Université Libanaise
Faculté d'Information
Br I

الجامعة اللبنانية
كلية الاعلام
الفرع الاول

الدورة الاولى للعام الجامعي
2024/2023

المادة: Data Security	المرحلة: اجازة
المدة:ساعتان	السنة المنهجية: الثالثة
الاستاذ: د. نادين زبيب	الدورة الأولى ١

Exercise I: Multiple choice: (10 points)

1- The physical layer is concerned with _____
   a) bit-by-bit delivery
   b) process to process delivery
   c) application to application delivery
   d) port to port delivery

2- TCP/IP model does not have _____ layer but OSI model have this layer.
   a) session layer
   b) transport layer
   c) application layer
   d) network layer

3- Which layer is used to link the network support layers and user support layers?
   a) session layer
   b) data link layer
   c) transport layer
   d) network layer

4- Which layer provides the services to user?
   a) application layer
   b) session layer
   c) presentation layer
   d) physical layer

5- Transmission data rate is decided by _____
   a) network layer
   b) physical layer
   c) data link layer
   d) transport layer

6- The data link layer takes the packets from _____ and encapsulates them into frames for transmission.
   a) network layer
   b) physical layer

c) transport layer
d) application layer

7- The network layer is concerned with _____ of data.
a) bits
b) frames
c) packets
d) bytes

8- Which one of the following is not a function of network layer?
a) routing
b) inter-networking
c) congestion control
d) error control

9- Which of the following statements about a network's infrastructure is true?
a. A network infrastructure includes hardware products only
b. A network infrastructure includes software products only
c. A network infrastructure includes both hardware and software products
d. A network infrastructure is a design that does not include specific hardware or software products

10- Which is not a application layer protocol?
a) HTTP
b) SMTP
c) FTP
d) TCP

Exercise II: Short answers (10 pts)

1) What is the difference between passive and active security attacks? (10 pts)
2) List and briefly define categories of security services. (10 pts)

Exercise III. Asymmetric Encryption 'RSA' (30 pts)

Asymmetric key encryption uses different keys for encryption and decryption. These two keys are mathematically related and they form a key pair. One of these two keys should be kept private, called private-key, and the other can be made, called public-key. Popular private-key algorithm is RSA (invented by Rivest, Shamir and Adlemen). The public key is (n, e) and the private key is (n,d).

Part A

Explain how these keys can be used for: 1) Confidentiality 2) authentication

Part B

Suppose you want to exchange data by using the RSA algorithm. By choosing p = 11, q = 23:

1. Compute n and z.
2. Which of the following values: e=2, e=3 and e=4 is the best suitable for encrypting? Justify.
3. User B want to send you the message m=165. Determine the cipher text C resulting from encryption of the message m.
4. In order to decrypt the cipher text C and obtain the same initial message m sent by the user B, e and d must verify the relation: $ed=1 \bmod(z)$.
5. Which of the following values, d=145, d=146 and d=147, is the best suitable for d? Justify.

6. Decrypt the cipher text C.

Exercise IV. CFB: Cipher Block Chaining (30 pts)

1. Describe and give the functions for the CFB encryption and decryption algorithms.

Let VI = 110000010000 the initialization vector, M = 10011 00111 00100 00001 10100 00010 01010 the plaintext and K the permutation encryption key which allows in our case to complement the block (example: for a block B of size 4, B= 1011 → K(B) = 0100). Notice if that there isn't a full 12 bits in the last block of plaintext. To resolve this problem, we will use padding. We will alternate 1's and 0's. until a complete block is made.

2. Determine the cipher text C.
3. Decrypt the cipher text C.
4. What is the difference between CBC and CFB algorithm?

Exercise V. Hashing (20 pts)

1- What is Hashing and its objective?
2- What is the SHA-256 Algorithm?
3- What are the Characteristics of the SHA-256 Algorithm?
4- Give the steps in SHA-256 Algorithm and illustrate then with a schema
5- Give two Applications when we use SHA.

