Seguretat en la societat de la informació

Antoni Martínez Ballesté

PID_00150286

Universitat Oberta de Catalunya
www.uoc.edu

Índex

Introducció

Els sistemes i protocols que han donat lloc a Internet i a les xarxes de computadors no es van dissenyar tenint en compte la seguretat en l'ús. En els inicis, els usuaris que accedien als ordinadors eren un grup controlable (se sabia qui hi accedia) i estaven carregats de bones intencions. Els atacs als sistemes informàtics eren molt poc freqüents comparat amb avui dia. Tanmateix, l'any 1969, Lance Hoffman va escriure l'article "Computers and Privacy", per a la revista *ACM Computing Surveys*. Explicava que si tot el relacionat amb el processament automàtic de dades no tenia en compte aspectes de seguretat i privadesa, el computador podria arribar a ser el malvat de la nostra societat. En conseqüència, la informàtica, un dels recursos més importants de la nostra civilització, no evolucionaria com havia d'evolucionar.

Afortunadament, paral·lelament a l'ús massiu de les tecnologies de la informació i les comunicacions i, en fer-se palès l'accés a aquestes tecnologies d'usuaris deshonestos, es van anar desenvolupant protocols i sistemes complementaris per a proporcionar seguretat. Així doncs, tot i que els protocols com ara IP o TCP no es van dissenyar tenint en compte milers d'usuaris malintencionats que es podrien connectar als sistemes informàtics des d'arreu del món, hi ha una sèrie de protocols que fan que les tecnologies de la informació i les comunicacions es puguin desplegar i utilitzar de manera segura.

Entendre i saber usar les eines de seguretat i privadesa és essencial per a veure si la societat de la informació pot confiar prou o no en les tecnologies que hi donen suport.

En aquest mòdul estudiarem els aspectes generals de la seguretat en els ordinadors i les xarxes. En primer lloc, veurem els atacs als quals estan exposats els equips, els usuaris i la informació que s'hi desa o es transmet. També veurem quines eines, basades en la criptografia, fonamenten els sistemes i eines de seguretat, com també alguns exemples en què s'utilitzen aquestes tècniques.

La privadesa dels usuaris dels ordinadors i Internet és un tema relacionat amb la seguretat prou important perquè també en vegem els aspectes més importants. Així, doncs, hi dediquem un apartat. Finalment, farem una introducció dels aspectes de seguretat en la gestió audiovisual.

Objectius

Els objectius que l'estudiant haurà assolit en finalitzar aquest mòdul són:

1. Conèixer els diferents tipus d'atac que pot patir un sistema informàtic.

2. Conèixer les tècniques bàsiques per a protegir un sistema.

3. Comprendre el funcionament dels sistemes de xifratge i distingir-ne els diferents tipus.

4. Comprendre el concepte i ús de la signatura digital, relacionant-la amb la identitat digital.

5. Conèixer exemples d'ús de la identitat digital.

6. Comprendre els riscos que les tecnologies de la informació i les comunicacions comporten per a la privadesa dels usuaris.

7. Tenir coneixements bàsics dels sistemes de seguretat en la gestió de continguts audiovisuals.

1. La seguretat en les xarxes i a Internet

En aquest apartat, estudiarem quina mena d'aspectes relacionats amb la seguretat podem trobar com a membres de la societat de la informació. Un cop vistos aquests aspectes, durant la resta del mòdul desgranarem les tècniques i solucions per a dotar de seguretat les tecnologies de la informació i les comunicacions.

1.1. Els atacants

En primer lloc, veurem quins són els diferents perfils d'atacants. De ben segur que la primera paraula que se'ns acut és *hacker*. Tot seguit veurem que hi ha diferents tipus d'atacants dels sistemes informàtics, però aquest terme és el més cèlebre pels mitjans de comunicació, la literatura o el cinema.

El terme *hacker* té dos significats. D'una banda, s'aplica freqüentment per a descriure delinqüents informàtics el principal objectiu dels quals és trencar les barreres de seguretat dels sistemes informàtics. D'altra banda, aquest terme també s'aplica als informàtics brillants que han fet història per algun fet important.

Per tant, el mot *hacker* es pot aplicar com a elogi o bé amb el seu vessant pejoratiu. De fet, un *hacker* entrarà il·legalment en un sistema i senzillament ho farà com a demostració que és un informàtic molt expert (amb la consegüent satisfacció personal), o bé per evidenciar la manca de seguretat del sistema informàtic atacat. Si s'entra en el sistema per a inutilitzar-lo, el terme que s'aplica és *cracker*. Sigui amb la finalitat que sigui, ser un *hacker* implica tenir coneixements molt avançats d'informàtica, i ser constant i imaginatiu.

Pirates informàtics

No s'han de confondre els *hackers* amb els pirates informàtics. Els pirates fan còpies il·legals a gran escala de programari. Tot sovint un pirata en desactivarà les funcions de registre legal, proporcionarà claus de registre, etc.

En aquest mòdul utilitzarem les expressions *usuaris deshonestos* o *atacants* per a referir-nos als usuaris que tinguin com a finalitat atacar les xarxes de computadors i els sistemes d'informació. En aquest grup d'usuaris incloem els espies informàtics: aquests usuaris aprofiten l'accés massiu d'usuaris a les tecnologies de la informació i les comunicacions per obtenir-ne informació privada.

1.2. Els atacs

Un cop hem definit qui són els atacants, vegem quina mena d'atacs poden patir les xarxes de computadors i els sistemes informàtics.

Uns dels atacs més elementals són els **atacs físics**, que consisteixen a impedir que el maquinari funcioni adequadament. Per a dur-los a terme és essencial que l'atacant tingui accés físic al sistema atacat. El ventall de possibilitats és ben variat: des de desconnectar la xarxa elèctrica o de comunicacions, malmetre l'equip a base de cops o robar-lo. Clarament, evitarem aquests atacs ubicant els equips que continguin informació important en llocs on l'accés estigui degudament controlat.

Els servidors d'una xarxa de comunicacions solen estar ubicats en les sales de servidors. Aquestes sales tenen l'accés més o menys controlat i, a més, disposen de detectors de fum, sistemes d'extinció d'incendis i sistemes de refrigeració per a contrarestar les altes temperatures a causa del funcionament dels equips.

Uns dels atacs que es produeixen més sovint i que tenen ressò mundial són els atacs de **denegació de servei**[1], que consisteixen a impedir que els usuaris d'un sistema rebin servei. Aquesta denegació de servei es produeix perquè el sistema és víctima d'un col·lapse provocat per un atacant. Aquests atacs són populars perquè alguns grans serveis d'Internet n'han estat víctimes.

(1)En anglès, *denial of service attack o DoS attack*.

Inundació de peticions

Un atac habitual de denegació de servei es produeix quan l'atacant genera milers de peticions de connexió a un servei d'Internet determinat. Aquestes peticions es deixen a mig fer, de manera que queden obertes. Arriba un moment en què el servidor està saturat i no pot atendre més peticions.

Uns altres atacs que també tenen ressò en els mitjans de comunicació són els **atacs d'accés**, és a dir, els que es produeixen quan algú ha entrat de manera il·lícita en un sistema informàtic. Pot passar que l'atacant hagi aconseguit burlar les barreres de seguretat o bé entrar com si es tractés d'un usuari legal del sistema.

Exemples d'atac d'accés

Un exemple d'atac d'accés seria el cas d'un atacant que entrés en els sistemes d'un òrgan governamental i fes un canvi en la pàgina web principal. Un altre exemple consistiria a entrar en una xarxa social o gestor de correu electrònic com una altra persona, amb l'objectiu d'enviar informació en nom de l'atacat.

Es pot entrar en els sistemes informàtics utilitzant tècniques complexes, com ara la d'aprofitar forats de seguretat del sistema operatiu per a infiltrar-hi un programa que permeti obtenir el control de l'equip. D'altra banda, si per a entrar en un sistema el que cal és una contrasenya, aquesta es pot aconseguir gràcies a les tècniques d'**enginyeria social**.

Exemples de tècniques d'enginyeria social

Vegem a continuació un parell d'exemples de tècniques d'enginyeria social:

- Rebem una trucada telefònica en què ens diuen que són els tècnics del nostre proveïdor a Internet, i ens demanen les dades corresponents al nostre servei de correu electrònic, incloent-hi la contrasenya.

- Rebem un missatge de correu electrònic, suposadament de la nostra entitat bancària, i se'ns demana introduir les credencials d'accés al gestor bancari. Aquesta mena de tècniques de l'enginyeria social rep el nom de ***phishing***.

Un dels atacs històricament més importants i per als quals s'han desenvolupat importants protocols de comunicacions és l'**atac sobre la informació**. Hi ha dues menes d'atacs en funció del paper de l'atacant:

- D'una banda, hi ha els **atacs passius**. En aquesta mena d'atacs, l'atacant es limita a interceptar informació i llegir-ne el contingut. Per exemple, un usuari d'una LAN es dedica a recollir totes les trames que s'hi produeixen per intentar trobar informació important (per exemple, contrasenyes).

- D'altra banda, en els **atacs actius** l'atacant modifica la informació. Per exemple, es podria modificar l'ordre de pagament d'una targeta de crèdit perquè el compte corrent del destinatari de l'ingrés fos el de l'atacant.

L'èxit d'aquests atacs és complet si, a més, l'atacant passa desapercebut. Per exemple, el fet que totes les trames passin per les mans de l'atacant no hauria d'impedir que aquestes arribessin a la destinació originària. Si no fos així, algú s'adonaria que hi ha alguna cosa que no funciona del tot bé.

2. Seguretat en els equips informàtics

Els sistemes informàtics estan formats per diversos components. El programari dels sistemes informàtics dels primers ordinadors personals ja era una possible víctima d'atacs per part de virus. Avui dia, malgrat la gran quantitat d'elements que intervenen en els sistemes i la gran diversitat de programes que hi ha en el mercat i a Internet, la gestió de la seguretat d'un equip informàtic personal és prou senzilla. Contràriament, en els sistemes multiusuari, la seguretat implica altres conceptes més complexos, els quals són fora l'abast d'aquest material.

Dediquem aquesta part a explicar els conceptes bàsics de seguretat en un equip informàtic i a veure quines eines hi ha per a poder-hi fer front.

D'una banda, veurem el programari maliciós. Es tracta d'una colla de programes que tenen com a objectiu inutilitzar els sistemes o fer que el seu ús esdevingui una molèstia. D'altra banda, estudiarem els atacs d'accés als sistemes.

2.1. Els virus informàtics

Els virus informàtics són els programes maliciosos més populars, bàsicament perquè són els que des de fa més anys han creat molèsties als usuaris o danys irreparables en els seus sistemes informàtics.

Els **virus informàtics** són petits programes que s'escampen aprofitant l'execució d'altres programes infectats. Quan l'usuari executa aquest programa infectat, el virus queda resident en la memòria i va infectant altres programes.

El primer virus

El primer virus informàtic es va crear l'any 1972. Un ordinador infectat emetia aleatòriament per pantalla un missatge en to burleta. Per a eliminar-lo, es va crear, evidentment, el primer antivirus.

Quan els ordinadors personals tenien accés limitat a Internet, el mitjà per excel·lència de transmissió de virus eren els disquets: un ordinador infectat anava infectant els programes que continguessin els disquets que s'introduïen en el sistema. Els programes antivirus, capaços de detectar i eliminar virus, eren essencials si els usuaris no volien ser víctimes dels virus: quan s'introduïa un disquet a l'ordinador i es desconeixia si estava infectat, s'hi passava l'antivirus. Malgrat que avui dia els disquets no s'utilitzen gaire per a passar informació d'un sistema a un altre, els virus es poden escampar per mitjà de dispositius de memòria USB, fitxers descarregats d'Internet o, fins i tot, amb fitxers adjunts a correus electrònics.

Els virus poden crear multitud de molèsties diferents. D'una banda, els virus benignes no destruiran mai la informació que conté l'ordinador i es limitaran a mostrar textos de broma, a obrir i tancar aleatòriament el DVD de l'ordinador, a moure el ratolí, etc.

Exemple de virus benigne

Un virus molt popular als anys vuitanta fou el de la pilota (*ping-pong* en anglès), que feia aparèixer una pilota fent bots per tota la pantalla.

Per contra, els virus malignes eliminaran dades del sistema informàtic o bé en provocaran el tancament, sense donar l'opció a l'usuari de desar el treball que estava fent.

