Introducció a la criptografia

Josep Domingo Ferrer

P03/05024/02259

UOC
www.uoc.edu

Índex

Introducció a la criptografia

Introducció

Criptografia és un terme d'origen grec que prové dels mots *krypto* ('amagar') i *grapho* ('escriure'). Podem dir que la **criptografia** és la ciència i l'estudi de l'escriptura secreta.

Inicialment, la criptografia va aparèixer per a resoldre la necessitat de comunicar-se en presència d'un adversari (normalment en un context militar o diplomàtic). Actualment, engloba molts altres problemes; per citar-ne només uns quants, podem parlar de xifratge, autentificació, distribució de claus, etc.

La criptografia moderna proporciona els fonaments teòrics necessaris per a poder:

- Entendre exactament els problemes que acabem d'enumerar.
- Avaluar els protocols que en teoria poden resoldre aquests problemes.
- Construir protocols en la seguretat dels quals puguem confiar.

Els protocols que resolen els problemes bàsics esmentats es poden emprar com a base per a resoldre altres problemes més complexos, com ara els sistemes de pagament electrònic segur, usats en el comerç electrònic, que fan servir protocols d'autentificació i de xifratge.

Objectius

En els materials didàctics d'aquest mòdul l'estudiant trobarà els continguts necessaris per a assolir els objectius següents:

1. Conèixer la terminologia bàsica emprada en criptografia.

2. Tenir una visió històrica de la criptografia.

3. Prendre consciència de l'omnipresència de la criptografia en el món actual.

1. Terminologia

Tu as tes procédés d'information que je ne pénètre point.
Guy de Maupassant

Una **xifra** o **criptosistema** és un mètode secret d'escriptura, mitjançant el qual un text en clar es transforma en un text xifrat*. El procés de transformar text en clar en text xifrat s'anomena *xifratge*; el procés invers, transformar text xifrat en text en clar, s'anomena *desxifratge*. Tant el xifratge com el desxifratge són controlats per una o més claus criptogràfiques.

*** A vegades s'anomena *criptograma*.**

La **criptografia** i una disciplina complementària anomenada **criptoanàlisi** es coneixen conjuntament amb el nom de **criptologia**. La criptografia s'ocupa del disseny de xifres. La criptoanàlisi s'ocupa de trencar xifres. La motivació del criptoanalista pot ser l'interès intrínsec de descobrir el text en clar xifrat i/o la clau emprada, o bé ser de caire cientificotècnic (verificació de la seguretat de la xifra). El vessant cientificotècnic de la criptoanàlisi és essencial per a la depuració de les xifres i és molt útil per al progrés de la criptografia.

La necessitat de la criptoanàlisi...

... és menys reconeguda socialment que la de la criptografia. "Els cavallers no llegeixen el correu dels altres", va respondre el 1929 el secretari d'estat nord-americà H.L. Stimson en saber que el seu departament trencava sistemàticament els telegrames diplomàtics xifrats de diversos països.

1.1. Xifres elementals

Hi ha dues menes bàsiques de xifres: les transposicions i les substitucions. A continuació descrivim i il·lustrem breument cadascuna d'aquestes xifres:

1) Una **xifra de transposició** reordena els bits o els caràcters del text en clar; la clau de la xifra és el criteri de reordenació emprat.

Exemple de xifra de transposició

Considereu la xifra que divideix el text en clar en grups de k lletres i inverteix l'ordre de les lletres dins de cada grup per a obtenir el text xifrat. La clau en aquest cas és k. Prenent el text en clar següent:

DALT DEL COTXE HI HA DUES NINES,

si fem servir $k = 5$ i negligim els espais en blanc, obtenim el text xifrat següent:

DTLADTOCLEHIHEXSEUDASENIN.

2) Una **xifra de substitució** canvia bits, caràcters o blocs de caràcters per substituts; la clau és el criteri de substitució emprat.

