$\alpha + \omega$, 2003, Nr. 1, 20–33

Kriptografija: menas, pavirtęs mokslu

Vilius Stakėnas
vilius@ktl.mii.lt

Kriptologija yra šifravimo mokslas. Informacinių technologijų amžiuje ji tapo matematikos sritimi. Straipsnyje apžvelgiama kriptologijos istorija ir dabarties uždaviniai.

Savoir est pouvoir — žinios yra jėga. Mūsų žinios yra mūsų jėga. O žinios apie mus? Kartais tai gali būti jėga, kurios vertėtų išvengti.

Jeigu informacija apie objektą egzistuoja tik kartu su juo, tai didelių problemų nekyla. Jei objekto nematyti, tai ir informacijos apie jį nėra. Tačiau žmonės sugalvojo būdą, kaip atskirti daiktus ir reiškinius nuo žinių apie juos. Paprastai sakant, jie sugalvojo raštą. Taigi, be savo pirminio realaus gyvenimo, žmonės įgijo antrinę „užrašytą", nekontroliuojamą būtį. Juk sakoma, kad žodis — ne žvirblis, išskridusio nepagausi.

Senųjų amžių kriptografijos apžvalga

Atsiradus raštui, kurį supranta visi raštingi žmonės, greitai pradėta bandyti rašyti taip, kad ne visi perskaitytų. Pirmuosius bandymus rašyti kitaip negu visi liudija maždaug 3–4 tūkst. m. pr. Kr. egiptiečių įrašai antkapiniuose akmenyse. Šių įrašų hieroglifai skiriasi nuo įprastinių kasdienio vartojimo hieroglifų. Galbūt šitaip siekta patraukti skaitytojų dėmesį, suteikti įrašams paslaptingumo. Šiaip ar taip, tai pirmieji žinomi bandymai apsunkinti skaitymą. Tačiau niekas negali patvirtinti, kad egiptiečiai tikrai naudojo slaptaraštį tiesiogine žodžio prasme, t. y. būdą rašyti taip, kad suprastų tik tie, kam tas raštas skirtas.

Neabejotina, kad slaptaraštį naudojo žydų raštininkai. Pavyzdžiui, Šventojo Rašto Jeremijo knygoje, parašytoje apie 500–600 m. pr. Kr., naudojamas vadinamasis ATBASH slaptaraštis. Jo esmė ta, kad vienos raidės keičiamos kitomis. Pavyzdžiui, lietuvių kalbos abėcėle parašytus tekstus perrašydami šiuo slaptaraščiu turėtume keisti raides tokia tvarka:

A	Ą	B	C	Č	D	E	Ę	Ė	F	G	H	I	Į	Y	J
↕	↕	↕	↕	↕	↕	↕	↕	↕	↕	↕	↕	↕	↕	↕	↕
Ž	Z	V	U	Ū	Ų	T	Š	S	R	P	O	N	M	L	K

Slaptaraščiai minimi ir klasikinės Graikijos šaltiniuose. Pavyzdžiui, Spartoje apie 500 m. pr. Kr. taikytas tekstų šifravimo būdas, kurį galime laikyti pirmuoju „šifravimo mašinos" panaudojimo atveju. Prietaisas labai paprastas: jį sudaro lazdelė (gr. *skytalė*) ir odos juosta, kurią reikia užvynioti ant lazdelės pagal sraigtinę liniją. Po to išilgai lazdelės ant odos reikia rašyti tekstą eilutė po eilutės. Baigus rašyti, juostelė nuvyniojama. Ant jos matomos tarsi atsitiktinai užrašytos raidės. Kad iš jų susidėtų prasmingas tekstas, juostelę vėl reikia užvynioti ant to paties skersmens lazdelės. Kai kurie autoriai abejoja, ar toks šifravimo būdas tikrai buvo naudojamas. Šiaip ar taip, idėja yra puiki.

Tačiau svarbiausias graikų įnašas į mokslą apie slaptąjį raštą — pats šio mokslo pavadinimas. *Kriptografija, kriptologija* — abu terminai prasideda tuo pačiu graikų kalbos žodžiu *kripto* ($\kappa\rho\upsilon\pi\tau\omega$) — slėpti.

Slaptaraštis minimas ir klasikiniuose indų civilizacijos šaltiniuose. Pavyzdžiui, apie 300 m. pr. Kr. parašytame politikos veikale „Artha-Sastra" informaciją apie žmonių lojalumą patariama rinkti šitaip:

> ...reikia pasiklausyti elgetų šnekų, taip pat girtuoklių ir kvailių, perskaityti užrašus ant sienų maldininkų lankomose vietose ir šventyklose, taip pat iššifruoti užrašus ir slaptus raštus...

„Kama-Sutroje" slaptaraščio menas įvardijamas kaip 44-asis iš 64 menų, kuriuos turi išmanyti vyrai ir moterys.

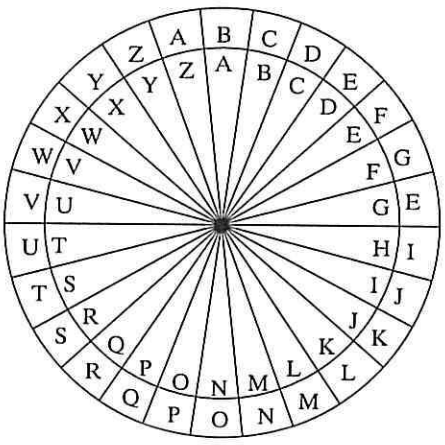
Tačiau grįžkime prie Vakarų civilizacijos.

Didysis Cezaris rašė Ciceronui naudodamasis labai paprastu teksto šifravimo būdu: kiekviena abėcėlės raidė keičiama raide, kuri abėcėlėje užrašyta trimis pozicijomis toliau. Norėdami suprasti, kaip keičiamos paskutinės trys abėcėlės raidės, įsivaizduokime, kad abėcėlė išrašyta apskritimu. Galima susitarti kiekvieną abėcėlės raidę keisti ne trečiąja, bet ketvirtąja, penktąja ir t. t. užrašyta raide. Tokį šifravimo būdą vadiname Cezario kriptosistema. Mūsų akimis, ji yra paprasta tarsi žaisliukas. Tačiau tuomet, kai net neužšifruotą tekstą skaityti ne tiek jau daug kas mokėjo, jos tikriausiai pakako. Mums ji tebėra įdomi kaip paprasto šifravimo pavyzdys, kuriuo pasinaudojus galima paaiškinti kai kurias gana sudėtingas kriptologijos sąvokas.

Apie viduriniųjų amžių kriptografiją nedaug įdomaus galima pasakyti. Slaptaraščiai buvo naudojami magiškiems receptams šifruoti. Jeigu kas ir domėjosi kriptografijos teorija, tai tik arabai. Užbaigtoje 1412 metais 14 tomų arabų mokslo enciklopedijoje buvo skyrius, skirtas kriptografijai. Tačiau dauguma jų kriptografijos veikalų neišliko.

Renesanso amžiaus kriptografija

1467 metai yra svarbi Vakarų pasaulio kriptografijos data. Tais metais Leonas Batista Alberti (1404–1472) parašė 25 puslapių „De cifris", kur išdėstė naują tekstų šifravimo būdą. L. Alberti buvo tikras Renesanso žmogus. Tokių įvairiapusių interesų žmogų mūsų laikais sunku sutikti. Jis buvo architektas, dailininkas, kompozitorius, vargonininkas, taip pat mokslininkas. L. Alberti žinojo, kaip perskaityti tekstus, užšifruotus vienas raides keičiant kitomis. Jis iškėlė mintį, kad galima šifruoti taikant ne vieną, bet kelias raidžių keitimo kitomis taisykles. Jis sugalvojo paprastą prietaisą, kuriu naudojantis tai galima lengvai daryti (1 pav.).