Hi ha virus que s'amaguen darrera de programes amb aparença inofensiva: per exemple, una presentació de diapositives per a desitjar-nos un bon any nou, o bé un programa que ens promet una navegació més ràpida. Quan executem el programa, obrim un programa maliciós que intentarà fer alguna malesa al nostre equip i escampar-se a d'altres. Aquesta mena de virus reben el nom de **cavalls de Troia**, que fa referència al cavall de Troia que els grecs van regalar als troians. Un mètode habitual de transmissió dels cavalls de Troia és l'ús del correu electrònic: el cavall de Troia és el fitxer adjunt i, per a escampar-se, s'envia per correu electrònic als contactes de la llibreta d'adreces.

2.2. Atacs des d'Internet

La infecció d'un sistema per part d'un virus és, en el fons, conseqüència de l'execució d'un programa per part de l'usuari del sistema informàtic. Tanmateix, l'accés massiu a Internet ha propiciat l'aparició i evolució de diferents sistemes d'atac per mitjà de l'accés, d'usuaris o programari externs, al mateix sistema informàtic.

Un exemple d'aquests sistemes són els **cucs**, que es consideren una variant dels virus informàtics. A diferència dels darrers, els cucs entren en el sistema directament des de la Xarxa. Donada la gran capacitat de reproducció dels cucs, aquests es poden arribar a escampar per milers d'equips d'Internet en qüestió de poc temps i esdevenir un problema seriós. Evidentment, quan un cuc entra en el sistema executa el seu atac, amb els mateixos efectes que pot tenir qualsevol virus.

En general, els cucs entren en el sistema per culpa de deficiències de programació. Tot sovint es tracta de factors que els programadors del sistema no van tenir en compte i que, un cop descoberts per la comunitat *hacker*, o bé són comunicats als programadors o bé són aprofitats pels *crackers* per a atacar o entrar en els sistemes per mitjà dels **exploits**.

Un ***exploit*** és un programari que aprofita una deficiència de programació del sistema operatiu per aconseguir algun objectiu relacionat amb l'accés al sistema tot trencant les barreres de seguretat.

Un *cracker* podria procedir de la manera següent: en primer lloc, detectaria que darrera una adreça IP determinada s'amaga una màquina amb un sistema operatiu determinat; un cop identificada la versió del sistema i els programes que s'hi estan executant, el *cracker* enviaria una sèrie d'*exploits*; si el sistema no està degudament protegit, se'ns podria instal·lar l'*exploit*; a partir d'ara, el *cracker* podria tenir accés a determinades parts del nostre sistema, o bé tenir-hi un accés total.

Actualitzacions del sistema operatiu

Noteu que, si el sistema està actualitzat, de ben segur tindrà arreglades les deficiències de programació que s'hagin detectat amb anterioritat.

2.2.1. Els segrestadors de navegador

El navegador d'Internet és un dels programaris més utilitzats avui dia. És per això que hi ha una part important del programari maliciós dedicada a afectar el comportament i l'ús dels navegadors. Aquest programari rep el nom, en anglès, de *browser hijacker*, que podríem traduir com a *segrestador de navegador*.

Exemples de segrestadors de navegadors

Il·lustrem amb un parell d'exemples el que podrien arribar a fer aquests programes segrestadors de navegadors:

- Un d'aquests programes podria obrir finestres del navegador que continguessin publicitat variada, com ara medicines de qualitat dubtosa, casinos en línia de poca confiança o, fins i tot, pornografia. Una variant seria que el programa hagués modificat la pàgina d'inici del navegador, la que s'obre automàticament en iniciar el navegador. Encara que la canviéssim des de les opcions del programa, el canvi no faria efecte, ja que el segrestador ens tornaria a canviar la pàgina.

- Un exemple més sofisticat és el del segrestador que modifica els resultats de les cerques que fem a Internet. Si, per exemple, cerquem informació sobre la UOC, els primers enllaços que mostraria serien pàgines que no hi tenen res a veure.

2.2.2. El programari espia

Finalment, esmentem el **programari espia**[2]. Es tracta d'un tipus de programari maliciós l'objectiu del qual és enviar a un servei remot informes de l'activitat de l'usuari, evidentment sense que aquest ho sàpiga. El que s'hi envia més habitualment és el nom dels serveis web que s'estan utilitzant, les paraules que s'estan cercant, etc. tot i que també hi pot haver programari espia capaç d'enviar contrasenyes i dades més importants.

(2)En anglès, el programari espia rep el nom de *spyware*.

2.3. Protecció del sistema

La protecció d'un sistema contra aquests atacs implica, en primer lloc, tenir consciència de la seva existència i del perill o incomoditat que poden comportar per als usuaris. En segon lloc, implica tenir una colla d'eines instal·lades en el sistema. Un sistema ben actualitzat amb les eines adequades estarà millor protegit que no pas un sistema sense cap mena de protecció.

Val a dir que els sistemes operatius actuals són susceptibles de patir la instal·lació de programari maliciós en major o menor mesura en funció del disseny del mateix sistema operatiu. Els sistemes que potencialment poden

rebre més atacs són els de Microsoft, donat el gran nombre d'usuaris que el fan servir i el seu disseny, sense considerar fortes mesures de seguretat. Les darreres versions d'aquests sistemes o bé incorporen eines que ajuden a la protecció del sistema o bé n'aconsellen la instal·lació a l'usuari.

Classifiquem les eines essencials de protecció en tres tipus: els programes antivirus, els programes de neteja i els tallafocs.

2.3.1. Programari antivirus

Els antivirus són programes encarregats de detectar virus al sistema i intentar eliminar-los. Actualment hi ha milers de virus informàtics. Cadascun d'ells té una empremta identificativa pròpia, és a dir:

- Un patró conegut relacionat amb el codi del programa que l'implementa. Alguns virus són més complexes, en el sentit que són capaços de mutar i generar variacions d'aquesta empremta.

- Una sèrie d'informació dipositada al registre del sistema operatiu, al sistema de fitxers, etc., que indica que el sistema està infectat.

Els programes antivirus es dediquen a comparar la informació del sistema informàtic (registre, sistema de fitxers, processos en execució, etc.) amb una base de dades d'empremtes i altra informació que permet identificar si hi ha un virus. Es cerquen virus a la memòria i als discs de l'ordinador. Si un virus es detecta, gairebé sempre es pot eliminar sense dificultat.

Per al bon funcionament d'aquest programari, convé que els usuaris estiguin sempre actualitzats: amb periodicitat freqüent s'actualitzen les bases de dades de definicions de virus per poder afrontar la detecció de nous virus i mutacions.

2.3.2. Programes de neteja

D'una manera semblant als antivirus, els programes de neteja examinen els equips per detectar i eliminar un altre tipus de programari maliciós, com ara segrestadors de navegador i tot allò relacionat amb el programari espia. Fins i tot hi ha eines que són una combinació d'antivirus i programes de neteja.

De la mateixa manera que en els antivirus, convé que les eines de neteja estiguin actualitzades, ja que la diversitat de programari maliciós augmenta amb una freqüència considerable.

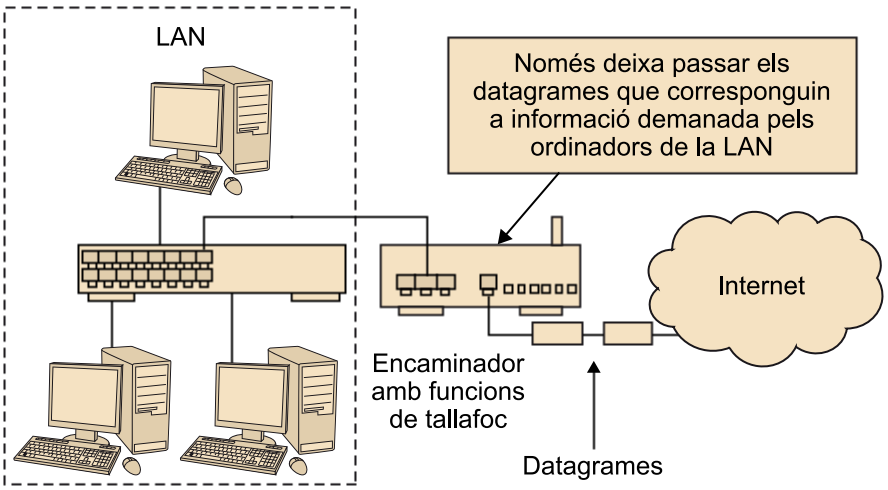
2.3.3. Tallafocs

Els tallafocs van ser concebuts com a elements per a controlar l'accés a les xarxes de computadors. Un tallafoc, per exemple, pot controlar les connexions que vénen de l'exterior i que tenen com a destinació un servidor web que es troba ubicat en la nostra LAN.

Els **tallafocs de xarxa** examinen els datagrames que van d'una xarxa a l'altra i, en funció de paràmetres com ara els ports d'origen o destinació i les adreces IP d'origen i destinació, denega o permet l'accés a aquests datagrames. La majoria d'encaminadors també poden fer la funció de tallafoc de xarxa.

La funció dels tallafocs s'il·lustra en la figura següent. Una de les configuracions típiques dels tallafocs de xarxa serveix per a denegar per defecte tots els accessos a la xarxa i deixar passar només les connexions que estiguin permeses. En el cas de la figura, només es permet l'entrada dels datagrames que corresponen a informació demanada pels ordinadors de la LAN. D'aquesta manera, els datagrames de connexions iniciades des d'Internet (i que podrien correspondre a atacs) no passaran pel tallafoc.

Exemple d'un encaminador amb funció de tallafoc



Així, doncs, un sistema sense tallafoc no té l'accés controlat i, en conseqüència, és susceptible de patir més atacs de l'exterior que un equip amb tallafoc.

Donat l'augment dels atacs externs contra equips informàtics personals, han anat apareixent diferents programes amb la funció de **tallafoc local**. Aquests tallafocs controlen el trànsit de xarxa que entra o surt de l'equip: programes que intenten accedir a serveis remots d'Internet, usuaris de la LAN que intenten entrar en el nostre sistema de fitxers, etc.

Amb un tallafoc instal·lat i ben configurat, l'equip està més ben protegit contra els cucs i els atacs per mitjà d'*exploits*.

3. Seguretat en la informació

En aquesta part ens dedicarem a conèixer les tècniques que permeten dotar de seguretat la informació que es transmet en una xarxa. Abans de concretar-ne diferents aspectes, anem a definir-los.

D'una banda, estudiarem com es pot aconseguir la **confidencialitat** de la informació que es transmet per una xarxa, és a dir: que la informació sols estigui disponible per als participants en la comunicació. També veurem com es pot garantir l'**autenticitat** de les dades, és a dir, garantir que la informació no ha estat modificada i que prové realment d'on se'ns indica. Aquest concepte d'autenticitat està fortament lligat amb el concepte de seguretat en la identitat, que desenvoluparem en l'apartat 4.

Per a tractar la confidencialitat disposem de les eines de xifratge, mentre que per a tractar l'autenticitat disposem de les eines d'integritat i les signatures digitals. Les tècniques que estudiarem en aquesta part formen part de la criptografia.

3.1. Xifratge de la informació

El xifratge de la informació i la mateixa criptografia es remunten a èpoques molt antigues. Els primers sistemes de xifratge –que daten de l'època de la Grècia clàssica i foren àmpliament usats durant l'Imperi Romà i l'edat mitjana– es basen en dues tècniques ben senzilles: la substitució de lletres i el canvi de posició.

> Els mètodes clàssics de xifratge es basen en la substitució d'una lletra per una altra i/o en el canvi d'ordre les lletres que conformen el text.

Mitjançant l'estudi d'un parell de sistemes clàssics de xifratge, aprendrem una sèrie de conceptes relacionats amb aquest i la criptografia en general.

3.1.1. El xifratge de Cèsar

Es veu que Juli Cèsar feia servir aquest sistema per a comunicar-se amb els generals: els enviava un missatge xifrat i solament el general a qui anava dirigit en podia llegir el contingut.

El general en qüestió coneixia la **clau** del xifratge, que evidentment també era coneguda per Juli Cèsar. Si, per exemple, la clau era 3, i el missatge original (tècnicament anomenat **text net**) era *lavidaesbella*, el missatge xifrat seria *odylgdlvehood*. Per a obtenir-lo s'avançava, en tres posicions, cada lletra de l'alfabet. Si la lletra a xifrar era la *a*, el resultat seria la *d*.

