Name: Abdus Salam
ID: IT-21016
4th Year 1st Semester
Sub: Cryptography and Cyber Law

IT-21016

Q1: How does Shor's algorithm threate the security of RSA and Elliptic Curve Cryptography (ECC), and what are the potential consequences for current digital infrastructure?

Solve: Shor's algorithm solves two problems in polynomial time on a fault-tolerant quantum computer.

- Integer factoring – breaks RSA (private key = factors of a large modules $N = pq$).
- Discrete logarithm (over multiplicative groups and elliptic curves) → breaks Diffie-Hellman and ECC.

This requires large, error-corrected quantum computers. We don't have those yet – but the risk is asymmetric: once they exist, all past traffic recorded today that used RSA/ECC without forward secrecy becomes readable.

IT-21016

Consequences for digital infrastructure :

- Confidentiality loss (retroactive): Recorded traffic without strong PFS can be decrypted later.
- Authenticity collapse (live): Attackers can forge signature, issue fake certificates, and push malicious updates.
- Systemic trust shock: PKI and software supply chains would require emergency rotations, outages and revocations would be widespread.
- Regulatory & liability exposure: Breach of data-retention and sectoral rules for data meant to stay secret for years.

IT-21016

Q-2:

Quantum Key Distribution (QKD) is a secure communication method that utilises principles of quantum mechanics to generate and distributes ~~encrypt~~ cryptographic keys. It allows two parties to create a shared secret key that can be used to encrypt and decrypt messages, with security guaranteed by the laws of physics.

Role of QKD in Future Cryptographic Systems:

1. Quantum-Safe Keys Exchange:
   - Secure key sharing using quantum physics
   - Resistant to quantum attacks
2. Unconditional Security:
   - QKD security is based on laws of quantum physics, such as:-
     - Heisenberg's uncertainty principle
     - No-cloning theorem

IT-2016

- Any attempt to eavesdrop on the quantum channel disturbes the system, alerting the legitimate parties.

3. Eavesdropping Detection:

- Detects any interception via quantum disturbance.
- Compromised keys are discarded.

4. Post-Quantum Ready:

- Used with symmetric encryption
- Builds quantum-secure communication

5. Quantum-Internet Backbone:

- Core tech for future secure quantum networks
- Already tested via satellites & fibe optics.

6. Physic-Based Trust:

- Security forces laws of networks, not hard maths.
- Not breakable by any computing power

IT-21016

7. High Security use:
   - Best for military, banking government
   - long-term sensitive data protection

8. Crypto-Agility:
   - Frequent secure key updates.
   - Adapts quickly to new threats.

Q-3 Solution:

Lattice-based cryptography and traditional number-theoretic cryptograpy (such as RSA and ECC) differ significalty in their mathmatical foundations in their mathmatical foundations security assumptions, and resistence to quantum attacks.

Lattice based cryptography offers a significant advantages over traditional number theoriatic approaches like RSA in terms of quantum resistance.

IT-21016

While traditional methods rely on problems that quantum computers can easily solve, lattice-based cryptography is built on problems that are believed to be difficult.

Here's more detailed breakdown of the diffences:

Security Foundation:

- Traditional (RSA, ECC)
  - Relies on the difficulty of factoring large numbers or solving the discrete logarithm problem
- Lattice-based cryptographic
  - Relies on the difficulty of solving problems on high-dimensional latti such as SIVP and SVE.

IT-21016

Mathematical Foundation:

- Traditional (RSA/ECC):
  - Based on hard number-theoretic problems like integer factorization (RSA) and discreate logarithm problems.
- Lattice-Based Cryptography:
  - Based on problems in high dimensional geometry such as the shortest vector problem (SVP) and LWE.

Quantum Resistence:

- Traditional (RSA/ECC):
  - Vulnerable to quantum algorithms like Shor's algorithm, which can solve their underlying problems in polynomical time.
- Lattice-Based Cryptography:
  - Considered quantum-resistant, as no efficient quantum algorithms are known to solve Lattice problems.