1 pav. Alberti skrituliai

Šį prietaisą sudaro du skrituliai — didesnis ir mažesnis. Jų pakraščiuose išrašytos 24 lotyniškos abėcėlės raidės, mažesnįjį galima sukioti apie ašį, einančią per bendrą abiejų skritulių centrą. Fiksavę mažojo skritulio padėtį didžiojo atžvilgiu, gauname raidžių keitimo kitomis raidėmis taisyklę: kiekviena ant didžiojo skritulio užrašyta raidė keičiama po ja stovinčia mažojo skritulio raide. Užšifravę pirmąją teksto raidę, galime pasukti mažąjį skritulį ir antrąją raidę jau šifruoti naudodamiesi kita raidžių keitimo taisykle! Taigi telieka susitarti, kaip sukioti mažąjį skritulį. Nesunku suprasti, kad šiais skrituliais galime naudotis ir dešifruodami tekstą.

Tai buvo tikrai saugus tų laikų šifras. Alberti galėtume vadinti moderniosios kriptologijos pradininku. Tačiau iš tiesų jo išradimas buvo pamirštas ir vėliau ne kartą išrastas iš naujo. Pavyzdžiui, panašią šifravimo sistemą 1518 metais pasiūlė benediktinų vienuolis Trithemius pirmojoje spausdintoje kriptografijos knygoje „Polygraphiae". Giovanis Batista Belaso 1553 metais sugalvojo, kaip paprastai nurodyti naudojimosi Alberti skrituliais taisyklę. Ją galima nusakyti vienu ar keliais žodžiais. Pavyzdžiui, taisyklė, nusakoma žodžiu BELASO, yra tokia: pasukame mažąjį skritulį, kad po didžiojo skritulio raide A būtų mažojo skritulio raidė B, užšifruojame pirmąją teksto raidę; pasukame mažąjį skritulį, kad po didžiojo skritulio raide A būtų mažojo skritulio raidė E, užšifruojame antrąją teksto raidę ir t. t. Užšifravę pirmąsias šešias teksto raides, naudojame tą patį žodį nuo pradžios. Taigi žodis yra šio šifro raktas. Atrodo, matematikui ir gydytojui Džirolamo Kardano atėjo į galvą mintis, kad šį šifrą galima dar patobulinti naudojant patį šifruojamą tekstą kaip raktą. Tai galima daryti įvairiais būdais. Pavyzdžiui, pirmąją teksto raidę galima užšifruoti naudojant iš anksto sutartą skritulių tarpusavio padėtį, o po to patį šifruojamą tekstą naudoti kaip raktą, t. y. sukioti mažąjį skritulį taip, kaip nurodo šifruojamo teksto raidės.

Alberti išrastas šifras dabar dažniausiai vadinamas Vigenere šifru. Blezas de Vigenere (1523–1596) buvo prancūzų diplomatas, daug keliavęs po Europą. Būdamas 47 metų jis atsidėjo vien rašymui. Rašė apie viską: alchemiją, magiją, kabalą, kometas, šifrus... 1585 metais parašė 600 puslapių veikalą apie šifrus „Traictè des Chiffres". Tai nebuvo vien kriptografijos veikalas. Jame buvo ir receptų, kaip pasigaminti aukso. Tačiau Vigenere gerai išdėstė ir to meto kriptografijos pagrindus.

Kriptografija politikos tarnyboje

XVII amžiuje kriptografija ir kriptoanalizė tapo kasdieniu didžiosios politikos įrankiu. Pirmasis profesionalus prancūzų kriptografas buvo Antuanas Rossignolis, o anglų — matematikas Džonas Valis. A. Rossignolio karjera prasidėjo 1628 metais, kai jis prisidėjo prie karaliaus, kovojančio prieš hugenotus. Karaliaus šalininkai buvo apsupę gerai įtvirtintą Realmonto miestą. Nesitikėdami jo paimti jie gal būtų ir pasitraukę, tačiau Rossignoliui pavyko iššifruoti slaptą hugenotų pranešimą, kuriame buvo rašoma, kad jų amunicijos atsargos baigiasi. Karaliaus šalininkai paėmė miestą, o Rossignolis gavo labai gerai atlyginamą kriptoanalitiko tarnybą karaliaus dvare.

Kriptoanalitikų tarnybas prie savo dvarų įsteigė ir kiti Europos valdovai. Šios tarnybos paprastai buvo vadinamos juodaisiais kambariais (*Black Chamber, Cabinet Noir, Geheimkabinett*). Juose dirbantys žmonės atplėšinėjo ir skaitė laiškus, dešifravo tekstus. Geriausią kriptoanalitikų grupę turėjo Austrijos imperatorius. Dešimties žmonių grupė kasdien užšifruodavo ir dešifruodavo apie 100 pranešimų. Jie mokėjo visas Europos kalbas.

Po Didžiosios prancūzų revoliucijos pažiūra į „juoduosius kambarius" ėmė keistis. Laisvės idealai ir privačios korespondencijos skaitymas — visiškai nesuderinami dalykai. „Juodieji kambariai" ėmė nykti. Su jais — ir klasikinė „pieštuko ir popieriaus" kriptografija.

Moderniosios kriptografijos principai

Nauja epocha 1837 metais prasidėjo (beveik kaip visos naujos epochos) be didelio triukšmo: Samuelis Morzė išrado telegrafą. Informacija, kurią reikia perduoti, virto paprasčiausiais brūkšneliais ir taškais. Tie brūkšneliai ir taškai daug ką pakeitė. Pavyzdžiui, mūšiams vadovaujančius generolus nukėlė nuo žirgų, ant kurių jie stebėdavo mūšių eigą, ir pasodino už stalų kažkur saugioje užfrontės vadavietėje. Moraliniu požiūriu pasauliui tikriausiai būtų buvę geriau, jeigu jie ir toliau būtų jodinėję ir kariavę pagal šimtmečiais nesikeičiančias taisykles, tačiau nenugalimas išradėjų ir mokslininkų troškimas viską išaiškinti ir pritaikyti galų gale įteikia jų sukurtus prietaisus į rankas tiems, kurių aistra — naikinti ir griauti.

Šiaip ar taip, ir kriptografija turėjo prisitaikyti prie pasikeitusio informacijos vaizdavimo ir perdavimo būdo.

Naujųjų amžių reikalavimus kriptografijai pirmasis labai aiškiai ir konkrečiai suformulavo Augustas Kerckhoffas savo straipsnyje „La cryptographie militaire“, 1883 metais išspausdintame žurnale „Journal de sciences militaires“. Jo maksimas verta apžvelgti, kadangi jos iš esmės lieka aktualios ir mūsų laikais.

A. Kerckhoffas konstatuoja, kad atsirado būtinybė šifruoti ne pavienius vienkartinius pranešimus, tačiau garantuoti nuolatinį šifruotos informacijos perdavimą tarp armijos vadaviečių tokiais kanalais, kurių savybės negali būti keičiamos. Jis suformulavo šešis reikalavimus informacijos šifravimo prietaisams, kurie gali būti naudojami.