Per a desxifrar el missatge, se seguia el procés invers, és a dir, es retrocedia en tres posicions de l'alfabet.

Si és interessant veure com es xifra la informació, també ho pot ser intentar conèixer els continguts dels missatges sense conèixer-ne la clau. Això és el que es coneix com a **trencar un criptosistema**.

Per a trencar el sistema, podem optar per un **atac de força bruta**, consistent a provar totes les claus possibles fins a trobar un text desxifrat que s'entengui.

Per tant, un atacant que interceptés el missatger i li robés el missatge podria provar totes les claus possibles fins a obtenir-ne una de correcta:

- Si retrocedís una posició, obtindria *ncxkfcgudgnnc*, que és inintel·ligible.
- Si retrocedís dues posicions, obtindria *mbwjebftcfmmb*, que també ho és.
- En retrocedir tres posicions, obtindria *lavidaesbella*, que ja es pot llegir.

Fixem-nos que, en el pitjor dels casos, caldria provar tantes vegades com claus hi poden haver. Noteu que l'atacant també hauria de saber que el sistema de xifratge és del Cèsar i no d'un altre! Tanmateix, fixem-nos en un detall: el fet que hi hagi dues *o* seguides (*odylgdlvehood*) podria indicar que la *l* s'ha convertit en *o* i, per tant, es podria arribar a deduir la clau. Per això per millorar el sistema de xifratge pot resultar interessant combinar aquest xifratge amb el que descrivim a continuació.

3.1.2. El xifratge amb rails

Ara veurem un sistema basat en el canvi d'ordre de les lletres del text net: el xifratge amb rails[3]. En aquest sistema el text es col·loca repartit en rails, en forma de zig-zag (per això també es coneix amb el nom de *zig-zag*). Suposant que la clau és 2 i fent servir el text net *lavidaesbella*, es procediria com segueix.

[3] En anglès, *rail fence cipher*.

En primer lloc, es col·locarien les lletres sobre dos rails, en zig-zag:

l		v		d		e		b		l		a
	a		i		a		s		e		l	

I es llegiria el missatge línia a línia, la qual cosa donaria lloc a *lvdeblaaiasel*. Perquè l'atacant pogués trencar aquest sistema, a més de saber que el xifratge segueix aquest mètode, hauria de provar amb tots els nombres possibles de rails.

3.2. Sistemes actuals de xifratge

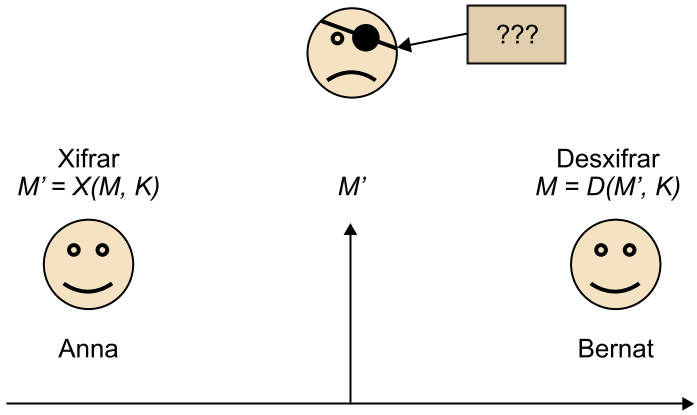
Durant segles s'han fet servir sistemes similars als anteriors, o combinacions complexes de tots dos sistemes. Hem de tenir present que l'aparició de màquines de xifratge va permetre xifrar missatges de manera complexa amb un temps prou curt. Tanmateix, l'aparició dels ordinadors en la segona meitat del segle XX va permetre l'èxit dels atacs de força bruta en un temps factible.

Amb l'aparició de la informàtica i l'ús d'aquesta per al xifratge de les comunicacions, els missatges no es xifren lletra a lletra, sinó a partir dels bits que els formen. En la figura següent hi ha un exemple. Es podria partir de la traducció amb codi ASCII d'un missatge de text per a tenir la tira de bits que el representa. Hi ha un algorisme *X* que xifra un missatge *M* fent servir la clau *K*. Paral·lelament, hi ha un algorisme *D* que obté el text net a partir del missatge xifrat *M'* sempre que es faci servir **la mateixa clau *K***.

Vegeu també

Recordeu que hem parlat del codi ASCII en el mòdul "Aspectes tecnològics dels sistemes informàtics".

Exemple d'aplicació de xifratge amb clau compartida. L'atacant no pot interpretar el missatge.



La màquina Enigma

La màquina Enigma és un giny electromecànic capaç de xifrar i desxifrar missatges. Inventada als anys vint, és famosa perquè els alemanys la van utilitzar durant la Segona Guerra Mundial.

Els exemples del xifratge de Cèsar i el de rails formen part del que s'anomena **xifratge de clau secreta**, **compartida** o **xifratge simètric**. En aquests casos la clau és coneguda tant per l'emissor com pel receptor. Per tant, qui no conegui la clau serà incapaç d'entendre la informació, tret que insisteixi en el trencament per força bruta.

D'altra banda, hi ha dues alternatives a l'hora de xifrar amb clau simètrica:

- En comptes de fer servir un algorisme complex, el missatge xifrat és el resultat de combinar el missatge amb una clau tan llarga com el missatge. Aquesta alternativa s'anomena **xifratge de flux**.

- Utilitzar combinacions molt complexes de les tècniques vistes en el subapartat 3.1. El text net es divideix en una sèrie de blocs que van entrant en el sistema de xifratge i van produint, en blocs, el text xifrat. Aquesta alternativa es coneix com a **xifratge de bloc**.

Tot seguit analitzarem aquestes propostes més a fons.

3.2.1. Xifratge de flux

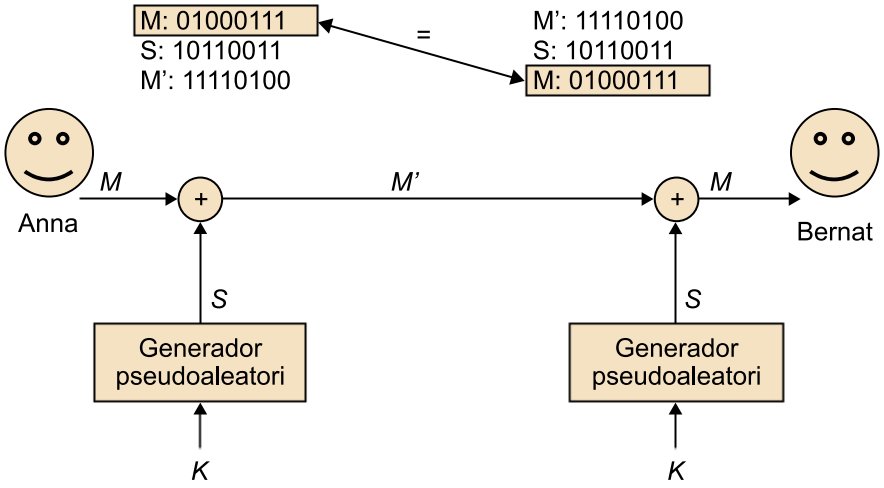
El xifratge de flux es fa servir molt en les telecomunicacions. Per exemple, en una conversa de telefonia mòbil, la veu es digitalitza (és a dir, es converteix a un flux de bits) i s'envia xifrada per la xarxa de comunicacions. Per a no entorpir la conversa, el procés de xifratge hauria de ser prou ràpid per a no afegir retard a la comunicació. És per això que convé que l'operació de xifratge sigui ràpida.

La figura següent mostra com s'utilitza el xifratge de flux. En concret, cada bit d'entrada al sistema de xifratge (el missatge *M*) es combinarà, usant la funció lògica XOR, amb el bit corresponent del flux clau *S* per a donar lloc al bit corresponent al flux de sortida. El receptor farà el mateix procés de combinació amb la XOR per obtenir el flux desxifrat.

Vegeu també

En el mòdul "Aspectes tecnològics dels sistemes informàtics" hem estudiat el concepte de funció lògica, com ara la XOR.

Exemple d'ús del xifratge de flux en què intervé un generador pseudoaleatori que fa servir una clau compartida



La fortalesa dels sistemes de xifratge de flux es basa en la clau utilitzada per a xifrar. Sense entrar en detalls, podríem dir que es tracta d'una clau aleatòria i molt llarga, sovint tan llarga com la tira de bits que s'acabarà xifrant. Ara bé, com podem tenir una clau aleatòria tan llarga? Si és aleatòria, com la podem fer conèixer al receptor de la informació? La solució a aquestes qüestions passa per conèixer el concepte de **generador pseudoaleatori**.

Un **generador pseudoaleatori** és un algorisme que, a partir d'un mateix valor d'entrada o clau, genera el mateix flux de bits de sortida, el qual té l'aspecte de seqüència aleatòria.

Perquè la seqüència sembli aleatòria cal que el nombre de zeros produïts sigui similar al nombre d'uns produïts. Tanmateix, hi haurà un moment en què aquesta seqüència es tornarà a repetir. Aquest moment defineix el període de la seqüència, i com més llarg sigui aquest període més aleatòria semblarà la seqüència. La seqüència pseudoaleatòria següent té el període en negreta:

0110011010110011011001100110101100110110011001 1

És evident que els generadors pseudoaleatoris van generant bits en un temps prou ràpid per a no introduir retards en les comunicacions.

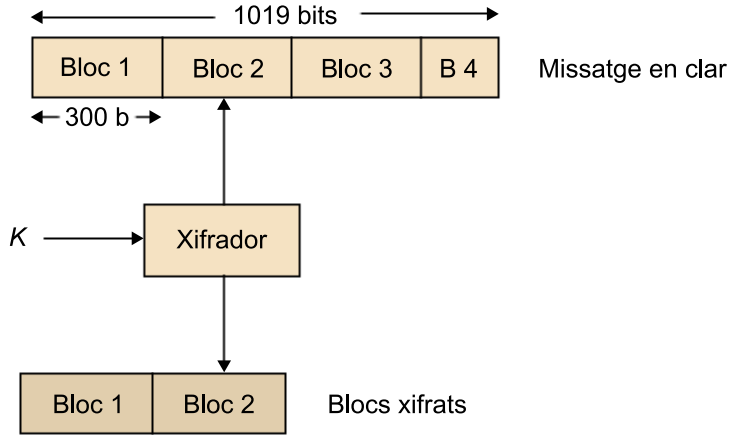
3.2.2. Xifratge de bloc

El xifratge de bloc utilitza combinacions complexes basades en substitucions i canvis de posició que es regiran per la clau de xifratge. Aquests sistemes són més costosos, tant pel que fa a la fabricació de dispositius com a la computació, que els sistemes de xifratge de flux (incloent-hi la generació de la seqüència). Per contra, amb claus relativament curtes, de 128 bits o 256 bits, ofereixen una seguretat prou bona contra els atacs de força bruta. El funcionament del xifratge de bloc té diferents variants. La més simple, el llibre de codis electrònic[4] (ECB), es caracteritza perquè la sortida corresponent a un determinat bloc depèn de la clau i del mateix bloc.

[(4)]En anglès, *electronic codebook*.

En la figura següent es mostra l'aplicació del xifratge de bloc amb la variant ECB. El missatge inicial, de 1.019 bits, s'ha de dividir en blocs. Com que el xifrador de l'exemple treballa amb blocs de 300 bits, es necessiten tres blocs: els tres primers de 300 bits, i el darrer de 119.

Exemple d'aplicació del xifratge de bloc



Aplicació del xifratge de bloc segons l'exemple del text, en un estat intermedi en què es xifra el segon bloc de text.

Un dels primers sistemes utilitzats en la informàtica fou l'estàndard per a l'encriptació de dades[5] (DES). Aquest sistema dividia el missatge d'entrada en blocs de 64 bits i feia servir una clau de 56 bits. A mesura que els ordinadors guanyaven potència de càlcul, el sistema DES era més a prop de quedar inutilitzat perquè es podria trencar, per força bruta, en un temps factible (potser en unes quantes hores). Així, doncs, es va començar a utilitzar una variant, el triple DES, amb claus de 192 bits i que equivalia a utilitzar el DES diverses vegades.

[5]En anglès, *data encryption standard*.