Exemple de xifra de substitució

Considereu la xifra que desplaça cada lletra de l'alfabet k posicions endavant (la lletra Z es desplaça cíclicament a l'inici de l'alfabet). La clau és k. Prenent el text en clar següent:

DALT DEL COTXE HI HA DUES NINES,

Els secrets de Cèsar

La xifra de substitució de l'exemple se sol anomenar **xifra de Cèsar**, perquè Juli Cèsar la feia servir amb $k = 3$ per comunicar-se amb Ciceró i altres amics seus.

si fem servir $k = 4$ i negligim els espais en blanc, obtenim el text xifrat que presentem a continuació:

HEPXHIPGSXBILMLEHYIWRMRIW.

1.2. Resistència de les xifres

Segons la resistència que tinguin als atacs dels criptoanalistes, les xifres es poden classificar de la manera següent:

a) Xifres trencables o febles: xifres per a les quals el criptoanalista té prou recursos de càlcul per a determinar el text en clar o la clau a partir del text xifrat, o per a determinar la clau a partir de parells de text en clar/text xifrat.

b) Xifres computacionalment segures o fortes: xifres que no poden ser trencades a partir d'una anàlisi sistemàtica amb els recursos de què disposa el criptoanalista.

c) Xifres incondicionalment segures: una xifra ho és si, independentment de la quantitat de text xifrat interceptada pel criptoanalista, no hi ha prou informació al text xifrat per a determinar el text en clar de manera única.

De fet, tan sols hi ha una xifra incondicionalment segura i veurem que en moltes situacions no és pràctica. La resta de xifres conegudes es poden trencar si els recursos de càlcul de l'enemic són il·limitats. Per tant, és més interessant parlar de xifres computacionalment segures.

Vegeu la xifra incondicionalment segura al subapartat 3.1 del mòdul didàctic "Fonaments de criptografia" d'aquesta assignatura.

1.3. Atacs criptoanalítics

Hi ha quatre mètodes bàsics d'atac criptoanalític:

1) En un **atac amb només text xifrat**, el criptoanalista ha de trobar la clau basant-se només en el text xifrat que ha pogut interceptar. El mètode de xifratge, la llengua en què és escrit el text en clar i algunes paraules probables es poden suposar coneguts.

Per a trobar la clau...

... d'un text que se sap que en clar és una ordre financera, el criptoanalista explotarà el fet que probablement inclourà paraules com "comprar", "vendre", "euro", etc.

2) En un **atac amb text en clar conegut**, el criptoanalista sap uns quants parells de text en clar/text xifrat i n'intenta deduir la clau o algun text en clar que no coneix.

Exemples d'atac amb text en clar conegut

Suposem que fem servir xifratge en les nostres sessions *telnet* contra un sistema UNIX; un espia que intercepti els nostres missatges sap que en una determinada posició apareixerà la forma xifrada de la paraula `login` i en una altra posició apareixerà la forma xifrada de `password`. A més, sap que és probable que més endavant aparegui la forma xifrada d'algunes comandes com `ls`, `pwd`, `whoami`, etc.

Els programes (codi font) xifrats són un altre exemple vulnerable a atacs amb text en clar conegut; en efecte, el criptoanalista sap que hi ha una bona part del text xifrat que correspon a paraules reservades del llenguatge.

3) En un **atac amb text en clar escollit**, el criptoanalista que intenta deduir la clau és capaç d'adquirir el text xifrat corresponent a un text en clar escollit per ell mateix. Aquest atac representa la situació més favorable per al criptoanalista, i és, per tant, el més perillós. Les bases de dades que guarden la informació en forma xifrada es presten a aquesta mena d'atacs si l'enemic pot inserir registres en clar i observar els canvis en el text xifrat emmagatzemat.

4) Un **atac amb text xifrat escollit** només té sentit en criptosistemes de clau pública, en els quals una de les dues transformacions de xifratge/desxifratge és pública. En aquesta modalitat d'atac, el criptoanalista és capaç d'adquirir el text en clar corresponent a un text xifrat escollit per ell mateix. Tot i que és poc probable que el text en clar que ha obtingut sigui intel·ligible, pot ajudar a deduir-ne la clau.

