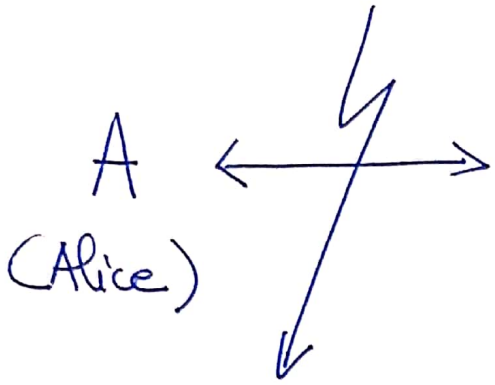
Cifruri simetrice

O (Oscar) sau E (eavesdropper)



- A și B cunosc o cheie comună secretă k
- folosind această cheie ei pot (cripta) sau (decripta) mesaje

(cripta = modifică textul simplu)

(decripta = reconstituie textul simplu inițial)

⇓

A și B au informații și puteri egale în cadrul acestui sistem (criptosistem)

Deaceea aceste criptosisteme se numesc simetrice (mai târziu vom vorbi și despre cele "asimetrice" sau cu cheie publică.

? = Criptografia (etimologie)

kryptos = secret

graphos = scriere

Steganografia

ascuns.

Definiție Criptosistem (simetric) $(\mathcal{A}, \mathcal{C}, \mathcal{K}, \mathcal{E}, \mathcal{D})$

$\mathcal{A}$ = mulțimea (finită) a mesajelor (texte simple – plaintext) posibile $m \in \mathcal{A}$.

$\mathcal{K}$ = mulțimea (spațiul) cheilor $k \in \mathcal{K}$

$\mathcal{C}$ = mulțimea textelor (mesajelor) criptate (ciphertext) $c \in \mathcal{C}$

- <u>Criptarea</u> e o funcție $e : \mathcal{K} \times \mathcal{A} \to \mathcal{C}$ sau (punând în evidență dependența de k): $e_k : \mathcal{A} \to \mathcal{C}$
$m \mapsto e_k(m) = c$.

$$\mathcal{E} = \{ e_k \mid k \in \mathcal{K} \}$$

- <u>Decriptarea</u> este (tot) o funcție $d : \mathcal{K} \times \mathcal{C} \to \mathcal{A}$ sau
$d_k : \mathcal{C} \to \mathcal{A}$
$c \mapsto d_k(c) = m$.

Cu proprietatea $\forall k_1 \in \mathcal{K}$, $\exists k_2 \in \mathcal{K}$ (poate fi $k_1 = k_2$) a.î.
$d_{k_2}(e_{k_1}(m)) = m \quad \forall m \in \mathcal{A}$.

<u>Obs</u> funcțiile e_k sunt <u>injective</u> (cum este și normal)

$$e_{k_1}(m) = e_{k_1}(\bar{m}) \Rightarrow d_2(e_{k_1}(m)) = d_2(e_{k_1}(\bar{m})) \Rightarrow m = \bar{m}$$

Exemplu Substituția monoalfabetică

$\mathcal{A} = \{A, B, C, \ldots Z\} = \{0, 1, 2, \ldots, 25\}$ (cu corespondența $A \to 0, B \to 1, \ldots, Z \to 25$) (alfabet)

$\mathcal{M} = \{$ cuvintele unei limbi $\}$ (Ele vor fi limba engleză)

$\mathcal{C} = \mathcal{A}^* = \{$ cuvinte (-degeaba) fără înțeles $\}$

$\mathcal{K} = S(\mathcal{A})$ grupul permutărilor lui $\mathcal{A}$.

Observație Sunt multe chei? Când $|\mathcal{K}| = 26! \simeq 4 \cdot 10^{26}$.

Dacă vrem să spargem sistemul prin forță brută (-încercând toate cheile) cam de cât timp o putem face?

Pp că încercăm 1 milion chei/secundă. Decât timp avem nevoie?

Problema Fermi!

$60 \times 60 \times 24 \times 365$ secunde/an $\simeq 10^2 \cdot 12 \cdot 2 \cdot 12 \times 36 \cdot 10 \simeq$

$\simeq 10^5 \cdot 72 \simeq 10^7$.

avem nevoie de $10^{26}/10^6 = 10^{20}$ secunde $\Rightarrow \frac{10^{20}}{10^7} \simeq 10^{13}$ ani.

Vârsta Universului este estimată la 10^{10} ani! $\Rightarrow$ Oscar nu are șanse să spargă sistemul prin forță brută.

Observație Deși avem atâtea multe chei, acest sistem nu este de spart. Cum?

Analiza frecvenței apariției literelor (cuvintelor).