Atacs de força bruta

Si un algorisme triga 1 nanosegon a executar-se i volem provar totes les claus de 256 bits possibles, haurem d'executar l'algorisme 2^{256} vegades. Per tant, seran 2^{256} nanosegons, és a dir, trigarem molts anys a trencar el sistema... El coneixement a fons dels sistemes de xifratge permet dissenyar estratègies de força bruta més elaborades, que permeten el trencament d'alguns sistemes en "menys anys".

Actualment, l'algorisme que substitueix el DES i el 3DES és l'AES[6], que utilitza blocs de 128 bits i claus de fins a 256 bits.

[6]En anglès, *advanced encryption standard*.

Fortalesa digital

El llibre *Fortalesa digital*, de Dan Brown, tracta sobre un escenari hipotètic on tothom creu que els sistemes de xifratge no es poden trencar. Tanmateix, els serveis d'intel·ligència saben desxifrar els missatges que la resta de la humanitat (incloent-hi els delinqüents) creu que ningú pot desxifrar.

3.3. Sistemes de clau pública

Fins ara hem parlat de diferents sistemes de xifratge i hem après alguns conceptes bàsics de la criptografia. Tot i això, no hem parat atenció al fet que els sistemes de clau compartida tenen com a punt feble la pròpia clau:

- La clau s'ha de compartir, amb la qual cosa cal un canal segur de transmissió de claus entre els comunicants. Una manera de transmetre la clau seria per mitjà d'una trobada presencial entre els participants en la comunica-

ció, en la qual es passarien la clau gravada, per exemple, en una memòria USB.

- A priori, necessitem una clau per a cadascuna de les diferents parelles de participants que es volen comunicar.

Tot això fa que generalitzar un sistema de xifratge de clau compartida en un entorn global com ara Internet sigui poc factible. Afortunadament, l'any 1976 tres matemàtics, Whitfield Diffie, Martin Hellman i Ralph Merkle van dissenyar un sistema que permet als dos participants calcular una clau compartida sense haver-se de passar informació compromesa, conegut com Diffie-Hellman.

Amb aquest sistema s'inicia la **criptografia de clau pública** o **criptografia asimètrica**.

La clau pública

La clau pública resol els problemes que tenien els sistemes de clau simètrica pel que fa a la quantitat de claus necessàries per a la comunicació amb un gran nombre d'usuaris potencials i la distribució de les claus.

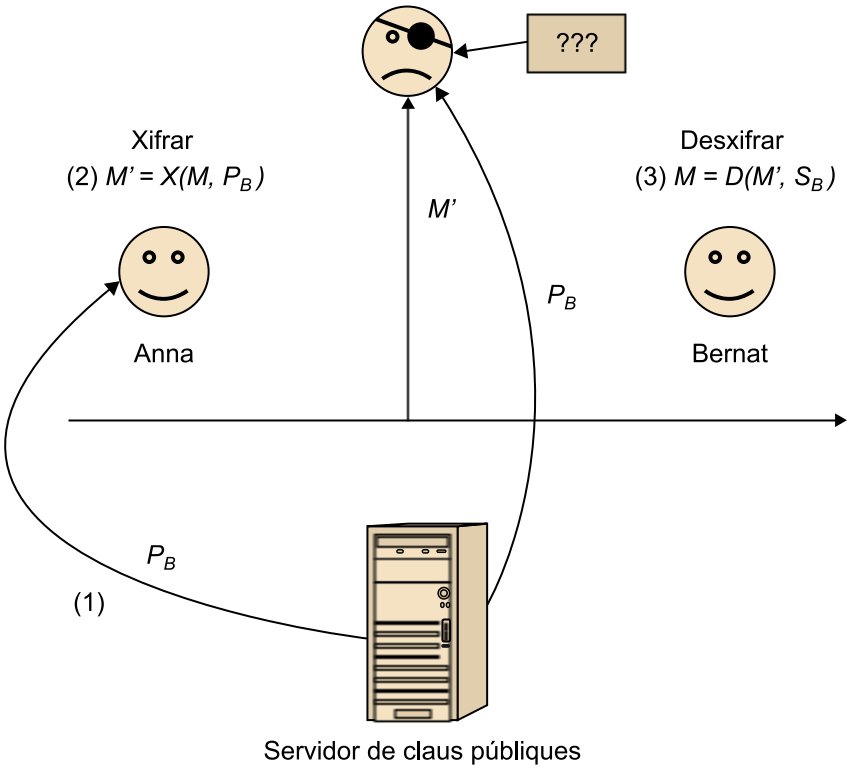
La criptografia de clau pública es basa en l'ús de dos valors o claus: l'un és la **clau pública** i tothom la pot conèixer, l'altre és la **clau privada** i ha d'estar custodiada pel seu propietari.

3.3.1. Xifratge de clau pública

Vegem un exemple sobre quin paper tenen les claus públiques i privades en el procés de xifratge.

Suposem que l'Anna vol enviar un missatge secret al Bernat. L'Anna té la clau privada S_A i la clau pública P_A. El Bernat també té el seu parell de claus S_B i P_B.

Procés de xifratge amb un sistema de clau pública



Tal com es mostra en la figura anterior, es procedirà de la manera següent:

- L'Anna obtindrà per mitjà d'un servei d'Internet la clau P_B (pas 1 de la figura).

- L'Anna utilitzarà un algorisme de xifratge X per a xifrar el missatge M i obtenir el missatge xifrat M' (pas 2 de la figura).

$$M' = X(M, P_B)$$

- En rebre M', el Bernat utilitzarà la clau S_B (és a dir, la seva clau secreta) per a executar l'algorisme de desxifratge i obtenir M (pas 3 de la figura).

$$M = D(M', S_B)$$

Vegeu que el Bernat és l'únic que podrà desxifrar el missatge, ja que és l'únic que hauria de tenir accés a S_B. Així, doncs, l'usuari deshonest de la figura, malgrat tenir accés al missatge xifrat M' i a la clau pública del Bernat, no serà capaç de desxifrar el missatge.

Protecció de la clau privada

Les claus privades es desen protegides amb una contrasenya o bé en un dispositiu segur com ara una targeta intel·ligent (al qual també s'accedeix mitjançant una contrasenya).

Ús de cadenats

Podem fer l'analogia entre la clau privada i els cadenats: el cadenat és la clau pública, i la clau que el pot obrir és la clau privada. Tothom pot fer servir un cadenat per a tancar una caixa de manera que només la pugui obrir el propietari de la clau del cadenat.

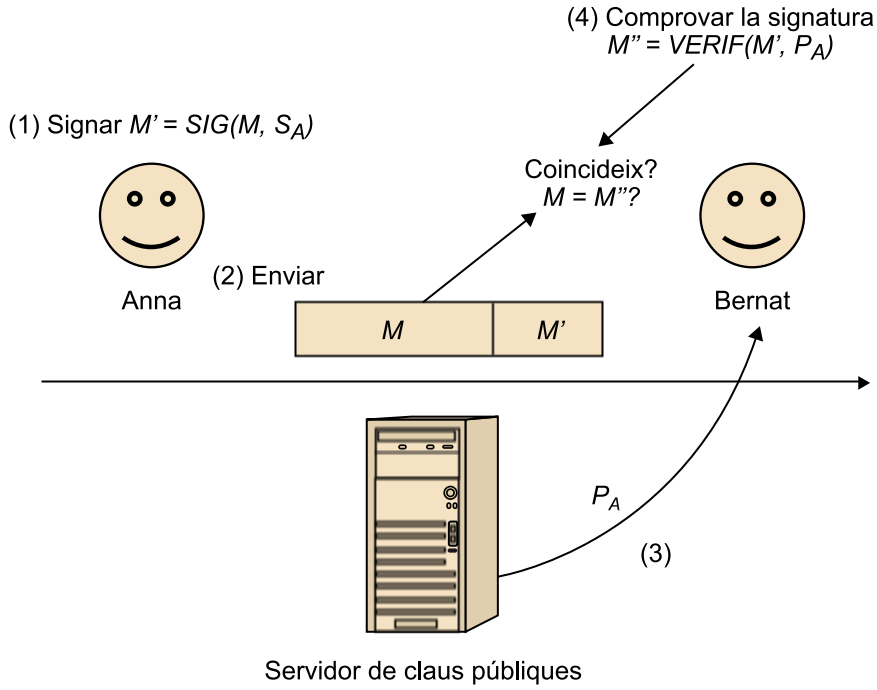
3.4. Signatures digitals

Ara veurem com s'aconsegueix comprovar l'autenticitat de la informació amb la mateixa criptografia de clau pública per mitjà del que s'anomenen **signatures digitals**.

Les **signatures digitals** són una aplicació de la criptografia de clau pública que permet donar autenticitat d'origen a la informació enviada, assegurar-ne la integritat i impedir el repudi de qui signa.

Seguim amb l'exemple de l'Anna i el Bernat, i les seves claus públiques i privades. La figura següent il·lustra aquest procés.

Procés de signatura amb un sistema de clau pública



Suposem que l'Anna vol fer una signatura digital d'un missatge *M* que enviarà al Bernat:

- L'Anna farà servir un algorisme *SIG* de signatura, amb la seva clau privada S_A, per a produir la signatura del missatge *M* (pas 1 de la figura):

$$M' = SIG(M, S_A)$$

- L'Anna enviarà al Bernat el missatge *M* juntament amb la seva signatura *M'* (pas 2 de la figura).

Un cop el Bernat rebi el missatge i la seva signatura, procedirà com segueix:

- El Bernat obtindrà la clau pública de l'Anna per mitjà d'un servei d'Internet (pas 3 de la figura).

- El Bernat usarà l'algorisme *VERIF* de verificació, aquest cop posant-hi la signatura i la clau pública de l'Anna (pas 4 de la figura):

$$M'' = VERIF(M', P_A)$$

- Si el resultat M'' de l'algorisme coincideix amb el missatge original M, voldrà dir que el missatge rebut és autèntic.

Com ja s'ha apuntat anteriorment, els sistemes de signatura digital asseguren diverses propietats. Vegem-les amb més detall sobre l'exemple anterior:

- Atès que l'Anna és l'única que té accés a la clau S_A, és l'única que pot haver signat el missatge. Per tant, **l'origen del missatge és autèntic**, ja que no el pot haver signat ningú més. Fixem-nos que una signatura "real" seria més fàcil de falsificar que no pas una de digital.

- Com que l'Anna és l'única que coneix la seva clau, no podrà dir mai que no ha signat el missatge. Aquesta propietat s'anomena **no-repudi**.

- Finalment, les propietats dels sistemes de signatura digital fan que si el missatge M es modifiqués durant el camí, ni que fos només en 1 bit, la comprovació de la signatura ja no funcionaria. Per tant, les signatures digitals garanteixen la **integritat** de la informació.

3.4.1. Funcions de resum

Una de les diferències entre els algorismes de criptografia de clau compartida i els de clau pública és que els darrers són més costosos computacionalment. Per exemple, un programa esmerça més temps a aplicar un algorisme de clau pública per a xifrar un missatge que no pas a xifrar-lo amb un mètode de clau compartida. A més, les claus dels sistemes de clau pública són més llargues que les usades en clau compartida (1.024 bits, 2.048 bits o més).

En el cas de les signatures digitals, per a fer les signatures més ràpidament no se signa el missatge, sinó un resum d'aquest.

Les **funcions de resum** generen una tira de bits d'una longitud determinada a partir d'un missatge de qualsevol longitud.

