Kriptoskiltis

Atviru kanalu perduodama šifruota informacija visada yra iššūkis. Bet arogancija dažnai pakenkia. Kaip gali reaguoti pašto cenzorius, išvydęs laiške nesuprantamų skaičių ir simbolių virtinę? Todėl žmonės dažnai griebiasi kito būdo – slėpimo. Tai „intelektuali veikla", kuria tenka užsiimti visiems – nuo mažų vaikų iki aukštų pareigūnų... Daugelis gyvūnų rūšių išliko todėl, kad išmoko gerai pasislėpti. Mums čia rūpi informacijos slėpimo būdai. Informacijos slėpimo teorija vadinama steganografija (gr. *steganos* – paslėptas). Trithemijaus veikalas, kurį jis pradėjo rašyti apie 1499 metus, taip ir vadinosi – „Steganographia". Informacijos slėpimas visuomet buvo daugiau praktika negu teorija. Tačiau... Beveik po 500 metų Kembridže mokslininkai susirinko į pirmąją konferenciją, skirtą steganografijai.[1]

Senos istorijos

Jeigu steganografijos istorija būtų parašyta[2] , tai būtų nepaprastai įdomus žmonių išradingumo pavyzdžių, anekdotų, komiškų ir tragiškų istorijų rinkinys. Antikos pasaulis ir šiuo požiūriu neprilygstamas šaltinis.

Pasakojama, kad Histėjus, norėdamas pranešti savo draugams, kad jau laikas sukilti prieš midiečius ir persus, nuskuto savo ištikimo vergo galvą ir ant jos užrašė pranešimą. Kai plaukai ataugo – pasiuntinys iškeliavo ir saugiai nugabeno pranešimą.

O štai kokią istoriją pasakoja Herodotas.

> Kai tik Kserksas nutarė žygiuoti į Heladą, Demaratas, būdamas Sūzuose ir sužinojęs apie tai, panoro lakedemoniečiams pranešti. Šiaip kokiu nors būdu jis negalėjo pranešti, nes buvo pavojinga – galėjo būti sučiuptas. Tai jis štai ką sugalvojo: paėmė dvilypę vašku aplietą rašomąją lentelę, nugrandė nuo jos visą vašką ir ant medžio parašė karaliaus nutarimą. Tai padaręs, prirašytą lentelę vėl apliejo vašku, kad nešama tuščia lentelė nesukeltų įtarimo ir nebūtų sulaikyta kelio sargybinių. Kai ji buvo nunešta į Lakedemoną, lakedemoniečiai niekaip nesuprato, ką tai reiškia, kol pagaliau, kaip sužinojau, Kleomeno duktė ir Leonido žmona Gorga sugalvojusi pasiūlė vašką nugrandyti, ir tada jie rasią užrašą ant lentelės medžio. Jie paklausė, rado, kas parašyta, perskaitė ir pasiuntė lentelę kitiems helėnams perskaityti. Tai taip sako buvę.

Taigi istorija išsaugojo pirmos moters kriptoanalitikės vardą!

---

[1] Konferencijos darbai išleisti atskiru leidiniu: *Information Hiding. First International Workshop, Cambridge, 1986, Proceedings (Ross Anderson, ed.) Lecture Notes in Computer Science 1174, Springer, 1986.*

[2] Ji trumpai apžvelgiama minėtos konferencijos darbų rinkinio straipsnyje: *Kahn D., The history of steganography, 1–5.*

Kitas graikas – Enėjas Taktikas sugalvojo astrogalą. Tai kaulas arba medžio gabalas su išgręžtomis skylėmis. Kiekvieną skylę atitinka abėcėlės raidė. Norėdami paslėpti žodį GRAIKAS turime verti virvutę per raidžių G, R, A, I, K, A, S skyles.

Kitokia skylučių-raidžių atitiktis naudota visai neseniai. Norėdami paslėpti svarbų pranešimą laikraščio puslapyje, imkite ploną adatą ir virš (arba po) laikraščio raidžių pradurkite skylutes taip, kad pažymėtos raidės sudarytų slaptą tekstą. Žinoma, kad net I pasaulinio karo metu vokiečiai šitaip perduodavo slaptas žinias.

