1. Introducció a la criptografia

En aquest capítol es presenten, d'una banda, els fonaments de la criptografia i, d'altra banda, es realitza un repàs històric de la criptografia premoderna.

Pel que fa als fonaments de la criptografia, descriurem els conceptes clau d'aquesta ciència, que farem servir al llarg del llibre per anar presentant les diferents tècniques que es fan servir en criptografia.

En relació amb el repàs històric, veurem com va sorgir la criptografia i quines tècniques es feien servir des dels seus orígens fins a l'inici de la criptografia moderna. La resta del llibre se centrarà precisament en descriure diversos aspectes de la criptografia moderna que, com veurem, ha evolucionat molt des de les seves arrels.

1.1 Conceptes bàsics

La **criptografia** és la ciència que estudia l'escriptura de secrets, amb l'objectiu d'ocultar el missatge que s'escriu.

Etimològicament, la paraula prové del grec i sorgeix de la unió de dos conceptes: *kryptós*, que vol dir secret i *graphein*, que vol dir escriptura. Els orígens de l'escriptura secreta es remunten a fa més de 4000 anys, però en aquells moments la criptografia es trobava lluny de considerar-se una ciència. A mig camí entre art i joc d'enigmes, civilitzacions com l'antic Egipte van desenvolupar els primers escrits on es transformava el missatge original. Es considera però que la criptografia com a ciència no va començar a desenvolupar-se fins a mitjans del segle XX, amb les contribucions realitzades per Claude E. Shannon.

La **criptoànalisi** és la ciència que se centra en trencar les tècniques que desenvolupa la criptografia, ja sigui per a descobrir el text amagat darrere un text xifrat o bé per a demostrar les febleses d'un determinat esquema criptogràfic.

Així doncs, la criptoanàlisi és indispensable per a l'avenç de la criptografia, ja que s'encarrega d'avaluar la seguretat dels criptosistemes que aquesta desenvolupa. Tot i que el mot criptoanàlisi és bastant recent, tenim constància d'una criptoanàlisis realitzada al segle IX per un matemàtic àrab, Al-Kindi.

El terme general **criptologia** es fa servir per englobar tant criptografia com criptoanàlisi.

En aquest llibre, ens centrarem en descriure les tècniques i algorismes que es fan servir per ocultar informació, és a dir, en la criptografia. Tot i així, en aquest capítol farem una petita introducció a la criptoanàlisi, per tal d'oferir unes nocions bàsiques dels models amb els quals s'avalua habitualment la seguretat dels esquemes criptogràfics.

Tradicionalment, la criptografia es basava únicament en protegir la **confidencialitat** dels missatges.

La **confidencialitat** és una propietat que garanteix que la informació no es fa pública a persones no autoritzades.

Els sistemes criptogràfics han evolucionat molt des dels seus orígens, i actualment poden oferir altres garanties, més enllà de la confidencialitat. Sovint, l'ús de la criptografia ens permet també garantir la integritat dels missatges o fins i tot el no-repudi.

La **integritat** és la propietat que garanteix que la informació no ha estat modificada.

Els sistemes que ofereixen integritat permeten detectar si hi ha hagut una modificació de la informació.

El **no-repudi** és la propietat que garanteix que l'autor d'una determinada acció no pugui negar haver-la realitzat.

Per tal de simplificar les explicacions, en criptografia es fan servir uns personatges ficticis, que acostumen a interpretar sempre els mateixos papers. Aquests personatges van ser creats per Ron

Rivest, Adi Shamir i Leonard Adleman, i el seu seu ús es troba molt extés.[1] L'Alice (A) i en Bob (B) són els dos personatges més populars i acostumen a ser dos usuaris que volen intercanviar algun missatge. L'Eve (E) és un atacant passiu, que pot escoltar les comunicacions entre l'Alice i en Bob, però no modificar-les. Mallory (M) és un atacant actiu, que pot escoltar les comunicacions entre l'Alice i en Bob, i també modificar el contingut de la transmissió.

Anem doncs a descriure l'escenari tradicional en què s'aplica la criptografia fent servir els personatges que acabem de presentar. En l'escenari bàsic, l'Alice vol enviar un missatge a en Bob a través d'un canal insegur. Com que el canal és insegur, l'Eve pot escoltar la comunicació entre l'Alice i en Bob. Amb aquest plantejament, l'Alice desitja enviar un missatge, m, a en Bob garantint-ne la confidencialitat. Per fer-ho l'Alice aplica un *algorisme de xifrat*, E, al text que vol enviar (anomenat *text en clar*) fent servir una determinada *clau*, k. El resultat d'aplicar l'algorisme de xifrat sobre el text en clar és el *text xifrat*, c, que és el que s'enviarà a través del canal insegur. En Bob, quan rebi el missatge xifrat, c, procedirà a aplicar un *algorisme de desxifrat*, D, al text xifrat fent servir la mateixa clau, k, obtenint el text en clar original, m. Per tal que l'esquema pugui aplicar-se, serà necessari doncs que l'Alice i en Bob disposin d'una clau compartida, k, que hauran hagut de comunicar-se anteriorment a través d'algun canal segur (potser fins i tot trobant-se físicament). L'Eve podrà recuperar el text xifrat de la comunicació c, però al no conéixer el valor de la clau, no serà capaç de recuperar-ne el text en clar corresponent.

