Introducció a la criptografia

PID_00235159

Cristina Pérez Solà
Jordi Herrera Joancomartí

Temps mínim de dedicació recomanat: 2 hores

Universitat Oberta de Catalunya

Cristina Pérez Solà

Doctora en Informàtica per la Universitat Autònoma de Barcelona i la Universitat Catòlica de Lovaina. Actualment és professora dels Estudis d'Informàtica, Multimèdia i Telecomunicacions de la Universitat Oberta de Catalunya. Els seus àmbits de recerca són les criptomonedes basades en *blockchain* i, en especial, els aspectes relacionats amb la seguretat i la privadesa d'aquestes. També està interessada en els problemes de privacitat que sorgeixen arran de l'ús de les xarxes socials i en l'adaptació de tècniques de mineria de dades a la naturalesa específica d'aquest tipus de xarxes.

Jordi Herrera Joancomartí

Llicenciat en Matemàtiques per la Universitat Autònoma de Barcelona i doctor per la Universitat Politècnica de Catalunya. Els seus àmbits de recerca són la criptografia, les criptomonedes i la tecnologia *blockchain*. Ha publicat nombrosos textos docents i més de cent articles de recerca en revistes i congressos nacionals i internacionals. Ha dirigit nou tesis doctorals i ha estat investigador principal de diversos projectes de recerca nacionals. Ha participat com a avaluador per a agències de recerca de diversos països europeus i també per a la Comissió Europea. Actualment és professor agregat del departament d'Enginyeria de la Informació i les Comunicacions a la Universitat Autònoma de Barcelona.

L'encàrrec i la creació d'aquest recurs d'aprenentatge UOC han estat coordinats per la professora: Helena Rifà Pous

Segona edició: febrer 2021

Av. Tibidabo, 39-43, 08035 Barcelona
Autoria: Jordi Herrera Joancomartí, Cristina Pérez Solà
Producció: FUOC

Índex

Introducció

En aquest mòdul didàctic, d'una banda, es presenten els fonaments de la criptografia i, de l'altra banda, es fa 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 de l'assignatura 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 de l'assignatura se centrarà precisament a descriure diversos aspectes de la criptografia moderna, que, com veurem, ha evolucionat molt des de les seves arrels.

Objectius

Els objectius d'aquest mòdul didàctic són els següents:

1. Descobrir els conceptes bàsics relacionats amb la criptografia i la criptoanàlisi.
2. Estudiar les fites clau a la història de la criptografia.
3. Analitzar els dos tipus bàsics de criptosistemes precientífics: les xifres de substitució i les xifres de transposició.

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 remonten a fa més de quatre mil 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 mitjan segle XX, amb les contribucions realitzades per Claude E. Shannon.

La **criptoànalisi** és la ciència que se centra a 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 de xifrat.

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 criptoanàlisi realitzada al segle IX per un matemàtic àrab, Al-Kindí.

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

En aquesta assignatura, ens centrarem a descriure les tècniques i els algorismes que es fan servir per ocultar informació, és a dir, en la criptografia. Tot i així, en aquest mòdul 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 a protegir la **confidencialitat** dels missatges.

La **confidencialitat** és una propietat que garanteix que la informació no es faci 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 també ens permet 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.

Origen dels personatges

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.

Per tal de simplificar les explicacions, en criptografia es fan servir uns personatges ficticis, que acostumen a interpretar sempre els mateixos papers. Aquests personatges, l'ús dels quals es troba molt estès, van ser creats per Ron Rivest, Adi Shamir i Leonard Adleman. L'Alice (*A*) i en Bob (*B*) són els dos personatges més populars i acostumen a ser dos usuaris que volen intercanviar-se 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.

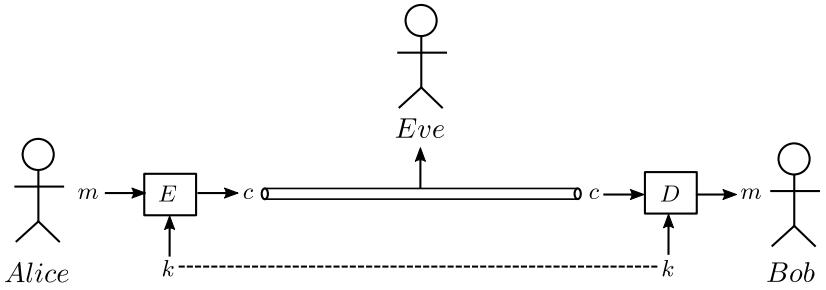
Escenari tradicional

L'escenari descrit correspon a una comunicació xifrada entre dues entitats fent servir criptografia de clau simètrica. Com veurem al llarg del semestre, existeixen altres tipus de criptosistemes que no segueixen aquest esquema.