Vegeu els criptosistemes de clau pública a l'apartat 4 del mòdul didàctic "Xifres de clau pública" d'aquesta assignatura.

Actualment es considera que una xifra ofereix una seguretat acceptable només si pot resistir un atac amb text en clar conegut en què el criptoanalista té un nombre arbitrari de parells text en clar/text xifrat.

1.4. Atacs als sistemes informàtics i de comunicació

Els atacs criptoanalítics proven de trencar l'algorisme de xifratge suposant el coneixement d'una determinada informació. Ara bé, normalment cal un atac de tipus informàtic per a obtenir la informació necessària a l'hora de muntar un atac criptoanalític. De fet, si l'atac informàtic és prou hàbil, pot ser que no calgui recórrer a la criptoanàlisi: imaginem que un pirata informàtic aconsegueix entrar al nostre ordinador i llegir el fitxer on guardem la clau de la nostra xifra.

Per a muntar un atac criptoanalític, normalment és necessari muntar conjuntament un atac informàtic.

La criptografia protegeix dades enviades per un mitjà de comunicació o guardades en un sistema informàtic. La protecció té dos vessants:

- El **secret** o la **privacitat**, que permet preservar la confidencialitat de les dades, és a dir, impedir-ne la revelació no autoritzada.

- La **integritat** o **autenticitat**, que impedeix la modificació no autoritzada de les dades.

Els **atacs als sistemes de comunicació** per on circulen dades xifrades consisteixen en escoltes i se'n poden distingir dos tipus:

1) Els **atacs contra el secret**, que consisteixen en l'anomenada **escolta passiva***. L'enemic es limita a interceptar el text xifrat, normalment sense ser

*** En anglès, *eavesdropping*.**

detectat, amb la finalitat de deduir-ne la clau o el text en clar. L'ús de bons mètodes de xifratge pot fer estèrils aquesta mena d'atacs.

2) Els **atacs contra l'autenticitat**, que consisteixen en l'anomenada **escolta activa***. L'enemic es dedica a modificar missatges interceptats o a inserir-ne de completament inventats, amb la finalitat que el receptor accepti els missatges modificats o inventats com a bons. La criptografia no pot impedir que l'enemic faci aquesta mena d'atacs (per exemple, que torni a inserir un text xifrat anterior), però sí que permet al receptor detectar-los.

*** En anglès, *tampering*.**

Els **atacs a un sistema informàtic** en què es guarden dades xifrades també atempten contra el secret i l'autenticitat:

1) Els **atacs contra el secret** poden ser de tres tipus diferents:

a) L'**escombratge de memòria**, que fa referència a la cerca d'informació confidencial en l'emmagatzematge primari (memòria) o secundari (disc).

b) La **filtració**, que és la transmissió de dades confidencials a usuaris no autoritzats per part de processos amb accés legítim a les dades en clar.

c) L'**atac d'inferència**, que intenta deduir informació confidencial sobre un individu a partir de la correlació d'estadístiques publicades sobre grups d'individus.

Un atac d'inferència...

... pot servir per a deduir el sou d'un analista de sistemes concret a partir del sou mitjà dels analistes de sistemes de l'empresa.

2) Els **atacs contra l'autenticitat** inclouen els dos tipus següents:

a) La **falsificació**, que consisteix a modificar, inserir o esborrar dades.

b) La **destrucció accidental**, que fa referència a l'esborrament o la sobreescriptura no intencionada de dades.

3) Els **atacs mixtos**, que bàsicament es redueixen a l'anomenat **emmascarament**. Si un usuari aconsegueix d'entrar al sistema amb el compte d'un altre usuari, llavors pot accedir a informació confidencial de l'altre usuari (atac contra el secret) i fer-se passar per l'altre usuari davant de tercers (atac contra l'autenticitat). L'emmagatzemament de les contrasenyes en forma xifrada contribueix a dificultar l'emmascarament, però cal prendre precaucions suplementàries.

Mentre que la falsificació pot ser detectada (no impedida) per tècniques criptogràfiques, la destrucció accidental ens pot passar inadvertida fins i tot si fem servir la criptografia.

