**MINISTERUL EDUCAŢIEI AL REPUBLICII MOLDOVA**

**UNIVERSITATEA DE STAT „ALECU RUSSO” DIN BĂLŢI**

**FACULTATEA DE ŞTIINŢE REALE, ECONOMICE ȘI ALE MEDIULUI**

**CATEDRA DE MATEMATICĂ ȘI INFORMATICĂ**

**Referat**

**La disciplina”Informatica generala”**

**ROLUL CRIPTOGRAFIEI IN SECURITATEA COMUNICATIILOR**

**Autor**

Studenta grupei IT11Z

**Vichilu Elena**

|  |
| --- |
|  |

**Conducător științific:**

Olesea SKUTNITKI

lect. Univ

|  |
| --- |
|  |

**BĂLȚI, 2022**

Cuprins

[Introducere 3](#_Toc102996116)

[Securitatea sistemelor informatice 4](#_Toc102996117)

[Atacuri asupra securitații sistemelor informatice 7](#_Toc102996118)

[Introducere în criptografie 8](#_Toc102996119)

[Criptografia 8](#_Toc102996120)

[Cifrul 8](#_Toc102996121)

[Criptografia clasică 10](#_Toc102996122)

[Securitatea criptării clasice 10](#_Toc102996123)

[Modelul criptării clasice 11](#_Toc102996124)

[Criptografia modernă 11](#_Toc102996125)

[Rolul Criptografiei in viața modernă. 13](#_Toc102996126)

[Concluzie 17](#_Toc102996127)

# Introducere

Informația a însemnat întotdeauna putere, prin urmare dorința de a o proteja, de a o face accesibilă doar unor elite, unor inițiați, s-a pus din cele mai vechi timpuri. Primele texte cifrate descoperite până în prezent datează de circa 4000 de ani și provin din Egiptul Antic.

Există date privind utilizarea scrierii cifrate în Grecia Antică încă din secolul al V-lea î.e.n. Pentru cifrare se folosea un baston în jurul căruia se înfășura, spirală lângă spirală, o panglică îngustă de piele, papirus sau pergament, pe care, paralel cu axa, se scriau literele mesajului. În Roma Antică, secretizarea informațiilor politice și militare se facea utilizând diverse tipuri de scrieri secrete; amintim cifrul lui Cesar, utilizat încă din timpul războiului galic. Contribuția arabă la dezvoltarea criptologiei, mai puțin cunoscută și mediatizată, este de o remarcabilă importanță. David Kahn, unul dintre cei mai de seamă istoriografi ai domeniului, subliniază în cartea sa The Codebreakers că, criptologia s-a născut în lumea arabă. Primele trei secole ale civilizației islamice (700-1000 e.n.) au constituit, pe lângă o mare extindere politică și militară și o epocă de intense traduceri în limba arabă ale principalelor opere ale antichității grecești, romane, indiene, armene, ebraice și siriene.

Unele cărți sursă erau scrise în limbi deja moarte, deci reprezentau în fapt texte cifrate, astfel încât traducerea lor constituie primii pași în criptanaliză, deci originile criptologiei pot fi atribuite arabilor. Dezvoltările criptanalizei au fost mult sprijinite de studiile lingvistice ale limbii arabe. Arabii au preluat cunoștințele matematice ale civilizațiilor grecești și indiene. Arabii sunt cei care au introdus sistemul zecimal de numerotație și cifrele “arabe”. Termenii “zero “, “algoritm”, “algebră” li se datoreză tot lor. Însuși termenul de “cifru” ne vine de la arabi. El provine de la cuvântul arab “sifr” care reprezintă traducerea în arabă a cifrei zero din 2009 - Anghel Cătălin Pagina 5 din 24 sanscrită. Conceptul de „zero” a fost deosebit de ambiguu la începuturile introducerii lui în Europa, în care sistemul de numerotație folosit era cel roman. De aceea se obișnuia să se spună despre cineva care vorbea neclar că vorbeste ambigu, ca un cifru. Acest înțeles de ambiguitate a unui mesaj poartă și azi denumirea de cifru. Prin urmare, putem concluziona că, încă din antichitate s-a încercat securizarea informației și a datelor transmise.