Així doncs, a continuació descriurem l'escenari tradicional en què s'aplica la criptografia fent servir els personatges que acabem de presentar. A l'escenari bàsic, l'Alice vol enviar un missatge a en Bob per mitjà 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 per mitjà 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, amb la qual cosa obtindrà 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 per mitjà d'algun canal segur (potser fins i tot

trobant-se físicament). L'Eve podrà recuperar el text xifrat de la comunicació c, però com que no coneix el valor de la clau, no serà capaç de recuperar-ne el text en clar corresponent.

Figura 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 text xifrat $c \in \mathfrak{C}$ corresponent;
- 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, i fins i tot alguns no s'assemblen gens a l'escenari tradicional. Així doncs, 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 totalment descentralitzats i segurs, i protocols de computació multipart, on diverses entitats podran col·laborar per calcular funcions sobre dades confidencials.

1.1. Introducció a la criptoanàlisi

La criptoanàlisi se centra a analitzar els criptosistemes amb l'objectiu d'avaluarne la 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.

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

- 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-plaintex 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 o xifrat escollit (respectivament, CPA2 i CCA2), permet al criptoanalista anar demanant els corresponents textos xifrats o 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 criptògrafs assumeixen el principi de Kerckhoffs.

El principi de **Kerckhoffs** afirma que, perquè 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 disposen de l'especificació completa de l'algorisme que es vol trencar. Auguste Kerchoffs va formular aquest principi al segle XIX i, actualment, la versió més estesa 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 el fet d'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 dificulta l'avaluació de la seva seguretat. Alguns exemples de l'adopció d'aquest paradigma es troben en els algorismes xifrats de telefonia mòbil GSM, que es van intentar mantenir ocults sense èxit; o en el sistema d'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, també hi ha atacs de canal lateral i atacs d'enginyeria social.

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

Depenent de la informació que s'extreu de la implementació per a realitzar l'atac, hi ha diferents classes d'atacs de canal lateral. Així, els atacs de sincronització (en anglès, *timing attacks*) analitzen el temps que es tarda a 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 en realitzar els càlculs, etc.

Atacs de monitoreig d'energia

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.

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

Els **atacs d'enginyeria social** consisteixen a manipular els usuaris d'un sistema per tal d'obtenir informació que permeti trencar-ne la seguretat.