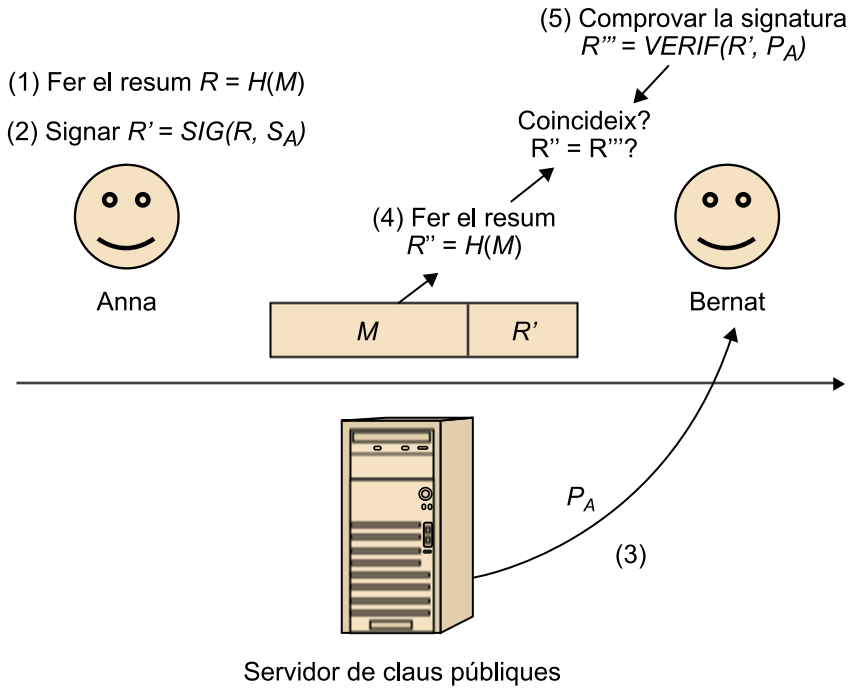
SHA

Una de les funcions de resum més utilitzades és la SHA (de l'anglès *secure hash algorithm*, algorisme de resum segur), la qual genera resums de 160 bits.

Perquè aquestes funcions de resum es puguin utilitzar en els algorismes de signatura digital, han de complir diverses propietats. Una és que una alteració mínima en el missatge ha de donar un resum diferent de si el missatge no s'hagués alterat (qüestió estretament relacionada amb la propietat d'integritat).

Així, doncs, tal com veiem en la figura següent, l'Anna primer farà el resum del missatge *M* fent servir la funció de resum *H* (pas 1 de la figura) i tot seguit farà la signatura d'aquest resum (pas 2 de la figura). Com en el cas anterior, el Bernat obtindrà la clau pública de l'Anna per mitjà d'un servei d'Internet (pas 3 de la figura). Tot seguit, el Bernat farà el resum del missatge rebut (pas 4 de la figura) i farà servir aquest resum per a verificar la validesa de la signatura digital rebuda de l'Anna (pas 5 de la figura). Noteu que fer el resum no requereix el coneixement de cap clau pública ni privada.

Procés de signatura de clau pública amb funcions de resum



4. Identitat digital

Si l'Anna envia un missatge xifrat al Bernat, ha de fer servir la clau pública del Bernat. Per exemple, se la descarregarà de la pàgina web del Bernat i la desarà en el disc de l'ordinador perquè el programari criptogràfic de xifratge la pugui fer servir. Fixem-nos que és fonamental estar segurs que la clau pública del Bernat és realment del Bernat.

La **identitat digital** és tot allò que fa referència a assegurar que una clau pública determinada es correspon amb un individu determinat.

Exemple d'identitat digital

Un dels exemples més clars del concepte d'identitat digital és el DNI electrònic: aquest consisteix en una targeta intel·ligent que conté la nostra clau privada i, alhora, la nostra clau pública. Amb aquesta clau ens podem identificar per a fer diversos tràmits per Internet.

Per a assegurar que una clau pública determinada correspon a una identitat concreta, es fa servir un sistema de certificats de clau pública.

Un **certificat de clau pública** és un document electrònic que vincula una clau pública a una identitat.

La informació bàsica que conté un certificat és:

- La identitat que certifica, per exemple, una adreça de correu electrònic o el número de DNI d'un ciutadà.
- El període de validesa, és a dir, una mena de data de caducitat a partir de la qual el certificat no serà reconegut com a vàlid.
- La clau pública que se certifica.
- El nom de l'emissor del certificat. Es tracta d'una **autoritat de certificació**, un organisme que pot expedir certificats de clau pública.

Les autoritats de certificació poden ser òrgans regulats pel govern dels estats, com ara la Fàbrica Nacional de Moneda i Timbre, o empreses certificadores de gran reputació (com ara VeriSign). Tanmateix, hi pot haver autoritats de certificació d'àmbit més petit (per exemple, per a fer certificats per a les claus públiques del personal de la UOC).

Autoritats de confiança

Les autoritats de certificació poden fer una petició als fabricants de programari perquè les incloguin com a autoritats de confiança.

Les grans empreses certificadores internacionals ja són reconegudes per la majoria de programari criptogràfic. En aquest sentit, quan el programari ha d'utilitzar una clau pública certificada per alguna d'aquestes empreses ho fa sense cap problema, ja que es tracta d'una autoritat de confiança.

Quan s'utilitza una clau pública certificada per una autoritat que no està reconeguda pel programari, aquest pregunta a l'usuari si confia en la veracitat de l'autoritat. Per tant, en el fons, són els usuaris els que decideixen si tirar endavant o no. Si es diu que sí, l'autoritat passarà a ser reconeguda, i el programari ja no ens preguntarà quan es facin servir altres claus públiques certificades per aquesta autoritat.

L'àmbit de l'autoritat de certificació té molt a veure amb l'ús de la clau pública. Per exemple, podria ser que una clau pública certificada per una autoritat de certificació dependent d'un organisme autonòmic només tingués validesa per a tràmits en línia d'aquest organisme. O fins i tot hi pot haver reconeixements entre autoritats: per exemple, la clau certificada per un organisme estatal pot utilitzar-se en tràmits de l'organisme autonòmic.

Les autoritats de certificació disposen d'un sistema generador i gestor de claus i certificats: les **infraestructures de clau pública**. Aquestes infrastructures també disposen de **llistes de revocació** que serveixen per a especificar quins certificats han deixat de ser vàlids abans que caduquin (per exemple, perquè l'usuari ha perdut la clau privada i algú altre la podria utilitzar).

Fins aquí hem estudiat els fonaments del xifratge i la signatura digital. En aquest apartat veurem, breument, uns exemples d'ús del xifratge i la signatura digital a Internet: el comerç electrònic, el correu electrònic segur i els tràmits en línia.

4.1. Comerç electrònic

El comerç electrònic ha representat una revolució en la manera de vendre i comprar. Des de casa nostra i fent servir el navegador podem comprar entrades de cinema, roba, bitllets d'avió, fer reserves d'hotel, etc. Pel que fa a la seguretat, un dels punts més importants és el moment de fer el pagament de la compra. Per exemple:

- Convé que la informació que enviem sigui confidencial, per exemple, a l'hora d'enviar les dades de la targeta de crèdit.

- També és important que el servei al qual ens connectem sigui autèntic. És a dir, que quan posem les dades de la targeta de crèdit ho fem en el servei en línia del banc, i no pas sobre un web fals creat per uns falsificadors de targetes.

En el comerç electrònic s'utilitzen sistemes de xifratge simètric i sistemes de clau pública. Quan ens connectem al servei del banc, ho fem sobre una connexió segura SSL[7] (una extensió de les connexions TCP que garanteixen propietats de seguretat de la informació transmesa). Aquestes connexions segures s'identifiquen per mitjà d'un cadenat que veiem en el mateix navegador que mostrem en la figura següent.

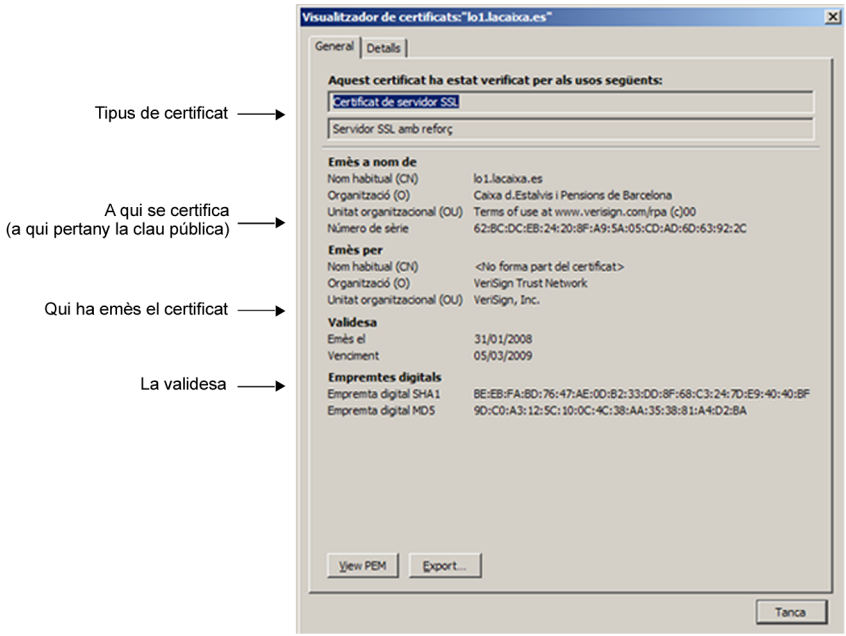
[7]En anglès, *secure socket layer*.

Cadenat en el navegador web

El cadenat en el navegador web indica que s'està fent servir una connexió que garanteix la seguretat de les dades.

El navegador també permet visualitzar la informació que conté el certificat que ens ha enviat el servei web. En la figura següent apareix la informació que ens proporciona el navegador web.

Informació sobre el certificat que mostra el navegador web



Durant el procés de connexió, el servidor envia un certificat. Aquest conté, entre altres, una clau pública i l'autoritat de certificació emissora del certificat. Si el nostre programari ja confia en aquesta autoritat, el procés seguirà endavant. Si, al contrari, no hi confia (no es tracta d'una autoritat àmpliament reconeguda), el navegador ens preguntarà si volem continuar o no amb el procés de connexió segura.

Seguretat electrònica

La seguretat que ofereixen els sistemes de comerç electrònic a l'hora d'efectuar els pagaments és superior a la dels pagaments tradicionals. En el comerç electrònic l'usuari controla l'ús de la seva targeta i les dades que introdueix viatgen de manera segura cap al servei en línia del banc. En canvi, quan donem la targeta a qualsevol no sabem quantes vegades la passarà o si en farà duplicats.

Si s'accepta la clau pública, aquesta es fa servir per a generar el que s'anomena una **clau de sessió**. Recordem que els sistemes de xifratge de clau pública són més lents que els de clau compartida. Per tant, es tria una clau compartida que serà la clau de sessió que es farà servir per a xifrar de manera ràpida les comunicacions (els datagrames) que s'enviaran dins la connexió segura.

El pagament amb targeta de crèdit

Tanmateix, si l'autenticació del servidor i el xifratge de les dades de pagament estan perfectament resolts, l'autenticació del client no és prou segura davant d'usos il·lícits de la targeta de crèdit. Tot i que cada cop és més habitual que es faci servir el telèfon mòbil per a enviar missatges de confirmació i que el servei de pagament pugui comprovar que qui fa el pagament és realment el posseïdor de la targeta de pagament. Això no és prou segur davant un robatori de bossa, en què el lladre té accés a la targeta de crèdit i al mòbil.

4.2. Correu electrònic segur

El correu electrònic segur permet enviar missatges signats i/o xifrats. El sistema S/MIME és una extensió del MIME que permet la signatura i xifratge de missatges. La pràctica totalitat de gestors de correu electrònic permeten aquestes funcions. Vegem què implica l'enviament de correu electrònic segur:

- Per a **enviar un missatge signat**, en el mateix correu electrònic s'envia la signatura del missatge i el certificat de la nostra clau pública. Així, doncs, el programari receptor del missatge accedirà a la nostra clau pública, inclosa dins el mateix missatge, i en podrà verificar la validesa gràcies al certificat també inclòs en el missatge. Es farà servir la clau pública per a verificar la signatura digital del missatge.

- Per a **enviar un missatge xifrat**, caldrà la clau pública del destinatari. Per a obtenir-la, serà suficient de demanar-la-hi. Si ens envia la clau (juntament amb el certificat), la podrem instal·lar en l'equip per a xifrar el missatge i també per a usos posteriors.