Pirma, jeigu šifravimo sistema gali būti įveikta, tai tik matematiškai (*le système doit être matériellement, sinon mathématiquement, indéchiffrable*). Taigi šifruota informacija negali būti atskleista taip, kaip iš dėlionės dalelių sudedamas paveikslas, t. y. sistemą galima įveikti tik atskleidus jos matematinius pagrindus.

Antra, sistema turi būti tokia, kad net ją turėdamas priešininkas negalėtų jos įveikti (*il faut qu'il n'exige pas le secret et qu'il puisse sans inconvénient tomber entre les mains de l'ennemi*).

Trečia, sistemos raktas turi būti įsimenamas ir perduodamas jo neužrašius, jis turi būti keičiamas (*la clè doit pouvoir en être communiquée et retenue sans le secours de notes écrites, et être changée et modifiée au gré des correspondants*).

Ketvirta, sistema turi būti pritaikyta telegrafo ryšiui (*il faut qu'il soit applicable à la correspondance télégraphique*).

Penkta, šifravimo sistema turi būti nešiojama ir naudojimuisi ja turi pakakti nedaug žmonių (*il faut qu'il soit portatif, et que son maniement ou son fonctionnement n'exige pas le concours de plusieurs personnes*).

Šešta, sistema turi būti paprasta: nereikalaujanti nei proto įtampos, nei ilgos taisyklių sekos (*le système doit être d'un usage facile ne demandant ni tension d'esprit, ni la connaissance d'une longue série de règles a observer*).

Taikant šį „kriptografijos kodeksą“ mūsų laikais pakaktų telegrafą pakeisti elektroniniu ryšiu.

Tačiau kriptografija Kerckhoffo laikais vis dar buvo kūdikystės amžiaus. Pats A. Kerckhoffas savo straipsnyje rašo, kad jį stebina mokyti žmonės, siūlantys šifravimo sistemas, kurias įveikti galima per pusvalandį.

Kriptografija I pasauliniame kare ir po jo

Suvokti kriptografijos reikšmę reikėjo sunkių išbandymų. Būtinybę kriptografijai kuo greičiau subręsti atskleidė Pirmasis pasaulinis karas.

$\alpha + \omega$

Kriptoanalitikų skyriai atsirado visų šalių slaptosiose tarnybose. Paprastai viena kriptoanalitikų grupė stengėsi dešifruoti diplomatinę, kita — karinę korespondenciją. Kriptoanalizė tapo kasdieniu juodu darbu. Šifruotoms telegramoms gauti didelių pastangų nebereikėjo — pakakdavo pasiklausyti radijo stočių.

Pirmojo pasaulinio karo metais kriptoanalitikų darbas pirmą kartą akivaizdžiai paveikė lemiamus politinius sprendimus. Anglų kriptoanalitikų tarnyba „Room 40" 1917 metais iššifravo vokiečių užsienio ministro Arthuro Zimmermano telegramą vokiečių ambasadoriui Meksikoje. Telegramoje buvo siūloma imtis veiksmų, nuteikiančių Meksiką prieš JAV. Kai telegramos tekstas tapo žinomas amerikiečiams, prezidentas Wilsonas priėmė sprendimą dėl karo paskelbimo vokiečiams.

Vokiečiai pradėjo karą neturėdami geros kriptoanalitikų tarnybos. Šioje srityje priešininkai juos gerokai pranoko. Nesudėtingus vokiečių šifrus „Room 40" darbuotojams nebuvo sunku įveikti, juoba kad raktai buvo retai keičiami. 1918 metais vokiečiai pradėjo naudoti vadinamąjį ADFGVX šifrą ir raktą keisdavo kasdien. Tačiau ir šį šifrą greitai įveikė prancūzų kriptoanalitikas leitenantas Georges-Jean Painvinas.

Pirmojo pasaulinio karo metai yra svarbus kriptologijos istorijos etapas. Per šiuos metus kriptologija iš antraeilio dalyko tapo svarbiu politikos ir karybos elementu.

Trečiojo XX amžiaus dešimtmečio kriptografijos pažanga visų pirma sietina su elektrinių-mechaninių šifravimo prietaisų konstravimu ir tobulinimu. Jaunas AT&T bendradarbis G. Vernamas dar 1917 metais JAV patentavo šifravimo įrenginį, kuriame naudojamas atsitiktinai generuotas, tokio pat ilgio kaip pats šifruojamas tekstas raktas. Savo šifravimo mašiną G. Vernamas pasiūlė JAV vyriausybei, tačiau pasiūlymas buvo atmestas. Išties naudotis tokia sistema gana sudėtinga, tačiau tai buvo vienintelė visiškai saugi kriptosistema. Apskritai nuo 1861 iki 1980 metų JAV buvo išduota apie 1700 su kriptografija susijusių patentų.

Pagrindinė XX amžiaus trečiojo dešimtmečio kriptografijos idėja buvo rotoriai. Tai diskai, suverti ant vienos ašies ir galintys sukiotis. Iš abiejų rotoriaus pusių yra elektriniai kontaktai, atitinkantys abėcėlės raides. Gretimų rotorių kontaktai liečiasi. Techninė rotoriais pagrįstų šifravimo mašinų konstrukcija yra gana sudėtinga, tačiau bendrąjį veikimo principą galima paaiškinti visiškai paprastai. Šifravimo mašinos priminė elektrines spausdinimo mašinėles: renkant klaviatūra tekstą ant popieriaus iš karto spausdinamas teksto šifras.

Prisiminkime Alberti skritulius: vienas jų yra didesnis, kitas mažesnis, galintis sukiotis apie bendrą skritulių ašį. Ant abiejų skritulių išrašytos abėcėlės raidės, mažojo skritulio raidės yra tiesiog po didžiojo skritulio raidėmis. Įsivaizduokime, kad naudojimasis šiais skirtuliais yra mechanizuotas: paspaudus didžiojo skritulio raidės klavišą, ant popieriaus atsiranda raidė, kuri mažajame skritulyje yra parašyta po ja, be to, skritulys per vieną raidę pasisuka. Paspaudus kitos raidės klavišą, vėl atspausdinamas jos šifras, o mažasis skritulys pasisuka ir t. t. Nesunku įsitikinti, kad ši sistema — Vigenere šifras, kurio ilgis lygus abėcėlės raidžių skaičiui n.

Prie dviejų skritulių galima pridėti dar ir trečiąjį, kuris taip pat sukiojasi. Galima padaryti taip, kad skrituliai suktųsi pagal tą pačią taisyklę kaip elektros, dujų ir kt. apskaitos skaitikliai: iš pradžių sukasi mažasis skritulys; jam apsisukus ratu, per vieną padalą pasisuka vidurinysis skritulys; vėl sukasi mažasis skritulys ir t. t. Tai būtų schemiškas šifravimo mašinos su trimis rotoriais modelis. Juo realizuojamas Vigenere šifras, kurio rakto ilgis yra n^2.

Rotorių idėja kilo keliems tarpusavyje nesusijusiems žmonėms. Vokietis Arthuras Scherbius patentavo išradimą 1918 metais, olandas Hugo Kochas ir švedas Arvidas Dammas — 1919 metais, amerikietis Edwardas Hebernas — 1921 metais. Didelės komercinės sėkmės išradėjai nesulaukė.