Final 2023/2024

Exercise I

1) a	2) a	3) c	4) a	5) b
6) a	7) c	8) d	9) c	10) d

Exercise II

1) Passive vs Active security attacks

→ Passive attacks: The attacker listens to network traffic without altering data (e.g. packet sniffing)

- Active attacks: The attacker modifies or ~~disp~~ disrupts data (e.g. message insertion, impersonation, denial of service DoS)

2) Categories of Security Services

1- Confidentiality: Protects data from unauthorized access (example: encryption)

2- Integrity: Ensure data is not altered (ex. hashing)

3- Authentication: Confirm identity of users or systems (ex: passwords)

4- Non-repudiation: Prevent denial of actions (ex: digital signatures)

5- Availability: Keeps services running (ex. DDoS protection)

Exercise III

A) 1) Confidentiality : Encryption / Decryption
- → Sender encrypts the message using the receiver's public key
- → Only the receiver can decrypt it using their private key
- → This ensures that only the intended recipient can read the message

2) Authentication : Digital Signatures
- → The sender signs a message using their private key
- → The receiver verifies the signature using the sender's public key
- → This ensures the message came from the claimed sender and wasn't altered

B) $p = 11$, $q = 23$ $\quad z : \phi(n)$

1) $n = p \times q = 253$

$z = (p-1)(q-1) = 10 \times 22 = 220$

2) we should choose e such that

. $1 < e < z \Rightarrow 1 < e < 220$

. $\gcd(e, z) = 1 \Rightarrow \gcd(e, 220) = 1$

→ $e = 2$ $\quad 220/2 = 110$ ✗ (not coprime)

→ $e = 3$ $\quad 220/3 = 73.3$ ✓ (coprime)

→ $e = 4$ $\quad 220/4 = 55$ ✗ (not coprime)

3) $m = 165$

$C = m^e \bmod n$

$C = 165^3 \bmod 253$

$C = 110$

KU : $\{e, n\} = \{3, 253\}$

$4492125 \mid 253$

$-4492015 \mid 17755$

110

4) $e.d = 1 \bmod (z)$

$e.d = 1 + K \times z$

let $K = 1$, $e = 3$

$\Rightarrow 3.d = 221$

$d = 73.6 \times$

let $K = 2$, $e = 3$

$3d = 1 + 440$

$3d = 441$

$d = 147$ ✓

5) Best $d = 147$ because it satisfies

$ed \equiv 1 \bmod 220$

$3 \times 147 = 1 \bmod 220$

6) $m = C^d \bmod n$

$m = 110^{147} \bmod 253$

$m = 165$

KR: $\{d, n\} = \{147, 253\}$

Exercise IV.

I.V = 1100000 100000 (Size = 12)

M = 1001 1 00111 00 | 10000001 1010 | 0
00010 01010 | 1 |

Key : B = 1011 K(B) = 0100

1) $C_i = K(c_{i-1}) \oplus P_i$

$$C_1 = K(1100\ 0001\ 0000) \oplus 1001\ 1001\ 1100$$

$$C_1 = 0011\ 1110\ 1111 \oplus 1001\ 1001\ 1100$$

$$C_1 = 1010\ 0111\ 0011$$

$$C_2 = K(1010\ 0111\ 0011) \oplus 1000\ 0001\ 1010$$

$$C_2 = 0101\ 1000\ 1100 \oplus 1000\ 0001\ 1010$$

$$C_2 = 1101\ 1001\ 0110$$

$$C_3 = K(1101\ \ 1001\ \ 0110) \oplus (0000\ \ 1001\ \ 0101)$$

$$C_3 = (0010\ \ 0110\ \ 1001) \oplus (0000\ \ 1001\ \ 0101)$$

$$\boxed{C_3 = 0010\ \ 1111\ \ 1100}$$

$$\Rightarrow C = 1010\ \ 0111\ \ 0011\ \ 1101\ \ 1001\ \ 0110\ \ 0010\ \ 1111\ \ 1100$$

2) $P_i = K(c_{i-1}) \oplus C_i$

$P_1 = K(1100\ 0001\ 0000) \oplus 1010\ 0111\ 0011$

$P_1 = 0011\ 1110\ 1111 \oplus 1010\ 0111\ 0011$

$P_1 = 1001\ 1001\ 1100$

$P_2 = K(1010\ 0111\ 0011) \oplus 1101\ 1001\ 0110$

$P_2 = 0101\ 1000\ 1100 \oplus 1101\ 1001\ 0110$

$P_2 = 1000\ 0001\ 1010$

$P_3 = K(1101\ 1001\ 0110) \oplus 0010\ 1111\ 1100$

$P_3 = 0010\ 0110\ 1001 \oplus 0010\ 1111\ 1100$

$P_3 = 0000\ 1001\ 0101$

$\Rightarrow P = 1001\ 1001\ 1100\ 1000\ 0001\ 1010\ 0000\ 1001\ 0110$