Q.1: Quantum computing poses a significant threat to traditional public key cryptosystems based on integer (RSA) and the discrete logarithm problem.

Implications of Quantum computing

(i) Breaking Public-key cryptosystem.
(ii) Impact on secure communication
(iii) Need for Post-Quantum cryptography.

Post Quantum Cryptographic

(i) Lattic Based
(ii) Code based
(iii) Multivariate.
(iv) Hash-Based
(v) Isogeny-Based

Algorithm Resist Quantum

(i) Lattic Problem
(ii) Error-correcting code Problem
(iii) Multivariate equation.

172611

Q.1: Quantum computing poses a significant threat to traditional public key cryptosystems based on integer (RSA) and the discrete logarithm problem.

Implications of Quantum computing

(i) Breaking Public-key cryptosystem.
(ii) Impact on secure communication
(iii) Need for Post-Quantum cryptography.

Post Quantum Cryptographic

(i) Lattic Based
(ii) Code based
(iii) Multivariate.
(iv) Hash-Based
(v) Isogeny-Based

Algorithm Resist Quantum

(i) Lattic Problem
(ii) Error-correcting code Problem
(iii) Multivariate equation.

J723611

3. Traditional ciphers (Classical Encryption Methods)

- Caesar cipher
  - (i) Description
  - (ii) key Length
  - (iii) Encryption speed
  - (iv) security
  - (v) vulnerability
- Vigenere cipher
  - (i) Description
  - (ii) key length
  - (iii) Encryption speed
  - (iv) security
- Playfair cipher
  - (i) Description
  - (ii) key length
  - (iii) Encryption speed
  - (iv) security
  - (v) vulnerability

2. Modern symmetric cipher

DES

- (i) Description
- (ii) key Length
- (iii) Encryption speed
- (iv) security
- (v) key size is to small.

AES (Advanced Encryption standard)

- (i) Description.
- (ii) key length.
- (iii) Encryption speed.
- (iv) Security :

General strengths of Modern

- (i) Stronger key Lengths
- (ii) Improved confusion and Diffu
- (iii) Resistant to Statistical Attacks
- (iv) Versatile and Efficient.

Q4. given that, $S_4 = \{1, 2, 3, 4\}$

For $\sigma \in S_4$ and 2- element subset $\{a, b\}$ of $\{1, 2, 3, 4\}$

$$\sigma \cdot \{a, b\} = \{\sigma(a), \sigma(b)\}$$

$\sigma \in S_4$ to a 2- element subset is still a 2- element of $\{1, 2, 3, 4\}$

This ensure that $\sigma \cdot \{a, b\} = \{\sigma(a), \sigma(b)\}$ is a valid 2 element subset of $\{1, 2, 3, 4\}$

Thus, the action is well-defind.

orbit of $\{1, 2\}$

The number of ways to choose a 2- element subset from $\{1, 2, 3, 4\}$ is

$$\binom{4}{2} = 6$$

These subsets are:

$\{1, 2\}, \{1, 3\}, \{1, 4\}, \{2, 3\}, \{2, 4\}, \{3, 4\}$

By the orbit - stabilizer theory

$$|S_4| = |\text{orbit}(\{1, 2\})| \times |\text{stabilizer}(\{1, 2\})|$$

since $|S_4| = 24$, and we found

$$|\text{orbit}(\{1, 2\})| = 6 \quad |\text{stabilizer}(\{1, 2\})| =$$

$$24 = 6 \times 4$$

IT23111

Q. 5 :- we are given the finite field GF(2). constructed the irreducible polynomial x^2+x+1 over GF(2).

$GF(2^2) = \{0, 1, \alpha, \alpha+1\}$

$\alpha^2 + \alpha + 1 = 0$

$\alpha^2 = \alpha + 1$

we can use this identity for all calculation in GF(E)

The nonzero elements of $GF(2^2)$ are

$G = \{1, \alpha, \alpha+1\}$

Closure.