A. Scherbiuso firma „Chiffriermaschinen Aktiengesellschaft" 1923 metais pristatė komercinį šifravimo mašinos, pagrįstos rotoriais, modelį ENIGMA A. Vėliau pasirodė modeliai B, C, D

ir kt. Daugelis vyriausybių nusipirko po egzempliorių, kad specialistai galėtų jį išstudijuoti ir modifikuoti. Pats A. Scherbius tragiškai žuvo 1927 metais, o jo bendrovė pakeistu pavadinimu gyvavo iki 1945 metų.

Kriptografija II pasauliniame kare

Neįvertinę kriptografijos reikšmės Pirmojo pasaulinio karo metu, naująjį karą vokiečiai norėjo pradėti tinkamai pasiruošę. Pagrindinė jų kriptografinė amunicija — keli modifikuoti ENIGMA variantai. Tačiau jiems vėl labai nepasisekė.

Lenkai buvo sukūrę gerą kriptoanalitikų grupę. Jaunas matematikas Marianas Rejewskis 1932 metais įstengė įveikti Wehrmachto ENIGMA su trimis rotoriais. Šifrogramų, kurios radijo bangomis buvo perduodamos Prūsijoje, lenkai turėjo pakankamai. Jie pasinaudojo vokiečių neatsargumu. Pavyzdžiui, gana dažnai būdavo šifruojami raidžių pakartojimai: bb, ss ir t. t. Lenkams padėjo ir iš prancūzų šnipo Hans-Thilo Schmidto, dirbusio vokiečių gynybos ministerijoje, gauta informacija. Jis perdavė instrukcijas, kaip naudotis ENIGMA, taip pat keletą raktų. 1943 metais H.-T. Schmidtas buvo demaskuotas ir nužudytas.

Tačiau 1938 metais vokiečiai pakeitė šifravimo sistemą. Buvo pridėti dar du rotoriai. Padėtis darėsi grėsminga. Reikėjo glaudesnio Vakarų šalių bendradarbiavimo. Tarpininkaujant prancūzams, 1939 metų liepos 25 dieną Varšuvoje buvo surengtas lenkų ir anglų kriptoanalitikų susitikimas. Suspėta pačiu laiku, nes po mėnesio prasidėjo Antrasis pasaulinis karas. Lenkai pasidalijo su anglais savo patirtimi dešifruojant ENIGMA. Prieš pat karą anglai savo kriptoanalizės tarnybą iš užsienio reikalų ministerijos perkėlė į Bletchley Park vietovę. Čia kriptoanalitikai dirbo per visą karą. Vienas iš svarbių kriptoalitikų grupės uždavinių buvo ENIGMA dešifravimas.

2 pav. Vokiečių šifravimo mašina ENIGMA

$\alpha + \omega$

1939 metų rugsėjo 4 dieną į Bletchley Park atvyko matematikas Alanas Turingas. Jis pradėjo studijuoti lenkų informaciją ir analizuoti ENIGMA. Anglų Bletchley Park kriptoanalitikams jau 1940 metais pavyko įveikti silpniausią ENIGMA variantą — tą, kuriuo naudojosi Geringo Luftwaffe. Nuo 1941 metų birželio jau buvo dešifruojama ir karinių jūros pajėgų Kriegsmarine korespondencija, nuo 1941 metų rugsėjo anglai skaitė maršalo Rommelio pranešimus Berlynui. Tik sausumos karo pajėgų šifrų nepavyko atskleisti iki 1942 metų. Ši ENIGMA istorija akivaizdžiai rodo, koks pavojingas kriptografijoje pasitikėjimas, kuris neparemtas išsamia analize. Vokiečiai manė, kad jų ENIGMA neįveikiama, o ji jau nebebuvo paslaptis priešininkams kone nuo pat sistemos naudojimo pradžios!

Panašiai atsitiko ir japonams. Jie neįvertino amerikiečių kriptoanalitikų, galbūt tikėjosi kad pati japonų kalba jau yra papildoma saugumo garantija.

Amerikoje dirbo Williamas Friedmanas. Jis laikomas vienu geriausių visų laikų kriptoanalitikų. Jo kelio į karinės kriptografijos tarnybą pradžia buvo labai nutolusi nuo valstybinių paslapčių. Jaunystėje jis tyrinėjo populiarią hipotezę, kad Šekspyro kūrinių autorius iš tikrųjų yra ne Šekspyras, bet filosofas Francis Baconas. Nuo 1917 metų W. Friedmanas kartu su savo žmona Elizabeth dirbo kriptoanalitikų darbą JAV vyriausybėje. Beje, W. Friedmanas pirmasis pradėjo vartoti ir patį kriptoanalizės terminą.

3 pav. Amerikiečių kriptografai William ir Elizabeth Friedman

Japonai taip pat naudojo šifravimo mašinas su rotoriais. Pirmąją iš jų, amerikiečių pavadintą RED, amerikiečiams pavyko įveikti dar 1936 metais. Nuo 1937 metų japonai pradėjo naudoti sudėtingesnį šifravimo įrenginį PURPLE. Jį perprasti amerikiečiams prireikė aštuoniolikos mėnesių.

Kriptografija virsta matematika

1948 metais išspausdintas C. Shannono straipsnis „A Mathematical Theory of Communication" reiškė naujos matematikos srities, nagrinėjančios informacijos perdavimo procesus, gimimą. Naujoji teorija išniro kone tobula forma — kaip kokia Botičelio Venera. Prieš tai buvo kitas straipsnis, tiksliau, slaptumo grifu pažymėtas C. Shannono veikalas „A Mathematical Theory of Cryptography". Taigi kriptografija iš neapibrėžtų kontūrų disciplinos tapo matematikos sritimi. Žinoma, tuomet niekas negalėjo nuspėti, kokią reikšmę ji įgis vos po kelių dešimtmečių, kad ji paliks uniformuotų kariškių ar smokinguotų diplomatų draugiją ir taps nelabai disciplinuotos ir tvarkingos universitetų bendruomenės diskusijų tema.

Baigęs studijas, Claude Shannonas 1936 m. atvyko į Masačiusetso universitetą ir pradėjo dirbti pas profesorių V. Bushą, kuris konstravo mechaninį skaičiavimo įrenginį. Tai buvo veikiau inžinieriaus ir mechaniko darbas negu tyrinėtojo. Profesoriaus paskatintas Shannonas pradėjo rašyti disertaciją apie logines operacijas, susijusias su konstruojama mašina. Jam kilo mintis patobulinti prietaisą panaudojus elektrines schemas. Kita puiki Shannono mintis — apie Būlio loginės algebros ir elektrinių schemų analogiją. Užbaigta 1937 m. disertacija buvo labai gerai įvertinta, o jos rezultatai beveik iš karto pritaikyti. Jo darbai svarbūs kompiuterių raidai. Kitas svarbus Shannono darbas pasirodė 1948 m., kai jis dirbo Bello laboratorijoje. „The Mathematical Theory of Communication" kartais vadinama informacijos amžiaus „Magna Charta".

4 pav. Claude Shannon (1916–2001)

Modernioji kriptografija: mokslas apie A, B, ir Z santykius

Industrinė visuomenė iš esmės virto informacine. Žemės paviršių tarsi voratinklis apraizgė informacijos perdavimo kanalai, kuriais keliauja milžiniški informacijos srautai.

Visas šis didžiulis ir sudėtingas tinklas susideda iš elementų, kuriuos galime apibūdinti labai paprastai:

- *subjektas A perduoda informaciją subjektui B.*

Gali būti, kad A ir B yra vienas subjektas; pavyzdžiui, kai informacija užrašoma ir laikoma.