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

2. Una mica d'història

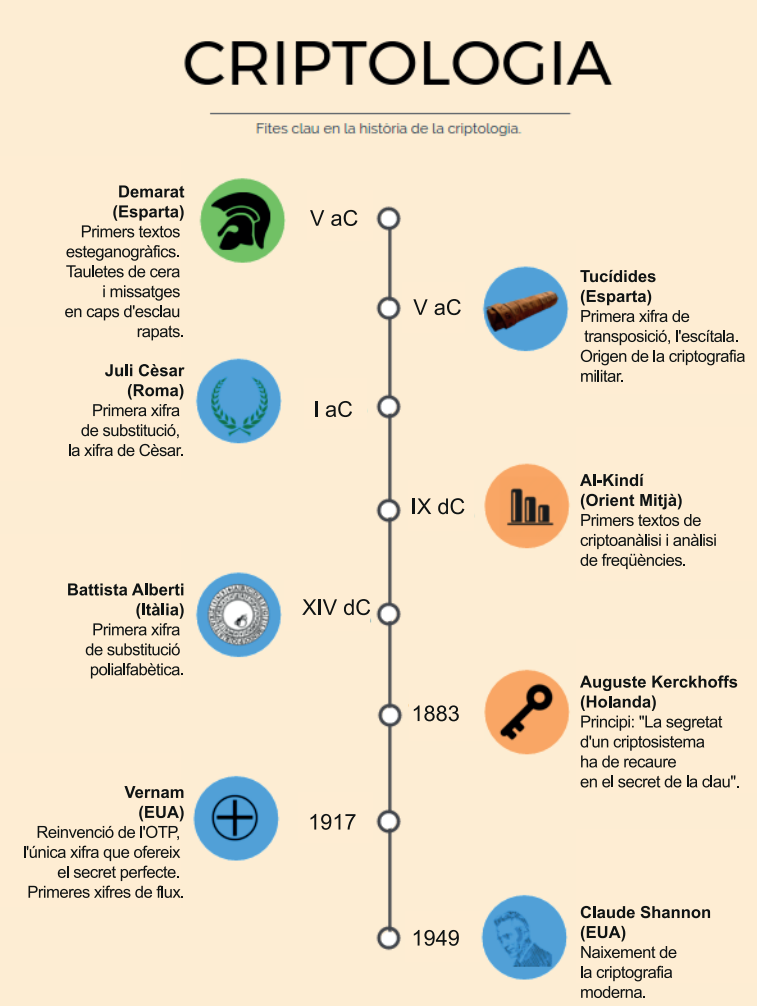
Història de la criptologia

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

Es diu que la història de la criptologia va començar l'any 1900 abans de Crist amb uns escrits realitzats a la tomba de Khnumhotep II, un nomarca de l'Alt Egipte. Als escrits trobats a la tomba hi ha alguns jeroglífics inusuals que l'escribà va escriure enlloc d'altres de 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 a la història en què el text que s'escriu es transforma deliveradament.

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 puzle.

Figura 2. Línia de temps amb les fites clau de la criptologia premoderna



Uns quants segles més tard, l'ús de la criptografia va prendre un altre rumb, i aquesta ciència es va començar a fer servir per ocultar missatges amb contingut crític en temps de guerra. D'una banda, els espartans, potència militar de l'antiga Grècia, van començar a fer servir sistemes esteganogràfics i, d'altra banda, van inventar la primera xifra de transposició coneguda, l'escítala.

Pel que fa a l'esteganografia, els primers usos que se'n coneixen daten de l'any 440 aC: Histieu va rapar el cap d'un dels seus servents per escriure-hi un missatge i va deixar que el cabell del servent tornés a créixer abans d'enviar-lo a Aristàgores, el receptor del missatge. 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, Demarat va enviar un missatge escrit en un parell de tauletes de cera; va marcar el missatge a la fusta que quedava sota la cera i va cobrir les tauletes de nou amb cera. Així, si les tauletes eren interceptades i se'n feia una revisió superficial, res revelaria el seu missatge ocult.

Esteganografia

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.

Pel que fa a l'escítala, es creu que aquest va ser el primer aparell utilitzat per la criptografia. Els espartans són coneguts per la utilització d'aquest primer sistema de criptografia militar, que descriurem posteriorment al subapartat 2.1. Tucídides, un historiador grec, recull l'ús que van fer d'aquest aparell els èfors, uns magistrats de l'antiga Grècia que van xifrar un missatge per al general espartà Pausànies.

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

Els primers textos on es parla de criptoanàlisi són atribuïts als àrabs. Al-Kindí, filòsof i matemàtic àrab del segle IX dC, 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 a documentar tècniques de criptoanàlisi i va crear el primer xifrat de substitució polialfabètic, la xifra d'Alberti.

Uns quants segles després, el 1883, Auguste Kerckhoffs, criptògraf d'origen holandès, 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 es va acabar convertint en el principi Kerckhoffs, respectat i seguit per la gran majoria de criptògrafs.

L'any 1948, el matemàtic nord-americà Claude Elwood Shannon va crear els fonaments de la teoria de la informació. L'any següent, el 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 el concepte de secret perfecte, va demostrar que la xifra de Vernam podia oferir aquest tipus de secret i va introduir el concepte de redundància.

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

2.1. Xifres de transposició

Les **xifres de transposició** es basen a 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.

2.1.1. Escítala

Al segle V abans de Crist, els espartans feien servir un criptosistema de transposició conegut com a 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 mateix bastó. Després, es desenrotllava la tira de papir, de manera que s'obtenia el missatge xifrat que podia ser enviat al receptor. Per tant, el gruix del bastó representava la clau compartida.