La criptografia pot fer estèril l'escombratge de memòria, però no pot combatre per si sola la filtració i la inferència.

Les tècniques criptogràfiques són suficients davant els atacs contra els sistemes de comunicació. En canvi, necessiten ser complementades per controls d'accés per contrarestar els atacs contra els sistemes informàtics.

2. Evolució històrica

Des de l'antiguitat fins a l'aparició dels ordinadors, la criptografia va ser més un art que una ciència. L'aparició de l'ordinador forçà la revolució científica de les tècniques criptogràfiques.

2.1. La criptografia com a art

El període que va des de l'antiguitat fins a l'any 1949 es pot anomenar *era de la criptografia precientífica*. Es tractava més aviat d'un art que d'una ciència, la qual cosa no vol dir que estigués mancada d'interès. Ja hem comentat que Juli Cèsar feia servir una xifra de substitució. No hi ha proves que demostrin que Brutus hagués trencat aquesta xifra, però és obvi que ara qualsevol noiet que sabés una mica de llatí no tindria cap problema per a sortir-se'n amb un atac amb només text xifrat sobre unes quantes frases xifrades. De fet, durant gairebé dos mil anys després de Cèsar, els criptoanalistes se'n sortien millor que els criptògrafs.

Atac a la xifra de Cèsar

Per a trencar la xifra de Cèsar, n'hi ha prou de comparar les freqüències de les lletres en el text xifrat amb les freqüències de les lletres en llatí clàssic; llavors se sap a quina lletra correspon la A, la B, etc.

L'any 1926, un enginyer de la companyia nord-americana AT&T anomenat G.S. Vernam va publicar una xifra remarcable per a ser usada amb el codi binari de Baudot. Com la de Cèsar, la **xifra de Vernam** consisteix a sumar una clau K aleatòria al text en clar M per a obtenir el text xifrat C. La diferència és que M, C i K prenen valors a $\{0, 1\}$ i que la suma és mòdul 2 (és a dir, una *o exclusiva*):

$$C = M \oplus K.$$

La innovació fonamental introduïda per Vernam fou fer servir la clau només una vegada, és a dir, xifrar cada bit de text en clar amb un nou bit de clau escollit a l'atzar. Això requereix la transferència segura (amb missatgers armats, per exemple) d'emissor a receptor de tants bits de clau com text en clar vulguem xifrar més tard. Malgrat aquest inconvenient, veurem que aquesta és l'única xifra incondicionalment segura*.

*** Aquesta propietat fou intuïda però no demostrada per Vernam.**

Durant la Segona Guerra Mundial, quan l'ús de la criptografia va ser generalitzat, es va començar a reconèixer que les matemàtiques podien ser útils en criptografia i en criptoanàlisi.

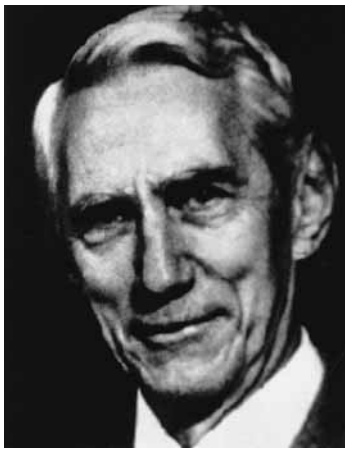
Turing i l'Enigma

Durant la Segona Guerra Mundial, un equip de matemàtics encapçalat per l'anglès A.M. Turing (inventor de la màquina que porta el seu nom) fou l'encarregat de trencar la xifra alemanya basada en les màquines de rotors *Enigma*.

2.2. La criptografia com a ciència moderna

La publicació l'any 1949 per part de C.E. Shannon de l'article "Communication Theory of Secrecy Systems" va inaugurar l'**era de la criptologia científ-**

fica de clau compartida. Shannon, que era enginyer i matemàtic, va elaborar una teoria dels sistemes secrets gairebé tan completa com la teoria de les comunicacions que havia publicat l'any anterior. Entre altres coses, l'article del 1949 demostrava la seguretat incondicional de la xifra de Vernam. Però a diferència de l'article sobre comunicacions del 1948, que va fer néixer la teoria de la informació com a disciplina, l'article del 1949 no va suposar un impuls comparable per a la recerca criptogràfica.



