Question 1:

1. The complexity of the brute force attack depends on:
   a) No. of bits of the message block
   b) No. of bits of the key
   c) No. of bits of the hash function of the key
   d) None of the above

2. The **additive inverse** of 2569 mod 555 is
   a) 206 → 2569mod 555 =349 → 555-349 = 206
   b) 229
   c) 1509
   d) None of the above

3. Which of the following is not a property of ECB block Cipher mode?
   a) Any repeated plaintext blocks will result in identical corresponding ciphertext blocks
   b) Encryption can be fully parallelized
   c) If a ciphertext block is modified or corrupted, then after decryption the corresponding plaintext block and all the following plaintext blocks will be affected
   d) None of the above

4. Message authentication codes (MAC) and digital signatures both serve to authenticate the content of a message. Which of the following best describes how they differ?
   a) A MAC can be verified based only on the message, but a digital signature can only be verified with the secret key used to sign that message.
   b) A MAC can be verified based only on the message, but a digital signature can only be verified with the public key of thea party that signed the message.
   c) A MAC can be verified with the secret key used to generate it, but a digital signature can only be verified based only on the message.
   d) A MAC can be verified with the secret key used to generate it, but a digital signature can only be verified with the public key of the party that signed the message.

5. Which of the following is a property of CBC block cipher mode?
   a) Any repeated plaintext blocks will result in identical corresponding ciphertext blocks
   b) Decryption can be fully parallelized
   c) If a ciphertext block is modified or corrupted, then after decryption the corresponding plaintext block and all the following plaintext blocks will be affected

Formatted: Font: Bold
Formatted: Font: Not Bold
Formatted: Font: Not Bold
Commented [1]: you saved my GPA <3
Commented [2]: no need to thank me ❤
Deleted: parallelizedt

d) None of the above

6. In RSA, the public key consists of the pair {PU, n} where n is the term after the mod (mod n). For security reasons "n" should be
   a) Prime Number
   b) Large Number
   c) Having at least one prime factor
   d) None of the above

7. In asymmetric cryptography, which of the following must be true?
   a) Different keys are used for encryption and decryption
   b) Different algorithms are used for encryption and decryption
   c) Cryptographic operations are one-way, and not reversible
   d) Both (a) and (b)

8. Which of the following issues is NOT critical to the secure use of public key cryptography?
   a) Key length
   b) Authentication of the owner of particular public key
   c) Inability of anyone to derive private key given matching public key
   d) Ensuring that only desired communication partners learn one's public key

Deleted: critical the

9. Alice wants to communicate with Bob while satisfying confidentiality. Accordingly, Alice would Encrypt her message to Bob using…
   a) Alice's public key
   b) Alice's private key
   c) Bob's public key
   d) None of the above

10. Caesar Cipher is which type of cipher
    a) Block
    b) Stream
    c) Asymmetric
    d) Permutation

Commented [3]: It is a substitution cipher

Commented [4]: It is a substitution stream cipher

Commented [5]: Yes, yes.
No objection, just mentioning xD

Question 2:

Encrypt the message below using the following encryption methods. Assume the English alphabet.

Message: **transmission**

Encryption methods

a- **Vigenere with key = system**

s y s t e m s y s t e m
t r a n s m i s s i o n
----
l p s g w y a q k b s z

b- Playfair with keyword = system

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

tr an sm is si on
----
mp gu ys gt tg po

Commented [6]: You changed my life <3

Commented [7]: خير الناس أنفعهم للناس

Deleted: Vignere

Deleted:

Deleted:

Deleted:

Deleted:

Deleted:

Deleted:

Deleted:

Deleted:

Deleted:

Deleted:

Deleted:

2-c: Determine the gcd of the following pairs of polynomials:

x^4+x^3+x and x^2+1 over GF(2)

	Q	R
GCD(x^4+x^3+x, x^2+1)	x^2+x+1	1
GCD(x^2+1, 1)=1		

Deleted: x+

2-d: Find the multiplicative inverse of: **826 mod 2789**

r_i	q_i	y_i
2789	**xxxxx**	**0**
826	**xxxxx**	**1**
311	**3**	**-3**
204	**2**	**7**
107	**1**	**-10**
97	**1**	**17**
10	**1**	**-27**
7	**9**	**260**
3	**1**	**-287**
1	**2**	**834**

Multiplicative inverse is 834

Question 3:

3-a: For RSA encryption, if the public key is **n = 187** and **e = 107**. You observe a **ciphertext C = 2**. What is the plaintext M?

