Paskaita 13

Blokiniai šifrai

Šie algoritmai naudoja P teksto fiksuoto ilgio n blokus ir juos užšifruoja tokio pačio ilgio šifruoto teksto blokais

$$P = \sum^n \xrightarrow{E} C = \sum^n$$

Pvz. $n = 1$, tokie blokiniai šifrai vadinami pakeitimo šifrais (substitution ciphers).

1) Cezario šifras $E_k(p) = p + k \bmod m$, $m = 26$.
2) Šerloko Holmso nuotykiai, šokančių žmogiukų alfabetas (Arthur Conan Doyle)
3) The Gold Bug - Edgar Allan Poe.
4) Žangada (Jules Verne)

Turime 26! skirtingas perstatas (bendroji atvejo $|\Sigma|!$ perstatas)

Tai labai didelis skaičius, bet kriptoanalizės technikos padeda smarkiai sumažinti variantų skaičių - raidžių dažnumai yra labai charakteringi kiekvienos kalbos atveju.

Todėl sudaromi sudėtingesni šifravimo algoritmai, kurie paslepia (sumaišo) atskirų alfabeto elementų dažnumus šifruotame tekste C.

Nagrinėkime blokinį šifravimo algoritmą

$$E : \Sigma^n \to \Sigma^n$$

Kadangi egzistuoja atvirkštinis dešifravimo algoritmas

$$D : \Sigma^n \to \Sigma^n,$$

tai E yra <u>surjekcija ir injekcija</u>

$\Rightarrow$ bijekcija (abipus vienareikšmis atitikmuo)

Todėl <u>visada</u> blokinių šifravimo algoritmų E_π galima užrašyti kaip perstatą

$$E_\pi : \Sigma^n \to \Sigma^n$$

$$\vec{\nu} \in \Sigma^n \quad E_\pi : \vec{\nu} \to \pi(\vec{\nu}).$$

$$D_\pi : \Sigma^n \to \Sigma^n, \quad \vec{\nu} \to \pi^{-1}(\vec{\nu})$$

Raktų aibė labai didelė: $|\Sigma|^n$ elementų (žodžių) gali būti sudaryta iš Σ raidžių, todėl perstatų skaičius

$$(|\Sigma|^n)!$$

Todėl apsiribojama tik paprastais, kuriuos galima efektyviai atvaizduoti ir realizuoti.

Pvz. tik sukeičiame vietomis bloko raides (elementus) panaudodami raktą $\pi \in S_n$. (žr. Paskaita 12)

$$E_\pi : (v_1, \dots, v_n) \to (v_{\pi(1)}, v_{\pi(2)}, \dots, v_{\pi(n)})$$

$|S_n| = n!$ skirtingų raktų.

Šifravimo patikimumo didinimui yra naudojami keli etapų algoritmai. Vienas populiariausių yra 3 etapų atvejis: $p \in P$, $c \in C$

$$c = E_{k_3}(D_{k_2}(E_{k_1}(p))),$$

naudojami ilgo rakto (k_1, k_2, k_3). Dažnas atvejis, kai $k_1 = k_3$, tada rakto ilgis padidėja 2 kartus.

Pateiksime vieną pavyzdį šifravimo algoritmo, kurimo siekiama suvienodinti simbolių (raidžių) pasirodymo dažnius.

Plaifair šifras, sukurtas 1854.
Tai blokinis šifras, $n=2$. Jis dar vadinamas Masonic Cipher.

Raktas yra 5×5 dydžio lentelė. Kadangi galimos tik 25 raidės, tai $I=J$, J raidė nenaudojama.

Lentelės sudarymui panaudojame pasirinktą raktą k, tai ir sudaro dešifravimo uždavinio sudėtingumą.

Pvz. imkime raktą $k =$ MONARCHY

$$\begin{pmatrix} M & O & N & A & R \\ C & H & Y & B & D \\ E & F & G & I & K \\ L & P & Q & S & T \\ U & V & W & X & Z \end{pmatrix}$$

šifravimo lentelė

$P =$ instruments

Užrašome poromis

in st ru me nt sz ← fiktyvi papildoma raidė.

Algoritmas

A1. Jei abi raidės yra tame pačiame stulpelyje, tai jas pakeičiame raidėmis, stovinčiomis po dešiniąja raide (paskutinei eilutei pratęsiame lentelę ciklinio būdu).

m e → C L

c u → E M

me → cl

cu → em

me → CL

cu → EM

A2. Jei abi raidės yra šalia pačioje eilutėje, tai pakeičiame kairiąją dešiniąja pusėje.

pq → qs

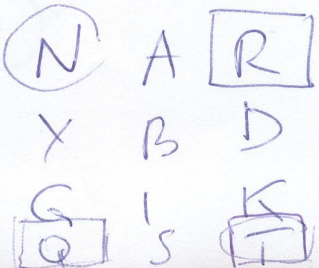
qt → sl

pq → QS

qt → SL

T3. Jeigu nei viena iš taisyklių A1, A2 negalioja, tai sudarome sudarome kvadratą, kuriam priklauso šios dvi raidės. ir pasirenkame kairiąsias horizontaliosios kampuose

nt → RQ



instruments → GATLMZCLRQTX

Klausimai (papildoma medžiaga).

1. Kaip dešifruoti tekstą nežinant rakto?
(~~raktų~~ digramų yra 625, o ne 25 raidės kaip buvo m=1 atveju).

Statistinė analizė jau daug sudėtinga.

2. moon → dvi o o nėra problem
mo + on.

spoon sp + oo + nz

Bet dažniausiai jas atskiriame x-raide

spoxon

sp + ox + on.