{i}{\sqrt{2}}|1,+> -\frac{1}{\sqrt{2}}|0,+>\,.$$

4.3 La mesura

Un dels conceptes de la mecànica quàntica que juga un paper primordial en aquesta distribució de clau és la mesura de la polarització del fotó. En el nostre marc de treball, utilitzarem dos tipus de polaritzadors per fer la mesura, P_+ i $P_\times$. El primer només deixa passar la llum si està polaritzada al llarg de l'eix X o l'eix Y mentre que el segon només deixa passar la llum polaritzada 45º respecte els eixos anteriors. Amb els conceptes de la mecànica quàntica es pot demostrar que aquests polaritzadors

els podem entendre com dos operadors $P_+, P_\times : \mathcal{B} \longrightarrow \mathcal{B}$ que s'apliquen en les dues bases de la manera següent.

$$P_+(|0,+>) = |0,+>, \quad P_+(|1,+>) = |1,+>,$$

$$P_+(|0,\times>) = \left\{ \begin{array}{l} |0,+> \ \text{ amb probabilitat } \frac{1}{2} \\ \\ |1,+> \ \text{ amb probabilitat } \frac{1}{2} \end{array} \right\},$$

$$P_+(|1,\times>) = \left\{ \begin{array}{l} |0,+> \ \text{ amb probabilitat } \frac{1}{2} \\ \\ |1,+> \ \text{ amb probabilitat } \frac{1}{2} \end{array} \right\},$$

$$P_\times(|0,\times>) = |0,\times>, \quad P_\times(|1,\times>) = |1,\times>,$$

$$P_\times(|0,+>) = \left\{ \begin{array}{l} |0,\times> \ \text{ amb probabilitat } \frac{1}{2} \\ \\ |1,\times> \ \text{ amb probabilitat } \frac{1}{2} \end{array} \right\},$$

$$P_\times(|1,+>) = \left\{ \begin{array}{l} |0,\times> \ \text{ amb probabilitat } \frac{1}{2} \\ \\ |1,\times> \ \text{ amb probabilitat } \frac{1}{2} \end{array} \right\}.$$

Tot i que sembla contraintuïtiu pensar que la mesura d'una propietat física pot donar un resultat o un altre amb una certa probabilitat, això entra dins del paradigma de la mecànica quàntica on cal introduir termes probabilístics per tal entendre els resultats que s'obtenen.

4.4 Protocol BB84

Actualment es coneixen molts protocols per transmetre claus mitjançant QKD (E91, S09, S013...) però un dels més coneguts és el BB84 que es regeix segons els conceptes introduïts anteriorment. En primer lloc, entendrem per un *canal quàntic* un canal de comunicació que permet l'enviament de fotons des d'un emissor fins a un receptor. Suposem que l'emissor i el receptor es volen posar d'acord en una clau de n bits; per tal de fer-ho, l'emissor enviarà m fotons ($m > n$) al receptor a través d'un canal quàntic de la manera següent.

1. L'emissor escull, de forma aleatòria, una base i un estat per a cada fotó i els envia al receptor a través del canal quàntic. Fixant-nos només en el nombre de l'etiqueta dels estats i no en la seva base, això determina una cadena d'uns i zeros pròpia de l'emissor.

2. El receptor, també de forma aleatòria, escull una base (un polaritzador) per fer la mesura de cada fotó que li arriba i obté una nova cadena d'uns i zeros pròpia del receptor.

3. Posteriorment, tant l'emissor com el receptor fan públiques les bases que han fet servir per a cada fotó. La clau final vindrà determinada pels valors de la cadena d'uns i zeros del receptor i de l'emissor en les posicions dels fotons que hagin estat enviats i mesurats amb la mateixa base. A aquesta clau l'anomenarem la clau quàntica.

4. Emissor i receptor fan públic un petit tros d'aquesta clau quàntica per veure que efectivament coincideix. Això es fa per evitar atacs de *man-in-the-middle* com s'explicarà a continuació.

Cal doncs enviar un nombre de fotons superior a la llargada de la clau desitjada ja que, de mitjana, només seran vàlids la meitat dels fotons enviats. A més, imperfeccions del canal quàntic poden fer que alguns fotons es perdin pel camí i per això, en la pràctica, es recomana agafar $m > 2n$.