SOLUTION

$$M = C^d \ mod \ n$$
$$d = e^{-1} \ mod \ \phi(n)$$

Factorizing n into p and q: $n = 11 * 17$

$$\phi(n) = (p-1)(q-1) = 160$$

ri	qi	yi
160	xxxxxxx	0
107	xxxxxxx	1
53	1	-1
1	2	3

d = 3

M = 2^3 mod 187 = 8

3-b: Using the Diffie-Helman algorithm, assume two users want to communicate with one another using symmetric encryption. Each of the two users is in possession of private key only known to him. For User A having the **private key 6**, and user B the **private key 12** and a commonly **known prime 71** and its **primitive element 7**

Describe in detail the procedure the two users use to obtain this common key.

1) The two users generate their public keys

a) $Y_A = a^{XA} \bmod q$

b) $Y_B = a^{XB} \bmod q$

2) Each user can obtain the common key using his own private key and the other user's public key

$K = Y_B^{XA} \bmod q = Y_A^{XB} \bmod q = a^{XA*XB} \bmod q$

Find the common key

$X_A = 6$ **$X_B = 12$** **$q = 71$**

$a = 7$

$Y_A = 7^6 \bmod 71 = 2$

$Y_B = 7^{12} \bmod 71 = 4$

$K = 2^{12} \bmod 71 = 4^6 \bmod 71 = 49$

Question 4:

4-a: Determine the multiplication of f(x) x g(x) mod m(x) where f(x) = x^3+x+1 and g(x) = x^3+1 mod m(x), in GF(2^4) and m(x) = x^4+x+1
(Use binary numbers' representation):

f(x) = 1 0 1 1
g(x) = 1 0 0 1
m(x)-x^4 = 0 0 1 1

x	**1 0 1 1 * 0 0 1 0**	**0 1 1 0** **+ 0 0 1 1** **= 0 1 0 1**
x^2		**1 0 1 0**
x^3		**0 1 0 0** **+ 0 0 1 1** **= 0 1 1 1**

(x^3 + 1) * f(x) mod m(x) = x3*f(x) mod m(x) + 1*f(x) mod m(x)

f(x)*g(x) mod m(x) = 0 1 1 1 + 1 0 1 1 = 1 1 0 0 = x^3 + x^2

Detailed example in the next page:

Multiplication

The technique is based on the observation that

$$x^8 \bmod m(x) = [m(x) - x^8] = (x^4 + x^3 + x + 1) \qquad \textbf{(4.12)}$$

$$x \times f(x) = \begin{cases} (b_6 b_5 b_4 b_3 b_2 b_1 b_0 0) & \text{if } b_7 = 0 \\ (b_6 b_5 b_4 b_3 b_2 b_1 b_0 0) \oplus (00011011) & \text{if } b_7 = 1 \end{cases}$$

In an earlier example, we showed that for $f(x) = x^6 + x^4 + x^2 + x + 1$, $g(x) = x^7 + x + 1$, and $m(x) = x^8 + x^4 + x^3 + x + 1$, we have $f(x) \times g(x) \bmod m(x) = x^7 + x^6 + 1$. Redoing this in binary arithmetic, we need to compute $(01010111) \times (10000011)$. First, we determine the results of multiplication by powers of x:

$$\begin{aligned}
(01010111) \times (00000010) &= (10101110) \\
(01010111) \times (00000100) &= (01011100) \oplus (00011011) = (01000111) \\
(01010111) \times (00001000) &= (10001110) \\
(01010111) \times (00010000) &= (00011100) \oplus (00011011) = (00000111) \\
(01010111) \times (00100000) &= (00001110) \\
(01010111) \times (01000000) &= (00011100) \\
(01010111) \times (10000000) &= (00111000)
\end{aligned}$$

So,

$$\begin{aligned}
(01010111) \times (10000011) &= (01010111) \times [(00000001) \oplus (00000010) \oplus (10000000)] \\
&= (01010111) \oplus (10101110) \oplus (00111000) = (11000001)
\end{aligned}$$

which is equivalent to $x^7 + x^6 + 1$.