Kad šie ryšio subjektai nebūtų grynos abstrakcijos, subjektą A dažnai vadinsime Algiu, o B — Birute.

Šioje paprastoje schemoje abu subjektai niekada nėra vieni du. Visų pirma visada dalyvauja tai, ką mes pavadinsime Gamta. Tad pranešimas, kurį A siunčia B, gali pasiekti adresatą iškraipytas arba visai jo nepasiekti. Apie šį trečiąjį informacijos perdavimo proceso dalyvį galima pasakyti štai ką:

- *gamta gali pakenkti informacijos perdavimo procesui, bet niekada nedaro to piktavališkai;*
- *gamta netobulina savo kenkimo būdų ir priemonių.*

Vis dėlto neigiamo Gamtos poveikio informacijos perdavimui dažnai negalima nepaisyti. Priešnuodžių galima rasti *kodavimo teorijoje.*

Tačiau kartais tenka daryti išvadą, kad ryšį veikia ne tik Gamta, bet ir paslaptingasis subjektas Z (Zigmas). Apie jį tenka daryti tokias prielaidas:

- *svarbiausias Z veiklos tikslas yra kontroliuoti A ir B ryšį;*
- *Z yra labai aukšto intelekto individas (galbūt daug kartų protingesnis už mus). Siunčiamai informacijai perskaityti ir analizuoti jis gali naudoti geriausias šiuo metu egzistuojančias technines priemones.*

Taigi norėdami išsaugoti savo ryšio privatumą Algis ir Birutė turi pasirūpinti jo saugumu. Sukurti ryšio saugumą garantuojančias priemones — tai ir yra iššūkis naujųjų laikų kriptografijai. Galvojant apie saugų ryšį visų pirma tenka atsižvelgti į tai, kad fizinės ryšio saugumo priemonės negali būti efektyvios. Juk elektroninio ryšio kanalų neįmanoma paslėpti. O nesinaudoti jais reiškia nedalyvauti informacinės visuomenės gyvenime. Be fizinių ryšio saugumo priemonių, dar yra teisinės ir matematinės. Matematinių ryšio saugumą garantuojančių priemonių kūrimas yra kriptografijos mokslo uždavinys.

$\alpha + \omega$

Siekiantis pažeisti Algio ir Birutės ryšio saugumą, Zigmas taip pat turi savo mokslą — *kriptoanalizę*. Kriptografija ir kriptoanalizė sudaro *kriptologiją*. Teorijos plėtojimo požiūriu Zigmas nėra Algio ir Birutės priešas. Juk pažeisdamas Algio ir Birutės ryšio saugumą Zigmas parodo, kad jų naudojama sistema nėra patikima.

Aptarkime, ką iš viso reiškia informacijos saugumas, t. y. kas gręsia informacijai, siunčiamai viešu perdavimo kanalu. Visų pirma Z gali tą informaciją perskaityti. Pavyzdžių, kai tai yra nepageidautina, galima nesunkiai pateikti iš politikos, karybos, verslo, taip pat ir žmonių tarpusavio bendravimo sričių. Perdavimo kanalo dažniausiai neįmanoma, o todėl ir neverta slėpti. Tad svarbu neatskleisti informacijos prasmės, t. y. reikia

- *atvirą tekstą* versti *šifru*, šifruoti.

Šifravimo būdą, arba algoritmą, tenka sugalvoti. Galima sugalvoti ką nors panašaus į egiptiečių raštą. Jei algoritmas labai paprastas — Zigmas jį nesunkiai atspės. Jeigu sudėtingas — algoritmą teks užrašyti ir saugoti. Tačiau reikia atsiminti Z savybes. Jei šifravimo algoritmu naudosimės pakankamai ilgai, Zigmas jį įmins arba paprasčiausiai gaus (jis lengvai įgyja žmonių pasitikėjimą ir negaili pinigų). Algoritmą sunku nuslėpti, tad to ir neverta daryti. Reikia, kad šifravimo algoritmas turėtų parametrą (*raktą*), jį ir reikia slėpti. Tai vienas iš pagrindinių moderniosios kriptografijos principų, suformuluotų Kerckhoffo von Nieuwenhofo. Tuos principus jau minėjome anksčiau.

Apžvelgdami senųjų amžių kriptografijos istoriją, taip pat jau minėjome keletą šifrų su raktais pavyzdžių. Štai dar vienas toks pavyzdys. Posakį

HE WHO TEACHES LEARNS

išrašykime zigzagine $k = 4$ aukščio laužte, primenančia geležinkelio tvorelę, skirtą apsaugoti bėgiams nuo užpustymo:

```
H       E       L
 E   T   A   S   E   S
  W O     C E     A N
   H       H       R
```

Skaitydami tekstą eilutėmis, gauname

HELETASESWOCEANHHR

Tai ir yra „geležinkelio tvorelės“ sistema šifras, gautas naudojant raktą $k = 4$.

Naudodamiesi tinkama šifravimo sistema, galime tikėtis, kad Zigmas, net ir turėdamas mūsų pranešimus, neįstengs atskleisti jų prasmės, t. y. informacijos slaptumas, arba lotyniškai tariant — konfidencialumas, bus garantuotas.

Tačiau Zigmas gali ne tik pasyviai skaityti Algio ir Birutės pranešimus. Jis gali aktyviai įsiterpti į ryšio kanalą ir pakeisti ką nors siunčiamoje informacijoje sau naudinga linkme. Net vieno bito pakeitimas gali sukelti labai nemalonių padarinių. Įsivaizduokime, kad pranešime finansų įstaigai „*Perveskite* 1000 $ *į sąskaitą Nr.* 1 000 000“ vietoje paskutinio nulio atsirado vienetas. Kita vertus, Zigmas Birutei dezinformaciją gali perduoti prisidengęs siuntėjo Algio vardu. Todėl dažnai pageidautina, kad pranešimo gavėjas turėtų galimybę patikrinti, ar jį pasiekusi informacija nėra pakeista bei trečiojo asmens sufalsifikuota. Taigi garantuoti informacijos vientisumą ir autentiškumą taip pat yra vienas iš kriptografijos uždavinių. Autentiškumo problema turi dar vieną aspektą. Kai Algį ir Birutę sieja tiesioginis ryšys, jiems svarbu žinoti, kad ryšio kanalas tikrai jungia juos, o ne, pavyzdžiui, Birute ar Algiu apsimetusį Zigmą. Todėl svarbu, kad būtų įmanoma kriptografijos priemonėmis patikrinti ryšio subjektų identitetą. Šis uždavinys vadinamas *subjekto identifikavimo problema*.

Tam tikrų problemų tarp Algio ir Birutės gali kilti ir be Zigmo įsikišimo. Tarkime, Algis pranešime Birutei kažką pažadėjo, o vėliau paneigė tvirtindamas, kad tas pranešimas yra piktavalio

Zigmo suklastotas. Taigi atsiranda būtinybė turėti priemonių, įrodančių, kad Algis tikrai ketina išsižadėti savo pranešimo.

Trumpai, nors ir neaprėpiant visų aspektų, galima teigti, kad pagrindiniai kriptografijos mokslo tikslai — sukurti priemones, kurios gali būti naudojamos garantuoti *informacijos slaptumą, vientisumą bei autentiškumą*, patikrinti ryšio subjektų *identitetą*, paneigti *išsižadėjimus*.

