University of M'sila
Faculty of MI
Department of computer science

EXAM Correction

Security Computer (3nd level Bachelor)
Academic year: 2025-2026

Duration : 2h

Important: Justification of answers is required for exercises 2, 3, and 4.

Exercise #1 (5 marks): (Correct: +0.5; Incorrect/No Answer: 0) **0.5 *10**

1. What are two symmetric encryption algorithms?
a) 3DES
b) MD5
c) AES
d) RSA

2. Does a digital signature ensure the entire message is encrypted?
a) Yes
b) No

3. The password is stored in database by using:
a) Public-key encryption
b) Secret-key encryption
c) Digital signature
d) Hash function

4. RSA can achieve authentication if we use it as:
a) Encryption scheme
b) Key exchange scheme
c) Digital signature
d) Hash function

5. Which algorithm can ensure data integrity?
a) AES
b) DES
c) SHA-1
d) RC4

6. Which statements describe RSA encryption algorithm?
a) It has key length 128 bits.
b) It is relatively slow than AES algorithm
c) It is called shared-secret key algorithm.
d) It is based on difficult computational algorithm.

7. Which of the following processes can convert ciphertext to plaintext
a) Encryption
b) Decryption
c) Hashing
d) Signing

8. Denial of Service threatens:
a) Confidentiality
b) Authentication
c) Integrity
d) Availability

9. What are the three main security requirments?
   a. Confidentiality
   b. Integrity
   c. Availability or Authentication

10. The output of hash function is a fixed length.
a) Yes
b) No

Exercise #2 (6 marks):

1. Given the key "R" encrypt the message M= "EXAM" using Caesar cipher
   C= "VORD" (1 mark)
   Inserting the table of encryption is necessary
2. What is the size of the keyspace for the affine cipher over the English alphabet?
   The keyspace is 26*12 = 312 (0.5)
3. Prove that $D_K(E_K(m))=m$ for affine cipher.

$D_k(y) = a^{-1}.(y*b) \bmod 26 = a^{-1}.(a*m + b - b) \bmod 26$
$= a^{-1}.a*m \bmod 26$
$= m$ (0.5)

4. Show that the composition of two affine ciphers is again an affine cipher.

If the first key is (a1, b1), the second is (a2, b2), then the composition is
Y= a1 x + b1
X= a2 x + b2
Y = a1 (a2 x + b2) + b1 = a1a2 x + (a1b2+b2) (1 mark)

5. Given the key (7, 3) encrypt the message M= "SEMESTER" using affine cipher.
   C= "ZFJFZGFS" (1,5 mark)
   Inserting the table of encryption is necessary
6. Consider a modified Vigenere cipher where the set of characters are the hexadecimal digits (0,1,…,F) (instead of letters from the English alphabet). For plaintext P="3AE60A3" and key K="17E", compute the ciphertext C?

   E(Pi,Ki) = Ci = (Pi + Ki) mod 16 (0,5)
   D(Ci,Ki) = Pi = (Ci - Ki) mod 16
   P 3 A E 6 0 A 3
   K 1 7 E 1 7 E 1
   C 4 1 C 7 7 8 4
   C= "41C7784" (1 mark)

Exercise #3 (5 marks):

1) What is the strength of RSA?
   The strength of RSA lies on the difficulty of factoring large numbers (0,5)
2) What length must the keys in RSA have?
   The keys used must have a length between 1024 and 2048 bits. (0,25)
3) What is the "trap-door" to generate the keys in RSA?
   The prime numbers p and q are the trap-door of the system. If p and q are known it is easy to calculate d having e. (0,25)

   Prove that $D_{SK}(E_{PK}(m))=m$.
   $E(D(m))= E(m^d \bmod n)= (m^d)^e \bmod n= m^{ed} \bmod n$
   We have $ed= 1 \bmod \Phi(n) = k\Phi(n)+1$ then $E(D(m))= m^{k\Phi(n)+1} \bmod n = m$ (0,5)
4) Amine wants to send an encrypted message to Salim using RSA, with p=5, q=11 and d=7. If the message is M=10.

a. Compute N and Φ (N)

N= 55 (0,5)

Φ (N)= 40 (0,5)

b. Computer the public key e.

ed= 1 mod ϕ (N) => e= d^{-1} mod ϕ (N)

$e=7^{-1}$ mod 40 (0,5)

By using extended Euclidean algorithm, we find:

1 = 3 * 40 + (-17) * 7

Then e= -17 + 40 = 23 (0,5)

c. What does Salim receive?

$C= m^e$ mod N

$C= 10^{23}$ mod 55 (0,25)

By using modular exponentiation algorithm (the table is obligatory), we find:

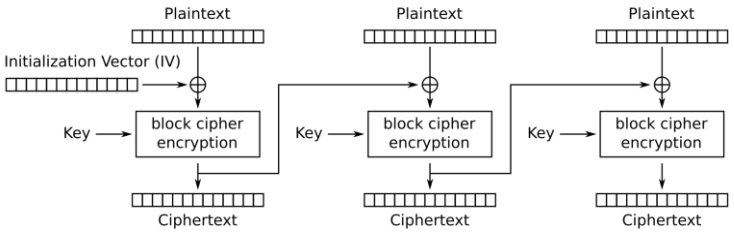
C = 10 (0,75)

d. Is it a good election p, q and d? Why?

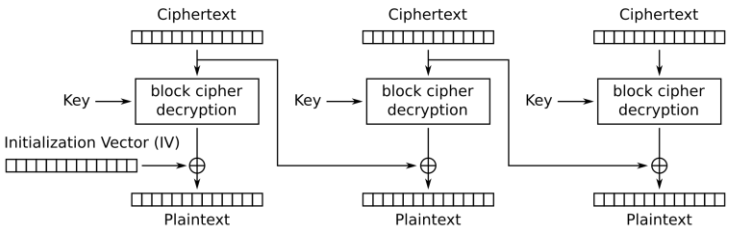
p, q and d must be large primes and besides we can see that Amine message is invariant after encryption (M=C). Therefore, the election of p, q and d is not good. (0,5)

Exercise #4 (4 marks):

1) Draw the CBC encryption and decryption diagrams. (0,5 * 2)



Cipher Block Chaining (CBC) mode encryption



Cipher Block Chaining (CBC) mode decryption

2) Write the CBC encryption and decryption functions.

$C_i = E_K(P_i \oplus C_{i-1})$, $C_0 = IV$ (0,5)

$P_i = D_K(C_i) \oplus C_{i-1}$, $C_0 = IV$ (0,5)

3) What is the limitation of this mode?

Its main drawbacks are that encryption is sequential (i.e., it cannot be parallelized). (0,5)

4) Let the plaintext message be M = 1111000101101, the vector VI = 111, and the key K = (f(2)=1, f(3)=2, f(1)=3) by a right shift of 1 bit. Encrypt the message M.

P1=111, P2=100, P3=010, P4=110, P5=100 (padding) (0,5)

C1 = E(111⊕111) = 000

C2 = E(100⊕000)= 010

C3= E(010⊕010)= 000

C4= E(110⊕000)= 011

C5= E(100⊕011)= 111

C= « 000010000011111 » (1 mark)

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
0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25