4-b: In RSA algorithm, if **p = 7** and **q = 13**, what are the **five smallest possible numbers for e**? Justify your answer **(Show how did you find the answer)**

n = p.q = 91

√(n) = (p-1)(q-1) = 72

1 < e < √(n)

e = 5, 7, 11, 13, 17

Numbers achieved by trial and error

Deleted: +

Commented [9]: also

Commented [10]: I think 7 & 13 is not right
as e should be coprime with (n, Φ(n))
so gcd(n, 7) = 7 (!= 1) also for 13
my answer is 5, 11, 17, 19, 31

Commented [11]: it should be gcd(phi(n),e) = 1 not n

Question 5:

In block cipher operations, during the transmission of C3 (the third cipher block) an error in the 5th bit occurred. How many plaintext blocks will be affected, if we are using:

5-a: 16-b it CFB mode? Explain why?

Ibrahim Radwan

هو بالنسبة لسؤال خمسة فالفكرة فيه ان CI بتأثر في اللي هتعمله decrypt
بعد كدا طول ما ال CI موجودة في ال register بمعنة لو فرضنا ان ال
register اللي بيتعمله encrypt (اللي عليها دايرة في الرسمة دا) طول ٦٤ (انا
مش فاكر كان بيبقى كام بالظبط بس يعني نفرض ٦٤) و هو قايل CFB-16
يعني ال s = 16 فاحنا كل step لما يجلنا CI بنعمل shift لل register بتاعنا ب
١٦ bit يبقى كدا:
١- اول لما تيجي C3 ال P3 هتطلع غلط نتيجة لل xor
٢- لما ندخل C3 في ال register علشان نفك C4 لما تيجي هيبقى كدا ال bit
رقم خمسة في ال register (اللي هو ٦٤) غلط فكدا P4 هتطلع غلط
٣- بعد اول شفت هتبقى ال bit رقم خمسة موجودة عند ٥ + ١٦ = ٢١ يبقى
كمان لسا P5 هتطلع غلط
٤- هنعمل شفت تاني ٢١ + ١٦ = ٣٧ يبقى P6 كمان غلط
٥- كمان شفت يبقى ٥٣ يعني P7 كمان غلط
٦- كمان شفت يبقى ٦٩ فكدا بقت برا ال register فخلاص كدا
يبقى P3-P7 غلط يعني

5-b: 8-bit OFB mode? Explain Why?
]

التاني بقى الغلطة هتكون بس في P3 عشان ال transmission error مش
بي propagate يعني

هذا والله اعلم يعني

5- c: In block cipher operations list two advantages of using CTR mode over other block cipher mode.

Commented [12]: Page 208 in reference.

1) **Can work in parallel with decryption**
2) **No error propagation**

Question 6:

What is the difference between each of the following pairs:
a- A block cipher and a stream cipher

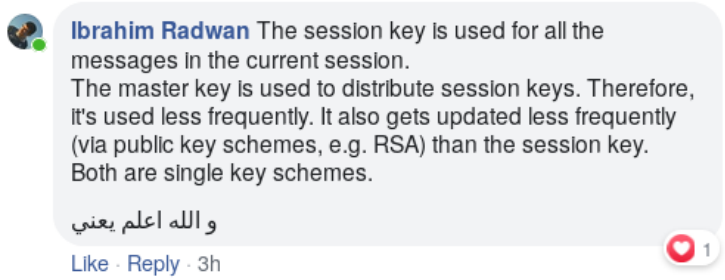
Block: Encrypt message in blocks of fixed size
Stream: Encrypts stream of bits

b- Active attacks and passive attacks

Active: Capture message, replay later
Passive: Read message contents

Comparison	Passive Attacks	Active Attacks
Definition	A passive attack attempts to learn or make use of information from the system but does not affect system resources.	Active attacks involve some modification of the data stream or the creation of a false stream
Types or Categories	Two types of passive attacks are: + release of message contents + traffic analysis	Four categories: + masquerade + replay + modification of messages + denial of service
Detection	difficult to detect	Can be detected
Prevention	Measures are available to prevent their success.	It is quite difficult to prevent active attacks absolutely, because of the wide variety of potential physical, software, and network vulnerabilities.
Handling	Prevention	Detection and recovering from disruption or delays caused by them

c- A session key and a master key
Session Key is smaller than master key.