Visi šie reikalavimai ne visada yra vienodai svarbūs. Minėtas pranešimas bankui gali būti perduotas ir atviru tekstu, tačiau labai svarbu, kad jis būtų autentiškas.

Simetrinės kriptosistemos

Sudarant šifravimo sistemą (kriptografijoje jos vadinamos tiesiog kriptosistemomis), reikia nustatyti: kokius pranešimus šifruosime, kokius raktus naudosime, kokie bus mūsų šifravimo ir dešifravimo algoritmai. Dabar šifravimo ir dešifravimo operacijas vykdo kompiuteriai, todėl prieš šifruojant tekstinius pranešimus patogu juos paversti skaičiais, arba tiesiog nulių ir vienetų srautais. Taigi moderniojoje kriptografijoje tiek pranešimai, tiek šifrai dažniausiai būna tiesiog skaičiai, o šifravimą ir dešifravimą sudaro tam tikrų matematinių operacijų seka.

Nešifruotų pranešimų aibę pažymėkime $\mathcal{M}$, o šifruotų — C. Nešifruoti pranešimai dažnai vadinami atvirais tekstais (*plaintext*), šifruoti — šifrais (*ciphers*). Kartais šifrai vadinami kodais. Kažkada kodai ir šifrai tikrai buvo tas pats. Tačiau mūsų laikais Algis ir Birutė naudoja kodus, kai jiems trukdo Gamta, o šifrus, kai kovoja su Zigmu. Praktiškai kiekvienas pranešimas gali būti labai ilgas simbolių (bitų) srautas. Šifravimo procedūra yra funkcija, kuri pagal tam tikrą algoritmą verčia atvirą tekstą šifru. Jei operuojama pavieniais simboliais (bitais), gaunamas šifras vadinamas srauto šifru (*stream cipher*); jeigu pranešimas skaidomas blokais ir šie blokai šifruojami, šifrai vadinami blokų šifrais (*block ciphers*).

Bendroji ryšio, saugomo minėta kriptosistema, schema yra tokia:

- *subjektas A, naudodamas raktą $K_{c,B}$, šifruoja pranešimą ir siunčia B šifrą $C = e(M, K_{c,B})$;*
- *subjektas B, naudodamas raktą $K_{d,B}$, dešifruoja tekstą ir skaito gautą pranešimą $M = d(C, K_{d,B})$;*
- *jei yra atgalinis ryšys, šifravimas ir dešifravimas vykdomas naudojantis raktais $K_{c,A}$ ir $K_{d,A}$.*

Gali atrodyti, kad tokia raktų gausybė yra nereikalinga. Išties paprasčiausių sistemų

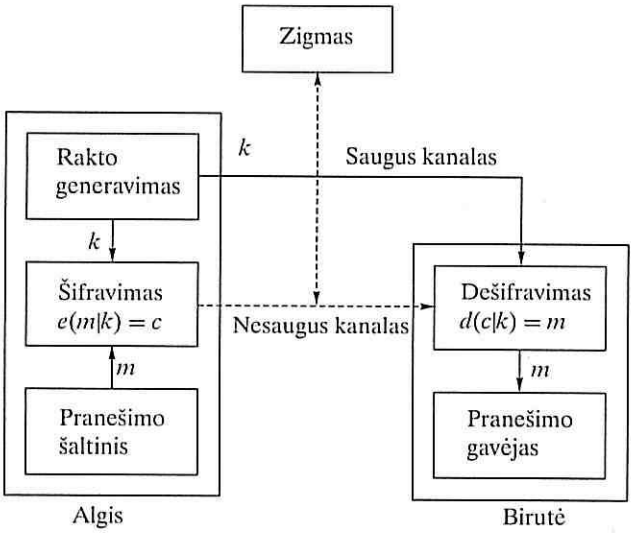
$$K_{c,A} = K_{d,A} = K_{c,B} = K_{d,B}.$$

Tokias sistemas vadiname *simetrinėmis*. Simetrinės yra ir tokios sistemos, kurių dešifravimo raktas nesutampa su šifravimo raktu, tačiau nesunkiai gali būti iš jo randamas. Vienas iš simetrinės kriptosistemos trūkumų — raktams perduoti reikia atskiro saugaus kanalo. Tai gali brangiai kainuoti (kiek kainuoja nuskristi iš Vilniaus į Čikagą?). Juk po tam tikro laikotarpio raktus reikia keisti!

Simetrinės sistemos pavyzdys — geležinkelio tvorelės sistema. Simetrinė sistema idealiai tinka tuo atveju, kai A ir B yra tas pats subjektas, t. y. privati informacija tiesiog šifruojama norint ją apsaugoti nuo negerų akių. Tačiau kai simetrine sistema nori naudotis du skirtingi subjektai, jie turi susitarti dėl rakto, kurį turi laikyti paslaptyje. Tačiau tai, ką žino bent du asmenys, jau nebėra paslaptis.

Simetrinėse sistemose informacijos slaptumas ir autentiškumas garantuojami arba pažeidžiami vienu metu. Tačiau simetrinėje sistemoje slypi kartais nepageidaujama galimybė išsiginti informacijos. Tarkime, naudodamasis simetrine kriptosistema Algis pasiuntė Birutei pranešimą: „*Sutinku su reikalavimais, tik atsiųsk* 1000 *litų.*“ Pinigus Algis gavo, tačiau reikalavimų nevykdė, motyvuodamas, kad Zigmas įspėjo raktą (greičiausiai tai įvyko dėl Birutės neapdairumo) ir nutrynė Algio siųstame pranešime žodžio „sutinku“ priešdėlį „ne“. Birutė turės nuryti šią karčią piliulę, nes jokių formalių galimybių įrodyti, kad Algis meluoja, nėra.

$\alpha + \omega$



5 pav. Ryšio, saugomo simetrine kriptosistema, schema

Viešojo rakto kriptosistemos

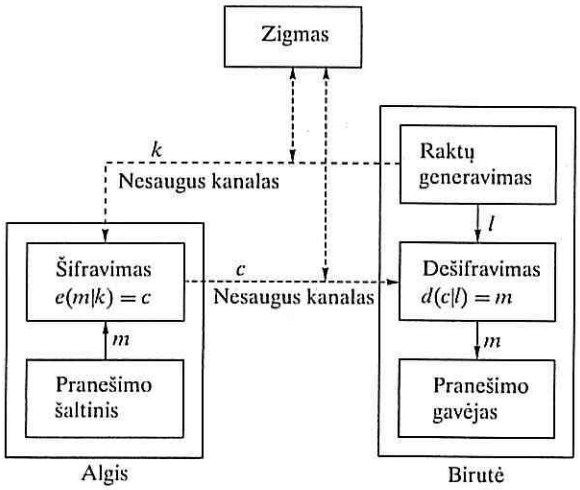
Diffie ir Hellmanas 1976 metais pasiūlė visiškai naują informacijos šifravimo principą. Jo esmė — šifravimui ir dešifravimui naudojami skirtingi raktai, be to, žinant šifravimo raktą praktiškai neįmanoma rasti dešifravimo rakto. Tokios sistemos vadinamos *asimetrinėmis*, arba *viešojo rakto* (*public-key*), sistemomis. Šitaip pabrėžiama, kad šifravimo raktas gali būti skelbiamas viešai, ryšio slaptumui tai nekenkia. Viešojo rakto sistemą galima palyginti su pašto dėžute: visi gali mesti savo laiškus pro plyšį, tačiau dėžutę atsirakinti ir skaityti laiškus (dešifruoti) gali tik turintis pašto dėžutės raktą.