Claude Elwood Shannon, matemàtic nord-americà (nascut el 1916).

L'eclosió real de la criptografia s'esdevingué amb la publicació l'any 1976 per part de W. Diffie i M.E. Hellman de l'article "New Directions in Cryptography". Diffie i Hellman van mostrar per primer cop que era possible la comunicació secreta sense cap transferència de clau secreta entre l'emissor i el receptor, i van encetar així l'**època de la criptografia de clau pública** en la qual ens trobem actualment.

3. Aplicacions de la criptografia

Actualment, la criptografia és omnipresent en la vida quotidiana, per bé que d'una manera silenciosa. Desenvolupaments d'una actualitat tan candent com la telefonia mòbil, la televisió de pagament o el comerç electrònic no serien viables sense les tècniques criptogràfiques. En particular, el desenvolupament de sistemes de comerç electrònic segur és una activitat que a hores d'ara absorbeix una bona quantitat de mà d'obra informàtica.

En aquest apartat pretenem donar una visió ràpida i estimulant d'algunes de les aplicacions més vistents de la criptografia. Confiem que això estimularà l'alumne a continuar endavant amb l'assignatura.

3.1. Seguretat de les comunicacions

L'objectiu i l'ús primari de la criptografia és proporcionar seguretat en les comunicacions i, en la mesura que pugui, seguretat en els sistemes informàtics. A continuació veiem alguns camps concrets on cal aplicar-la:

1) En una **xarxa de paquets commutats** com IP o X.25, la seguretat de la informació transmesa es pot aconseguir amb un xifratge d'enllaç (al nivell d'enllaç de la jerarquia OSI) o bé extrem a extrem (als nivells alts de la jerarquia OSI). En el cas d'un xifratge d'enllaç calen equips de xifratge a cada node de la xarxa. En el cas d'un xifratge extrem a extrem, els equips terminals són els encarregats de fer el xifratge i el desxifratge.

El correu electrònic segur,...

... implementat per paquets tan coneguts com *Pretty Good Privacy* (PGP) o *Privacy Enhanced Mail* (PEM), és un exemple de xifratge extrem a extrem a nivell d'aplicació.

2) La **telefonia mòbil** és una altra gran consumidora de criptografia. Els primers sistemes de telefonia mòbil no feien servir xifratge de cap mena, a semblança de la telefonia fixa. La diferència, però, entre ambdós sistemes és que una trucada d'un telèfon mòbil pot ser escoltada sense necessitat de punxar cap cable: n'hi ha prou amb un equip sintonitzador. Actualment, la tecnologia GSM fa servir un algorisme de xifratge en flux que permet xifrar i desxifrar la conversa en temps real.

Els perills dels mòbils

Al seu dia, fou molt comentada la intercepció de converses comprometedores mantingudes per dirigents socialistes espanyols amb telèfons mòbils sense xifratge.

3) La **televisió de pagament** és una aplicació de la criptografia que es pot veure tant des del punt de vista de la seguretat de les comunicacions com des del punt de vista del comerç electrònic. En efecte, cal protegir els continguts televisius respecte d'aquells espectadors que no són abonats. Els descodificadors habituals són en realitat dispositius desxifradors; com en el cas de la telefonia mòbil, es fa servir una xifra en flux que permet xifrar i desxifrar les imatges en temps real.

3.2. Votacions i contractes electrònics

Una **votació electrònica** és una votació en la qual el votant no es desplaça físicament a un col·legi electoral per votar, sinó que vota per mitjà del seu terminal, que està connectat a una xarxa. Els problemes de seguretat que planteja la votació electrònica són complexos:

La criptografia proporciona la seguretat necessària per a fer possible el vot electrònic.