Correu electrònic segur

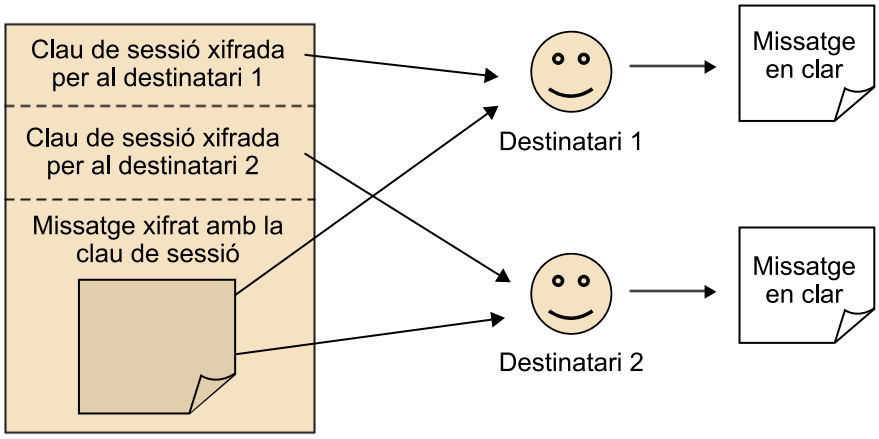
Si prèviament havíem rebut un missatge signat pel que ara serà destinatari del missatge xifrat, ja disposarem de la seva clau pública en el nostre sistema.

El sistema S/MIME fa servir la tècnica del **sobre digital** per a enviar un missatge xifrat. El sobre digital que es mostra en la figura consisteix en el següent:

1) Triar aleatòriament una clau de sessió que es farà servir per a xifrar el missatge mitjançant un sistema de xifratge simètric.

2) Adjuntar, amb el mateix missatge signat, la clau de sessió xifrada per a cadascun dels diferents destinataris que pugui tenir el missatge. Així, doncs, en el cas de la figura, en què cal enviar un mateix missatge a dos usuaris diferents, hi afegirem dues versions de la clau de sessió: una xifrada amb la clau pública del destinatari 1, i una altra xifrada amb la clau pública del destinatari 2.

Estructura d'un missatge xifrat per a dos destinataris



D'aquesta manera podem enviar un únic missatge xifrat per a diversos destinataris i, alhora, evitem el cost computacional que implicaria xifrar tot el missatge (incloent-hi fitxers adjunts) amb un sistema de clau pública.

4.3. Tràmits en línia

Els tràmits en línia haurien de donar més o menys garanties de seguretat en funció del risc que representen.

Exemple de garantia de seguretat

L'obtenció d'una llista de productes sol·licitats a una botiga en línia representa un risc més baix que demanar el canvi de dades bancàries per al cobrament de la nòmina.

Actualment hi ha tràmits en línia que demanen un registre en el servei a partir de determinades dades i n'hi ha que demanen específicament que l'usuari estigui autenticat amb un certificat de clau pública. Tota aquesta heterogeneïtat de sistemes d'autenticació per als tràmits en línia se soluciona utilitzant la identitat digital ciutadana.

Exemple de registre en el servei

L'import de la factura telefònica per al cas de tràmits en línia amb la companyia telefònica és un exemple de tràmit que demana un registre al servei.

La **identitat digital ciutadana** permet que l'usuari estigui degudament autenticat davant les administracions per a fer qualsevol mena de tràmit en línia.

Així com l'estat és qui controla la identitat dels seus habitants, assignant-los un nombre que els identifica, també pot generar una clau pública amb el certificat corresponent perquè s'identifiqui davant els diferents serveis d'Internet.

El certificat es troba emmagatzemat en un dispositiu segur que s'introdueix en el sistema informàtic de l'usuari quan el servei en línia en demana la identificació. Per a garantir més seguretat, l'accés al dispositiu segur s'hauria de fer sempre que l'usuari introdueix correctament una contrasenya.

El DNI electrònic espanyol

En el cas del DNI electrònic per a l'Estat espanyol, el dispositiu segur és una targeta intel·ligent (en anglès *smartcard*). Dins la targeta hi ha un xip de seguretat, que conté informació com ara claus privades, claus públiques i certificats.

El DNI electrònic per a l'Estat Espanyol

La realització de tràmits en línia genera documents electrònics als quals es pot demanar d'aplicar una signatura electrònica abans d'enviar-se pel servei d'Internet.

5. Privadesa i Internet

És evident que avui dia milions de persones de diferents edats i nivells educatius utilitzen Internet. Com veurem en el mòdul "El World Wide Web", aquests usuaris, que poden ser persones amb coneixements mínims sobre tecnologia o bé persones molt expertes, no solament accedeixen a Internet per obtenir informació, sinó per comunicar-se i, darrerament, contribuir a posar-hi informació.

Les tecnologies d'Internet permeten registrar l'activitat diària dels usuaris, de manera que es pot analitzar la informació i es poden arribar a crear perfils d'usuaris: hàbits de cerca en els cercadors, historial de compres realitzades, pàgines web freqüentades, etc. Els cercadors poden utilitzar aquests perfils, per a donar resultats que s'ajustin millor a la personalitat de l'usuari, per a mostrar-li anuncis personalitzats quan estigui en webs que mostrin propaganda, etc. Sigui com sigui, el cert és que per mitjà dels perfils hi ha algú que podrà saber com és la nostra activitat a Internet, cosa que en principi envaeix la privadesa dels usuaris que la fem servir.

En els exemples anteriors els usuaris potser no són conscients que la seva privadesa pot ser envaïda, ja que utilitzar un ordinador en privat dóna la sensació de no estar essent controlat.

A part de la informació privada que es pot obtenir d'un usuari mitjançant un virus espia, hi ha altres maneres d'obtenir informació. En el que queda d'aquesta part sobre privadesa, tractarem de la privadesa en la navegació web, el tema de la privadesa en les xarxes socials i l'obtenció de dades privades per mitjà de l'enginyeria social.

5.1. Privadesa en la navegació web

Quan visitem una pàgina web, aquesta pot recollir una gran quantitat d'informació sobre qui hi accedeix i amb quina freqüència. Aquest monitoratge es fa per mitjà de les anomenades *galetes*[8].

[8] En anglès, *cookies*.

> Una **galeta** és un petit fitxer de text que pot enviar el servei web quan un usuari s'hi connecta. És l'únic fitxer que un servidor web remot pot escriure en el nostre equip.

Les galetes se solen fer servir per a recordar la identitat d'un usuari que ja ha visitat un servei web. El primer cop que s'hi connecta, el servei web comprova si en l'equip de l'usuari hi ha una galeta d'aquest servei web. Si no és el cas,

es demana a l'usuari la creació d'un compte d'accés (és a dir, un nom d'usuari i una contrasenya). Un cop registrat, el servei web envia una galeta amb la identitat de l'usuari. Quan en un altre moment l'usuari torni accedir al mateix servei web, aquest ja hi trobarà una galeta, amb la qual cosa s'haurà comprovat la identitat de l'usuari i s'evitarà que aquest hagi d'introduir de nou el nom d'usuari.

Tanmateix, per mitjà de les galetes el proveïdor d'un servei web pot saber la freqüència amb què cada usuari utilitza el servei.

Aquests usos de les galetes representen un risc lleu per a la privadesa de l'usuari. Això canvia en el cas de les **galetes de rastreig**[9]. Aquestes galetes tenen com a objectiu rastrejar el comportament d'un usuari conforme utilitza diferents serveis web. Aquesta informació queda recollida en el sistema d'informació de qui gestiona aquestes galetes.

(9)En anglès, *tracking cookies*.

Una tercera entitat, dedicada a fer publicitat per Internet, gestionarà aquestes galetes.

Exemple de galetes de rastreig

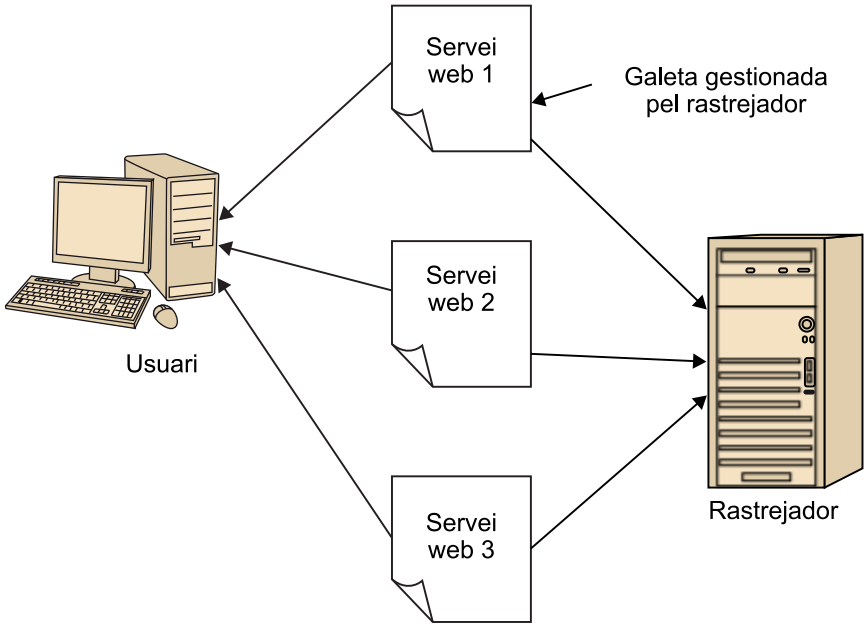
Si fem cerques sobre motocicletes, busquem motocicletes antigues en els serveis web de subhastes, etc. Aquesta tercera part deduirà que ens agraden les motocicletes. Així, doncs, quan anem a un servei web que mostri publicitat, l'entitat gestora de les galetes de rastreig indicarà que la publicitat que se'ns ha de mostrar tingui alguna cosa a veure amb les motocicletes.

Hi ha qui veu les galetes de rastreig com una mena de programari espia, ja que l'entitat que les gestiona pren consciència dels serveis web que visitem, què hi fem i amb quina freqüència ho fem.

Els programes de neteja

Els programes de neteja també detecten i eliminen aquestes galetes de rastreig del nostre sistema.

Rastreig d'un usuari durant la visita a tres serveis web diferents



En aquest exemple, l'usuari es va connectant a diferents serveis web que contenen galetes gestionades per una tercera part. Aquesta, pren nota de quan l'usuari visita aquests serveis web i, en conseqüència, sap per on ha navegat i amb quina freqüència.

5.1.1. El gran germà a Internet

Si bé són moltes les companyies que es dediquen a produir programari per a ordinadors personals i Internet, el cert és que només dues o tres acaparen la gran part del pastís. Per exemple, una única companyia és responsable del sistema operatiu i el programari ofimàtic que milions d'usuaris utilitzen habitualment. D'altra banda, els serveis populars a Internet de cerca d'informació han esdevingut molt més que això: avui dia els seus serveis incorporen eines complementàries com ara cerques als documents de l'ordinador personal, edició en línia de documents, gestió de cites i calendaris, etc.

D'altra banda, milions d'usuaris fan servir els grans gestors de correu electrònic d'aquestes companyies als quals accedeixen pel web. Per tant, el seu correu electrònic enviat i rebut es desa permanentment en servidors compartits per milions d'usuaris en comptes de tenir-los desats en el disc de l'ordinador personal. Les tecnologies de la informació permeten analitzar aquests correus electrònics no solament per a localitzar terroristes i usuaris potencialment perillosos, sinó que també poden servir per a crear perfils que ajudin als cercadors de les mateixes companyies.

De tot això es desprèn que un parell de grans companyies tenen accés a informació privada de milions d'usuaris d'Internet. Públicament, se sap que aquestes companyies recullen certa informació dels usuaris per a fins relacionats amb oferir-los un servei "més personalitzat". Tanmateix, si aquesta enorme quantitat d'informació es fes servir de manera deshonesta, la figura del gran germà de la novel·la de George Orwell podria acabar esdevenint una realitat.

5.2. Les xarxes socials

Els serveis de xarxes socials permeten que la gent es connecti per mitjà d'una comunitat en línia. Hi ha diferents tipus de xarxes socials, des de les que agrupen usuaris amb aficions molt concretes fins a grans xarxes socials en què l'objectiu és estar connectat amb un gran grup d'amics.

Les xarxes socials

Les xarxes socials més populars arriben a ultrapassar els 200 milions d'usuaris cada una.

Les grans xarxes socials comporten una sèrie de riscos associats a la privadesa. En aquests serveis en línia, els usuaris publiquen el seu perfil: descriuen com són, indiquen la data de naixement, inclouen una fotografia o, fins i tot, arriben a posar l'adreça personal i el número de telèfon. Fins i tot es poden especificar les tendències polítiques, creences religioses i l'orientació sexual.