# Securitatea sistemelor informatice

Apariția și dezvoltarea continuă a utilizării calculatoarelor în toate domeniile vieții, existența și evoluția rețelelor informatice de comunicații la nivel național și internațional, globalizarea comunicațiilor, existența unor baze de date puternice, constituie premisele societății informaționale în care trăim.

Protecția acestor sisteme, de transmitere și stocare a datelor, presupune existența unor servicii de rețea care să asigure securitatea datelor, cum ar fi :

* Confidențialitatea
* Nerepudierea
* Autenticitatea
* Controlul accesului
* Integritatea
* Disponibilitatea

**Confidențialitatea** este serviciul care are rolul de a proteja datele de atacurile pasive, adică de interceptarea datelor de persoane neautorizate. Se pot identifica mai multe nivele de protecție a acestui serviciu. Cel mai larg nivel a acestuia protejează datele transmise de toți utilizatorii unui sistem.

**Autenticitatea** este serviciul legat de garantarea autenticității comunicației. În cazul unui singur mesaj, cum ar fi un semnal de avertisment, funcția serviciului de autenticitate este de a garanta destinatarului că sursa mesajului este aceea care se pretinde a fi. În cazul unei interacțiuni, cum ar fi conectarea unui terminal la un server, două aspecte sunt implicate.

**Integritatea** este serviciul care trebuie să asigure recepționarea mesajelor așa cum au fost transmise fără copierea, inserția, modificarea, rearanjarea sau retransmiterea acestora. Acest serviciu include și protecția împotriva distrugerii datelor. El mai poate include și recuperarea datelor după un atac.

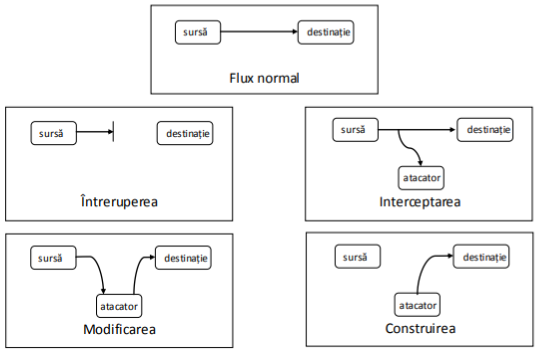
**Nerepudierea** împiedică atât expeditorul cât și destinatarul de a nega transmiterea sau recepționarea unui mesaj. Când un mesaj este trimis, destinatarul poate dovedi că mesajul a fost trimis de pretinsul expeditor.

**Controlul** accesului este abilitatea de a limita și controla accesul la sisteme gazdă și aplicații prin legături de comunicație.

**Disponibilitatea** se referă la asigurarea că sistemele de calcul sunt accesibile utilizatorilor autorizați când și unde acestia au nevoie și în forma necesară, adică informația stocată electronic este unde trebuie să fie, când trebuie să fie și în forma în care trebuie să fie.

## Atacuri asupra securitații sistemelor informatice

Informația care circulă într-un sistem de transmitere și stocare a datelor are un flux normal adică de la sursă la destinație. Atacurile asupra securității sistemelor de transmitere și stocare a datelor sunt acele acțiuni care interceptează, modifică, distrug sau întârzie fluxul normal de date. O clasificare a acestor atacuri este reprezentată în figura 1 :



**Intreruperea**: O componentă a sistemului este distrusă, devine indisponibilă sau inutilizabilă total sau pentru o anumită perioadă de timp. Acest tip de atac este un atac asupra disponibilității. Exemple de astfel de atacuri ar fi: distrugerea unor echipamente hardware, tăierea liniilor de comunicație.