IT-21016

Q-4 Solution:

Here's a python PRNG (Pseudo-Random Generator) that uses current system time and a custom seed value to generate random numbers. S'U also include sample output S'D

Python program:

```
import time
def custom-prng (seed, count):
    current-time = int(time.time-ns())
    combined-seed = seed ^ current-time
    a = 1664525
    c = 1013904223
    m = 2**32
    random-numbers = []
    X = combined-seed
    for _ in range(count):
        X = (a* X+C) % m
        random-numbers.append(X)
    return random-numbers
Seed-value = 12345
```

RT - 21016

count = 5

Numbers = custom - prng (seed value, count)

print ("custom PRNG output:")

for ; num in enumerate (numbers, 1):

print ("Random Number {i}: {num}")

Sample Output:

Custom PRNG output:

Random Number 1: 1885951992

Random Number 2: 2910389135

Random Number 3: 2475739278

Random Number 4: 33994785

Random Number 5: 1326364488

Explanation:

① - Seed initialization → Combines custom seed and system time (nanoseconds) using XOR for randomness

- LCG Formula → Uses $(a * X + c) \% m$ to generate pseudo-random numbers.

IT-21016

Q-5 Solution:

Sieve of Eratosthenes is an ancient and efficient method for finding all prime numbers up to a given limit n. It works by progressively eliminating the multiples of each prime number, starting from the smallest prime (2).

Algorithm steps:

1. Create a list of integers from 2 to n
2. Start with the first numbers in the list (p=2), which is prime.
3. Eliminate all multiples of p.
4. Find the next numbers in the list that is not marked, this the next prime.
5. Repeat steps 3-4 until all multiples up to $\sqrt{n}$ have been processed
6. The reanaining unmarked numbers are all primes.

DT-21016

Find all primes less than 50

Let's use the sieve of Eratosthenes to find all prime numbers less than 50.

1. Create a list of numbers from 2 to 49:

2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31, 32, 33, 34, 35, 36, 37, 38, 39, 40, 41, 42, 43, 44, 45, 46 47, 48, 49.

2. Start with the first prime 2 then eliminates all multiplese of 2:

2, 3, 5, 7, 9, 11, 13, 15, 17, 19, 21, 22, 23, 25, 27, 29, 31, 33, 35, 37, 39, 41, 43, 45, 47, 49

3. The next unmarked number 3. Eliminate all multiple of 3:

2, 3, 5, 7, 11, 13, 17, 19, 23, 25, 29, 31, 35, 37, 41, 43, 47, 49

4. The next unmarked number 5 Eliminate all multiple of 5:

2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47, 49.

IT-21016

Q-6 Solution

Definition: A carmichael number is a composite integer n such that

$$a^{n-1} \equiv 1 \pmod{n}$$

for every integer a with $\gcd(a, n) = 1$

A positive composite integer n is a carmichael number if all three conditions hold:

1. n is composite
2. n is square-free
3. for every prime p dividing n, $(p-1)$ divides $(n-1)$; i.e. $p-1 \mid n-1$

Verification for the given numbers:

We check each n against Korselt's criterion.

1. $n = 561$
   - Factorization: $561 = 3 \times 11 \times 17$ → Composite and square free.
   - Compute $n-1 = 560$

IT-21016

- For $p = 3$: $p-1 = 2.2 \mid 560$ $(560/2 = 280)$
- For $p = 11$: $p-1 = 10.10 \mid 560$ $(560/10 = 56)$
- For $p = 17$: $p-1 = 16.16 \mid 560$ $(560/16 = 35)$

All conditions satisfied → 561 is a carmichael number.

2. $n = 1105$
   - Factorization: $1105 = 5 \times 13 \times 17$ → Composite and square-free
   - Compute $n-1 = 1104$

3. $n = 1729$
   - Factorization: $1729 = 7 \times 13 \times 19$ → Composite and square-free.
   - Compute $n-1 = 1728$
   - For $p = 7$: $p-1 = 6.6 \mid 1728$ $(1728/6 = 288)$
   - For $p = 13$: $p-1 = 12.12 \mid 1728$ $(1728/12 = 144)$
   - For $p = 19$: $p-1 = 18.18 \mid 1728$ $(1728/18 = 96)$

All conditions are satisfied → 1729 is a carmicheal number.

IT-21016

Q-7

Yes, In fact $\mathbb{Z}_{11}$ is a commutative ring with unity and moreover a field.

Justification:

- $(\mathbb{Z}_{11}, +)$ is an abelian group : closure, associativity, identity 0, inverses ($-a \equiv 11-a$) and commutativity hold (addition mod 11)
- multiplication mod 11 is closed and associative, and distributes over addition
- There is a multiplicative identity $1 \in \mathbb{Z}_{11}$
- Because 11 is prime, every nonzero element $a \in \mathbb{Z}_{11}$ has a multiplicative inverse mod 11,

Thus all ring axioms hold and every nonzero element is invertible → $\mathbb{Z}_{11}$ is a Field.