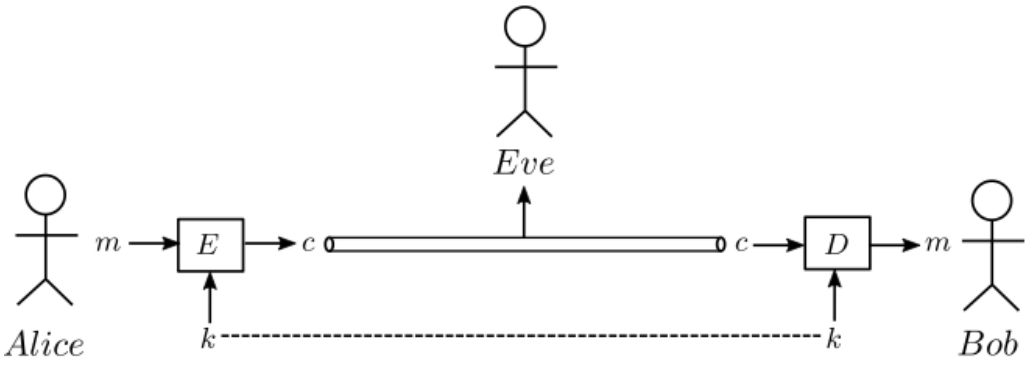

Figura 1.1: Escenari bàsic d'aplicació de la criptografia en les comunicacions entre dos usuaris.

Més formalment, direm que un criposistema queda definit per cinc paràmetres:

- El conjunt de possibles *textos en clar*, $\mathfrak{M}$
- El conjunt de possibles *textos xifrats*, $\mathfrak{C}$
- El conjunt de possibles *claus*, $\mathfrak{K}$
- E, una *funció de xifrat*, que detalla per a cada possible clau $k \in \mathfrak{K}$ i missatge $m \in \mathfrak{M}$, quin és el corresponent text xifrat $c \in \mathfrak{C}$.
- D, una *funció de desxifrat*, que realitza el procés invers de la funció de xifrat, és a dir, una funció tal que $D_k(E_k(m)) = m$, per a tot $m \in \mathfrak{M}$ i $k \in \mathfrak{K}$.

A partir d'aquest escenari bàsic, els escenaris en els quals s'aplica la criptografia avui en dia són molt diversos i variats, alguns dels quals no s'assemblen gens a l'escenari tradicional. Així, per exemple, la criptografia ens permet crear sistemes de credencials anònimes, que serviran per autenticar-se de manera anònima; sistemes de compartició de secrets, on caldrà la col·laboració d'n parts d'un conjunt d'm per recuperar el secret; criptomonedes, que oferiran mètodes de pagament

[1] Rivest, Shamir i Adleman van crear els personatges de l'Alice i en Bob a l'article "*A Method for Obtaining Digital Signatures and Public-Key Cryptosystems*", publicat l'any 1978.

totalment descentralitzats i segurs; i protocols de computació multipart, on diverses entitats podran col·laborar per calcular funcions sobre dades confidencials.

1.1.1 Introducció a la criptoanàlisi

La criptoanàlisi se centra en analitzar els criptosistemes, amb l'objectiu d'avaluar-ne la seva seguretat. Depenent de si l'anàlisi es focalitza en l'algorisme, la implementació o el sistema complet que l'integra, distingim diferents atacs que el criptoanalista pot intentar realitzar contra un esquema criptogràfic.

> Els **atacs clàssics** intenten recuperar un text en clar a partir d'un text xifrat o bé recuperar una clau.

Existeixen diferents escenaris o models en els quals avaluar els criptosistemes, en funció de la informació de la qual disposa el criptoanalista per trencar els esquemes:

- En el model de **només text xifrat** (o COA, de l'anglès, *ciphertext-only attack*) l'atacant només disposa d'un conjunt de textos xifrats.
- En el model de **text en clar conegut** (o KPA, de l'anglès, *known-plaintext attack*), l'atacant disposa d'un conjunt de textos en clar i els seus corresponents textos xifrats.
- En el model de **text en clar escollit** (o CPA, de l'anglès, *chosen-plaintext attack*), el criptoanalista pot obtenir els textos xifrats corresponents a un conjunt de textos en clar seleccionats per ell mateix.
- En el model de **text xifrat escollit** (o CCA, de l'anglès, *chosen-ciphertext attack*), el criptoanalista pot obtenir els textos en clar corresponents a un conjunt de textos xifrats seleccionats per ell mateix.

Els models de text en clar i text xifrat escollit assumeixen normalment que el criptoanalista tria una única vegada el conjunt de textos en clar (respectivament, textos xifrats) i pot demanar-ne els corresponents textos xifrats (respectivament, en clar). Una variant d'aquests models, coneguda com a model **adaptatiu** de text en clar/xifrat escollit (respectivament, CPA2 i CCA2), permet al criptoanalista anar demanant els corresponents textos xifrats/en clar successivament, modificant els textos que demana en funció de les respostes que ha rebut fins al moment.

Avui en dia gairebé tots els criptogràfs assumeixen el principi de Kerckhoffs:

> El principi de **Kerckhoffs** afirma que, per a què un criptosistema pugui considerar-se segur, aquest ho ha de ser encara que l'atacant conegui tots els detalls del criptosistema, exceptuant-ne la clau.

És a dir, s'assumeix que l'atacant o el criptoanalista disposa de l'especificació completa de l'algorisme a trencar. Auguste Kerchoffs va formular aquest principi al segle XIX, i actualment, la versió més extesa del seu principi afirma que la seguretat d'un criptosistema ha de dependre únicament de la clau.