**Interceptarea**: Inamicul obține acces la o componentă a sistemului.

**Modificarea**: Inamicul obține nu numai acces la o componentă din sistem, dar și falsifică informația obținută. Acesta este un atac asupra integrității. Exemplele includ modificarea unor valori din fișiere de date, modificarea unor programe sau transmiterea unor mesaje false prin rețea.

**Construirea**: Inamicul pătrunde în sistem și imită unele componente din acesta. Un atac de acest tip este un atac asupra autenticității. Un exemplu de acest gen ar putea fi introducerea unor mesaje false în rețea care sunt interpretate ca mesaje reale și inventarea unor fișiere care pot induce în eroare utilizatorii reali.

# Introducere în criptografie

Criptografie = κρσπτός {kryptós} (ascuns) + γράφειν {gráfein} (a scrie)

Criptografia (cuvânt derivat din limba greacă a cuvintelor kryptós și gráfein reprezentând scriere ascunsă) este știința care se ocupă cu studiul codurilor și cifrurilor. Un cifru este de fapt un algoritm criptografic care poate fi folosit pentru a transforma un mesaj clar (text clar) într-un mesaj indescifrabil (text cifrat). Acest proces de transformare se numește criptare iar procesul invers se numește decriptare. Textul cifrat poate fi transmis ulterior prin orice canal de comunicații fără a ne face griji că informații sensibile ar putea ajunge în mâinile inamicilor.

Știința care se ocupă cu decriptarea (spargerea) cifrurilor se numește criptanaliză. Criptanaliza se ocupă cu studiul transformării unui text neinteligibil înapoi în cel inteligibil fără a cunoaşte cheia de criptare.

Sistemul format dintr-un algoritm de criptare și o cheie de criptare se numește criptosistem.

Inițial, securitatea unui cifru depindea de faptul că inamicul nu cunoștea algoritmul de criptare folosit, dar pe măsură ce criptografia a evoluat, securitatea cifrului s-a bazat pe utilizarea unei chei secrete care se poate extrage din textul cifrat. Până la jumătatea secolului XX, nu a fost demonstrat faptul că un anumit cifru nu poate fi spart, ba chiar întreaga istorie a criptografiei este plină de relatări în care anumit cifru era spart iar ulterior erau creați alți algoritmi care la rândul lor erau sparți.

Cifrul este o metodă de conversie a informațiilor pentru a le proteja de vizualizare. Informația inițială în acest caz va fi numită text simplu, iar rezultatul aplicării unui cifr va fi numit text închis sau text cifrat. Procesele de transformare a informațiilor se numesc, respectiv, criptare și decriptare.

Este extrem de dificil să dezvolți un nou cifr, așa că este necesar ca cifrul să dureze mult timp. În acest scop, un element înlocuibil numit cheie este izolat în cifr. Acum, dacă cifrul actual a devenit cunoscut inamicului, nu este nevoie să inventezi unul nou, doar să schimbi cheia. De asemenea, face posibil ca același cifr să fie utilizat independent de diferite grupuri de persoane (cu chei diferite). Matematicianul olandez Kerckhoff, care a trăit în secolul al XIX-lea, a formulat regula conform căreia puterea cifrului nu ar trebui să se bazeze pe obscuritatea (secreția) algoritmului de cifrare în sine, ci doar pe păstrarea secretului cheii.

Unul dintre primele cifruri a fost cifrul Caesar (Fig. 1). Marele împărat, pentru a ascunde conținutul celor scrise, a înlocuit fiecare literă cu a treia literă a alfabetului urmând-o la rând. Caesar a aplicat o schimbare de trei litere; în general, poate fi orice număr mai mic decât lungimea alfabetului. Acest număr este cheia acestui cifr.