Yes, $(\mathbb{Z}_{37}, +)$ is a Abelian groups.

IT-21016

Justification:

- Set $Z_{37} = \{0, 1, \ldots, 36\}$ with addition modulo 37
- closure, associativity and commutativity follow from integer addition.
- Identity is 0. For each a, additive inverse is $37 - a$.

Thus $(Z_{37}, +)$ satisfied all group axioms and is abelian.

No, $(Z_{35}, +)$ is not a group.

Although multiplication mod 35 is associative and has identity 1, not every element has a multiplicative inverse in Z_{35}.

IT-21016

Q-8

Ans:

We want r with $0 \le r < 31$ and $-52 \equiv r \pmod{31}$

Compute:

$$-52 + 2 \cdot 31 = -52 + 62 = 10$$

So, $-52 \equiv 10 \pmod{31}$

alternate: $-52 \equiv -52 + 31 = -21 = -21 + 31 \equiv 10$

So, the remainder is 10.

Q-9 Ans:

We solve $7x \equiv 1 \pmod{26}$ or find integers x, y with $7x + 26y = 1$

Use the Euclidean algorithm:

$$26 = 3 \cdot 7 + 5,$$
$$7 = 1 \cdot 5 + 2,$$
$$5 = 2 \cdot 2 + 1,$$
$$2 = 2 \cdot 1 + 0$$

IT-21016

Back-Substitute to express 1 as a linear combination:

$$1 = 5 - 2 \cdot 2$$
$$= 5 - 2(7 - 1 \cdot 5) = 3 \cdot 5 - 2 \cdot 7$$
$$= 3 \cdot (26 - 3 \cdot 7) - 2 \cdot 7 = 3 \cdot 26 - 11 \cdot 7$$

Thus $-11 \cdot 7 + 3 \cdot 26 = 1$. Therefore $x \equiv -11 \pmod{26}$

$$x \equiv -11 \equiv 15 \pmod{26}$$

The multiplicative inverse of 7 modulo 26 is 15.

Q-10 Ans:

Step-1 - Multiply the number:

$$-8 \times 5 = -40$$

Step-2-Reduce module 17:

We find the equivalent positive remainder:

$$-40 + 3 \times 17 = -40 + 51 = 11$$
$$-40 \equiv 11 \pmod{17}$$
$$(-8 \times 5) \bmod 17 = 11$$

IT-21016

Explain of Simplification method:

Negative numbers in modular arithmetic can be converted to their positive equivalent before multiplying.

$$-8 \equiv 9 \pmod{17}$$

$$9 \times 5 = 45$$

Reduce 45 module 17:

$$45 - 2 \times 17 = 45 - 34 = 11$$

This match the previous result

∴ Final answer = 11.

IT-21016

Q-11 Ans:

For a integers a and b not both zero, there exist integers x, y such that

$$ax + by = \gcd(a, b)$$

In particular, if $\gcd(a, b) = 1$ there are integers x, y with $ax + by = 1$; then x is the multiplicative inverse of a modulo b.

Proof: Let, $d = \gcd(a, b)$.

- By the Euclidian algorithm, d divides both a and b
- The set of all integers of the form $ax + by$ is closed under addition and subtraction.
- Let m be the smallest positive number in this set then m divides both a and b.

IT-21016

• Hence $m = d$, and there exist integers x, y such that

$$ax + by = d$$

Finding the multiplicative inverse of 97.

Modulo 385:

We want x such that:

$$97x \equiv 1 \pmod{385}$$

This is equivalent to:

$$97x + 385y = 1$$

We have

$$1 = (-127) \cdot 97 + 32 \cdot 385$$

Therefore $x = -127 \pmod{385}$

We want the positive inverse:

$$-127 \equiv 385 - 127 = 258 \pmod{385}$$

The multiplicative inverse of 97 mod 385 is 258.