Tot i això, en productes criptogràfics comercials sovint es fa cas omís d'aquest principi i s'opta

per l'alternativa, la seguretat per ofuscació (en anglès, *security through obscurity*). En aquest paradigma, la seguretat dels sistemes es basa en amagar els detalls sobre l'algorisme de xifrat, amb l'objectiu de dificultar-ne, suposadament, la criptoanàlisi. A la pràctica, però, normalment aquests detalls s'acaben fent públics igualment, de manera que amagar l'algorisme és contraproduent ja que únicament en dificulta l'avaluació de la seva seguretat. Alguns exemples de l'adopció d'aquest paradigma són en els algorismes xifrat de telefonia mòbil GSM, que es van intentar mantenir ocults sense èxit, o en el sistema de DRM dels DVDs, on calia pagar una llicència i signar un acord de no revel·lació per tal de tenir accés als detalls de l'algorisme.

Més enllà dels atacs clàssics, que consideren únicament l'algorisme utilitzat, existeixen també atacs de canal lateral i atacs d'enginyeria social.

> Els **atacs de canal lateral** (en anglès, *side-channel attacks*) es basen en atacar un criptosistema a través d'informació extreta d'una implementació física.

Hi ha diferents classes d'atacs de canal lateral, depenent de la informació que s'extreu de la implementació per a realitzar l'atac. Així, els atacs de sincronització (en anglès, *timing attacks*) analitzen el temps que es tarda en realitzar diferents càlculs; els atacs de monitoreig d'energia estudien el consum energètic que té el dispositiu durant l'operació; el atacs electromagnètics mesuren les fugues de radiació electromagnètica; els atacs acústics tenen en compte el so que es produeix al realitzar els càlculs, etc.[2]

Més enllà dels atacs als algorismes i a les implementacions dels criptosistemes, els sistemes d'informació en general són susceptibles també de patir atacs d'enginyeria social.

> Els **atacs d'enginyeria social** es basen en manipular als usuaris d'un sistema per tal d'obtenir informació que ens permeti trencar-ne la seguretat.

Així, els atacs d'enginyeria social es realitzent interactuant amb els usuaris, i sovint inclouen l'engany d'aquests per tal d'obtenir dades confidencials. Per exemple, un atacant pot intentar trucar a un usuari, fent-se passar per un tècnic informàtic i sol·licitant la clau de xifratge per tal de realitzar, suposadament, alguna comprovació. Evidentment, la criptografia poc té a fer amb aquests tipus d'atacs i, per aquest motiu, són dels més estesos i dels més perillosos.

1.2 Una mica d'història

Es diu que la història de la criptologia[3] comença l'any 1900 abans de Crist, amb uns escrits realitzats a la tomba de Khnumhotep II, un monarca de l'Alt Egipte. Als escrits trobats a la tomba s'hi troben alguns jeroglífics inusuals, que l'escribà va escriure enlloc d'altres més comuns, suposadament amb l'objectiu de dignificar el text. Tot i que en aquest cas no hi havia intenció d'ocultar el missatge, els escrits suposen el primer cas en la història on hi havia una tranformació deliverada del text que

[2] Per a un exemple concret d'atac de monitoreig d'energia al criptosistema RSA podeu consultar el Capítol 7 del llibre *Understanding cryptography*, de C. Paar i J. Pelzl.

[3] Una lectura recomanada per aprofundir en la història de la criptologia és el llibre *The codebreakers*, de David Khan.

s'escrivia.

També a l'Antic Egipte apareixen els primers escrits amb la intenció, ara sí, d'ocultar el missatge escrit. Es creu que l'objectiu era dotar el textos de cert aire de misteri i màgia, de manera que cridessin l'atenció del lector i que aquest s'entretingués desxifrant-los, com si fos un joc o un puzzle.

Uns quants segles després, l'ús de la criptografia va prendre un altre rumb i va començar-se a fer servir per ocultar missages amb contingut crític en temps de guerra. Els espartans, potència militar de l'antiga Grècia, van començar a fer servir, d'una banda, sistemes esteganogràfics i, d'altra banda, van inventar la primera xifra de transposició coneguda, l'escítala.

Pel que fa a l'esteganografia,[4] els primers usos que se'n coneixen daten de l'any 440 a.C.: Histiaeus va rapar el cap d'un dels seus servents per tatuar-hi un missatge, deixant que el cabell del servent tornés a créixer abans d'enviar-lo a Aristagoras, el receptor del misatge. Així, si l'esclau era capturat per l'enemic durant el viatge, el fet que l'esclau transportava un missatge romandria ocult. També en aquella època, Demaratus va enviar un missatge escrit en un parell de tabletes de cera, marcant el missatge a la fusta que quedava sota la cera i cobrint les tauletes de nou de cera. Així, si les tauletes eren interceptades, una revisió superficial de les mateixes no revel·laria que incorporaven un missatge ocult.

Pel que fa a la criptografia, els espartans són coneguts també per la utilització del primer sistema de criptografia militar, l'escítala, que descriurem posteriorment en l'apartat de xifres de transposició. Es creu que l'escítala va ser el primer aparell utilitzat per la criptografia. Thucydides, un historiador grec, recull l'ús d'aquest aparell per a xifrar un missatge dels èfors (uns magistrats de l'antiga Grècia) al general espartà Pausanius.

El primer ús conegut d'un criptosistema de substitució és atribuït als romans i, en concret, a Juli Cèsar, que el feia servir per escriure a Ciceró i d'altres amics. En els següents apartats descriurem també en detall aquesta xifra, així com les seves febleses.

Els primers textos on es parla de criptoanàlisi són atribuïts als àrabs. Al-Kindi, filòsof i matemàtic àrab del segle IX d.C., va descriure com utilitzar el fet que la freqüència d'aparició de les lletres de l'alfabet en un idioma determinat no és uniforme per trencar criptosistemes.

Ja al segle XIV, l'italià Leon Battista Alberti, va ser el primer occidental en documentar tècniques de criptoanàlisi i va crear el primer xifrat de substitució polialfabètic, la xifra d'Alberti.