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

D E E F 3 I J K L M N O P R S T U V Y Z A B C

CRIPTOGRAFIE -> NULTHSEUGCHLV

Cifrul lui Cezar

O modificare a cifrului Caesar este cifrul Vigenère, în care valoarea deplasării este variabilă și depinde de cuvântul cheie. De exemplu, dacă cuvântul „SECRET” este folosit ca cuvânt cheie (Fig. 2), atunci aceasta va însemna că prima literă a mesajului trebuie deplasată cu 20 (numărul de serie al literei „T”), a doua - cu 1 (numărul de serie al literei "A"), al treilea - cu 11, al patrulea - cu 15, al cincilea - cu 1, al șaselea - cu 20 din nou (începem să folosim cuvântul cheie de la început), etc. Astfel, cuvântul cheie este „suprapus” pe textul protejat.

Desigur, astfel de cifruri sunt destul de ușor de spart chiar și fără cunoașterea cheii și utilizarea tehnologiei computerului. În special, cunoscând frecvența de apariție a literelor în textul mediu pentru o limbă dată, este posibil să le identificăm cu un grad ridicat de certitudine și în textul cifrat. De exemplu, pentru un text în limba rusă criptat folosind cifrul Caesar, se poate argumenta cu un grad ridicat de probabilitate că litera care apare cel mai frecvent înseamnă litera „o”. Pentru textul în limba engleză, această literă va fi cel mai probabil „t”.

Era abordării științifice a problemelor criptografiei a început odată cu publicarea lucrărilor despre teoria informației de Claude Shannon. În scrierile sale, el a introdus conceptul de securitate cifră și a arătat că există un cifr absolut sigur. Poate fi, de exemplu, cifrul Vigenère, cu condiția ca un cuvânt cheie infinit de lung să fie folosit și distribuția caracterelor din acest cuvânt să fie absolut aleatorie. Pentru prima dată, în 1917, un astfel de cifr a fost propus de G.S. Vernam, dar Shannon a fost cea care a dat dovada oficială. Evident, implementarea practică a unui astfel de cifr (o bandă aleatorie fără sfârșit) este imposibilă (mai precis, în majoritatea cazurilor este neprofitabilă din punct de vedere economic) - cantitatea de informații cheie care trebuie livrată corespondentului printr-un canal de încredere este egală cu cantitatea de informații utile. Prin urmare, de obicei se ia în considerare puterea practică a unui cifr, măsurată numeric prin timpul necesar pentru a-l sparge (ținând cont de stadiul actual al tehnicii).

# Criptografia clasică

Toate criptosistemele pot fi impărțite în două tipuri: criptosisteme simetrice numite și clasice sau convenționale și criptosisteme asimetrice numite și moderne. Criptosistemele simetrice, sau cu cheie secretă, sunt acele criptosisteme în care numai emițătorul și receptorul cunosc cheia secretă pe care o aplică la fiecare criptare sau decriptare.

Criptosistemele asimetrice, sau cu cheie publică, se bazează pe perechi de chei. Una din chei (cheia publică) este folosită la criptare, iar celaltă (cheia privată) este folosită la decriptare.

În criptografia clasică mesajul clar, numit şi text clar, este convertit într-o secvență aparent aleatoare şi fără sens, numită text cifrat. Procesul de criptare presupune un algoritm de criptare şi o cheie de criptare.

Această cheie este o valoare independentă de textul care se doreşte a fi criptat. Odată produs, textul criptat trebuie transmis destinatarului. La recepție acest text criptat trebuie transformat în textul original folosind un algoritm de decriptare bazat pe aceeaşi cheie folosită la criptare.

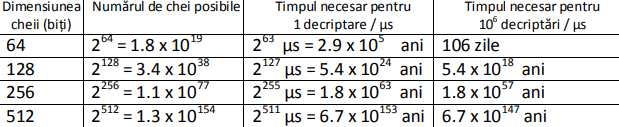
## Securitatea criptării clasice

Securitatea criptării convenționale depinde de două aspecte esențiale: algoritmul de criptare și cheia de criptare. Algoritmul de criptare, care trebuie să fie destul de puternic pentru a face imposibilă o decriptare numai pe baza textului criptat.