Steganografija anaiptol neapsiribojo tokiais paprastais ir naivokais būdais. Chemija ir technika – štai naujų priemonių šaltiniai! Daug pastangų padėta kuriant nematomus rašalus. Patį paprasčiausią – pieną tikriausiai visi vaikystėje išbandėme. Palaikius popierių virš nekaitrios liepsnos, parudavusiame popieriuje išryškėja pienu rašytas tekstas.

Mikrofotografija atvėrė naujas galimybes. Kai prancūzų-prūsų karo metu Paryžius buvo apsiaustas, paryžiečiai darydavo laiškų kopijas maždaug $2,5\times1,5$ cm filmo juostelėse, apvyniodavo jomis pašto balandžių kojas ir korespondencija iškeliaudavo.

Tačiau, lyginant su vėlesnėmis fotografijos galimybėmis, paryžiečių mikrofotografija yra tiesiog gigantiška. Tikrąją mikrofotografiją 1920 metais išrado Emanuelis Goldbergas. Jau II pasaulinio karo metu vokiečiai naudojo tokio dydžio mikrofotografijas kaip šio teksto šrifto taškas. Slapta techninė dokumentacija keliaudavo iš Meksikos paprasčiausiuose laiškuose.

Beveik visi minėti informacijos slėpimo būdai naudoja technines priemones. Informacija paslėpta, nes paslėptas materialus informacijos nešėjas. Tai – techninė steganografija. Kitokius principus naudoja lingvistinė steganografija.

Semagramos

Semagrama (gr. *sēma* – ženklas) – tai informacija, paslėpta akivaizdžiame nešėjuje. Taigi ženklai matomi, tačiau jie turi sudaryti įspūdį, kad jokios slaptos reikšmės nėra. Norint semagrama perduoti informaciją, abi šalys turi būti susitarusios, kaip suprasti ženklus.

Vokiečių *šnipai I pasaulinio karo metu iš Anglijos siuntinėjo fiktyvius* komercinius užsakymus cigarams. Pavyzdžiui, 5000 cigarų užsakymas į Portsmouthą reiškė, kad Portsmouthe yra 5 kariniai kreiseriai. Semagramos naivumas jiems brangiai kainavo – gyvybes.

Valerie Dickinson II pasaulinio karo metu perdavinėjo japonams žinias apie amerikiečių laivyną laiškuose rašydama apie lėles. Mažos lėlės reiškė eskadrilės minininkus, didelės – lėktuvnešius. Jos veiklą slėpė ir tai, kad šnipė iš tikrųjų prekiavo lėlėmis.

Laikrodžių siunta II pasaulinio karo metų cenzoriams sukėlė įtarimą. Dėl

šventos ramybės jie pakeitė visų rodyklių padėtis, manyta, kad jos kažką reiškia.

Panašiai pasielgė I pasaulinio karo metų cenzorius[3] , įtaręs, kad laiško sakinys „Tėvas yra negyvas" (*Father is dead*) yra semagrama. Jis pakeitė sakinį, išlaikydamas prasmę: „Tėvas miręs" (*Father is deseased*). Atsakydamas adresatas labai norėjo patikslinimo: „Ar tėvas negyvas, ar miręs?" (*Is father dead or deseased?*).

Štai dar keletas istorinių pavyzdžių. Francis Baconas (1561–1626) sugalvojo, kaip informacijai paslėpti galima naudoti du skirtingus šriftus. Iliustruosime jo idėją naudodami savo priemones. Galime tarti, kad jis naudojo dvinarį kodą, t. y. keitė raides nulių ir vienetų penketais. Taikykime panašią taisyklę: lietuvių kalbos abėcėlės raidę keiskime jos numeriu, užrašytu dvejetainėje sistemoje:

$$\mathrm{A} \longrightarrow 00000, \quad \mathrm{B} \longrightarrow 00001, \quad \mathrm{C} \longrightarrow 00010 \quad \text{ir taip toliau.}$$

Dabar susitarkime, kad bet kuri štai tokio šrifto raidė reiškia vienetą, o tokio šrifto raidė – nulį (skyrybos ženklus praleidžiame). Ar nepastebėjote nieko keisto teksto, prasidedančio sakiniu „Vokiečių šnipai ...", fragmente?