Uns quants segles després, al 1883, Auguste Kerckhoffs, criptògraf d'origen holandés, va publicar un llibre sobre criptografia militar, on donava consells pràctics per al disseny de criptosistemes. Un d'aquests consells afirmava que un criptosistema havia de ser segur encara que l'atacant en conegués tots els detalls, a excepció de la clau feta servir per a xifrar. Aquest consell va rebre una àmplia acceptació i va acabant-se convertint en el principi Kerckhoffs, principi el qual la gran majoria de criptògrafs actuals respecten i segueixen.

L'any 1948 el matemàtic nordamericà Claude Elwood Shannon va crear els fonaments de la teoria de la informació. L'any següent, al 1949, ell mateix va publicar l'article *Communication Theory of Secrecy Systems*, que assentava les bases de la criptografia com a ciència i inaugurava la criptografia moderna. Entre moltes altres contribucions, Shannon va definir els conceptes de secret perfecte, va demostrar que la xifra de Vernam podia oferir aquest tipus de secret i va introduir el concepte de

[4] L'**esteganografia** és la pràctica que amaga un missatge dins d'un altre missatge, amb la intenció d'ocultar el primer. Així, per exemple, hom pot intentar amagar un missatge de text en una imatge, fent servir els bits menys significatius de cada píxel per tal de modificar al mínim la visualització de la imatge.

redundància.

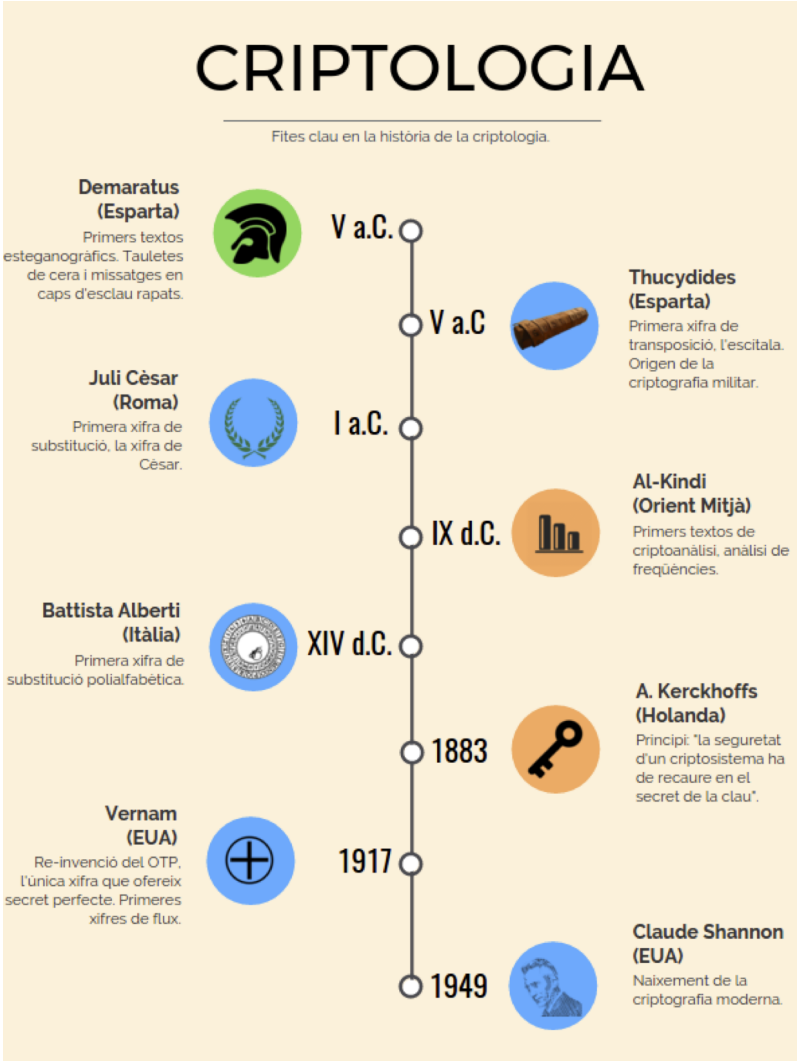

Figura 1.2: Línia de temps amb le fites clau de la criptologia pre-moderna.

A continuació descriurem els dos tipus de criptosistemes utilitzats en la criptografia història, les xifres de transposició i les xifres de substitució, i en presentarem alguns exemples concrets.

1.2.1 Xifres de transposició

> Les xifres de **transposició** es basen en canviar l'ordre dels caràcters del text en clar d'entrada per tal de generar el text xifrat.

És a dir, les xifres de transposició reordenen el text d'entrada, de manera que el text en clar és una permutació dels caràcters del text xifrat.

Escítala

Els espartans (al segle V a.C.) feien servir un criptosistema de transposició conegut pel nom d'escítala. La clau de xifrat era un pal o bastó d'un determinat gruix.

Per a xifrar, s'enrotllava una tira de papir al voltant del bastó i s'escrivia el missatge en sentit longitudinal, és a dir, seguint la direcció del propi bastó. Després, es desenrotllava la tira de papir, obtenint el missatge xifrat que podia ser enviat al receptor. Per tant, el gruix del bastó representava la clau compartida.

Al rebre la tira de papir, el receptor, que també disposava d'un bastó del mateix gruix que el de l'emissor, procedia a enrotllar la tira al voltant del bastó i podia així llegir el missatge original enviat.

La tira de papir, per si sola, era difícil de llegir, ja que contenia les mateixes lletres que el missatge en clar però desordenades per l'efecte de desenrotllar el papir. A més, si no es disposava d'un bastó del gruix adequat, el resultat d'enrotllar el papir al bastó no revel·lava el missatge original.