Există două cerințe esențiale care trebuie să le îndeplinească un **algoritm de criptare** :

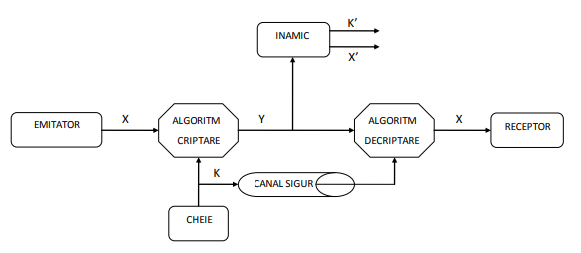
1. Costul spargerii codului să depășească valoarea informației criptate;
2. Timpul necesar spargerii codului să depășească timpul de viață al informației, adică timpul până când informația are valoare.

Un algoritm de criptare care satisface aceste două cerințe este numit algoritm cu securitate computațională. Prezentăm în tabelul 1, cât timp este necesar pentru a decripta un text cifrat, folosind metoda forței brute (brute force), pentru diferite dimensiuni ale cheii de criptare.



## Modelul criptării clasice

Un model de criptosistem simetric (clasic) este prezentat în figura 2.



## Criptografia modernă

Un criptosistem asimetric care deocamdată este considerat a fi sigur poate fi implementat folosind algoritmul RSA [5], creat în 1978 de către Ronald Rivest, Adi Shamir și Leonard Adleman. Algoritmul RSA este folosit în prezent pentru securizarea comunicațiilor din internet, a tranzacțiilor bancare sau a comerțului electronic.

Securitatea lui se bazează pe complexitatea matematică pe care o impune factorizarea numerelor prime. Pentru securizarea comunicațiilor, guvernul Statelor Unite folosește algoritmul AES (Advanced Encryption Standard) [8], dezvoltat de către Joan Daemen și Vincent Rijmen și acceptat ca standard de către NIST (National Institute of Standards and Technology) în anul 2001.

Algoritmul AES este un cifru bloc (128 biți) simetric capabil să cripteze sau să decripteze informația folosind chei criptografice pe 128,192, respectiv 256 de biți. AES se remarcă prin simplitate și prin performanțe criptografice ridicate, fiind ușor de implementat atât software cât și hardware. Deci, criptosistemele cu chei publice suplinesc dezavantajul major al celor cu cheie secretă datorită faptului că nu mai este necesar schimbul de chei.

Totuși, criptosistemele RSA și AES au marele inconvenient că securitatea lor se bazează pe complexitatea matematică a calculelor; în funcție de dimensiunea cheii folosite, pentru decriptare pot fi necesari și câteva mii de ani, la puterea de calcul actuală. Având în vedere faptul că, încă din 1985, David Deutsch a descris principiile de funcționare ale unui calculator cuantic [9] – un supercalculator cu o putere de calcul extraordinar de mare care funcționează pe principiile fizicii cuantice, putem presupune că în viitor criptosistemele cu chei publice ar putea deveni nesigure.

În concluzie, singurul criptosistem absolut sigur rămâne one-time pad. Problema schimbului de chei poate fi rezolvată printr-un sistem de distribuire a cheilor cuantice (QKD – Quantum Key Distribuiton).