Vienoje 1976 metais išleistos vokiškos kombinatorikos knygos tekste apie Karaliaučiaus tiltų uždavinį buvo paslėptas sakinys „ *nieder mit dem Sowjetimperialismus* " (šalin tarybinį imperializmą). Šis sakinys susidėjo iš raidžių, kurios buvo vos vos žemiau negu kitos. Įdėmiai įsižiūrėkite į šio teksto pastraipą, prasidedančią žodžiais „kitas graikas". Ar nieko įtartino nematyti?

Panašius pavyzdžius galima vardyti ir vardyti. Tačiau kas gi naujo mūsų informacijos amžiuje?

Informacijos amžiaus slaptavietės

Dažnai žodžiai būna lyg nesikeičiantys indai, kuriuos bėgantys amžiai pripildo savos reikšmės. Modernioji steganografija skiriasi nuo klasikinės ne tik tuo, kad atsirado naujų techninių galimybių bei gudrybių, svarbiausia – savo tikslais. Klasikinės steganografijos pagrindinę problemą galima nusakyti taip: kaip Algiui ir Birutei[4] , būnantiems atskirose kalėjimo vienutėse, susitarti dėl pabėgimo plano, jeigu palaikyti ryšį įmanoma tik per nepaperkamą prižiūrėtoją Zigmą perduodant įtarimo nekeliančius daiktus?

Taigi Zigmas neturi įtarti, kad iš pažiūros „nekaltuose" daiktuose (stegoobjektuose) slypi informacija (stegoinformacija).

Informacijos amžiaus steganografijos tikslai įvairesni. Kaip steganografija naudojasi nusikaltėliai neminėsime. Tačiau štai aktuali intelektualinės nuosavybės apsaugos problema. Birutė, parduodama Algiui muzikos kūrinio įrašą,

[3] Šis ir keletas kitų pavyzdžių atpasakoti iš knygos: *Bauer F. L., Decrypted secrets, Springer, 1997.*

[4] Angliškoje kriptologijos literatūroje priimta slaptai palaikomo ryšio partnerius vadinti Alisa ir Bobu. Trečiasis (nepageidaujamas) asmuo vadinamas įvairiai: Oskaru, Wiliu ir t. t.

nenorėtų, kad tas kūrinys būtų transliuojamas per Algio draugo Zigmo radijo stotį. Steganografinis sprendimas gali būti toks: paslėpti tame kūrinyje informaciją, kad įrašą įsigijo Algis; ši informacija turi būti nepastebima klausytojui, tačiau ją turi registruoti Birutės prietaisai. Tokiu būdu Birutė įgyja galimybę įrodyti, kad Algis su Zigmu pirataują. Taigi vietoje klasikinės priešpriešos: gudruoliai Algis ir Birutė prieš naivųjį Zigmą atsiranda priešprieša: Birutė prieš Algį ir Zigmą. Ir visi šios schemos subjektai gudrūs: juk nėra jokios paslapties, kad muzikos kūrinys yra stegoobjektas. Birutės priešininkų uždavinys ne surasti stegooinformaciją, bet pakeisti ją taip, kad Birutės prietaisai negalėtų pastebėti pažeidimo.

Štai kitas pavyzdys, kai gali prireikti steganografinio sprendimo. Jeigu medicininės apžiūros metu gauto vaizdo skaitmeninis formatas yra toks, kad tekstinė informacija turi būti saugoma atskirai, tai iškyla grėsmė, kad failai gali būti supainioti ir pacientui gali būti priskirti ne jo duomenys. Steganografinis sprendimas – paciento identifikacijos duomenis reikia įterpti į vaizdo failą neiškraipant paties vaizdo.

Šie pavyzdžiai ne tik rodo pasikeitusius steganografijos uždavinius, bet ir slaptavietes, kuriomis naudojasi išradingi mūsų amžininkai. Tai nulių ir vienetų srautai, kuriais koduojami vaizdai ir garsai. Sukurta daugybė algoritmų ir juos realizuojančių programų. Pakeliavus Interneto puslapiais galima greitai įsitikinti, kaip sparčiai plėtojama ir teorija, ir praktika. Galbūt ir todėl, kad kai kurių šalių vyriausybės kontroliuoja arba siekia kontroliuoti privačios informacijos šifravimą. Taigi kibernetinėje, bežadžių nulių-vienetų srautų sklidinoje erdvėje mokomasi žaisti slėpynių.

Vilius Stakėnas