Paskaita 16

Trumpai apžvelgsime kaip blokiniai šifrai naudojami ~~pero~~ šifruojant bet kokio ilgio dokumentus

1. ECB algoritmas (electronic code book)

Alfabetas Σ, bloko ilgis n, K - raktų aibė, E_k - šifravimo f-ja $k \in K$, D_k - dešifravimo f-ja

Pranešimo ilgis N. Tada jį dalijame į atskirus n-ilgio blokus. Paskutinio pranešimo papildome atsitiktiniais ~~skaičiais~~ simboliais iki n-ilgio bloko

blokai iš n raidžių

6. P_j, $j = 1, \dots, J$. $|P_j| = n$.

$C_j = E_e(P_j)$, $\Rightarrow$ $P_j = D_d(C_j)$

Pav: $\Sigma = \{0, 1\}$, $n = 4$, $K = S_4$

(bitų ketvertų perstatų šifravimas) $\pi \in S_4$.

$$E_\pi : \{0,1\}^4 \to \{0,1\}^4$$

$$b_1\, b_2\, b_3\, b_4 \to b_{\pi(1)}\, b_{\pi(2)}\, b_{\pi(3)}\, b_{\pi(4)}$$

$$\pi = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 4 & 1 \end{pmatrix}$$ ciklinis postūmis į kairę per 1 poziciją

$m = \underbrace{1011}\,\underbrace{0001}\,\underbrace{0100}\,\underbrace{101}_{3.}$

$m_1 = 1011$, $m_2 = 0001$, $m_3 = 0100$, $m_4 = 1010$

$c_1 = 0111$, $c_2 = 0010$, $c_3 = 1000$, $c_4 = 0101$

$$\boxed{C = 0111001010000101}$$

Vienodi blokai yra šifruojami vienodai, todėl padidėja statistinės kriptoanalizės (atakos) pavojus. Taip pat priešininkas gali pakeisti pranešimo blokus / tvarką, net nežinodamas plaintext

2. CBC algoritmas (šifruojamo bloko grandinės cipher block chaining mode)

Šiame protokole šifravimo rezultatas priklauso ne tik nuo vieno, bet ir nuo ankstesnio bloko teksto. Todėl vienodo teksto blokai nebus užšifruojami vienodai.

Pasinaudojame XOR logine operacija (exclusive or)

$0 \oplus 0 = 0$

$1 \oplus 0 = 1$

$0 \oplus 1 = 1$

$1 \oplus 1 = 0$

$(a \oplus b = (a+b) \bmod 2)$

$\mathbb{Z}/2\mathbb{Z}$ grupė.

operacija +.

$a = 0100$, $b = 1101$,

$a \oplus b = 1001$

0100
1101
1001

Pasirenkame pradinį vektorių c_0.
(jis irgi rišas, galime paskelbti internete). $m = m_1 m_2 \dots m_J$

$$c_j = E_e(c_{j-1} \oplus m_j) \quad 1 \le j \le J.$$

$\Rightarrow$

$$c = c_1 \dots c_J. \quad \text{(šifruotas pranešimas)}$$

Kaip dešifruoti ~~pranešimą~~ šifruotą pranešimą c?

$$m_j = c_{j-1} \oplus D_d(c_j).$$

Patikrinkime:

$$c_{j-1} \oplus D_d\left(E_e(c_{j-1} \oplus m_j)\right)$$

$$= \underbrace{c_{j-1} \oplus c_{j-1}} \oplus m_j = m_j$$

e - neutralus elementas

Pav.

$m_1 = 1011$, $m_2 = 0001$, $m_3 = 0100$, $m_4 = 1010$.

$$C_0 = 1010, \quad \pi = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 4 & 1 \end{pmatrix}$$

$$C_1 = E_\pi(C_0 \oplus 1011) = E_\pi(0001) = 0010$$

$$C_2 = E_\pi(C_1 \oplus 0001) = E_\pi(0011) = 0110$$

$$C_3 = 0100, \quad C_4 = 1101$$

$$C = 0010011001001101$$

Pratybos: Atlikti dešifravimo žingsnį.

Klaidos paieškos analizė

~~Tačiau~~, jeigu c_j perduotas su klaida, tai galės pasireikšti tik m_j ir m_{j+1} dešifravimo, tolimesnieji blokai yra ~~generuoti~~ dešifruojami teisingai.

Taigi klaida veikia rezultatus (dešifruojant) tik lokaliai.

Yra ir daugiau protokolų (pvz. orientuotas į pokalbius telefonu) informacijos šifravimui ir dešifravimui.

Afininiai šifravimo algoritmai

m yra teigiamas sveikas skaičius.
Alfabetas sudarytas iš m raidžių
$\Sigma = \mathbb{Z}_m = \{0, 1, \dots, m-1\}$.

Tai blokinis šifravimo algoritmas, $n=1$
(bloko ilgis vienas elementas)

Raktų aibė K yra sudaryta iš porų $k=(a, b) \in \mathbb{Z}_m^2$, $\gcd(a, m)=1$.

$$E_k : \Sigma \to \Sigma, \quad x \to ax+b \bmod m.$$

Dešifravimo funkcija

$$D_k : \Sigma \to \Sigma, \quad x \to a'(x-b) \bmod m.$$

$$aa' \equiv 1 \bmod m.$$

(čia a' yra atvirkštinis elementas)

Naudojame Euklido modif. algoritmą

Pav. $m = 26$, $(a, b) = (7, 3)$

↑ abecelės raidžių skaičius

$x \to 7x + 3$

KAUNAS

10 0 20 13 0 18

21 3 13 16 3 25

V D N Q D Z

$73 = 52 + 21$
$143 = 130 + 13$
$94 = 78 + 16$
$129 = 130 - 1$

A B C D E F ...
0 1 2 3 4 5 ...

Bob surenda $a' = 15$ (patikrinkite)

$x \to 15(x - 3)$

V D N Q D Z

21 3 13 16 3 25

10 0 20 13 0 18

K A U N A S

$15 \cdot 18 = 270$
$15 \cdot 10 = 150$

šifro sudėtingumas

$|K| = \varphi(m)\, m = 12 \cdot 26 = 312$

$\gcd(a, m) = 1$! Patikriname visus variantus ir randame raktą (kai žinome tik šifruotą tekstą)!

Jeigu turime dviejų elementų (plain text) variantus → tai išsprendžiame ~~išspręsti~~ 2x2 sistemą? (plain text attack)

(a, b) ↓ nieznane

$E \to R$
$S \to H.$

} Plain-text attack

$e = 4$
$s = 18$

$R = 17$
$H = 7.$

$$\begin{cases} 4a + b \equiv 17 \mod 26 \\ 18a + b \equiv 7 \mod 26. \end{cases}$$

Is pirmoji lygtis išreiškiame b:

$$b \equiv 17 - 4a \mod 26$$

{statome į antrąją lygtį:

$$18a + 17 - 4a \equiv 7 \mod 26$$

$$14a \equiv -10 \mod 26$$

$$\| \quad 16 \qquad /:2$$

$$\Rightarrow \quad 7a \equiv 8 \mod 13$$

$7' = 2 \mod 13$

$2 \cdot 7 \equiv 1 \mod 13$

$a \equiv 16 \mod 13$

$\boxed{a = 3}$

$b \equiv 17 - 4 \cdot 3 \equiv 5 \mod 13$

Radome raktą $k = (3, 5)$.