# Rolul Criptografiei in viața modernă.

În prezent, toate țările dezvoltate au dezvoltat algoritmi de criptare standard care au putere garantată. Aceasta înseamnă că fără a cunoaște cheia (chiar cunoscând algoritmul în sine), atacatorul nu va putea decripta mesajul într-un timp rezonabil (mai puțin de 20 de ani). În Rusia, acesta este GOST 28147-89, în SUA - DES (Standard de criptare a datelor). Acești algoritmi au fost dezvoltați foarte atent; în plus, ele sunt publicate (adică, disponibile pentru toată lumea să le studieze), ceea ce exclude prezența unor posibile defecte în ele, care suferă adesea de evoluții „acasă”. Incidentul din 1998 cu descoperirea unui defect în algoritmul criptografic utilizat în telefoanele mobile GSM a confirmat încă o dată această teză. Firma de dezvoltare nu și-a publicat algoritmul cripto pentru cercetare, iar slăbiciunea sa a fost dezvăluită doar atunci când milioane de oameni din întreaga lume foloseau deja aceste modele de telefoane mobile. Este de remarcat faptul că algoritmul DES a fost dezvoltat cu destul de mult timp în urmă și practic s-a epuizat până acum - conform standardelor moderne, are o lungime prea mică a cheii, ceea ce îl face vulnerabil la un atac prin enumerarea exhaustivă a posibilelor chei. Astfel, nu este potrivit pentru stocarea marilor secrete pentru o perioadă lungă de timp, dar poate servi în aplicații în care informațiile trebuie închise pentru o perioadă scurtă de timp (de exemplu, are sens să ascundeți informații despre volumul achizițiilor planificate la licitație numai până în chiar momentul tranzacției, după care totul este egal cu „autodeclasificare”). Ca urmare a unei recente competiții pentru un nou standard de criptare, a fost ales un alt algoritm - Rijndael, care va fi introdus în curând oficial ca standard.

Toate cele de mai sus se referă la criptografia clasică, așa-numita criptografie cu o cheie „închisă” („secretă”) – o cheie pe care ambele părți care fac schimb de informații trebuie să o cunoască și să o păstreze în cea mai strictă confidențialitate. Cu toate acestea, când în 1977 matematicienii Ron Rivest (R. Rivest), Adi Shamir (A. Shamir) și Leonard Adelman (L. Adleman) și-au dezvoltat algoritmul RSA (Rivest-Shamir-Adleman), a apărut o nouă eră - era criptografie open source.cheie. Acum nu este nevoie să trimiteți cheia secretă partenerului printr-un canal de încredere, cheile pot fi distribuite în mod deschis, prin orice canal de comunicare (de exemplu, Internet). Pentru a cripta informațiile, se folosește o cheie publică (publică, comună), cunoscută de toată lumea, iar pentru decriptare se folosește o cheie privată corespunzătoare (secretă, privată), cunoscută doar de proprietar. Astfel, oricine poate cripta informațiile, dar numai proprietarul le poate citi (decripta). Mai mult, obținerea cheii private de la cheia publică este o sarcină de o complexitate computațională enormă. Astfel de sisteme mai sunt numite sisteme asimetrice sau sisteme cu cheie publică. Pentru o persoană care intră în contact cu problemele criptografiei pentru prima dată, acest lucru poate părea neplauzibil, dar aici nu există misticism - totul se bazează exclusiv pe legile matematicii.

Această descoperire în matematică a făcut posibilă aplicarea metodelor criptografice în domenii anterior neconvenționale, în special în domeniul bancar. Desigur, este necesar să se păstreze confidențialitatea informațiilor bancare, dar o sarcină mai importantă în afacerile legate de managementul financiar este autentificarea fiabilă (proces de autentificare, autoritate) a participanților la procesul de gestionare a fluxului de numerar. Acest proces este ușor de implementat cu ajutorul unei semnături digitale electronice. O semnătură electronică este un număr de lungime fixă. Valoarea acestui număr depinde de conținutul documentului (mesaj) și de cheia privată (privată) a expeditorului. Oricine poate „verifica” semnătura de pe un document, având în vedere cheia publică corespunzătoare. Verificarea semnăturii confirmă că documentul nu este corupt (întrucât semnătura depinde de conținutul său) și că a fost creat de expeditor (întrucât cheia privată a expeditorului, de care depinde și ea, nu este cunoscută de nimeni altcineva). În acest sens, o semnătură electronică este chiar mai fiabilă decât o semnătură convențională pe un document pe hârtie.