IT-21016

Q-12 Ans:

Bezout Identity Statement:

For any integers a and b, there exist integers x and y such that:

$$ax + by = \gcd(a, b)$$

Proof:

1. Let $d = \gcd(a, b)$ By definition, d divides both a and b, so $a = da'$ and $b = db'$ where a', b' are integers with $\gcd(d, b) = 1$

2. Science a' and b' are comprime, there exists integers x_0, y_0 such that:

$$a'x_0 + b'y_0 = 1$$

3. Multiplying through by d gives:

$$a(dx_0) + b(dy_0) = d$$

Thus $x = x_0$ and $y = y_0$ are integer solutions to: $ax + by = \gcd(a, b)$

IT-21016

Find x such that $43x \equiv 1 \pmod{240}$:

This asks for the multiplicative inverse of 43 module 240. We solve the Diophantine equation: $43x - 240y = 1$

by the Extended Euclidean Algorithm

Compute gcd chain (Euclidean Algorithm):

$$240 = 5 \cdot 43 + 25$$
$$43 = 1 \cdot 25 + 18$$
$$25 = 1 \cdot 18 + 7$$
$$18 = 2 \cdot 7 + 4$$
$$7 = 1 \cdot 4 + 3$$
$$4 = 1 \cdot 3 + 1$$
$$3 = 3 \cdot 1 + 0$$

Thus $43 \cdot 67 - 240 \cdot 12 = 1$

So, $x = 67$ is a solution

$$43^{-1} \equiv 67 \pmod{240} \text{ or } 0$$
$$43 \cdot 67 \equiv 1 \pmod{240}.$$

IT-2016

Q-13 Solution:

Fermat's little theorem (FLT) - statement:

If p is a prime number and a is any integer with $\gcd(a,p) = 1$, then

$$a^{p-1} \equiv 1 \pmod{p}.$$

proof:

Consider the nonzero residues modulo p: $1, 2, \ldots, p-1$ multiply each by a (with $\gcd(a,p) = 1$) the set $a.1, a.2, \ldots, a.(p-1)$ is a permutation of $1.2 \ldots p-1$ modulo p.

Taking the product of all elements in both sets and reducing mod p gives —

$$a^{p-1} \cdot (1.2 \ldots (p-1)) \equiv 1.2 \ldots (p-1) \pmod{p}$$

cancelling the nonzero product $1.2 \ldots (p-1)$ which is invertible (mod p) yields $a^{p-1} \equiv 1 \pmod{p}$

IT-21616

Primality Test using FLT:

Choose a with $1 < a < p$ and $\gcd(a, p) = 1$

If $a^{p-1} \not\equiv 1 \pmod{p} \Rightarrow p$ is composite. If it is 1, p may be prime - but there are composites (carmichael numbers) that also pass.

Is 561 prime?

Take $a = 2$, $\gcd(2, 561) = 1$,

$$561 = 3 \cdot 11 \cdot 17$$

By chinese Remainder Theorem and FLT:

$$2^{560} \equiv 1 \pmod{3}, 1 \pmod{11}, 1 \pmod{17}$$

So, $2^{560} \equiv 1 \pmod{561}$ - 561 passes FLT. But is not prime. It is a carmichael number.

IT-21016

Q-14 Ans:

Statement: The chinese Remainder Theorem states that a system of linear congruences with pairwise coprime modulo has a unique solution modulo the product of the moduli. If $m_1, m_2, \ldots m_k$ are pairwise coprime positive integers and $a_1 \ldots a_k$ are any integers, Then the system

$$x \equiv a_i \pmod{m_i}, \quad (i = 1, \ldots k)$$

has a unique solution modulo $M = m_1 m_2 \ldots m_k$

Proof:

Let $M = \prod_{i=1}^{k} m_i$ and $M_i = M/m_i$ Since $\gcd(m_i, m) = 1$, there exists an inverse y_i such that $M_i \cdot y_i \equiv 1 \pmod{m_i}$ Then

$$x = \sum_{i=1}^{k} a_i M_i y_i$$

IT-21016

Solve the system:

Start with $x \equiv 2 \pmod 3$ put $x = 2+3k$

Plug into mod 5:

$$2+3k \equiv 3 \pmod 5 \Rightarrow 3k \equiv 1 \pmod 5$$

Inverse of 3 mod 5 is 2 (since $3 \cdot 2 = 6 \equiv 1$) So,

$$k \equiv 2 \pmod 5 \Rightarrow k = 2+5t$$

Thus $x = 2+3k = 2+3(2+5t) = 8+15t$

Now impose mod 7:

$$8+15t \equiv 2 \pmod 7 \Rightarrow 15t \equiv 6 \equiv 1 \pmod 7$$

Since $15 \equiv 1 \pmod 7$, this gives $t \equiv 1 \pmod 7$

So, $t = 1+7s$, then

$$x = 8+15(1+7s) = 8+15+105s = 23+105s$$

Therefore the solution modulo $3 \cdot 5 \cdot 7 \equiv 105$

$$x \equiv 23 \pmod{105}$$

IT-21016

Q-15 Ans:

The CIA triad stands for confidentiality, Integrity and Availability. It is a fundamental for information security.