Exemple 1.1 Exemple de xifra amb escítala

Xifrem el missatge `THESEARESPARTASWALLS` fent servir una escítala. Suposem que el gruix del bastó utilitzat com a clau permet escriure quatre línies de text i que la longitud del bastó limita cada línia a cinc caràcters. Aleshores, el missatge quedaria escrit en quatre línies que serien:

```
THESE
ARESP
ARTAS
WALLS
```

Al desenrotllar el papir del bastó, el missatge que quedaria escrit en la tira de papir (i que correspondria al missatge xifrat) seria: `TAAWHRRAEETLSSALEPSS`.

Noteu com, efectivament, les lletres del missatge en clar han quedat desordenades, ocultant així el missatge original.

Exercici 1.1 Xifreu el missatge `THESEARESPARTASWALLS` fent servir una escítala amb un gruix de bastó que permeti escriure cinc línies de text i una longitud que permeti escriure quatre caràcters per línia.

1.2.2 Xifres de substitució

En contraposició a les xifres de transposició, les xifres de substitució no desordenen el text en clar per tal de xifrar, sinó que substitueixen les lletres del text en clar per altres símbols. Depenent de la tècnica utilitzada per realitzar les substitucions, distingirem entre xifres de substitució simple, polialfabètica i homofònica.

Substitució simple

La xifra de substitució simple és un dels mètodes més senzills per a xifrar text.

La xifra de **substitució simple** consisteix a substituir cada lletra individual del missatge en clar per una altra lletra.

La clau feta servir per xifrar és, aleshores, una taula que indica per cada lletra de l'alfabet d'entrada, quina és la seva corresponent lletra de l'alfabet xifrat.

El procediment a realitzar per xifrar consisteix a buscar cada lletra del text en clar a la taula utilitzada com a clau i substituir-la per la lletra indicada. Per a desxifrar, se segueix el mateix procediment, fent servir ara la taula en sentit invers.

La mida de l'espai de claus (és a dir, el número de possibles taules que podem crear indicant correspondències entre lletres) ve donada per les mides dels alfabets en clar i xifrat. Així, per exemple, si fem servir un alfabet de 26 caràcters tant per al text en clar com per al text xifrat, l'espai de claus té una mida de:

$$|\mathscr{K}| = 26 \cdot 25 \cdot 24 \cdot \ldots \cdot 1 = 26!$$

ja que, per al primer caràcter de l'alfabet en clar, podem triar 26 possibles lletres xifrades; per al segon caràcter, en podrem triar 25 (les 26 disponibles excepte la que ja hem triat per al primer caràcter); etc.

L'espai de claus de les xifres de substitució simple pot semblar prou gran per oferir un nivell de seguretat adequat. Tot i així, aquestes xifres són en realitat molt fàcils de trencar, en part perquè preserven la freqüència d'aparició de les lletres. En efecte, si una determinada lletra del text en clar x queda xifrada sempre per una lletra de l'alfabet xifrat y, la freqüència d'aparició de la lletra y en el text xifrat serà exactament la mateixa que la freqüència d'aparició d'x en el text en clar. Atès que les freqüències d'aparició de les lletres en els textos escrits presenten marcades diferències, quan els textos tenen certa longitud és fàcil identificar algunes lletres del text xifrat i acabar desxifrant el missatge sense conéixer la clau feta servir per xifrar.

La Figura 1.3 mostra les freqüències d'aparició mitjanes de les lletres de l'alfabet en textos escrits en català:

Es diu que Juli Cèsar va fer servir una variant de la xifra de substitució simple per escriure a Ciceró i d'altres amics. La variant que feia servir Cèsar xifrava cada lletra de l'alfabet en clar per la lletra que es troba tres posicions després en l'alfabet. Així, Cèsar feia servir les següents correspondències:

$$\begin{array}{c} \mathrm{A} \to \mathrm{D} \\ \mathrm{B} \to \mathrm{E} \\ \mathrm{C} \to \mathrm{F} \\ \mathrm{D} \to \mathrm{G} \\ \mathrm{E} \to \mathrm{H} \\ \ldots \\ \mathrm{X} \to \mathrm{A} \\ \mathrm{Y} \to \mathrm{B} \\ \mathrm{Z} \to \mathrm{C} \end{array}$$

Una generalització immediata de l'esquema que feia servir Cèsar resulta de xifrar cada lletra per la que es troba k posicions després en l'alfabet, on k pot ser qualsevol valor en $[0, 25]$ (en comptes de fixar $k = 3$).[5] Aquesta generalització és el que es coneix habitualment com a **xifra de Cèsar**.

[5] El nebot de Cèsar, Augustus, feia servir una variant de la xifra de Cèsar amb $k = 1$.

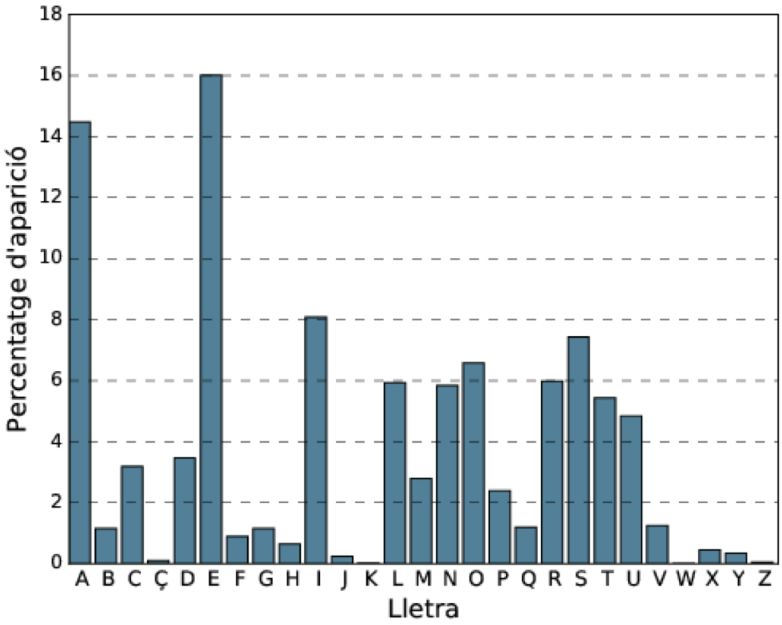

Figura 1.3: Freqüències d'aparició de les lletres en català.

