SECURITY IN NETWORKED COMPUTING SYSTEMS

Master in Computer Engineering

14 September 2015

❖: all
◆: all but DSS

EXERCISE NO. 1 (❖) #MARKS: 10

With reference to the CBC encryption mode,

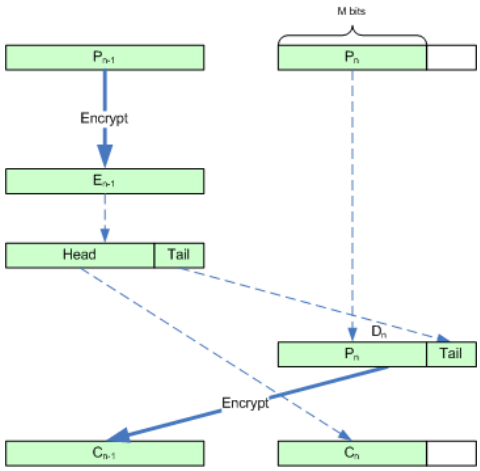
1. Illustrate the scheme and present the related equations;
2. Discuss the advantages and disadvantages w.r.t. ECB;
3. Argue whether it can be used with an asymmetric cipher.

EXERCISE NO. 2 (◆) #MARKS: 10

Alice and Bob wish to establish a session key K_{AB}. To this purpose they run a key establishment protocol that exploits the presence of Trent, a trusted third party that plays the key server role. Alice and Bob share a long-term secret key with Trent. Let K_A and K_B these keys, respectively. Design the key establishment protocol that has to fulfil the following requirements:

A. Clocks are not synchronized;
B. The protocol is not subject to replay;
C. At the end of the protocol, each principal has the proof that the peer holds the key;
D. Alice cannot talk to Trent directly but indirectly through Bob

EXERCISE NO. 3 (❖) #marks: 10



The picture shows the encryption steps of the ECB ciphertext stealing (ECB-CTS) encryption mode. This mode allows for processing of messages that are not evenly divisible into blocks without resulting in any expansion of the ciphertext (no padding is required).

In the picture, broken arrows denote bit copy whereas solid arrows labeled "Encryption" denote encryption by means of key *K*.

1. Determine the decryption steps.
2. Argue about bit-error propagation

In answering the questions assume: i) blocks are numbered from 1 to *n*; ii) *B*-bit block; iii) function *Head*(*blk*, n) that returns the *n* most-significant bits of block *blk*; iv) function *Tail*(*blk*, *n*) that returns the *n* least-significant bits of block *blk*.

SECURITY IN NETWORKED COMPUTING SYSTEMS

Master in Computer Engineering

14 September 2015

SOLUTION

EXERCISE N.1

See theory.

EXERCISE N.2

$M1 \quad A \rightarrow B: \quad A, B, n_A$

$M2 \quad B \rightarrow T: \quad A, B, n_A, n_B$

$M3 \quad T \rightarrow B: \quad \{A, B, n_A, K_{AB}\}_{K_A}, \{A, B, n_A, n_B, K_{AB}\}_{K_B}$

$M4 \quad B \rightarrow A: \quad \{A, B, n_A, K_{AB}\}_{K_A}, \{A, B, n_A, n_B\}_{K_{AB}}$

$M5 \quad B \rightarrow A: \quad \{A, B, n_B, n_A\}_{K_{AB}}$

EXERCISE N. 3

Question #1.

$$P_i = \mathcal{D}\left(K, C_i\right), 1 \le i < n-1$$

$$D_n = \mathcal{D}\left(K, C_{n-1}\right)$$

$$P_n = Head(D_n, M)$$

$$E_{n-1} = C_n \| Tail(D_n, B - M)$$

$$P_{n-i} = \mathcal{D}(K, E_{n-1})$$

Question #2.

A bit-error in any block C_i, $i < n - 1$, affects P_i only.
A bit-error in C_{n-1} causes the block-wide loss of P_n and P_{n-1}.
A bit-error in C_n causes the block-wide loss of P_{n-1}.

14 September 2015

martedì 23 maggio 2017 15:17

sncs-150914

Exercise 1

1. .
2. .
3. In linea teorica, un cifrario asimmmetrico può essere utilizzato anche per grosse quantità. in cui ogni blocco può avere una rappresentazione minore di n.

? Si può fare (non conviene dal punto di vista delle prestazioni),

Exercise 2

- My unfinished attempting

1	A → B	A, n_a, {A, B}_Ka
2	B → T	{A, B}_Ka
3	T → B	{Kab}_Kb, {Kab}_Ka
4	B → A	{Kab}_Ka

  - I basically have to copy Kerberos
  - Especially for tickets and authenticators that will confirm keys

Exercise 3 (molto molto facile)

CTS is an encrypting mode that avoids expanding the ciphertext by adding padding.

1. O in forma algoritmica, o come disegno.
   - Algoritmica (mia)
     - ☑ È giusta, ma più in generale, avrei dovuto scrivere come si decriptano **tutti** i blocchi, e non solo gli ultimi due (mostrati in figura, di incide n-1 ed n)

```
Pn = Head(D(C_n-1), M)
P_n-1 = D(Tail(D(C_n-1), B-M) || Cn)
```

   - Algoritica (prof)

```
P_i = D(K, C_i), i = 1, n-2
D = D(K, C_n-1)
P_n = Head(D, M)
E = Cn || Tail(D, B-M)
P_n-1 = D(K, E)
```

2. P'_i = D(K, C'_i), i = 1, n-2
   P'_i viene cambiato in maniera random, quindi se C_i viene alterato, viene perso tutto il suo corrispondente blocco.

   D' = D(K, C'_n-1)
   anche questo è random
   P'_n = Head(D', M)
   E' = Cn || Tail(D', B-M)
   P'_n-1 = D(K, E')
   Un errore su C_n-1 si riflette sia su P_n-1 che su P_n (situazione peggiore)

   Sempre da sopra, si vede che un errore su C_n si propaga solo su P_n-1 (anche dalla figura si vede molto bene).