1) Tan sols els votants autoritzats haurien de poder votar i només ho podrien fer un sol cop. En un col·legi electoral, el votant presenta un document acreditatiu, es comprova si apareix a la llista censual i, en cas afirmatiu, es fa constar. Fer aquest procediment de manera electrònica requereix proporcionar una credencial electrònica al votant i mantenir la integritat del cens. Les tècniques criptogràfiques poden satisfer aquests requeriments.

2) El vot ha de ser secret. En un col·legi electoral, el votant diposita el seu vot en un sobre tancat abans de ficar-lo a l'urna. La criptografia pot ajudar a mantenir el secret del vot en un entorn electrònic.

3) No s'hauria de poder duplicar el vot de ningú. A diferència dels vots de paper en una urna, la còpia de vots electrònics és trivial si no s'utilitza la criptografia.

4) El votant ha de poder comprovar que el seu vot s'ha tingut en compte. Quan dipositem un vot de paper a l'urna, sabem que els interventors i la mesa no permetran que es descarti el nostre vot. En un entorn electrònic, hauríem de tenir la mateixa tranquil·litat.

La **signatura electrònica de contractes** planteja uns problemes similars als de la votació electrònica. En efecte, signar un contracte sobre paper de

manera presencial és trivial: dues parts A i B es reuneixen en una sala; A no deixa marxar B fins que A no obté una còpia del contracte signada per B; igualment, B no deixa marxar A fins que B no obté una còpia del contracte signada per A.

Veurem que hi ha tècniques criptogràfiques que permeten signar documents en format electrònic; ara bé, sense la presència física d'ambdues parts interessades a la mateixa sala, quina gosarà signar primer el contracte electrònic? Si no es fa servir una tercera part de confiança (notari electrònic), podria passar que B obtingués una còpia del contracte signada per A, i que en canvi A es quedés sense res. Per a resoldre aquest problema, hi ha protocols criptogràfics que asseguren que ambdues parts es troben en igualtat de condicions durant tot el procés de signatura del contracte.

3.3. Comerç electrònic

Com les votacions i els contractes electrònics, el comerç electrònic és un altre pas cap a la informatització de les relacions socioeconòmiques. Ja hem vist que la pèrdua de presència física en les relacions humanes genera problemes de seguretat complexos. El comerç electrònic no n'és una excepció i tampoc no seria viable sense la criptografia.

El problema bàsic del comerç electrònic és el pagament: com es pot pagar per mitjà d'una xarxa? La manera usual de fer transaccions monetàries per Internet és, avui dia, enviant el número de la targeta de crèdit. Això té inconvenients si ho comparem amb el pagament en efectiu: d'una banda, ens poden cobrar més del que volíem pagar; de l'altra, el pagament no és anònim: el client s'identifica cada cop que fa una compra i per tant el venedor sap qui compra què. En el seu article "Untraceable electronic mail, return addresses, and digital pseudonyms", D. Chaum va suggerir un protocol criptogràfic per a obtenir **diners electrònics** que no suposessin cap inconvenient respecte dels diners convencionals.

Quan la mercaderia objecte de comerç electrònic és informació en format digital (música, llibres, pel·lícules, etc.), apareix un altre problema, el de la **protecció del copyright**. En efecte, si fotocopiar paper ja és fàcil, copiar informació en format digital és trivial, barat i es troba a l'abast de tothom. La criptografia no pot impedir la pirateria informàtica, però sí que pot ajudar a identificar els pirates.

La supressió de la presència física en les relacions socioeconòmiques seria inviable per raons de seguretat sense l'existència de la criptografia.

Resum

Amb l'aparició dels primers ordinadors, la criptografia deixa de ser un art mil·lenari i esdevé una ciència, l'objectiu bàsic de la qual és permetre la comunicació i l'emmagatzematge segur d'informació en presència d'un adversari. Juntament amb aquest **objectiu bàsic de secret o privacitat**, la criptografia moderna permet resoldre el **problema de l'autenticitat o integritat de la informació**.

