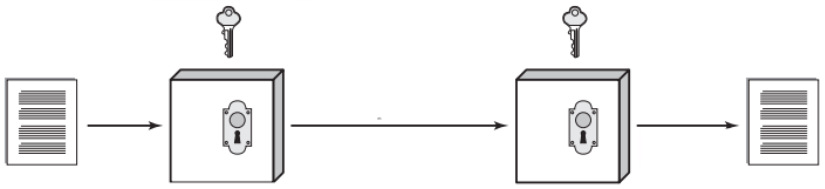
Criptografie şi Securitate (ROL) - Seminar 1

Introducere

1. Sisteme de criptare.



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

   (a) Plasaţi pe figură următoarele concepte / noţiuni: *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? Algoritmul de criptare ar trebui sa 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 afirmaţiile de mai jos, indicaţi proprietatea CIA.

   (a) Dosarul medical al unui pacient nu trebuie făcut public.

   (b) Un client nu poate modifica suma pe care o deţine în contul de economii fără să facă o tranzacţie autorizată (plată, încasare, transfer, etc.)

   (c) Un student nu îşi poate modifica nota de la examen în catalog.

   (d) Medicul de gardă trebuie să aibă acces la dosarul pacientului.

   (e) În unele state, notele studenţilor trebuie să fie accesibile doar acestora, părinţilor / tutorilor şi personalului administrativ.

   (f) Sistemul bancar trebuie să permită plata cu cardul.

   (g) Doctorul trebuie să fie sigur că informaţia din dosarul electronic al pacientului este corectă.

3. Se consideră o cheie de criptare pe 128 biţi / 256 biţi.

   (a) Câte chei posibile distincte există?

   (b) Cât timp necesită determinarea cheii printr-un atac de forţă brută (căutare exhaustivă) dacă se pot efectua 2^{10} / 2^{20} decriptări pe secundă?

(c) Este atacul fezabil?

Sisteme de criptare clasice

4. Sistemul cavalerilor de Malta.

$A:$	$B:$	$C:$
$D:$	$E:$	$F:$
$G:$	$H:$	$I:$

$J.$	$K.$	$L.$
$M.$	$N.$	$O.$
$P.$	$Q.$	$R.$

S	T	U
V	W	X
Y	Z	

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

(b) Decriptaţi mesajul 

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

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

(a) Criptaţi mesajul SUBSTITUTIE / MESAJ CRIPTAT / SECRET folosind cheia de criptare POLO / KEY / RON.

(b) Decriptaţi mesajul 21 32 24 42 45, criptat folosind cheia POLO.
Decriptaţi mesajul 21 25 12 31 12, criptat folosind cheia KEY.
Decriptaţi 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 însăşi).

(a) Criptaţi mesajul CRIPTOGRAFIE / SECURITATE / IMPERIUL ROMAN folosind cheia de criptare $k = 3$ / $k = 5$ / $k = 7$.

(b) Decriptaţi mesajul ECFDEPO ALCEJ, criptat folosind cheia $k = 11$.
Decriptaţi mesajul HADPH QFULS WRJUD ILH, criptat folosind cheia $k = 3$.
Decriptaţi mesajul OERWE WGMXC, criptat folosind cheia $k = 4$.

(c) Câte chei posibile există ?

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

(a) Criptaţi mesajul TEXT / MESAJ / AFIN folosind cheia de criptare $k = (5, 9)$ / $k = (7, 2)$ / $k = (17, 5)$.

(b) Decriptaţi mesajul TSDX, criptat folosind cheia $k = (5, 9)$.
Decriptaţi mesajul XWG, criptat folosind cheia $k = (7, 2)$.
Decriptaţi mesajul QJA, criptat folosind cheia $k = (17, 5)$.
(*Să ne aducem aminte:* Algoritmul lui Euclid pentru calculul unui invers $\pmod n$)

(c) Ce proprietate trebuie să satisfacă cheia k pentru ca sistemul să fie bine definit?

(d) Câte chei posibile există?

8. Sisteme de substituţie simplă.

(a) Criptaţi mesajul WEB DESIGN folosind cuvântul cheie BROWSER.
Criptaţi mesajul CRIPTOGRAFIE folosind cuvântul cheie CHEIE.

(b) Decriptaţi mesajul KQSFC YDEX folosind cuvântul cheie ASYMMETRIC.
Decriptaţi mesajul LNAVB PEFEY folosind cuvântul cheie BUCURESTI.

(c) Câte chei posibile există ?

9. Sisteme de transpoziţie.

(a) Criptaţi mesajul STANDARDUL DE CRIPTARE cu ajutorul permutării $\sigma = (2, 3, 1)$.
Criptaţi mesajul CERCETARI OPERATIONALE cu ajutorul permutării $\sigma = (2, 1, 3)$.

(b) Decriptaţi mesajul SFCME TAEAE NLR, cifrat cu ajutorul permutării $\sigma = (1, 2, 3)$.
Decriptaţi mesajul PTASC OANER RORAE ILEH, cifrat cu ajutorul permutării $\sigma = (2, 1, 4, 3)$.

10. Sisteme mixte.

(a) Criptaţi mesajul SISTEM MIXT cu ajutorul sistemului Cezar şi al permutării $\sigma = (2, 3, 1)$.

(b) Decriptaţi mesajul CPKQCG ZGTVTK GOERIH, cifrat cu ajutorul sistemului Cezar $k = 2$ şi al permutării $\sigma = (3, 2, 1)$.

11. Sistemul Playfair (I=J).

(a) Criptaţi mesajul THE CIRCLE cu ajutorul parolei $ALBUM$.
Criptaţi mesajul MESAJ CLAR cu ajutorul parolei $CHEIE$.

(b) Decriptaţi mesajul PIGOY CLETY AEYLQ VSFWN, parola utilizată fiind CRYPTOOL.
Decriptaţi mesajul TAAK SUCP, parola utilizată fiind ATAC.

(c) Câte chei posibile există?