Si assignem a cada lletra de l'alfabet una representació numèrica, on la A és representada pel 0, la B per l'1, etc., aleshores podem definir formalment la funció de xifrat de cada lletra del missatge com a:

$$E(x) = x + k \mod 26$$

on k és la clau secreta que comparteixen l'emissor i el receptor.

Simètricament, la funció de desxifrat és:

$$D(y) = y - k \mod 26$$

Exemple 1.2 Exemple de xifra de Cèsar

Volem xifrar el missatge $m = \texttt{THEDIEISCAST}$ fent servir la xifra de Cèsar original, amb $k = 3$. Procedim doncs a substituir cada lletra del missatge en clar per la lletra que es troba tres posicions després a l'alfabet, obtenint el missatge xifrat:

$$c = \texttt{WKHGLHLVFDVW}$$

Si volem fer servir la formulació matemàtica, convertirem primer el missatge m en una seqüència d'enters:

$$m' = 19\ 7\ 4\ 3\ 8\ 4\ 8\ 18\ 2\ 0\ 18\ 19$$

Sumarem $k = 3$ a cada valor, reduint el resultat mòdul 26 (noteu que en aquest cas concret, no cal reduir cap valor ja que tots són inferiors a 26):

$$c' = 22\ 10\ 7\ 6\ 11\ 7\ 11\ 21\ 5\ 3\ 21\ 22$$

i finalment convertirem la seqüència xifrada a cadena de caràcters, obtenint el text xifrat c:

$$c = \texttt{WKHGLHLVFDVW}$$

Exercici 1.2 Desxifreu el missatge `XADKTIWTCPBTDUWDCDGBDGTIWPCXUTPGSTPIW` sabent que ha estat xifrat amb una xifra de Cèsar amb $k = 15$.

Tant la xifra de substitució simple com la xifra de Cèsar són xifres de substitució monoalfabètiques:

> Les xifres de **substitució monoalfabètiques** es caracteritzen per fer servir una substitució de caràcters fixa, on una mateixa lletra del text en clar sempre correspondrà a la mateixa lletra del text xifrat, independentment de la posició que ocupi la lletra en el text en clar.

Substitució polialfabètica

Les xifres de substitució polialfabètiques van aparéixer bastants anys després que les xifres monoalfabètiques. Es creu que la primera xifra polialfabètica va ser creada per Leon Battista Alberti, sobre l'any 1467. De totes maneres, alguns historiadors argüeixen que les xifres polialfabètiques van ser ideades per Al Kindi molt abans (sobre l'any 800). La variant més popular de la xifra polialfabètica és atribuida a Blaise de Vigenère (tot i que ell no en va ser l'inventor) i es coneguda com a xifra de Vigenère.

> Les xifres de **substitució polialfabètiques** es caracteritzen per fer servir múltiples alfabets de substitució, fent que una mateixa lletra del text en clar pugui quedar xifrada amb diferents lletres, depenent de la posició que aquesta ocupi en el text en clar.

La **xifra de Vigenère** és una xifra de substitució polialfabètica periòdica, on es combinen diferents xifres de Cèsar. El període n ve determinat per la mida (en caràcters) de la clau de xifrat de Vigenère, i cada lletra individual de la clau es fa servir com a clau d'una xifra de Cèsar. Així, per a un missatge $m = m_1, m_2, \cdots, m_l$, una clau $k = k_1, k_2, \cdots, k_n$ i un alfabet de 26 caràcters, la funció de xifrat és:

$$E(m_i) = m_i + k_{i \bmod n} \mod 26$$

De manera similar, la funció de desxifrat és:

$$D(c_i) = c_i - k_{i \bmod n} \mod 26$$

Exemple 1.3 Exemple de xifra de Vigenère

Suposem que volem xifrar el missatge

$$m = \texttt{VIGENERECIPHERWASCREATEDBYGIOVANBATTISTA}$$

amb la clau:

$$k = \texttt{ENEGIV}$$

Procedim a convertir tant el missatge com la clau a la seva representació numèrica, i a calcular la representació numèrica de la lletra xifrada corresponent a cada lletra en clar (sumant els valors mòdul 26). Finalment, convertim la seqüència numèrica a caràcters i obtenim el missatge xifrat:

V	I	G	E	N	E	R	E	C	I	P	H	E	R	W	A	S	C	R	E
21	8	6	4	13	4	17	4	2	8	15	7	4	17	22	0	18	2	17	4
E	N	E	G	I	V	E	N	E	G	I	V	E	N	E	G	I	V	E	N
4	13	4	6	8	21	4	13	4	6	8	21	4	13	4	6	8	21	4	13
25	21	10	10	21	25	21	17	6	14	23	2	8	4	0	6	0	23	21	17
Z	V	K	K	V	Z	V	R	G	O	X	C	I	E	A	G	A	X	V	R