Una **xifra** o **criptosistema** transforma un text en clar en un text xifrat o criptograma. Els processos de xifratge i de desxifratge són controlats per una o més claus, que solen ser secretes. Les xifres elementals es basen en transposicions i en substitucions.

En funció de la seguretat, les xifres es poden classificar en febles, fortes i incondicionalment segures. La **criptoanàlisi** té com a objectiu trencar una xifra determinant-ne la clau a partir del text en clar i del text xifrat; segons el coneixement que se suposa que té el criptoanalista, hi ha diversos **tipus d'atac criptoanalític**.

A banda dels atacs criptoanalítics, cal tenir en compte els **atacs als sistemes informàtics i de comunicacions**. A diferència dels atacs criptoanalítics, aquesta modalitat d'atacs no es basa en l'explotació de les febleses dels algorismes de xifra. La idea és aprofitar febleses dels sistemes informàtics o de les comunicacions per a recuperar la clau o el text en clar.

Les **aplicacions de la criptografia moderna** van molt més enllà de la seguretat de les comunicacions militars i diplomàtiques. Pel que fa a comunicacions segures, la criptografia permet garantir la seguretat de les xarxes obertes, del correu electrònic i de la telefonia mòbil. Processos com les votacions, la signatura de contractes, etc., també poden ser fets de manera electrònica i sense coincidència física de les parts mitjançant tècniques criptogràfiques. El comerç electrònic és una altra "aplicació estrella" en els nostres dies.

Activitats

1. Identifiqueu en el vostre entorn algun dispositiu que utilitzi el xifratge.

2. Els pirates informàtics es valen d'atacs criptoanalítics o bé d'atacs als sistemes informàtics i de comunicacions?

3. Cerqueu a Internet informació sobre els programes analitzadors de trànsit (en anglès, *sniffers)*, que permeten escoltar el trànsit que circula per una xarxa local a l'usuari d'una estació que hi és connectada.

4. Quins problemes de seguretat planteja efectuar una votació de manera electrònica? Com es resolen aquests problemes en les votacions convencionals?

Glossari

Atac: estratègia o mètode que té per objectiu descobrir la clau de xifratge o bé el text en clar. Els atacs criptoanalítics exploten les febleses dels algorismes de xifra. Els atacs als sistemes informàtics i de comunicacions exploten les vulnerabilitats d'aquests sistemes.

Autenticitat: propietat de trobar-se, en relació amb la informació, en el mateix estat en què va ser produïda, sense modificacions no autoritzades; és sinònim d'integritat.

Autentificació: comprovació de l'autenticitat.

Clau: paràmetre, normalment secret, que controla els processos de xifratge i/o de desxifratge.

Criptoanàlisi: ciència que s'ocupa de trencar xifres, és a dir, descobrir la clau o el text en clar usats com a entrades de la xifra.

Criptografia: ciència i estudi de l'escriptura secreta.

Criptograma: text xifrat.

Criptologia: denominació conjunta de la criptografia i de la criptoanàlisi.

Criptosistema: xifra.

Desxifratge: procés de transformació del text xifrat en text en clar.

Integritat: propietat de no haver sofert, en relació amb la informació, modificacions ni supressions parcials no autoritzades.

Privacitat: dret de les persones a salvaguardar la seva intimitat, especialment pel que fa a les dades de què disposen les entitats públiques o privades.

Xifra: mètode secret d'escriptura, mitjançant el qual un text en clar es transforma en un text xifrat.

Xifra de substitució: xifra basada a canviar els bits o els caràcters del text en clar per substituts.

Xifra de transposició: xifra basada a reordenar els bits o els caràcters del text en clar.

Xifratge: procés de transformació d'un text en clar en un text xifrat.

Bibliografia

Denning, D.E. (1982). *Cryptography and Data Security*. Reading (Massachusetts): Addison-Wesley.

Fúster, A.; De la Guía, D.; Hernández, L.; Montoya, F.; Muñoz, J. (1997). *Técnicas criptográficas de protección de datos*. Madrid: Ra-ma.

Simmons, G.J. (1992). *Contemporary Cryptology: the Science of Information Integrity*. Nova York: IEEE Press.