En 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; així podia llegir el missatge original que li havien 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 revelava el missatge original.

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 com les següents:

```
THESE
ARESP
ARTAS
WALLS
```

En desenrotllar el papir del bastó, el missatge que quedaria escrit a la tira de papir, i que correspondria al missatge xifrat, seria: `TAAWHRRAEETLSSALEPSS`.

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

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.

2.2.1. 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 que es fa servir per a xifrar és, doncs, una taula que indica quina lletra de l'alfabet xifrat correspon a cada lletra de l'alfabet d'entrada.

El procediment que cal dur a terme 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. A l'hora de desxifrar, cal seguir el mateix procediment, però fent servir ara la taula en sentit invers.

La mida de l'espai de claus, és a dir, el nombre de possibles taules que podem crear indicant correspondències entre lletres, ve donada per les mides de l'alfabet en clar i el 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 tindrà la mida següent:

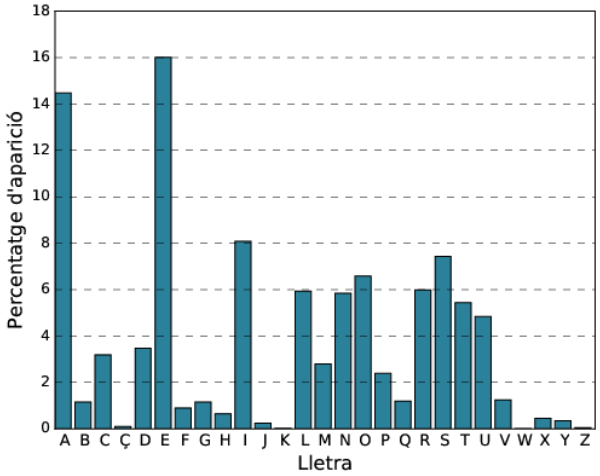
$$|\mathcal{K}| = 26 \cdot 25 \cdot 24 \cdot \ldots \cdot 1 = 26!$$

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, en realitat aquestes xifres són 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 que s'ha fet servir per a xifrar.

La figura 3 mostra les freqüències d'aparició mitjanes de les lletres de l'alfabet en textos escrits en català.

Figura 3. Freqüències d'aparició de les lletres en català



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

$$\begin{aligned} A &\to D \\ B &\to E \\ C &\to F \\ D &\to G \\ E &\to H \\ &\dots \\ X &\to A \\ Y &\to B \\ Z &\to C \end{aligned}$$

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 de 0 a 25 (en comptes de fixar $k = 3$). Aquesta generalització és el que es coneix habitualment com a **xifra de Cèsar**.

Altres usos en l'antiga Roma

El nebot de Cèsar, August, feia servir una variant de la xifra de Cèsar amb $k = 1$.

Si assignem a cada lletra de l'alfabet una representació numèrica, en què la lletra *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 de xifra de Cèsar

Volem xifrar el missatge m = `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. Obtenim el missatge xifrat següent:

$$c = \texttt{WKHGLHLVFDVW}$$

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:

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

Finalment, convertirem la seqüència xifrada en una cadena de caràcters, de manera que obtindrem el text xifrat c:

$$c = \texttt{WKHGLHLVFDVW}$$

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.

2.2.2. Substitució polialfabètica

Les xifres de substitució polialfabètiques van aparéixer força anys després que les xifres monoalfabètiques. Es creu que la primera xifra polialfabètica va ser creada per Leon Battista Alberti cap a l'any 1467. De totes maneres, alguns historiadors argüeixen que les xifres polialfabètiques van ser ideades per Al-Kindí molt abans, pels volts de l'any 800. La variant més popular de la xifra polialfabètica és atrïbuida a Blaise de Vigenère; tot i que ell no en va ser l'inventor, és coneguda com a xifra de Vigenère.