- Confidentiality:
  - → Ensures data is disclosed only authorized parties.
  - → Machanisms: encryption, access controls, authentication, secure channels.
- Integrity:
  - → Ensures data is accurate and has not been tampered with
  - → Machanisms: Cryptographic hashes, digital signatures, MACs, checksums, version control.
- Availability:
  - → Ensures authorized users can access data and services when needed
  - → Machanisms: redundancy, backups, DDoS protection, fault tolerance, monitoring.

IT-21016

Q-16 Ans:

Difference: Steganography vs cryptography

- Cryptography transforms plaintext into an unreadable form (ciphertext) so that the content is hidden (confidential), but the existence of the message is usually the exists obvious. Good Unreadability without the key.

- Steganography: hides the existence of the message by embedding it into another innocuous subject (image, audio, video, text)
  Goal: Secrecy of existence (covert communication)

They can be used together. First encrypt the secret, then hide the ciphertext with steganography.

IT-2016

Common Steganography techniques (digital media):

1. LSB (Least significant Bit) Substitution change (audio): replaces least significant bits of pixels/samples with message bits /simple and high capacity but vulnerable to processing/noise.

2. Masking and dittering (images): hide data in perceptually significant areas (watermarking) style robust against image processing.

3. Transform-domain methods: embaded data in frequency co-efficients. More robust to compression and common edits.

4. Spread-spectrum steganography: spread message bits across many samples, low detectability and robust.

IT-21016

Q-17 Ans:

Phishing:

Method: Social engineering - attackers send deceptive emails/message or create fake website to trick users into revealing credentials, personal data, or clicking malicious links.

Goal/Impact: Credential theft, identity theft initial foothold in networks.

Defences: User education, email, filtering multi, factor, authentication (MFA). URL/website scanners, anti phishing policies.

Malware:

Method: Software (viruses, worms, Trojans, ransomware, spyware) delivered via email attachments, drive-by-downloads, infected devices or, malicious installers.

DT-21016

Goal/Impact: Data theft, destruction, system compromise, encryption for ransom, establishing persistent backdoors.

Defences: Endpoint protection/AV; application white-listing, patch management, Least privilege, network segmentation, backups.

Q-18 Ans)

Legal frameworks and cybersecurity: Role of GDPR:

The General Data Protection Regulation (GDPR) is a European Union (EU) law designed to strengthen the protection of personal data and privacy of individuals. It plays an important role in mitigating cyber attack and protecting user privacy through the following ways.

IT-2016

Data Minimization: GDPR requires organizations to collect only necessary personal data, reducing the amount of sensitive information that can be stolen in a cyber-attack.

Security Measures: It mandates strong technical and organizational measures to safe-guard data against unauthorized access, altercation, or loss,

Breach Notification: Organizations must report personal data breaches to authorities within 72 hours. This ensures quick containment and response to cyber attacks.

User Rights: Individuals have rights such as access to their data connection, detection and data probability.

IT-21016

Q-19 Ans:

Basic working of the DES Algorithm:

The Data Encryption Standard (DES) is a symmetric-key block cipher that encrypts data in fixed-size blocks.

It operates on:

- plaintext block: 64 bits (8 bytes)
- key = 56 bits
- output: 64-bit ciphertext

1. Initial permutation (IP)

- The 64-bit plaintext is rearranged according to a fixed table.
- This step does not involve the key

it simply changes bit positions to prepare for the rounds.

- Example: If the plaintext is P = [$P_1, P_2, P_3 \ldots P_{64}$] the IP might move P_{58} to position 1, P_{50} to position 2, etc.

IT-21016

2. Rounds (16 Iterations)

The output of R_{16} is divided into two halves:

- Left half (L_0) = first 32 bits.
- Right half (R_0) = last 32 bits.

a) Expansion (E-box):

- The 32-bit might half (R_i) is expanded to 48 bits by duplicating certain bits, using the E expansion table.

b) Key mixing

- A 48 bit subkey is generated from the main 56-bit key using a key schedule.
- The expanded R is XORed with the subkey: R-expanded $\oplus$ subkey.