Aquesta informació, de caire clarament personal, és accessible als usuaris de la xarxa social, d'acord amb determinades restriccions. L'usuari final, és a dir, qui ha introduït la informació del seu perfil, és qui decideix qui pot accedir a aquesta informació. Per exemple, es pot donar el cas que aquesta informació sigui accessible a tots els usuaris de la xarxa social, amb els riscos de privadesa que això podria comportar. En cas de voler ser més restrictius, els usuaris poden especificar que la seva informació sols sigui accessible per als seus amics. En general, per a ser amic sols cal localitzar un usuari concret dins la xarxa social i enviar-li una petició d'amistat. Si aquest accepta, passarà a formar part del gros d'amics.

Tanmateix, i malgrat que el mateix usuari controli qui pot accedir a la seva informació, les xarxes socials continuen posant en risc la privadesa de l'usuari:

- Per exemple, en aquestes xarxes socials es poden posar fotos. Imaginem que algun amic nostre posa una foto en què, de retruc, apareixem nosaltres en una situació que considerem compromesa. A més, el sistema permet "etiquetar" les persones que surten en les fotografies, de manera que si algú busca la nostra identitat dins la xarxa social podria arribar a tenir accés a la fotografia compromesa.

- D'altra banda, un usuari deshonest podria arribar a crear un perfil fals amb el nostre nom per a fer-se passar per nosaltres o bé fer-se passar per una persona ben diferent de la que és realment.

Les polítiques de privadesa d'aquestes xarxes socials avisen els usuaris que la responsabilitat de controlar la informació i, de retruc, el risc en què posen la seva privadesa recau exclusivament en ells.

5.3. El *phishing*

En el primer apartat d'aquest mòdul hem descrit en què consisteixen els atacs per mitjà de l'enginyeria social. Un cas concret de l'enginyeria social l'hem exemplificat amb la recepció d'un missatge de correu electrònic, suposadament de la nostra entitat bancària, en el qual se'ns demana d'introduir les credencials d'accés al gestor bancari.

Aquest cas específic d'enginyeria social rep el nom de *phishing*, que en català es tradueix per *pesca*.

> El ***phishing*** és la tècnica consistent a suplantar la identitat electrònica d'una organització determinada amb l'objectiu de convèncer algú perquè reveli informació confidencial que posteriorment serà utilitzada amb finalitats fraudulentes.

Si l'usuari fa cas del missatge de correu electrònic, farà cap a la pàgina web de la suposada entitat bancària. Convé adonar-se del següent:

- De vegades, l'adreça on s'ubica el servei web no s'assembla a la real. Per exemple, se'ns obre el servei web de `http://elmeubanc.dangerwebs.ru` en comptes de `http://www.elmeubanc.com`.

- El servei web en qüestió no està protegit, és a dir, no es veurà el cadenat que indica connexió sota SSL. També podria passar que estigués certificat per una autoritat de certificació que el programari del nostre equip no reconeix.

- La pàgina està sovint plena d'errades d'ortografia o si més no d'expressions estranyes, ja que sol estar dissenyada per gent d'altres països.

Que els atacs de *phishing* tinguin èxit depèn, en gran part, de les possibilitats que hi ha perquè l'usuari cregui que el missatge és autèntic. Avui dia aquesta mena d'atacs és àmpliament coneguda, i és evident que es desconfiarà d'un missatge d'aquesta mena sobretot quan vingui d'una entitat bancària que no és la nostra.

6. Seguretat en la gestió audiovisual

L'entrada de la producció audiovisual (música i cinema) en el món digital i d'Internet s'ha traduït en la difusió massiva i il·legal d'obres per mitjà de còpies directes, en CD o DVD, o bé per Internet. En conseqüència, s'han anat desenvolupant i utilitzant diferents sistemes l'objectiu dels quals és donar seguretat a la gestió audiovisual. Aquesta seguretat és important tant per al venedor com per al comprador del material audiovisual:

- Al venedor li interessa que el contingut que ven no es pugui copiar sense permís. També li interessa controlar les còpies que ha venut.

- Al comprador li interessa poder gaudir del contingut que ha comprat tantes vegades com convingui. També convé evitar que un usuari deshonest pugui obtenir el contingut que ha comprat un altre i el distribueixi fent-se passar pel comprador autèntic.

Les tècniques que s'han anat desenvolupant es poden classificar en dos grups: les tècniques de control de reproducció i còpia, i les tècniques de marcatge. Les veurem en aquest darrer apartat del mòdul.

6.1. Sistemes de control de còpia i reproducció

Impedir les còpies és un tema tractat des de l'inici de la distribució d'àudio i vídeo al públic general. Els sistemes de vídeo amb cinta analògica disposen d'un sistema de còpia amb el qual qualsevol còpia que es fa d'una cinta original (connectant dos vídeos, un reproduint la cinta i l'altre gravant-la) presenta errors de sincronia que es tradueixen en una qualitat d'imatge molt dolenta i pèrdues del so.

Amb l'arribada de sistemes digitals d'àudio i vídeo reproduïbles sense pèrdua de qualitat en qualsevol ordinador personal, s'han anat fent servir diferents mètodes d'impediment de còpia. En general, la idea consisteix a pervertir el contingut digital que conté el CD o el DVD de manera que continuï essent visible en un reproductor domèstic alhora que no pugui ser reproduïble en un ordinador personal: el contingut erroni genera errors en el programari i atura el procés de còpia. Tanmateix, quan el sistema anticòpia porta cert temps en el mercat, sempre hi ha qui fa un programari de còpia capaç de saltar-se aquesta protecció.

Còpies analògiques

Els sistemes de protecció esmentats no tenen en compte que l'usuari pot fer una còpia analògica del contingut per a després tornar-lo a passar a l'ordinador, per a saltar-se la

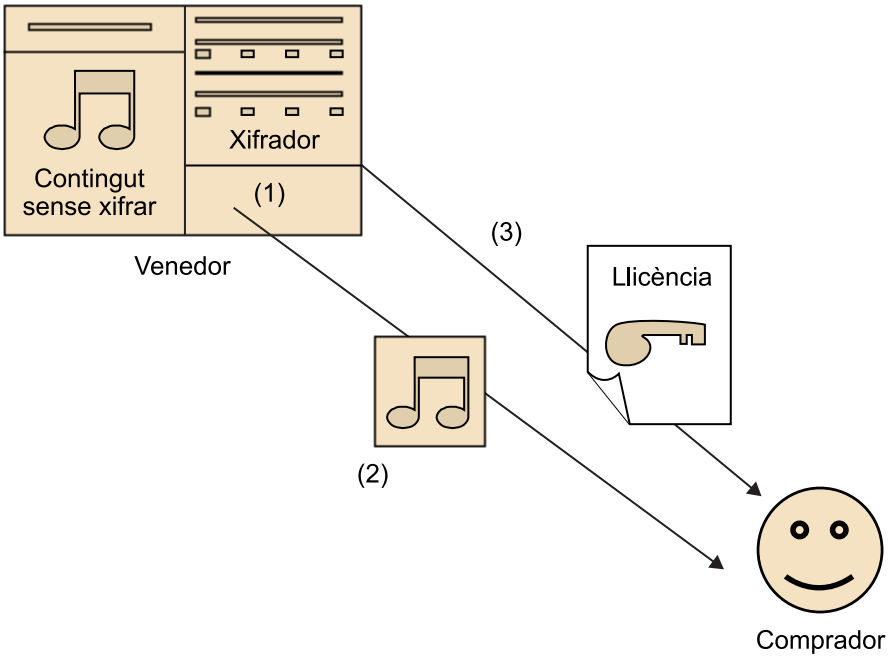
còpia. Malgrat ser possible, es produeix una pèrdua de qualitat notòria en passar de digital a analògic.

Protecció dels DVD

De fet, tots els DVD que trobem a la venda estan xifrats. El problema és que els reproductors de DVD contenen les claus que permeten desxifrar-los i, en definitiva, això ha permès crear programari que desxifra i copia el contingut d'un vídeo en DVD.

Una alternativa interessant consisteix a xifrar el contingut i vendre la clau de desxifratge al comprador d'aquest. Això solament és factible en continguts comprats per Internet i no pas en els CD o DVD. Ho il·lustrem en la figura següent.

Exemple de protecció del contingut per mitjà de xifratge i llicències



Quan un comprador adquireix, per exemple, una cançó, el venedor en fa una còpia i la xifra amb una clau secreta (1). El client es pot descarregar la versió xifrada (2). Quan aquest efectua el pagament, es descarrega **una llicència** (3) que conté la clau de desxifratge. Així, doncs, el programari reproductor serà capaç de desxifrar el contingut i, en conseqüència, de fer sonar la cançó les vegades que vulgui.

El sistema de llicències és el més estès, tot i que sempre hi ha algun programa que acaba saltant-se aquestes proteccions i desxifrant el contingut a base d'atacs específics per a obtenir la clau de manera deshonesta.

6.2. Sistemes de marcatge

Els sistemes de marcatge poden arribar a ser una alternativa al control de còpia i reproducció. Tot seguit estudiarem en què consisteixen les marques d'aigua en el contingut audiovisual i veurem alguns exemples concrets d'ús.

6.2.1. Les marques d'aigua

El marcatge d'aigua digital[10] és la tècnica que permet amagar un missatge (una tira de bits) en un contingut audiovisual. Per exemple, un fotògraf professional podria disposar d'un programari de marques d'aigua per a amagar a les seves fotografies, un missatge que indiqués qui és l'autor de la fotografia. Un cop la fotografia està marcada, ja està a punt per a vendre.

(10)En anglès, *digital watermarking*.

Si resulta que el fotògraf troba una fotografia seva en una pàgina web que no té permisos d'explotació de la fotografia, pot demostrar que ell és l'autor de la fotografia.

Perquè això sigui factible, convé complir una sèrie de requisits:

- El programari que amaga la marca d'aigua utilitza una clau privada. Només amb aquesta clau privada es podria recuperar correctament el missatge, per tant, el fotògraf (l'únic posseïdor d'aquesta clau) és l'únic que pot recuperar la marca.

- El sistema de marcatge ha de ser robust, és a dir, ha de permetre recuperar la marca encara que la fotografia es faci més petita, es canviïn lleugerament els colors, se'n retalli una part, etc. Evidentment, si no es pot recuperar la marca és perquè la fotografia ha quedat tan malmesa que ja no té interès comercial.

Encara que hàgim posat exemples de fotografies, el cert és que hi ha sistemes de marcatge prou robustos no solament per a imatges, sinó també per a música i vídeos.

6.2.2. Les empremtes digitals

En el cas anterior, totes les còpies venudes de la mateixa fotografia duien amagat el mateix del missatge: "L'autor de la fotografia és"... Tanmateix, si amaguem el nom del comprador en comptes del nom de l'autor, usem la tècnica que s'anomena **empremta digital**[11].

(11)En anglès, *digital fingerprint*.

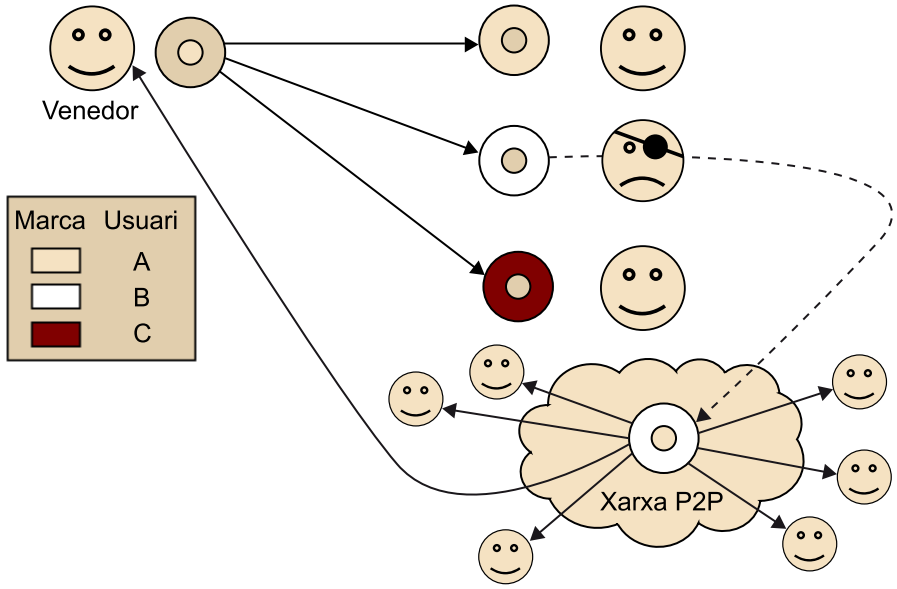
Ara canviem d'exemple per il·lustrar el funcionament de les empremtes digitals. Suposem que un grup de música conegut ha acabat l'enregistrament del seu nou disc. El seu segell discogràfic vol promocionar les noves cançons un mes abans de posar el disc a la venda i, per tant, envia cinquanta còpies del nou CD a emissores de ràdio, crítics musicals, etc.

