

# Criptografie și Securitate (ROL) - Seminar 1

## Introducere

### 1. Sisteme de criptare.



[Adaptare după Computer Security: Principles and Practice, W.Stallings și L.Brown]

- (a) Plasați pe figură următoarele concepte / noțiuni: *text clar (plaintext)*, *text criptat (ciphertext)*, *cheie de criptare (encryption key)*, *cheie de decriptare (decryption key)*, *algoritm de criptare (encryption algorithm)*, *algoritm de decriptare (decryption algorithm)*, *Alice*, *Bob*.
  - (b) Cine este *Eve / Oscar*? Ce încearcă să facă?
  - (c) Adevărat sau Fals? Algoritm de criptare ar trebui să fie ascuns lui *Eve / Oscar*.
  - (d) Adevărat sau Fals? Scopul principal al lui *Eve / Oscar* este să determine cheia secretă.
2. CIA (Confidentiality, Integrity, Availability). Pentru fiecare dintre afirmațiile de mai jos, indicați proprietatea CIA.
- (a) Dosarul medical al unui pacient nu trebuie făcut public.
  - (b) Un client nu poate modifica suma pe care o deține în contul de economii fără să facă o tranzacție autorizată (plată, încasare, transfer, etc.)
  - (c) Un student nu își poate modifica nota de la examen în catalog.
  - (d) Medicul de gardă trebuie să aibă acces la dosarul pacientului.
  - (e) În unele state, notele studenților trebuie să fie accesibile doar acestora, părinților / tutorilor și personalului administrativ.
  - (f) Sistemul bancar trebuie să permită plata cu cardul.
  - (g) Doctorul trebuie să fie sigur că informația din dosarul electronic al pacientului este corectă.
3. Se consideră o cheie de criptare pe 80 biți / 128 biți.
- (a) Câte chei posibile distincte există?
  - (b) Cât timp necesită determinarea cheii printr-un atac de forță brută (căutare exhaustivă) dacă se pot efectua  $2^{10}$  /  $2^{20}$  criptări pe secundă?

- (c) Este atacul fezabil?

### Sisteme de criptare clasice

4. Sistemul cavalerilor de Malta.

$A :$	$B :$	$C :$	$J .$	$K .$	$L .$	$S$	$T$	$U$
$D :$	$E :$	$F :$	$M .$	$N .$	$O .$	$V$	$W$	$X$
$G :$	$H :$	$I :$	$P .$	$Q .$	$R .$	$Y$	$Z$	

- (a) Criptați mesajul TEXT CLAR / SUBSTITUTIE SIMPLA / CRIPTARE.  
Ce este un "text clar" în criptografie? / De ce "substituție simplă"? / Ce este un sistem de criptare?

- (b) Decriptați mesajul 

--

:
---

--

:
---

.
---

- (c) Este acesta un sistem de criptare sigur? De ce / de ce nu?

5. Sistemul Polybius cu cheie (I=J).

- (a) Criptați mesajul SUBSTITUTIE / MESAJ CRIPTAT / SECRET folosind cheia de criptare POL / KEY / RON.  
(b) Decriptați mesajul 21 32 24 42 45, criptat folosind cheia POL.  
Decriptați mesajul 21 25 12 31 12, criptat folosind cheia KEY.  
Decriptați mesajul 43 23 21 11 23 44, criptat folosind cheia RON.  
(c) Câte chei posibile există ?

6. Sistemul Cezar cu cheie (se consideră cheia  $k = 0$  cheia care criptează o literă în ea însăși).

- (a) Criptați mesajul CRIPTOGRAFIE / SECURITATE / IMPERIUL ROMAN folosind cheia de criptare  $k = 3$  /  $k = 5$  /  $k = 7$ .  
(b) Decriptați mesajul ECFDEPO ALCEJ, criptat folosind cheia  $k = 11$ .  
Decriptați mesajul HADPH QFULS WRJUD ILH, criptat folosind cheia  $k = 3$ .  
Decriptați mesajul OERWE WGMXC, criptat folosind cheia  $k = 4$ .  
(c) Câte chei posibile există ?

7. Sistemul afin ( $k = (k_1, k_2)$ ;  $Enk_k(m) = k_1m + k_2 \pmod{26}$ ;  $A = 0, B = 1, \dots$ ).

- (a) Criptați mesajul TEXT / MESAJ / AFIN folosind cheia de criptare  $k = (5, 9)$  /  $k = (7, 2)$  /  $k = (17, 5)$ .
- (b) Decriptați mesajul TSDX, criptat folosind cheia  $k = (5, 9)$ .  
Decriptați mesajul XWG, criptat folosind cheia  $k = (7, 2)$ .  
Decriptați mesajul QJA, criptat folosind cheia  $k = (17, 5)$ .  
(*Să ne aducem aminte: Algoritmul lui Euclid pentru calculul unui invers (mod  $n$ )*)
- (c) Ce proprietate trebuie să satisfacă cheia  $k$  pentru ca sistemul să fie bine definit?
- (d) Câte chei posibile există?

#### 8. Sisteme de substituție simplă.

- (a) Criptați mesajul WEB DESIGN folosind cuvântul cheie BROWSER.  
Criptați mesajul CRIPTOGRAFIE folosind cuvântul cheie CHEIE.
- (b) Decriptați mesajul KQSFC YDEX folosind cuvântul cheie ASYMMETRIC.  
Decriptați mesajul LNAV B PEF EY folosind cuvântul cheie BUCURESTI.
- (c) Câte chei posibile există ?

#### 9. Sisteme de transpoziție.

- (a) Criptați mesajul STANDARDUL DE CRIPTARE cu ajutorul permutării  $\sigma = (2, 3, 1)$ .  
Criptați mesajul CERCETARI OPERATIONALE cu ajutorul permutării  $\sigma = (2, 1, 3)$ .
- (b) Decriptați mesajul SFCME TAEAE NLR, cifrat cu ajutorul permutării  $\sigma = (1, 2, 3)$ .  
Decriptați mesajul PTASC OANER RORAE ILEH, cifrat cu ajutorul permutării  $\sigma = (2, 1, 4, 3)$ .

#### 10. Sisteme mixte.

- (a) Criptați mesajul SISTEM MIXT cu ajutorul sistemului Cezar și al permutării  $\sigma = (2, 3, 1)$ .
- (b) Decriptați mesajul CPKQCG ZGTVTK GOERIH, cifrat cu ajutorul sistemului Cezar  $k = 2$  și al permutării  $\sigma = (3, 2, 1)$ .

#### 11. Sistemul Playfair (I=J).

- (a) Criptați mesajul THE CIRCLE cu ajutorul parolei *ALBUM*.  
Criptați mesajul MESAJ CLAR cu ajutorul parolei *CHEIE*.
- (b) Decriptați mesajul PIGOY CLETY AEYLQ VSFWN, parola utilizată fiind CRYPT-TOOL.  
Decriptați mesajul TAAK SUCP, parola utilizată fiind ATAC.
- (c) Câte chei posibile există?