Les xifres de **substitució polialfabètiques** es caracteritzen per fer servir múltiples alfabets de substitució, per la qual cosa una mateixa lletra del text en clar pot quedar xifrada amb diferents lletres, depenent de la posició que aquesta ocupi al 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 de xifra de Vigenère

Suposem que volem xifrar el missatge següent:

$$m = \texttt{VIGENERECIPHERWASCREATEDBYGIOVANBATTISTA}$$

Amb la clau:

$$k = \texttt{ENEGIV}$$

Procedim a convertir tant el missatge com la clau en 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 en 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

Així doncs, el missatge xifrat resultant és:

c = ZVKKVZVRGOXCIEAGAXVREZMYFLKOWQEAFGBOMFXG

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

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

La **xifra de Vernam** és una xifra polialfabètica en què el nombre d'alfabets que codifica la clau és igual o més gran que el nombre de caràcters del text en clar que es vol 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.

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.

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

2.2.3. Substitució homofònica

Una altra alternativa per a evitar revelar 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, en què 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 de xifra homofònica

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

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

Cal tenir en compte que si disposem de més d'una alternativa per a xifrar una lletra, seleccionarem aleatòriament la lletra que es vol 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).

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

Per a desxifrar el codi, seguiríem el procés invers: buscar les lletres de l'alfabet xifrat a la taula i extreure'n la lletra en clar corresponent. 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.

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 pels volts de la dè-

cada 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 desaparèixer i el taverner va donar la capsa amb els criptogrames a un amic just abans de morir. L'amic, del qual no es 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 del document i va anar substituint cada número del text xifrat per la lletra inicial de la paraula que es trobava a 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, va decidir 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 que la història és, en realitat, un engany. Els arguments principals que 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.

Resum

En aquest mòdul didàctic 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** la ciència que estudia l'escriptura de secrets. En canvi, la **criptoànalisi** és la ciència que se centra a 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 la criptografia com la 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.

Exercicis d'autoavaluació

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.

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

3. Xifreu el missatge `USINGASERIESOFINTERWOVENCAESARCIPHERS` amb una xifra de Vigenère i fent servir com a clau `KASISKI`.

4. Genereu cinc textos xifrats diferents que corresponguin al missatge `THEBEALEPAPERS` fent servir la xifra de substitució homofònica amb la clau següent:

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
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 cinc textos xifrats i que sàpiga que es tracta d'un xifrat homofònic?

Solucionari

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`.

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 un altre cop en lletres:

`ILOVETHENAMEOFHONORMORETHANIFEARDEATH`

3. Convertim tant el missatge com la clau en 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`.

4. Cinc possibles textos xifrats són aquests:

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

Noteu que la solució no és única. A primer cop d'ull, un criptoanalista pot deduir que, amb una 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.

Glossari

adaptatiu de text en clar escollit *m* Model d'avaluació de la seguretat dels criptosistemes en què l'atacant pot obtenir els textos xifrats corresponents a un conjunt de textos en clar seleccionats per ell mateix de manera adaptativa; és a dir, l'atacant pot anar demanant els corresponents textos en clar successivament, modificant els textos que demana en funció de les respostes que ha rebut fins al moment.
sigla **CPA2**
en adaptive chosen-plaintext attack

adaptatiu de text en xifrat escollit *m* Model d'avaluació de la seguretat dels criptosistemes en què l'atacant pot obtenir els textos en clar corresponents a un conjunt de textos xifrats seleccionats per ell mateix de manera adaptativa; és a dir, l'atacant pot anar demanant els corresponents textos xifrats successivament, modificant els textos que demana en funció de les respostes que ha rebut fins al moment.
sigla **CCA2**
en adaptive chosen-ciphertext attack

adaptive chosen-ciphertext attack *m* Vegeu **adaptatiu de text xifrat escollit**.

adaptive chosen-plaintext attack *m* Vegeu **adaptatiu de text en clar escollit**.

atac de canal lateral *m* Acció d'atacar basada en la informació extreta d'una implementació física d'un criptosistema.
en side-channel attacks

atac d'enginyeria social *m* Acció d'atacar basada en el fet de manipular els usuaris d'un sistema per tal d'obtenir informació que ens permeti trencar-ne la seguretat.

chosen-ciphertext attack *m* Vegeu **text xifrat escollit**.

chosen-plaintext attack *m* Vegeu **text en clar escollit**.

ciphertext-only attack *m* Vegeu **només text xifrat**.

confidencialitat *f* Propietat que garanteix que la informació no es fa pública a persones no autoritzades.

COA *m* Vegeu **només text xifrat**.

CCA *m* Vegeu **text xifrat escollit**.