IT-21016

Q-20 Ans:

Given: $R_0 = 0_x$ FOFOFOFO

Round key $K_1 = X_0$ OFOFOFOF

$L_0 = 0_x$ AAAAAAAA

Step-1: Compute $f(R_0, 14)$ assuming XOR operation only

$f(R_0, 14) = R_0 \oplus R_1 = 0_x$ FOFOFOFO $\oplus$ 0_x OFOFOFOF

Perform XOR byte-wise:

- FO $\oplus$ OF = FF
- FO $\oplus$ OF = FF
- FO $\oplus$ OF = FF
- FO $\oplus$ OF = FF

So, $f(R_0, 14) = 0_x$ FFFFFFFF

Step-2: Compute $L_1 = R_0 = X_0$ OFOFOFOF

Step-3: Compute $R_1 = L_0 \oplus f(R_0, 14)$

- $R_1 = 0_x$ AAAAAAAA $\oplus$ 0_x FFFFFFFF

XOR byte-wise:

- AA $\oplus$ FF = 55
- AA $\oplus$ FF = 55
- AA $\oplus$ FF = 55
- AA $\oplus$ FF = 55

So, $R_1 = 0_x$ 55555555

$\therefore L_1 = 0_x$ FOFOFOFO, $R_1 = 0_x$ 55555555

(Answer).

IT-21016

Q-21 Ans:

Given the input word:

[0x23, 0xA7, 0x4C, 0x19]

use the following partial AES, S-box to perform the subbytes transformation provide the result output word.

↓Row \ Col →	3	4	7	9	A	C
1	6D	.	.	C6	.	.
2	D4	.	.	.	.	.
4	.	A1	.	.	.	2E
A	.	.	63	.	D2	.

Given Input word: [X.23, 0xA7, 0x4C, 0x19]

Partial AES S-box table:

Row\Col →	3	4	7	9	A	C
1	6D	.	.	C6	.	.
2	D4	.	.	.	.	.
4	.	A1	.	.	2E	.
A	.	.	63	D2	.	.

For each byte, the high nibble (4 bits) is the row and the low nibble is the column.

IT-21016

Q-22 Ans:

The Add Roundkey step in AES encryption involve performing a bitwise X-OR operation between the input word and the round keyword,

Given: input word: [0x14, 0x2B, 0x3C, 0x4D]

Round keyword: [0x55, 0x66, 0x77, 0x88]

Compute the output word (XOR each byte)

Solution (byte-wise XOR):

$0x1A \oplus 0x56 = 0x4F$ ($00011010 + 01010110 = 01001111$)

$0x2B \oplus 0x66 = 0x4D$ ($00101011 \oplus 01100110 = 01001101$)

$0x3C \oplus 0x77 = 0x4B$ ($00111100 \oplus 01110111 = 01001011$)

$0x4D \oplus 0x88 = 0xC5$ ($01001101 \oplus 10001000 = 11000101$)

Resulting output word: [0x4F, 0x4D, 0x4B, 0xC5]

Explaination: The Add Roundkey step performs a bitwise XOR between each byte of the round key producing the output word shown above.

RT-21016

Q-23 Ans:

The MixColumns operation in AES works by multiplying each column of the state matrix by a fixed matrix over the Galois field GF(2^8). Given that,

Input column (bytes):

$$a = \begin{bmatrix} a_0 \\ a_1 \\ a_2 \\ a_3 \end{bmatrix} = \begin{bmatrix} 0x01 \\ 0x02 \\ 0x03 \\ 0x04 \end{bmatrix}$$

MixColumns matrix:

$$M = \begin{bmatrix} 02 & 03 & 01 & 01 \\ 01 & 02 & 03 & 01 \\ 01 & 01 & 02 & 03 \\ 03 & 01 & 01 & 02 \end{bmatrix}$$

So the output column is $b = M \cdot a$ where each entry is byte-wise GF(2^8) arithmetic (XOR ⊕ for addition)

Multiplication rules used (AES)

- Multiply by 01: value itself
- Multiply by 02 (called x time): left shift
- Multiply by 03: $03 \cdot x = 02 \cdot x \oplus 01 \cdot x$

IT-21016

Q-25 Ans

AES Modes causing Error Propagation:

Some AES Modes Error Propagation cause an error in a ciphertext block to affect multiple plaintext blocks during decryption. This reduces the integerity of the decrypted message because even a single-bit error can corrupt more that one block.