A	T	E	D	B	Y	G	I	O	V	A	N	B	A	T	T	I	S	T	A
0	19	4	3	1	24	6	8	14	21	0	13	1	0	19	19	8	18	19	0
E	G	I	V	E	N	E	G	I	V	E	N	E	G	I	V	E	N	E	G
4	6	8	21	4	13	4	6	8	21	4	13	4	6	8	21	4	13	4	6
4	25	12	24	5	11	10	14	22	16	4	0	5	6	1	14	12	5	23	6
E	Z	M	Y	F	L	K	O	W	Q	E	A	F	G	B	O	M	F	X	G

El missatge xifrat resultant és doncs:

$$c = \texttt{ZVKKVZVRGOXCIEAGAXVREZMYFLKOWQEAFGBOMFXG}$$

Exercici 1.3 Xifreu el missatge `USINGASERIESOFINTERWOVENCAESARCIPHERS` amb Vigenere, fent servir com a clau `KASISKI`.

Amb les xifres polialfabètiques s'aconsegueix que una mateixa lletra del text en clar no sempre quedi xifrada per la mateixa lletra, dificultant l'anàlisi de freqüències.

Un cas especialment interessant de xifra polialfabètica és la **xifra de Vernam**.

La **xifra de Vernam** és una xifra polialfabètica on el número d'alfabets que codifica la clau és igual o major al número de caràcters del text en clar a xifrar.

Quan es fa servir adequadament, amb claus aleatòries i d'un sol ús, la xifra de Vernam ofereix secret perfecte. De fet, la xifra de Vernam és l'única xifra coneguda, encara avui, que ofereix aquesta propietat.[6]

La xifra de Vernam és coneix també, en anglès, com a *one-time pad*. El nom prové dels primers usos del xifrat, on les claus es distribuien als espies en llibretes de paper (a vegades de paper altament imflamable), el que permetia fer servir la clau una vegada i destruir després el full de paper que contenia aquella clau.

Substitució homofònica

Una altra alternativa per tal d'evitar revel·lar les freqüències d'aparició de les lletres en el text xifrat és la que presenten les xifres homofòniques.

> La xifra de **substitució homofònica** permet substituir cada lletra del missatge en clar per un conjunt de lletres de l'alfabet xifrat.

Així doncs, a diferència de les xifres de substitució simple, on una lletra de l'alfabet en clar correspon a una única lletra de l'alfabet xifrat, en les xifres homofòniques una lletra del text en clar pot correspondre a vàries lletres de l'alfabet xifrat. Això fa que l'alfabet xifrat hagi de tenir més caràcters que l'alfabet en clar.

Per tal d'aconseguir amagar les freqüències d'aparició de les lletres, el que fan les xifres de substitució homofòniques és assignar més alternatives de xifrat a les lletres de l'alfabet en clar que apareixen més sovint, de manera que les freqüències d'aparició de les lletres en el text xifrat s'assemblin el màxim possible.

Exemple 1.4 Exemple de xifra homofònica

Suposem que volem xifrar el missatge `THEBEALEPAPERS` fent servir subsitució homofònica amb la següent clau:

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
j	B	N	P	s	T	i	S	q	l	e	h	D	W	R	f	E	d	w	y	O	M	a	X	t	Z
g			Q	z	u		H	U			p	k	L	m			A	K	x	r		v			
J			o	C			c	V					I	Y			F	b	n						
				G																					

i tenint en compte que si disposem de més d'una alternativa per a xifrar una lletra, seleccionarem aleatòriament la lletra a xifrar d'entre les alternatives.

Noteu que, en aquest cas, l'alfabet del text en clar està format per 26 caràcters (les lletres de la A a la Z en majúscula, sense incloure la Ç), mentre que l'alfabet xifrat disposa de 52 caràcters (les lletres tant en majúscula com en minúscula).

[6] **Secret perfecte:** Claude Shannon va definir les mesures amb les quals s'avalua el nivell de secret que ofereix una determinada xifra. Informalment, diem que un criptosistema ofereix secret perfecte si el text xifrat no ofereix cap informació sobre el text en clar.

Així, un possible text xifrat seria `yHCBsjpGfgfzdw`, que correspondria a seleccionar la lletra `y` d'entre les tres alternatives per a xifrar `T` (`y`, `x` i `n`); la lletra `H` d'entre les tres alternatives per a xifrar `H` (`S`, `H` i `c`); etc.

Per a desxifrar seguiríem el procés invers, buscant les lletres de l'alfabet xifrat a la taula i extraient-ne la corresponent lletra en clar. En aquest cas, el desxifrat és únic. És a dir, per a un mateix text en clar, podem generar diferents textos xifrats. En canvi, per a un text xifrat, només hi haurà un únic text en clar.

Exercici 1.4 Genereu 5 textos xifrats diferents corresponent al missatge `THEBEALEPAPERS` fent servir la xifra de substitució homofònica amb la següent clau:

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
j	B	N	P	s	T	i	S	q	l	e	h	D	W	R	f	E	d	w	y	O	M	a	X	t	Z
g			Q	z	u		H	U			p	k	L	m			A	K	x	r		v			
J			o	C			c	V					I	Y			F	b	n						
				G																					

Quina informació en pot extreure un criptoanalista que tingui accés als 5 textos xifrats (i sàpiga que es tracta d'un xifrat homofònic)?

La **xifra de Beale** és una xifra homofònica que feia servir com a clau la declaració d'independència dels Estats Units d'Amèrica.