4.4.1 Seguretat

L'avantatge que presenta aquest protocol és que no pot ser interceptat per un *man-in-the-middle* de manera que aquest pugui fer servir la clau sense que ni receptor ni emissor se n'adonin. Si un tercer aconseguís posar-se a mig camí i volgués mesurar l'estat dels fotons, com no sap amb quina base han estat enviats, haurà d'escollir aleatòriament entre un dels dos operadors per fer la mesura de cada fotó. Si no escull el polaritzador adequat, modificarà l'estat del fotó. Quan hagi fet les mesures, envïi els fotons cap al receptor i aquest faci les corresponents noves mesures no notarà que hagi passat res. Posteriorment, quan emissor i receptor facin públiques les bases que han fet servir i exposin un petit tros de la clau quàntica, s'adonaran que en fotons on havien de coincidir en la mesura obtenen resultats contraris. Això serà degut doncs a la presència d'un *man-in-the-middle* i per tant aquesta clau no serà útil per fer una posterior encriptació del missatge.

Exemple 4.5. Suposem que l'emissor envia un fotó en estat 0 al receptor amb la base + i un tercer aconsegueix mesurar el seu estat però escull la base $\times$ per fer la mesura. La mecànica quàntica prediu que l'estat del fotó resultant serà o bé $|0, \times>$ o bé $|1, \times>$ amb probabilitat $\frac{1}{2}$. Posteriorment, envia el fotó resultant cap al receptor.

Si el receptor mesura l'estat del fotó amb la mateixa base que l'emissor, obtindrà un 1 o 0 amb probabilitat $\frac{1}{2}$. Suposem que, en aquest cas, la mesura dóna 1 com a resultat. A l'hora de fer la comprovació s'adonarien que aquest fotó, que en principi hauria de ser un 0, és un 1 i per tant arribaran a la conclusió que algú ha estat espiant i avortarien la comunicació.

Naturalment, és possible que el tercer tingui sort i esculli la base adequada per no modificar aquest fotó o bé que el receptor faci la mesura i, amb una probabilitat de $\frac{1}{2}$, obtingui el bit esperat. El que és molt poc probable és que això passi pels m bits enviats per m prou gran. De fet, si el tercer interceptés tots els fotons, la probabilitat que no modifqués la clau quàntica seria de $(\frac{1}{2})^m$. Avui dia s'empren

claus de l'ordre de com a mínim 256 bits i per tant aquesta probabilitat seria de l'ordre de 1 entre 10^{78}.

En la pràctica, les imperfeccions del canal poden donar lloc a petites discrepàncies en aquesta clau quàntica i, per aquest motiu, l'emissor i el receptor acceptaran un petit percentatge d'error en l'acord de la clau. Naturalment, faran servir només els bits on els resultats coincideixin.

A continuació, ens qüestionarem si un tercer té la capacitat de mesurar els fotons i tornar-los a enviar de la mateixa manera que els havia rebut, és a dir, sense alterar el seu estat. Això possibilitaria un atac per *man-in-the-middle* ja que el receptor rebria exactament els mateixos fotons que l'emissor ha enviat.

Teorema 4.6. *(Teorema de no-clonació, Wootters, Zurek i Dieks, 1982). No hi ha cap procediment que permeti clonar un estat quàntic arbitrari sense alterar l'original.*

Més concretament, suposem que tenim un fotó en un estat $|\alpha>$ desconegut i volem copiar aquest estat en un altre fotó que en principi està en un estat $|\beta>$ conegut. Per a tal fi, dissenyem un dispositiu capaç de fer-ho. En mecànica quàntica, les interaccions amb la matèria es tracten amb operadors hermítics U ($UU^\dagger = 1$) de manera que si

$$|\alpha>= a_1|\alpha_1> +a_2|\alpha_2>,$$

amb $(a_1, a_2) \in \mathcal{B}$, hem d'imposar que

$$U(|\alpha_i> \otimes\ |\beta>) = |\alpha_i> \otimes\ |\alpha_i> .$$

On $\otimes$ denota el producte tensorial. Això implica que hem de copiar cada component de l'estat. Si ho apliquem a l'estat complet,

$$U(|\alpha> \otimes\ |\beta>) = \sum_{i=1}^{2} a_i\ U(|\alpha_i> \otimes\ |\beta>) = \sum_{i=1}^{2} a_i\ (|\alpha_i> \otimes\ |\alpha_i>).$$