Apžvelkime, kaip viešojo rakto sistemoje garantuojamas informacijos slaptumas. Subjektas A siunčia pranešimą M subjektui B, šifravimui naudodamas raktą $K_c = K_{c,B}$, kuris yra *viešas*, t. y. ne tik neslepiamas, bet galbūt viešai visiems paskelbtas (kaip adresas adresų knygoje). Gautą šifruotą tekstą $C = e(M, K_c)$ galima perskaityti tik turint raktą $K_{d,B}$, kuris yra žinomas tik B. Net pats siuntėjas A nebegali dešifruoti teksto C, nes pagal raktą $K_{c,B}$ praktiškai negalima sudaryti rakto $K_{d,B}$. Suprantama, tokiu būdu garantuojamas pranešimo slaptumas, tačiau jokiu būdu ne autentiškumas, nes kas nori, tas gali rašyti B vardu.

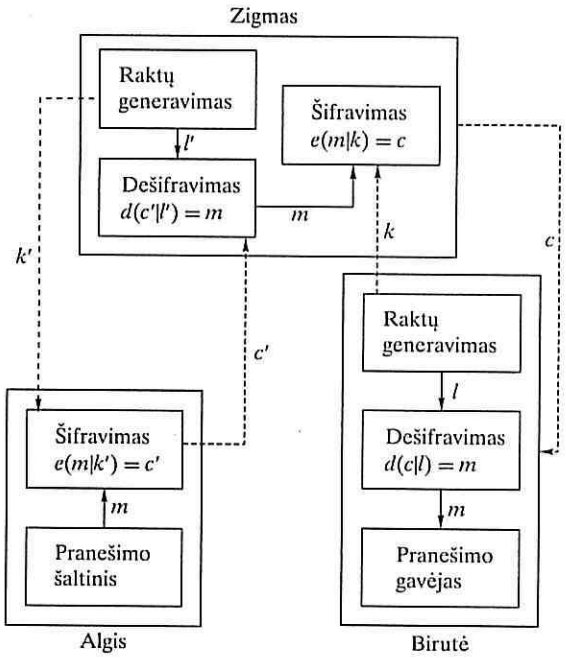
Nors viešojo rakto sistemai nereikia saugaus kanalo, tačiau Zigmas vis dėlto gali sukelti tam tikrų problemų. Tarkime, Zigmas, įsiterpęs į nesaugų kanalą, aptiko Algiui siunčiamą viešąjį Birutės raktą, jį užsirašė, o Algiui pasiuntė savo viešąjį raktą. Vargšas Algis liko apgautas — saugaus ryšio su Birute jis nebeturės!

Taigi ir viešojo rakto sistemose gali tekti spręsti raktų paskirstymo problemą.

Dabar tarkime, kad reikia garantuoti pranešimo autentiškumą nesirūpinant jo slaptumu. Tada saugomas tas raktas, kuriuo informacija šifruojama, t. y. K_c. Už jo saugojimą atsakingas pats siuntėjas A, ir jeigu Z jį sužinojo — tai paties siuntėjo kaltė. Skaitymui skirtas raktas K_d gali būti viešas, nes pagal jį praktiškai negalima atkurti K_c. Žinoma, teorinė galimybė tai padaryti egzistuoja, tačiau patikrinti reikiamą skaičių variantų reikia sugaišti metų metus...



6 pav. Ryšio, saugomo viešojo rakto kriptosistema, schema



7 pav. Kriptosistemos ataka apsimetus teisėtu ryšio subjektu

Skaitmeniniai parašai

Viešojo rakto schemoje realizuojama *skaitmeninio parašo* (*digital signature*) idėja. Subjekto A parašą suprantame kaip tam tikrą informaciją, kurią:

- *gali sukurti tik A*;
- *B gali patikrinti, ar parašas tikrai sukurtas A*;
- *tuo atveju, kai A bando išsiginti parašo, trečiasis asmuo turi turėti nei nuo A, nei nuo B, nei nuo savo simpatijų ir antipatijų nepriklausantį mechanizmą, nustatantį, ar parašas tikrai priklauso A.*

Nors tai atrodo keistokai, būna atvejų, kai pranešimų autentiškumas yra būtinas, o slaptumas nepageidautinas. Pavyzdys gali būti tokia branduolinio nusiginklavimo sutarties kontrolės sistema, kuri iš tikrųjų buvo pasiūlyta.

Šalis X įgyja teisę šalyje Y turėti seismologijos laboratoriją ir surinktą informaciją siųsti iš Y į X ryšio kanalu. Šaliai X rūpi, kad informacija, kurią ji gauna, ateitų būtent iš jos laboratorijos, o ne iš šalies Y kompiuterių. Tad X suinteresuota informacijos autentiškumu. Kita vertus, Y nenori, kad ryšio kanalu naudotųsi ne tik laboratorija, bet ir X žvalgybos Y teritorijoje rezidentai, todėl nori siunčiamą informaciją skaityti. Savo ruožtu autentiškumas rūpi ir šaliai Y. Nors ji ir skaito visą siunčiamą informaciją, kai kas gali būti sufabrikuota X šalies specialistų, o politikai tiesiog gali apkaltinti Y, kad pastaroji neigia tai, kas jai kenkia. Tokiu atveju trečiasis asmuo (Jungtinių Tautų techninės tarnybos) turi turėti galimybę patikrinti šalies X pateikiamus failus ir nustatyti, ar jie tikrai galėjo būti perduoti iš laboratorijos.

Viešojo rakto schemoje slaptumo ir tapatumo reikalavimai gali būti garantuoti tuo pat metu. Tarkime, A turi pasiųsti B slaptą ir autentišką pranešimą. Tada A turi turėti privatų raktą $K_{c,1}$ autentiškiems, bet nebūtinai slaptiems pranešimams pasirašyti ir viešą raktą $K_{c,2}$ slaptiems

pranešimams subjektui B šifruoti. Tada A pranešimą M šifruoja du kartus:

$$C_1 = e(M, K_{c,1}), \qquad C_2 = e(C_1, K_{c,2}).$$

Subjektas B taip pat turi du raktus: privatų raktą $K_{d,1}$ slaptiems pranešimams skaityti ir raktą $K_{d,2}$ autentiškumo reikalaujantiems nebūtinai slaptiems pranešimams skaityti. Dešifruojama taip pat dviem etapais:

$$C_1 = d(C_2, K_{d,1}), \qquad M = d(C_1, K_{d,2}).$$

Paminėsime, kad skaitmeninis parašas naudojamas apsaugoti programinę įrangą. Kad prisidengus svetimu vardu sistemai nebūtų įperšama diversinė programinė įranga, prieš ja naudojantis patikrinama, ar ji gamintojo pasirašyta.

Tenka pridurti, kad nuostabiomis savybėmis išsiskirianti viešojo rakto sistema gyvuoja tiek dėl matematikos jėgos, tiek dėl jos silpnumo. Viešojo rakto sistemų saugumas remiasi tuo, kad nėra žinoma efektyvių algoritmų tam tikriems skaičiavimo uždaviniams spręsti. Pavyzdžiui, kai matematikai sukurs efektyvius labai didelių natūraliųjų skaičių skaidymo pirminiais daugikliais algoritmus, ji taps kai kurių viešojo rakto sistemų laidotuvių diena.