CBC (Cipher block chaining)

→ Decryption formula: $P_i = AES^{-1}(c_i) \oplus C_{i-1}$

→ Effort effect:

- if c_i has a 1-bit error → P_i completely random
- The same bit position in P_{i+1} will also be flipped

CFB (Cipher Feedback) Mode

→ Decryption Formula: $P_i = c_i \oplus AES(c_{i-1})$

→ Error effect:

- if c_i has a 1-bit error → the same bit in P_i is wrong
- P_{i+1} becomes completely random
- After that, decryption returns to normal.

IT-2016

Q-26 Ans

Recommended Modes: AES-CTR° (Counter-Mode)

Justification:

- Parallel processing
  - In CTR, each block is encrypted by XORing the plaintext with a key stream generated from AES (key, counter)
  - The counter values for all blocks are known in advance, so encryption and decryption of different blocks can happen independently and in parallel.
- Performance:
  - No chaining between block - faster than CBC for large files
- Security
  - Unlike ECB, CTR does not produce identical ciphertext for identical plaintext blocks.
  - As secure as CBC when IV/nonce is unique.

IT-21016

Why not ECB?

- Reveals patterns in the data - insecure for large files.

Why not CBC?

- Each block depends on the previous ciphertext block → Cannot be parallel in cryption

For large file encryption with parallel processing AES-GR is best because it is secure and highly parallelizable.

Q-27 Ans:

Given, $M=1$, $C=5$, $n=14$, $d=11$

Encryption: $C \equiv M^e \bmod n = 1^5 \bmod 14 = 1$

Decryption: $M = C^d \bmod n = 1^{11} \bmod 14 = 1$

Why this works: RSA relies on $M^{ed} \equiv M \pmod n$ when $ed \equiv 1 \pmod{\phi(n)}$.

RT-21016

Here, $\phi(14) = 6$ and $e.d = 5.11 = 55 \equiv 1 \pmod 6$

So, decryption recovers M.

∴ Ciphertext $c = 1$ and Decrypted Message, $M = 1$

Q-28 Ans:

Given: hash $H(m) = 5$, $d = 3$, $n = 33$

Signature generation (Sign with private key d):

We need to general a digital signature for a message hash.

- The message hash is $H(m) = 5$
- The RSA private key is $P_S(d, n) = (3, 33)$
- The digital signature s is computed using the formula:

$$S = H(m)^d \pmod n$$

$$S = 125 \pmod{}$$

- $125 = 3 \times 33 + 26$, So, $125 \pmod{33} = 26$
- The Digital signature is 26.

IT-21016

Q-29 Ans:

We'll compute the public keys for aleya and Badal based on the Diffie-Hellmen protocal.

- Public values: prime modulo p = 17, base g = 3.
- Aleya's private key : a = 4
- Badal's private key : b = 5
- Aleya's public key (A):
  - → $A = g^a \pmod p = 3^4 \pmod{17} = 81 \pmod{17}$
  - → $81 = 4 \times 17 + 13$. So $81 \pmod{17} = 13$
  - → Aleya's public key is 13
  - → Badal's public key (B):
  - → $B = g^b \pmod p = 3^5 \pmod{17} = 243 \pmod{17}$
  - → $243 = 14 \times 17 + 5$, so, $243 \pmod{17} = 5$
  - → Badal's public key is 5

IT-21016

Q-30 Ans:

Definition:

$$H(x) = (\Sigma \text{ ASCII(chars in } x)) \pmod{100}$$

ASCII values: A = 65, B = 66

Compute hashes:

$H("AB") = (65+66) \bmod 100 = 131 \bmod 100 = 31$

$H("BA") = (66+65) \bmod 100 = 131 \text{ and } 100 = 31$

Result:

Both "AB" and "BA" produce the same hash → collision

Collision Resistance:

- The two different messages, "AB" and "BA" produce the same hash value. This is called collision.
- This hash function is not collision resistant because it's based on a simple modular sum.

IT-21016

Q-31 Ans:

Given, message, M = 15, K = 7

Compute MAC:

$$MAC = (15 * 7) \bmod 17 = 22 \pmod{17} = 5$$

Attacks scenario: Suppose attacker's changes message to M' = 10 but does not knows K

Read MAC m' is:

$$MAC' = (10 + 7) \bmod 17 = 17 \pmod{17} = 0$$

Why forging is easy (Explain):

Because MAC is Linear: $MAC = M + K \pmod{17}$

if, attacker knows one valid pair (M, MAC) and wants to create M' = M + 4, they can compute MAC' = 5 + 12 = 17 = 0, which matches the true MAC.