Trebuie remarcat faptul că semnătura electronică nu protejează documentul de vizualizare - criptarea este încă folosită pentru aceasta. În plus, în implementarea practică a sistemelor de semnătură electronică, este necesar să se țină seama de nuanțe precum luarea în considerare a momentului semnării, posibilitatea ca expeditorul să refuze să semneze, destinatarul să refuze să primească un mesaj semnat, falsificarea ora primirii etc.

Semnătura electronică nu este singura aplicație a sistemelor asimetrice. Pe baza lor, au fost dezvoltați mulți cripto-algoritmi interesanți, care sunt folosiți pe scară largă, inclusiv în domeniul bancar.

Odată cu dezvoltarea telecomunicațiilor și tehnologiei informatice, activitățile comerciale au început să se desfășoare electronic. În viața reală coexistă mijloace personalizate de efectuare a plăților (cecuri, mandate de plată) și cele anonime (numerar). Era nevoie de un analog al numerarului și al comerțului electronic.

Un cumpărător al unui magazin electronic dorește să plătească pentru bunurile comandate din contul său personal. Dar, în același timp, vrea să-și păstreze secrete numărul contului, cardul de credit și alte detalii. În acest caz, cumpărătorul trimite băncii sale un mesaj semnat cu semnătură electronică, care indică suma plății. Banca (după ce a verificat starea contului clientului și semnătura acestuia) semnează mesajul cu semnătura sa și îl trimite înapoi clientului. Clientul (cumpărătorul) își îndepărtează semnătura de sub mesaj și primește astfel o obligație semnată de bancă de a plăti o anumită sumă la cerere (desigur, banca a șters deja suma necesară din contul clientului într-un cont intermediar fără chip) . Cumpărătorul transmite această obligație vânzătorului ca mijloc de plată. În această situație, banca nu știe cui și pentru ce plătește banii clientul său (cumpărătorul); vânzătorul, la rândul său, primind bani de la bancă, nu știe din ce cont au fost retrase. Această tehnologie se numește semnătură oarbă.

Sistemele de criptare asimetrică a informațiilor au două mari dezavantaje. Aceasta este dimensiunea tastelor și complexitatea operațiunilor efectuate. Prin urmare, sistemele asimetrice în forma lor pură sunt rareori utilizate. Cele mai răspândite sunt așa-numitele sisteme hibride. Ei folosesc algoritmi simetrici pentru a cripta informațiile, iar criptografia asimetrică este folosită pentru a genera o cheie partajată. Un exemplu este algoritmul de distribuție a cheilor Diffie-Hellman. În acest algoritm, cheia publică este obținută din cheia privată (privată) a expeditorului și cheia publică a destinatarului. Destinatarul calculează aceeași cheie folosind cheia sa privată (privată) și cheia publică a expeditorului. Un atacator care observă procesul de schimb de chei primește la dispoziție cheile publice ale ambilor abonați, dar nu poate calcula cheia secretă pe care se va efectua criptarea efectivă. Acest lucru se datorează faptului că ecuația care raportează cheile secrete și publice este ușor de rezolvat într-o direcție și foarte dificilă în cealaltă. Dacă desemnăm cheia secretă ca X și cheia publică ca Y, atunci raportul lor va arăta ca

Y=AX

Cu valori mari ale lui A, X și Y (notația lor zecimală va lua mai mult de o linie), este imposibil să se calculeze X într-un timp rezonabil de la cunoscute A și Y (este necesar să se calculeze logaritmul lui Y la baza lui A), în timp ce operația de exponențiere este relativ ușoară.

