05.10.2020

Curs I

Criptografie și teoria codurilor

Planul cursului

1. Cifruri "istorice" simetrice. Substituții monoalfabetice. Substituții polialfabetice (Vigenère, Hill). Criptanaliza
2. Criptosisteme "perfect sigure". Cifrul Vernam (one-time-pad) Teorema lui Shannon
3. Criptosisteme simetrice moderne. (baby) DES, (baby) AES
4. Criptografia cu cheie publică
   a) logaritmul discret, atacuri (Shanks (coliziuni), Pollig-Hellman. Polland ρ)
   b) protocolul Diffie-Hellman, criptosistemul ElGamal, signatura digitală ElGamal
   c) criptosistemul RSA, signatura digitală RSA, atacuri (asupra modulului comun, Hastad (asupra exponentului de criptare mic), Wiener, atacul ciclic

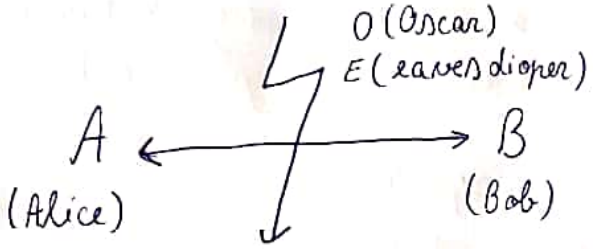
d) criptosistemul knapsack, criptanaliza; aplicații ale teoriei laticelor în criptografie

5. Criptografie pe curbe eliptice
6. Criptografia cuantică (doar o poveste fantastică ?)

Bibiografie

1. J. Hoffstein, J. Pipher, J. Silverman, An Introduction to Mathematical Cryptography, Springer, 2008
2. S. Singh, Cartea Codurilor, Humanitas, 2005
3. C. Gheorghe, D. Popescu, Criptografie, Coduri, Algoritmi, Ed. Univ. 2005

1. Cifruri simetrice : avem 3 personaje
A, B comunică și O vrea să intercepteze



- A și B cunosc o cheie comună secretă k
- folosind cheia k ei pot cripta și decripta

cripta → modificarea mesajului inițial (transformarea)

decripta → constituie mesajul inițial

A și B au informații și puteri egale în cadrul sistemului → de aceea cifru simetric

există și sisteme asimetrice (cu cheie publică)

Criptografie → graphos (= scriere)

kriptos (secret)

Steganografic

ascuns

Definiție Criptosisteme (simetric)

E format dintr-un 5-tuplu (M, C, K, E, D)

- M = mulțimea finită a mesajelor necifrate (necriptate) (texte simple - plaintext)
- C = mulțimea mesajelor criptate
- K = mulțimea (spațiul) cheilor

- Criptarea e o funcție, $e: M \times K \to C$
  $K \times M$
  $(k, m) \to e(k, m)$

  Dacă fixez k, $e_k: M \to C$
  $m \to e_k(m)$

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

- Decriptarea e tot o funcție, $d: K \times C \to M$
  $(k, c) \to d(k, c)$

- $D = \{ d_k \mid k \in K \}$ $\quad d_k: C \to M$, $d_k(c) = m$

cu proprietatea că

$\forall k_1 \in K, \exists k_2 \in K$ a.î. $d_{k_2}(e_{k_1}(m)) = m, \forall m$

OBS $\Rightarrow$ e_k sunt injective

Exemplu: Substituția monoalfabetică

Avem un alfabet $\mathcal{A} = \{A, B, C, \dots, Z\} \simeq \{0, 1, 2, \dots, 25\}$

$M = \{$cuvintele unei limbi$\}$ (limba engleză)

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

$K = S(A)$ grupul permutărilor lui A

$\Gamma \in S(A)$ măr $\longmapsto \Gamma(m)\Gamma(a)\Gamma(r)$

M

"șiftare" $\Gamma: \mathbb{Z}_{26} \to \mathbb{Z}_{26}$ $\Gamma(x) = x + k \pmod{26}$ (cheia)

Cifrul Caesar este de acest tip

Câte chei avem? $26! \in$ nr de permutări

$\simeq 4 \cdot 10^{26}$

Putem sparge sistemul prin forță brută? (încerc toate cheile)

Pp. că putem încerca 1 milion (10^6) chei pe secundă

Avem nevoie de 10^{20} secunde $\simeq 10^{13}$ ani (Fermi)

Pare că sunt foarte sigure!? R: NU

Metoda analizei frecvenței apariției literelor / cuvintelor

Criptanaliză → spargerea mesajelor