Tiek simetrinės, tiek viešojo rakto kriptosistemos turi savų pranašumų ir trūkumų. Pavyzdžiui, šifravimas ir dešifravimas viešojo rakto sistemose paprastai reikalauja kur kas daugiau darbo negu simetrinėse. Derinant abiejų tipų sistemas galima sukurti efektyvią informacijos apsaugą. Pavyzdžiui, paskirstant raktus galima naudotis viešo rakto kriptosistema, o šifruojant informaciją — simetrine kriptosistema.

Dideles resursų sąnaudas viešojo rakto kriptosistemose galima sumažinti naudojant maišos funkcijas (*h-functions*, angl. *hash* — kapoti smulkinti).

Maišos funkcija (dažniausiai vadinama tiesiog h funkcija) yra atvaizdis, priskiriantis bet kokio ilgio abėcėlės $\{0, 1\}$ simbolių srautui fiksuoto ilgio vienetų ir nulių bloką. Taigi h funkcija iš pranešimo padaro fiksuoto ilgio santrauką (angl. *digest*). Svarbu, kad pagal santrauką būtų sunku rasti kokį nors ją atitinkantį pranešimą (suprantama, jų yra ne vienas). Sudarant parašą, galima naudotis ne visu (galbūt labai ilgu) pranešimu, bet jo santrauka.

Kaip jau minėta, raktų paskirstymas yra svarbi tiek simetrinių, tiek viešojo rakto kriptosistemų problema. Ją galima spręsti naudojant dar vieną ryšio sistemos subjektą — trečiąjį patikimą asmenį (TPA) (angl. *TTP — Trusted Third Person*). Galima susitarti, kad galioja tik tie viešieji raktai, kuriuos registravo TPA ir patvirtino savo skaitmeniniu parašu.

Kriptosistemų atakos ir saugumas

O dabar aptarkime, kriptoanalitiko Zigmo problemas.

Atvejai, kai šifruotas tekstas dešifruojamas ne matematinėmis priemonėmis, yra politikos, diplomatijos, žvalgybos ir kino filmų sritis. Kokia ryšio kanalo „žaliava“ gali naudotis kriptoanalitikas, siekdamas „sulaužyti“ kriptosistemą? Kalbame ne apie pavienio šifruoto teksto dešifravimą, bet apie dešifravimo algoritmo (rakto) įminimą, suteikiantį galimybę Z skaityti siunčiamą informaciją tol, kol raktas nebus pakeistas.

Šifro kriptoanalizė, t. y. bandymas atkurti pranešimą be rakto, vadinama *ataka*. Jos sėkmė priklauso nuo to, kokia informacija kriptoanalitikas gali naudotis. Kiekvieną ataką galima suformuluoti kaip atskirą uždavinį.

Jeigu naudojamasi tik šifrais, tai ataka vadinama

- *pavienių šifrų ataka* (*ciphertext-only attack*).

Žinoma: $C_1 = e(M_1, K), \ldots, C_i = e(M_i, K)$.

Ieškoma: arba $M_1, \ldots, M_i$ ir K, arba algoritmo, kuris bet kokiam $C_{i+1} = e(M_{i+1}, K)$ rastų M_{i+1}.

Jeigu pavyko gauti ne tik šifruotų, bet ir juos atitinkančių pradinių tekstų, kriptoanalitikas atlieka

- *teksto-šifro porų ataką* (*known-plaintext attack*).

Žinoma: $M_1, C_1 = e(M_1, K), \ldots, M_i, C_i = e(M_i, K)$.

Ieškoma: K arba algoritmo, kuris bet kokiam $C_{i+1} = e(M_{i+1}, K)$ nustatytų M_{i+1}.

Suprantama, šifravimą atlieka kompiuteriai. Zigmas gali pateikti šifravimo sistemai kokius nori tekstus ir gauti atitinkamus šifrus. Tada jis gali atlikti rimtą kriptosistemos išbandymą:

- *pasirinktų teksto-šifro porų ataką* (*chosen-plaintext attack*).

Žinoma: $M_1, C_1 = e(M_1, K), \ldots, M_i, C_i = e(M_i, K)$; čia pranešimus $M_1, \ldots, M_i$ pasirinko pats kriptoanalitikas.

Ieškoma: K arba algoritmo, kuris bet kokiam $C_{i+1} = e(M_{i+1}, K)$ nustatytų M_{i+1}.

Tačiau Zigmo galimybės dar neišsemtos. Vieną kartą atlikęs pasirinktų teksto-šifro porų ataką, atsižvelgdamas į kriptoanalizės rezultatus jis gali pasirinkti naujus pranešimus ir vėl gauti jų šifrus. Ši ataka vadinama

- *adaptyviąja pasirinktų teksto-šifro porų ataka* (*adaptive-chosen-plaintext attack*).

Kartais įmanoma ataka, kai kriptoanalitikas pasirenka šifrus ir gauna juos atitinkančius pranešimus. Tai

- *pasirinktų šifrų ataka* (*chosen-ciphertext attack*).

Pavyzdžiui, įvairius pranešimus jis gali dešifruoti parašo tikrinimui skirtu raktu ir bandyti gauti netiesioginės informacijos apie parašų sudarymui naudojamą raktą.

Kaip galima vertinti kriptosistemos saugumą? Yra keli požiūriai, ką laikyti saugia kriptosistema.

Kriptosistema vadinama *besąlygiškai saugia* (*unconditional security*), jei kriptoanalitikas, net ir turėdamas beribius skaičiavimo resursus, gavęs šifrą, bet nežinodamas rakto, negali nustatyti, koks pranešimas buvo siųstas. Tai griežčiausias saugios kriptosistemos apibrėžimas.

Sudėtingumo teorijos požiūriu kriptosistema vadinama *saugia* (*complexity-theoretic security*), jei jos negali įveikti Zigmas, kurio skaičiavimo resursai leidžia jam taikyti tik polinominio laiko algoritmus (naudojamas laikas ir atmintis polinomiškai priklauso nuo įvedamų duomenų apimties).

Sakoma, kad kriptosistemos *saugumas yra įrodomas* (*provable security*), jeigu galima įrodyti, kad sistemą įveikti yra tolygu išspręsti matematinę (dažniausiai skaičių teorijos) problemą, kuri laikoma sunkia.

Skaičiavimų požiūriu kriptosistema vadinama *saugia* (*computational security*), jeigu pasiektas skaičiavimo resursų lygis yra pernelyg žemas, kad naudojant geriausius algoritmus sistema būtų įveikta.

Pagaliau *ad hoc*, arba euristiškai, *saugia* kriptosistema vadinama tokia, kurios saugumą patvirtina tam tikri dažnai euristiniai argumentai. Suprantama, šis terminas tereiškia, kad specialistai atliko tam tikrą sistemos analizę, tačiau įveikti kriptosistemos nepavyko.

Modernioji kriptografija yra kartu labai jaunas ir labai senas mokslas. Viena vertus, tai naujųjų informacinių technologijų (kompiuterių ir ryšio priemonių) epochos kūdikis, kita vertus, joje taikomos matematinės žinios, įgytos labai seniai. Nuo pat P. Fermat laikų skaičių teorija buvo itin grynos matematikos teritorija, žmonės domėjosi pirminiais skaičiais nė nemanydami, kad kada nors jie vaidins itin svarbų vaidmenį kasdieniame gyvenime. Ir staiga... Ji tapo taikomosios matematikos sritimi!