Conclusion: This MAC is insecure it is trivially forgeable because it leaks linear relation with the message.

CT-21016

Q-32 Ans:

TLS Handshake steps and symmetric key Establishment:

1. Client Hello: Client sends supported TLS version, cipher suites, random numbers.
2. ServerHello: Server selects TLS version and cipher suite sends its random number
3. Server certificate: Contains servers public key, signed by CA for Authentication,
4. Key Exchange → • RSA Mode
   • ECDHE / DHE Mode
5. Pre-Master Secrete: → Master secret
6. Session Key: From master secret
7. Finished Messages → Both parties send encrypted "Finished" message to confirm the handshake.

IT-21016

Q-33 Ans:

SSH refers to "secure shell" is a protocol that provides a secure channel over an unsecured network. It has a layered architecture consisting of three main layers.

1. Transport layer protocol:

This is the lowest layer, responsible for managing the secure connection:

- → Handles encryption
- → integrity protection
- - compression

2. User Authentication Protocol:

This layer runs on top of the transport layer and handles client authentication.

3. Connection Protocol:

Multiplexes the encrypted channel into multiple logical channels. This is the highest layer.

IT-210/b

Q-34 Ans:

TLS handshake process steps:

1. Client Hello → purposes connection parameters
2. Server Hello → Proposes connection parameter
3. Certificate → ~~Proposes conn~~ and key exchang
4. Generate Master secrit
5. Generate session keys
6. Finished Messages
7. Secure communication.

Q-35 Ans:

The general form of an elliptic curve equation over a finite field is:

$$y^2 = x^3 + ax + b \pmod p$$

Here, p is a large prime number that defines the finite field, and a and b are constants such that

$$4a^3 + 27b^2 \neq 0 \pmod p$$

ensures no singularities)

IT-21016

Use in cryptography:

Provides a group structure for Elliptic curve cryptography (ECC), enabling secure key exchange, signature and encryption with smaller keys.

Q-36 Ans:

Elliptic curve ~~cor~~ cryptography (ECC) is a public key cryptography technique that provides the same cryptographic strength as RSA but with much smaller key sizes. The main reason lies in the underlying mathmatical problems.

Mathematical Foundation:

→ RSA is based on the Integer factorization problem (IFP)

→ ECC is based on the Elliptic curve ECDLP.

RT-21816

Key size comparison:

- Ecc 256-bit ≈ RSA 3072-bit security level
- ECC 384-bit ≈ RSA 7680-bit security level

Conclusion:

Ecc provides strong security with reduced key sizes due to the computational handles of the ECDLP compared to integer.

Q-37 Ans

Given that,

Curve: $y^2 \equiv x^3 + 2x + 3 \pmod{97}$

point: $P = (3,6)$

$LHS = y^2 = 6^2 = 36 \pmod{97}$

$RHS = x^3 + 2x + 3 = 27 + 6 + 3 = 36 \pmod{97}$

Since, L.H.S = R.H.S. point lies on the curve.

IT-21016

Q-38 Ans:

To compute the ElGamal ciphertext, we use the following public values:

$p = 23$, $g = 5$, $h = 8$, and the message $m = 10$, The random number is $k = 6$.

The ciphertext consist of two points (C_1, C_2)

C_1 computation:

$$C_1 = g^k \pmod p$$
$$C_1 = 5^6 \pmod{23}$$
$$5^2 = 25 \equiv 2 \pmod{23}$$
$$5^4 = (5^2)^2 = 2^2 = 4 \pmod{23}$$
$$5^6 = 5^4 \times 5^2 = 4 \times 2 = 8 \pmod{23}$$

So, $C_1 = 8$

C_2 computation: $C_2 = m \times h^k \bmod p$

First, we calculate h^k: $h^k = 8^6 \pmod{23}$

$$8^2 = 64 = 2 \times 23 + 18 \equiv 18 \pmod{23}$$
$$8^4 = (8^2)^2 = 18^2 = 328 = 14 \times 23 + 2 \equiv 2 \pmod{23}$$
$$8^6 = 8^4 \times 8^2 = 2 \times 18 = 36 = 12 * 23 + 13 \equiv 13 \pmod{23}$$
$$C_2 = 10 \times 13 \pmod{23} = 130 \pmod{23}$$
$$130 = 5 \times 23 + 15 = 15 \pmod{23}$$

So, $C_2 = 15$

$C_1, C_2 = (8, 15)$