Fixem-nos que aquest estat obtingut no coincideix sempre amb $|\alpha> \otimes |\alpha>$.

$$|\alpha> \otimes\ |\alpha>= \sum_{i,j} a_i a_j (|\alpha_i> \otimes\ |\alpha_j>).$$

De fet, per a què aquests dos estats coincideixin, cal que algun $a_i = 0$ i l'altre $a_j = 1$ per a $i, j = 0, 1$, $i \neq j$; es a dir, la clonació només serà possible en aquells estats que no es modifiquin en fer la mesura. Per tant, si no s'escull el polaritzador correcte, es perd la informació sobre quin era l'estat del fotó anterior a la mesura. □

D'aquesta manera provem que, efectivament, aquesta distribució de clau no permet un atac per *man-in-the-middle*

4.4.2 Avenç tecnològic

Per acabar, a nivell tecnològic, s'han fet grans avenços per tal d'implantar aquest mètode. A Suïssa, l'empresa Swiss Quantum hi treballa desde fa anys i han aconseguit fabricar canals de fibra òptica de fins a 100km. El major problema que hi ha actualment és que no es pot aconseguir amplificar el senyal (pel teorema de no clonació) però tot i així alguns prototips han arribat als 250km i fins i tot seria possible construir una xarxa de manera que la comunicació no fos només unidireccional. Veurem si en el futur és possible aplicar aquesta tecnologia o si les seves limitacions impedeixen el seu avenç.

Conclusions

Aquesta memòria constitueix una introducció al món de la criptografia fent èmfasi en alguns dels mètodes de xifratge i de distribució de clau que s'empren avui dia. A més, incidim en la necessitat de generar nombres de manera aleatòria per garantir la seguretat en certs protocols de transmissió d'informació.

Al final del treball hem arribat a la conclusió que el xifrat de Vernam, que té la propietat de secret perfecte si s'empra una clau generada aleatòriament, juntament amb la distribució quàntica de claus, que permet l'acord de la clau sense permetre atacs passius o actius amb èxit, proporcionen un protocol de comunicació perfecte des del punt de vista matemàtic. Estudis posteriors podrien determinar la viabilitat d'aquest protocol a nivell computacional, tècnic i d'usabilitat.

Malauradament, la criptografia no és un tema present en les assignatures obligatòries del Grau de Matemàtiques i per això hem hagut de fer recerca en multitud de llibres, papers i altres recursos aliens a la facultat. També s'han consultat aplicacions d'ús corporatiu com Amazon, Cleopatra o llibreries de signatura digital i certificats per contrastar la informació de la literatura amb els recursos que s'empren a nivell d'usuari en les comunicacions digitals actuals.

Referències

[1] Shannon, C. E.: A mathematical theory of comunication, *The Bell System Technical Journal* (1949).

[2] Shannon, C. E.; Weaver, W.: The mathematical theory of comunication, *University of Illionis Press* (1963).

[3] Burkhardt, C; Leventhal J: Foundations of Quantum Physics, *Springer* (2008).

[4] Stinson, D:Cryptography, theory and practice, *CRC Press LLC* (1995).

[5] Sharma, M: Compression Using Huffman Coding, *IJCSNS International Journal of Computer Science and Network Security*, **10**, n.5 (2010).

[6] Daley, W, M; Kammer, R. G.: Data Encryption Standard, *FIBS PUB* **46**-3 (1999).

[7] Biham,E; Shamir, A: Differential Cryptanalysis of DES-like Cryptosystems, *Advances in Cryptology, Springer* (1990).

[8] Travesa, A.: Aritmètica, *Col·leció UB*, (1997).

[9] Tausworthe, R. C.: Random Numbers Generated by Linear Recurrence Modulo Two, *Jet Propulsion Laboratory, California Institute of Technology.*

[10] Stein, A; Teske, E: Optimized Baby Step-Giant Step Methods, *J. Ramanujan Math. Soc. 20, No.1* **1**-32 (2005).

[11] https://docs.aws.amazon.com/AmazonS3/latest/dev/serv-side-encryption.html