En utilitzar l'empremta digital es faran un total de cinquanta còpies diferents del CD. Cada una tindrà una marca d'aigua única que indicarà a qui es lliura la còpia promocional.

Resulta que en un parell de setmanes ja es pot descarregar d'Internet el nou disc, abans que hagi sortit a la venda; paral·lelament, les parades "top manta" ja venen còpies dels CD. Doncs, bé, recuperant la marca d'aigua del contingut piratejat se sabrà qui ha estat el que ha iniciat la distribució il·legal del CD.

En la figura següent s'il·lustra aquest fet: el distribuïdor, per mitjà de la recuperació de la marca, és capaç de saber qui ha posat el contingut musical en la xarxa de distribució. El venedor té una relació de la marca que s'ha posat en cadascuna de les còpies distribuïdes. Un d'aquests usuaris, posa el contingut en una xarxa P2P. El venedor, que troba el contingut en la xarxa P2P, recupera la marca i sap, en principi, qui és el responsable de la distribució il·legal.

Exemple d'identificació del distribuïdor il·legal per mitjà d'empremtes digitals



Xarxes P2P

Les xarxes P2P (*peer to peer*, punt a punt) es van dissenyar per a l'intercanvi d'arxius. Actualment, la majoria d'arxius que s'hi intercanvien tenen un *copyright* que no ho permet, amb la qual cosa l'intercanvi d'aquests arxius en concret (per exemple, música i pel·lícules) és de legalitat dubtosa.

Aquest sistema té alguns problemes, que passem a comentar a continuació:

- El contingut pot ser robat del destinatari original i ser posat en circulació de manera il·legal. El "culpable" seria el destinatari original, cosa que es revelaria en la recuperació de la marca.

- Com que cada còpia és diferent (justament hi ha diferència en els bits que serveixen per a amagar la marca), dos destinataris podrien comparar els bits de les seves còpies i així detectar quins formen part de la marca. Aleshores canviarien el valor d'aquests bits per valors aleatoris, per intentar esborrar les marques que identificarien als dos destinataris deshonestos.

Tot i aquests problemes, que tenen algunes solucions que es poden dur a la pràctica perfectament, els sistemes d'empremta digital s'utilitzen de manera cada cop més generalitzada, per exemple, en el cas de les còpies promocionals.

Resum

En aquest mòdul hem tractat dels temes més importants relacionats amb la seguretat dins les tecnologies de la informació i les comunicacions.

En la primera part hem presentat la varietat d'atacs que es poden produir, i també hem definit què és un atacant.

La segona part l'hem dedicada a revisar quina mena d'atacs poden patir els equips informàtics. Hem vist el problema que causen els virus i les seves variants. Hem descrit què són i què impliquen els atacs d'accés des d'Internet. També hem vist que els antivirus, els programes de neteja i els tallafocs són eines fonamentals que cal tenir en el sistema per a garantir-ne, almenys teòricament, la resistència a atacs.

Després hem parlat de la seguretat en la informació, definint propietats importants com ara la confidencialitat i l'autenticitat. Hem fet una aproximació als sistemes que permeten garantir aquestes propietats, des de sistemes senzills de criptografia clàssica, que ens han servit per a comprendre alguns conceptes bàsics, fins a les tècniques de signatura digital.

Els sistemes de clau pública van estretament lligats al que hem anomenat *identitat digital*, gestionada pels certificats i les infraestructures de clau pública. Hem vist tres casos d'aplicació de les tècniques estudiades i de la identitat digital: el comerç electrònic, el correu electrònic i els tràmits en línia.

La penúltima part del mòdul l'hem dedicada a parlar d'un tema relacionat amb la seguretat: la privadesa dels usuaris de les tecnologies que sustenten la societat de la informació. Hem apuntat com els serveis d'Internet poden rastrejar el comportament dels usuaris. També hem reflexionat sobre el fet que dues o tres grans companyies poden arribar a tenir un gran control sobre les activitats que duen a terme els usuaris d'ordinadors i d'Internet.

Finalment, hem acabat el contingut teòric del mòdul tractant del tema de la seguretat en la gestió audiovisual, en què hem presentat sistemes basats en l'impediment de còpia, o control de la reproducció i sistemes de marcatge.

Activitats

1. Busqueu informació a Internet i expliqueu quins avantatges pot portar a la ciutadania l'ús del DNI electrònic.

2. El sistema PGP (*pretty good privacy*, en català privadesa prou bona) és un sistema d'eines de clau pública per a una gran varietat d'aplicacions: xifratge i signatura de correu electrònic, de fitxers, etc. Malgrat tot, el sistema no utilitza certificats de clau pública a l'hora de garantir la validesa de les claus públiques. Esbrineu quin sistema s'utilitza i diferencieu-lo del que hem vist en el mòdul (infraestructures de clau pública).

3. Connecteu-vos a diferents portals web segurs (per exemple, banca en línia) i mireu quina informació porta el certificat d'identitat de servidor (en principi, podeu fer doble clic en el cadenat que apareix en el navegador per a obtenir informació).

4. Busqueu en les hemeroteques digitals articles sobre les xarxes socials i els seus efectes sobre la privadesa dels usuaris. Llegiu-los i compareu-los amb el que hem explicat en aquest mòdul.

5. Aneu a la pàgina web d'algun fabricant d'antivirus i busqueu informació sobre quants virus diferents identifiquen els seus productes.

Exercicis d'autoavaluació

1. Diferencieu els sistemes de criptografia simètrica i asimètrica.

2. Es fa servir el sistema següent d'autenticació de missatges entre els usuaris A i B: Per enviar un missatge M s'envia $\{M, h(M)\}$, en què h és la funció de resum SHA-1 de 160 bits de sortida. Responeu si, en cas que algú hagi modificat el missatge, queda garantit que es detectarà. Justifiqueu la resposta.

3. Suposeu que voleu enviar un missatge de correu electrònic de manera que el contingut sigui secret per a tothom menys per a nosaltres i per a vosaltres. Expliqueu:

a) Com es faria amb un sistema de clau simètrica i quines claus necessitaríeu.

b) Com ho faríeu amb un sistema de clau pública i quines claus necessitaríeu.

4. Ara volem enviar un únic fitxer missatge adreçat a tres usuaris i que estigui xifrat. Com ho podem fer enviant únicament un fitxer xifrat?

5. Descriviu quines aplicacions del sistema solen tenir obert l'accés a Internet per mitjà del tallafoc.

6. En funció del que hem vist en el mòdul, dieu per què la reproducció amb llicències no és extensible als CD. I els sistemes d'empremta digital, ho són?

7. Una discogràfica prepara cinquanta còpies promocionals d'un CD que enviarà a les ràdios i als crítics de música abans que es posi a la venda. Als dos dies, una còpia en MP3 d'un dels *singles* es troba en l'eMule. Indiqueu com s'hauria pogut utilitzar un sistema d'empremta digital per a detectar qui és (en teoria) qui ha posat aquest contingut en el sistema de distribució P2P.

Solucionari

Exercicis d'autoavaluació

1. En la criptografia simètrica es fa servir la mateixa clau per a xifrar i per a desxifrar; fa falta una clau per a cada parella possible de comunicants; comunicar la clau compartida a l'altre participant en la comunicació pot representar un problema; els algorismes són més ràpids d'executar per un sistema informàtic. En la criptografia asimètrica, la clau secreta es fa servir per a desxifrar/signar i la clau pública per a xifrar/comprovar la signatura; només fa falta un parell de claus per a cada usuari (la pública i la privada); tothom pot accedir a la clau pública, per tant, la seva distribució no representa un problema; els algorismes són menys ràpids d'executar.

2. El sistema no garanteix res: qualsevol que tingui accés al $\{M, h(M)\}$ pot agafar el missatge M, modificar-lo, calcular-ne el resum fent $h(M)$ i reenviar la informació com si no hagués passat res.

3. En el cas de clau simètrica caldria posar-se d'acord en una clau comuna, o bé nosaltres n'hauríem de triar una i fer-vos-la saber. Amb aquesta clau xifraríem el missatge i us l'enviaríem. Vosaltres faríeu servir la clau que us hauríem enviat o hauríem consensuat per desxifrar el missatge. En el cas de clau pública, si nosaltres us enviem el missatge haurem de fer servir la vostra clau pública per a xifrar-lo, mentre que vosaltres fareu servir la clau privada corresponent per a desxifrar-lo un cop l'hàgiu rebut.

4. Farem servir el sobre digital. Primer el programari de xifratge triarà una clau per xifrar simètricament el fitxer només una vegada. Al fitxer resultant s'adjuntarà la clau simètrica triada xifrada per cadascun dels tres destinataris, és a dir, amb les seves claus públiques.

5. Hauran de tenir el camí obert pel tallafoc les aplicacions més habituals: el navegador web, el gestor de correu electrònic, la missatgeria instantània, etc.

6. La reproducció amb llicències comporta que el contingut venut s'ha de xifrar de manera específica per a l'usuari. Això va en contra del procés de fabricació del CD, en què es fa un nombre elevat de còpies. Un sistema factible fóra xifrar el CD amb una clau k i que per a obtenir aquesta clau k s'hagués de comprar una llicència, però passaria que aquesta clau circularia per les pàgines web de pirateria... Passa el mateix amb els sistemes d'empremta digital, en què cada CD s'hauria de marcar de manera específica i, a més, s'haurien de gestionar les relacions entre marca i usuari. Tanmateix, hem vist que aquestes tècniques es fan servir per a les còpies promocionals.

7. Caldria que cada còpia tingués encastada una marca que identifiqués a qui s'ha distribuït el contingut (empremta digital o *fingerprint*). Si el distribuïdor discogràfic troba el contingut en una xarxa de distribució, podrà recuperar la marca i saber, en teoria, quin dels cinquanta destinataris l'hi ha posat.

Glossari

certificat de clau pública *m* Document electrònic que relaciona una clau pública amb una identitat, com ara una adreça web o de correu electrònic.

clau pública *f* Clau que es pot posar a disposició de tots els usuaris que vulguin fer servir un criptosistema de clau pública per a assegurar la comunicació amb el seu propietari.

cracker *m* *Hacker* que es dedica a malmetre els sistemes que ataca.

denegació de servei *f* Atac que té èxit quan el servei atacat és incapaç de donar servei als seus usuaris.

enginyeria social *f* Tècnica que permet obtenir informació confidencial dels usuaris mitjançant la persuasió.

funció de resum *f* Algorisme que, donat un missatge de longitud arbitrària, retorna una tira de bits de mida fixa.

galeta *f* Fitxer de text que els servidors web poden deixar dins els equips informàtics quan es visiten els webs que allotgen.

hacker *m* Delinqüent informàtic. D'altra banda, defineix algú amb elevats coneixements d'informàtica i seguretat.

identitat digital *f* Certificat emès per l'Administració que identifica els ciutadans i alhora els proporciona una clau pública per fer tràmits en línia.

marca d'aigua *f* Missatge en forma de tira de bits que s'insereix en un fitxer sense que es noti.

segrestador de sistema *m* Programari maligne que canvia les propietats del sistema i el seu comportament.

signatura digital *f* Tècnica que garanteix que un missatge és autèntic, és a dir, que ve d'on diu que ve i del qual no s'ha alterat el contingut.

tallafoc *m* Eina que controla el trànsit que circula entre dues xarxes, o entre un ordinador i la xarxa.

xarxa social *f* Servei basat en les noves tecnologies web que permeten a usuaris establir relacions, comunicar-se i compartir informació.

Bibliografia

Gutiérrez, J. D. i altres (2008). *Seguridad en Redes Locales* (*Guía Pràctica*). Anaya Multimedia Interactiva.

Herrera, J. i altres (2003). *Tecnologia del comerç electrònic*. Barcelona: Editorial UOC.

Stallings, W. (2003). *Fundamentos de Seguridad en Redes*. Pearson Educación.