La història diu que Thomas J. Beale va enterrar un tresor d'una expedició de miners que havien fet fortuna a les mines de l'oest llunyà a la dècada de 1820. El tresor, format per or, plata i joies, tindria actualment un valor d'uns 43 milions de dòlars. Beale va crear un conjunt de tres criptogrames que descrivien, respectivament, la localització, el contingut i els noms dels propietaris del tresor enterrat, i va deixar una capsa de ferro amb els criptogrames a un taverner anomenat Robert Morriss. Beale va desaparéixer, i el taverner va donar la capsa amb els criptogrames a un amic just abans de morir. L'amic, del qual no se'n coneix el nom, va aconseguir desxifrar el segon dels criptogrames fent servir un criptosistema homofònic amb la declaració d'independència dels Estats Units d'Amèrica com a clau. Per desxifrar el criptograma, l'amic va numerar cadascuna de les paraules de la declaració i va anar substituint cada número del text xifrat per la lletra inicial de la paraula que es trobava en la posició descrita pel número.

Es diu que l'amic no va ser capaç de trencar els altres dos criptogrames, motiu pel qual, l'any 1885, decideix fer pública la història i els criptogrames, amb l'esperança que algú altre pogués trencar-los. Des de llavors, hi ha hagut múltiples intents sense èxit de trencar els dos criptogrames restants.

De fet, les teories actuals apunten a què la història és en realitat un engany. Els arguments principals que en qüestionen la seva veracitat són que el text en clar del segon dels criptogrames fa servir paraules que no existien quan suposadament es van crear els criptogrames i que les característiques estadístiques dels dos criptogrames restants no semblen coincidir amb les que s'esperaria d'un text en anglès.

1.3 Resum

En aquest capítol hem presentat els conceptes bàsics relacionats amb la criptografia i hem descrit les fites històriques clau pel que fa al seu desenvolupament, tot introduint els criptosistemes que es van anar dissenyant durant l'era de la criptografia precientífica.

Anomenem **criptografia** a la ciència que estudia l'escriptura de secrets. En canvi, la **criptoànalisi** és la ciència que se centra en trencar les tècniques que desenvolupa la criptografia. Ambdues ciències treballen paral·lelament, de manera que els avenços d'una ajuden a avançar l'altra. Fem servir el mot general **criptologia** per englobar tant criptografia com criptoanàlisi.

Podem agrupar les xifres històriques en dos grans grups segons la tècnica que fan servir per xifrar: les xifres de **transposició** i les xifres de **substitució**. Les xifres de transposició modifiquen l'ordre dels caràcters del text en clar per generar el text xifrat. En canvi, les xifres de substitució canvien els caràcters del text en clar per altres caràcters.

1.4 Solucions dels exercicis

Exercici 1.1:

Tenint en compte les mides del bastó, procediríem a escriure el missatge longitudinalment:

```
THES
EARE
SPAR
TASW
ALLS
```

El missatge xifrat resultant seria, per tant: `TESTAHAPALERASLSERWS`.

Exercici 1.2:

En primer lloc convertim les lletres del missatge en la seva representació numèrica:

```
23 0 3 10 19 8 22 19 2 15 1 19 3 20 22 3 2 3 6 1 3 6 19 8 22 15 2
23 20 19 15 6 18 19 15 8 22
```

Seguidament, calculem $x - 15 \mod 26$ per cada valor x de la representació numèrica de les lletres:

```
8 11 14 21 4 19 7 4 13 0 12 4 14 5 7 14 13 14 17 12 14 17 4 19 7 0 13
8 5 4 0 17 3 4 0 19 7
```

Finalment, recuperem el missatge en clar, convertint la seqüència numèrica de nou a lletres:
`ILOVETHENAMEOFHONORMORETHANIFEARDEATH`

Exercici 1.3:

Convertim tant el missatge com la clau a la seva representació numèrica, i calculem el text en clar sumant els dos valors mòdul 26:

U	S	I	N	G	A	S	E	R	I	E	S	O	F	I	N	T	E	R	W	O	V	E	N	C	A	E	S	A	R	C	I	P	H	E	R	S
20	18	8	13	6	0	18	4	17	8	4	18	14	5	8	13	19	4	17	22	14	21	4	13	2	0	4	18	0	17	2	8	15	7	4	17	18
K	A	S	I	S	K	I	K	A	S	I	S	K	I	K	A	S	I	S	K	I	K	A	S	I	S	K	I	K	A	S	I	S	K	I	K	A
10	0	18	8	18	10	8	10	0	18	8	18	10	8	10	0	18	8	18	10	8	10	0	18	8	18	10	8	10	0	18	8	18	10	8	10	0
4	18	0	21	24	10	0	14	17	0	12	10	24	13	18	13	11	12	9	6	22	5	4	5	10	18	14	0	10	17	20	16	7	17	12	1	18
E	S	A	V	Y	K	A	O	R	A	M	K	Y	N	S	N	L	M	J	G	W	F	E	F	K	S	O	A	K	R	U	Q	H	R	M	B	S

El text xifrat resultant és doncs `ESAVYKAORAMKYNSNLMJGWFEFKSOAKRUQHRMBS`.

Exercici 1.4:

Cinc possibles textos xifrats són:

- `nHCBsJpsfjfGdK`
- `xHGBsJpCfJfCAb`
- `ycCBsjpzfgfsAw`
- `nczBzgpCfgfzFK`
- `xHsBCjpsfJfsFb`

Noteu que la solució no és única. A primer cop d'ull, un criptoanalista pot deduir que, amb probabilitat molt alta, les lletres xifrades `B`, `p` i `f` corresponen a lletres del text en pla que només tenen una única lletra xifrada assignada.

1.5 Bibliografia

Shannon, Claude E. (1949). *Communication theory of secrecy systems*. The Bell system technical journal, 28(4), 656-715.