O altă problemă care neagă practic toate avantajele distribuției cheilor deschise este problema încrederii între participanții la schimb. De fapt, atunci când primim cheia publică a unui corespondent printr-un canal de comunicare nesigur, nu putem fi siguri că aceasta este cheia persoanei cu care dorim să facem schimb de informații confidențiale. Nu costă nimic ca un atacator să „rupă” canalul de comunicare și, după ce a schimbat cheile publice cu ambii abonați, să citească întreaga corespondență, re-criptând-o înainte de a o trimite către destinatarul real. Acest atac, numit „om la mijloc”, afectează toți algoritmii criptografici asimetrici. Cum să te descurci cu asta? Pentru a schimba cheile la o întâlnire personală cu toți corespondenții? Atunci este mai profitabil să folosiți abordarea clasică cu chei simetrice. Cea mai optimă soluție este crearea unei autorități cheie de certificare. Ca autoritate de certificare, este aleasă o organizație în care toți participanții la schimb au încredere și căreia îi prezintă personal cheile publice. Centrul generează certificate din cheile colectate prin semnarea acestora cu semnătura sa electronică. După aceea, fiecare participant primește un certificat (propria cheie publică semnată de centru) și cheia publică a centrului. Acum, la stabilirea unei conexiuni, corespondenții schimbă nu doar chei publice, ci și certificate, ceea ce face posibilă identificarea unică a celui de-al doilea participant la schimb prin verificarea semnăturii electronice a centrului sub certificatul său.

Realizările criptografiei moderne vă permit să protejați în mod fiabil informațiile de accesul neautorizat, denaturare; vă permit să rezolvați problemele legate de autorul documentului și multe altele. Cu toate acestea, nu totul este atât de roz. Una dintre cele mai dificile probleme în funcționarea criptosistemelor este păstrarea secretă a cheilor. Siguranța cheii este foarte influențată de factorul uman, iar aceasta este cea mai slabă verigă a sistemului de protecție. Oamenii tind să facă greșeli; îi este greu să stocheze cantități mari de informații cheie în memorie, așa că este forțat să le noteze undeva - de exemplu, pe un smart card. Pentru a preveni utilizarea neautorizată a unui smart card în cazul furtului acestuia, accesul la acesta este posibil numai după prezentarea unui cod PIN (PIN - număr personal de identificare, număr personal de identificare). Lungimea codului PIN este de obicei de 4 cifre (pe care mulți preferă să le țină notate pe o bucată de hârtie și chiar să o păstreze împreună cu cardul). Se știe că securitatea generală a unui sistem este determinată de cea mai slabă verigă a sa. O persoană poate fi forțată să efectueze anumite acțiuni sub amenințarea violenței fizice, șantajului, luării de ostatici etc. Pe lângă erorile personalului de operare și acțiunile rău intenționate, erorile și calculele greșite sunt posibile în implementarea practică chiar și a unui algoritm matematic foarte bun și verificat în mod repetat. Pentru a evita furtul unei chei folosind „marcaje” software sau hardware, este necesară verificarea calculatoarelor pe care vor fi operate criptosistemele, precum și protejarea acestor calculatoare și a incintelor în care se află de accesul neautorizat.

De asemenea, trebuie avut în vedere faptul că mulți criptoalgoritmi se bazează pe imposibilitatea rezolvării anumitor probleme matematice într-un interval de timp acceptabil (problema „împachetarea unui rucsac”, „cea mai ieftină cale”, logaritmul discret, descompunerea în factori primi etc. .), cu toate acestea, posibilitatea de a găsi noi algoritmi care să permită rezolvarea acestor probleme într-un timp mai scurt. În plus, nu este exclusă posibilitatea de a găsi o modalitate rapidă de rezolvare a acestor probleme folosind rețele neuronale sau metode non-matematice (de exemplu, modelarea fizică a proceselor).

Astfel, în ciuda tuturor beneficiilor evidente ale utilizării sale, criptografie este plină de pericolul iluziei de securitate completă și, ca urmare, slăbește atenția față de alte metode de protecție a informațiilor.

În același timp, criptografia rămâne una dintre domeniile de cunoaștere cu cea mai rapidă dezvoltare și ocupă un loc demn printre mijloacele de asigurare a securității informațiilor.

# Concluzie