CCA2 *m* Vegeu **adaptatiu de text xifrat escollit**.

CPA *m* Vegeu **text en clar escollit**.

CPA2 *m* Vegeu **adaptatiu de text en clar escollit**.

criptoanàlisi *f* Ciència centrada a trencar les tècniques que desenvolupa la criptografia.

criptografia *f* Del grec, *kryptós* ('secret') i *graphein* ('escriptura'), ciència que estudia l'escriptura de secrets.

criptologia *f* Ciència que engloba tant la criptografia com la criptoanàlisi.

escítala *f* Xifra de transposició que consisteix a enrotllar un papir al voltant d'un bastó, el gruix del qual determina la clau de xifrat.

esteganografia *f* Pràctica d'amagar un missatge dins d'un altre missatge, amb la intenció d'ocultar el primer.

integritat *f* Propietat que garanteix que la informació no ha estat modificada.

known-plaintext attack *m* Vegeu **text en clar conegut**.

KPA *m* Vegeu **text en clar conegut**.

només text xifrat *m* Model d'avaluació de la seguretat dels criptosistemes en què l'atacant només disposa d'un conjunt de textos xifrats.
sigla **COA**
en ciphertext-only attack

no-repudi *m* Propietat que garanteix que l'autor d'una determinada acció no pugui negar haver-la realitzat.

principi de Kerckhoffs *m* Principi que afirma que perquè 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.

seguretat per ofuscació *f* Paradigma que promou que la seguretat dels sistemes es basi en el fet d'amagar els detalls sobre l'algorisme de xifrat, amb l'objectiu de dificultar-ne, suposadament, la criptoanàlisi.

side-channel attacks *m* Vegeu **atac de canal lateral**.

substitució simple *f* Tècnica de xifrat que constitueix a substituir cada lletra individual del missatge en clar per una altra lletra.

text en clar conegut *m* Model d'avaluació de la seguretat dels criptosistemes en què l'atacant disposa d'un conjunt de textos en clar i els seus corresponents textos xifrats.
sigla **KPA**
en known-plaintext attack

text en clar escollit *m* Model d'avaluació de la seguretat dels criptosistemes en què l'atacant pot obtenir els textos xifrats corresponents a un conjunt de textos en clar seleccionats per ell mateix.
sigla **CPA**
en chosen-plaintext attack

text xifrat escollit *m* Model d'avaluació de la seguretat dels criptosistemes en què l'atacant pot obtenir els textos en clar corresponents a un conjunt de textos xifrats seleccionats per ell mateix.
sigla **CCA**
en chosen-ciphertext attack

xifra de Beale *f* Xifra homofònica que feia servir com a clau la Declaració d'Independència dels Estats Units d'Amèrica.

xifra de Cèsar *f* Xifra de substitució simple utilitzada per Juli Cèsar.

xifra de substitució homofònica *f* Xifra de substitució en què cada lletra del missatge en clar pot ser substituïda per més d'una lletra de l'alfabet xifrat.

xifra de substitució monoalfabètica *f* Xifra caracteritzada per fer servir una substitució de caràcters fixa, en què una mateixa lletra del text en clar sempre correspondrà a la mateixa lletra del text xifrat

xifra de substitució polialfabètica *f* Xifra caracteritzada 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 al text en clar.

xifra de Vernam *f* Xifra polialfabètica en què el nombre d'alfabets que codifica la clau és igual o més gran que el nombre de caràcters del text en clar que es volen xifrar.

xifra de Vigenère *f* Xifra de substitució polialfabètica periòdica en què es combinen diferents xifres de Cèsar.

xifra de transposició *f* Xifra basada en el fet d'alterar l'ordre dels caràcters del text en clar.

Bibliografia

Kahn, D. (1974). *The codebreakers*. Londres: Weidenfeld and Nicolson.
<http://www.simonandschuster.com/books/The-Codebreakers/David-Kahn/9780684831305>

Menezes, A.; Oorschot, P. van; Vanstone, S. (1996). *Handbook of Applied Cryptography*. Florida: CRC Press. <http://cacr.uwaterloo.ca/hac/>

Paar, C.; Pelzl, J. (2009). *Understanding Cryptography: A Textbook for Students and Practitioners*. Nova York: Springer.