Slide 7 CH.14

Key Hierarchy

- typically have a hierarchy of keys
- session key
  - temporary key
  - used for encryption of data between users
  - for one logical session then discarded
- master key
  - used to encrypt session keys
  - shared by user & key distribution center

d- Symmetric and Asymmetric encryption

Symmetric: Use only private key
Asymmetric: Use public and private keys

Question 7:

7-a: State the requirements needed in any certificate issued by a certificate authority:

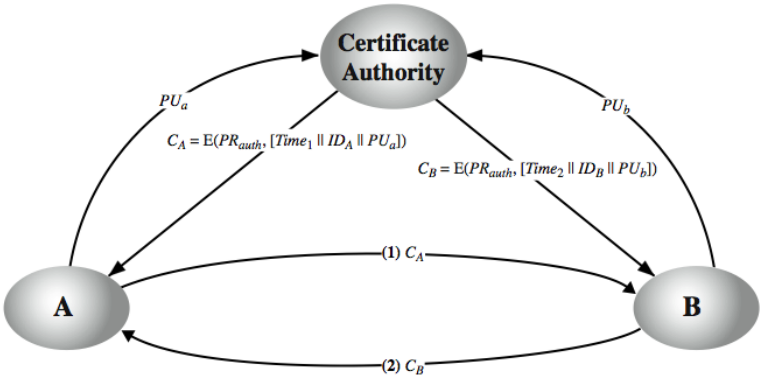
1.
2.
3.
4.

Sol:

7-b: Sketch and explain clearly on your sketch how public key certificates are used. You show how certificates are generated and how each entity uses it later to distribute its keys.

Deleted: is later

[PUT on your sketch all necessary explanation to show how the operation is performed, its order and any necessary explanation]


Certificate Authority
PU_a
PU_b
$C_A = \mathrm{E}(PR_{auth}, [Time_1 \| ID_A \| PU_a])$
$C_B = \mathrm{E}(PR_{auth}, [Time_2 \| ID_B \| PU_b])$
(1) C_A
A
B
(2) C_B

7-c: Briefly describe Triple DES with 2 keys (use only the space below). You can sketch it.

$C_i = E_{k1}(D_{k2}(E_{k1}(P_i)))$

1) **Message is encrypted by first key**
2) **Message is decrypted by second key**
3) **Message is again encrypted by first key**

Encryption = Decryption in security

7-d: Briefly describe Double DES with 2 keys (use only the space below). You can sketch it.

$C_i = E_{k1}(E_{k2}(P_i))$

It Encrypts message with first key, takes it, and encrypts is with second key

7-e: Which one is more secure, Double DES or Triple DES and why:

…**Triple DES**… is more secure

WHY, EXPLAIN:

Double DES is vulnerable to meet in the middle attack by encrypting message with all possible keys, saving values and decrypting by keys until values are equal to know keys takes $O(2^{56})$

Question 8:

8-a: What are the requirement of hash function

Requirement	Description
Variable input size	H can be applied to a block of data of any size.
Fixed output size	H produces a fixed-length output.
Efficiency	H(x) is relatively easy to compute for any given x, making both hardware and software implementations practical.
Preimage resistant (one-way property)	For any given hash value h, it is computationally infeasible to find y such that H(y) = h.
Second preimage resistant (weak collision resistant)	For any given block x, it is computationally infeasible to find y ! x with H(y) = H(x).
Collision resistant (strong collision resistant)	It is computationally infeasible to find any pair (x, y) such that H(x) = H(y).
Pseudorandomness	Output of H meets standard tests for pseudorandomness

8-b: What types of attacks are addressed by message authentication
(State and describe briefly at least 3 attacks)?

- **Masquerade: Insertion of messages into the network from a fraudulent source**
- **Content modification: of the contents of a message**
- **Sequence modification: to a sequence of messages between parties**
- **Timing modification: Delay or replay of messages**

Question 9:

9-a: What are the design objectives of HMAC?

1. **use, without modifications, hash functions**
2. **allow for easy replaceability of embedded hash function**
3. **preserve original performance of hash function without significant degradation**
4. **use and handle keys in a simple way.**
5. **have well understood cryptographic analysis of authentication mechanism strength**

9-b: Draw the block diagram of HMAC operation and put all explanation on the diagram.