$1.\alpha = \alpha$

$1.(\alpha+1) = \alpha+1$

$\alpha.(\alpha+1) = \alpha^2+\alpha = (\alpha+1)+\alpha = 1$

$\alpha.\alpha = \alpha^2 = \alpha+1$

$(\alpha+1)(\alpha+1) = \alpha^2 + 2\alpha + 1 = \alpha^2 + 1 = (\alpha+1)+1 = \alpha$

Inverse

$1^{-1} = 1$

$\alpha = \alpha+1$, so $\alpha^{-1} = \alpha+1$

for $\alpha+1$, we solve $(\alpha+1).\alpha = 1$

$G(g^0, g^1, g^2)$

- $\alpha^1 = \alpha$
- $\alpha^2 = \alpha+1$

$\alpha^3 = \alpha(\alpha+1)$

Thus G is cyclic, generator by either α or

IT 2364

Q.6 ⇒

The general linear group $GL(2,R)$ consist of all 2×2

$$GL(2,R) = \{A \in M_{2\times 2}(R) \mid \det A \neq 0\}$$

A scalar matrix is a

$$\lambda I = \lambda \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$$

matrix form subgroup

$$Z(GL(2,R)) = \{\lambda I \mid \lambda \in R^*\} = R^* I$$

where $R^* = R \setminus \{0\}$ group of non zero real numb

A sub group H of G is normal if for normal

for every $g \in G$ and every $h \in H$,

$$ghg^{-1} \in H$$

Let $S = \lambda I$ be a scalar matrix and $A \in GL$

Then, $A(\lambda I)A^{-1} = \lambda(AIA^{-1}) = \lambda(AA^{-1}) = \lambda I$

IT23611

Q7. Diffie-Hellman key Exchange Protocol.

Protocol steps

1. Public Parameters
2. key Exchange Process

$$A = g^a \cdot \text{mod } p$$

$$B = g^b \text{ mod } p$$

3. computing the shared secret

$$s = B^a \text{ mod } p = (g^b)^a \text{ mod } p$$

$$s = A^b \text{ mod } p = (g^a)^b \text{ mod } p$$

Common Attacks and Security Considerations.

1. Man-in-the middle Attack.
2. Mitigation
3. Small Prime modulus Attacks
4. Login attacks

IT23611

Q8.

Proof:

Let H_1 and H_2 be subgroups of a group G. We need to show $H_1 \cap H_2$ is also a subgroup of G.

1. Closure under the group

If $a, b \in H_1 \cap H_2$, then $a \in H_1$ and $a \in H_2$, and similarly $b \in H_1$ and H_2.

Hence $H_1 \cap H_2$ is closed under the operation.

2. Existence of the identity element.

Therefore, $e \in H_1 \cap H_2$ ensuring that $H_1 \cap H_2$ contains the identity elements.

3. Closure under inverses:

If $a \in H_1 \cap H_2$, then $a \in H_1$ and $a \in H_2$

since both H_1 and H_2 are subgroups the inverse of

Therefore $a^{-1} \in H_1$ and $a^{-1} \in H_2$ implying that $a^{-1} \in H$

This confirms that $H_1 \cap H_2$ is closed under under inverses.

IT23611

8.9. Proof the Z_n is commutative:

The ring Z_n consists of the set $\{0, 1, 2, \ldots, n-1\}$ with addition and multiplication defind module n. To show that Z_n is commulatitive, we chack the commutativity of multiplication:

For any two element $a, b \in Z_n$,

$$a.b = b.a \pmod n.$$

Hence, Z_n is a commutative ring

Identifying zero Divisor in Z_n:

An element $a \in Z_n$ is a zero divisor if there exists a nonero $b \in Z_n$ such that

$$a.b = 0 \pmod n$$

The occurs if and only if $\gcd(a, n) \neq 1$. in this a is not Invertible and has a nontrivial mu that is conjurent to zero modulo n.

I723611

B. to vulnerabilities of the DES cipher

1. short key length
2. to brute force attacks
3. weakness to cryptanalysis
4. small block size

How AES address DES shortcomings

1. increasing key size
2. larger block size
3. stronger cryptographic structure

- AES is based on the Rijndael cipher which uses a substitution - permutation network rather than the feistel structure of DES

- It is designed to resist modern cryptanalytic techniques like differential cryptanalysis, linear cryptanalysis, and related-key attacks.

DES is small key size and vulnerability to brute-force attacks. AES with is larger key sizes and stronger cryptographic design.

IT23611

Q.11.

Feistel structure of DES and Different cryptanalysis

① Avalanche Effect: The feistel structure ensure that even a small change in the plaintext propagates rapidly across multiple rounds.

② s-box Non-linearity: The key defense of DES against different cryptanalysis lies in the box used its feistel function.

③ Permutation (P-box): The permutation step in the feistel function future diffuse difference across the cipher's state.

④ 16 Round of Encryption: The multiple rounds of DES

AES Resistance Against Differental Cryptanalysis

① SubBytes (S box Layer): AES employs a highly non-linear s-box that is based on the inverse in GF(2^8)

② shiftRow (Row shuffling): This step shifts the bytes the state matrix.

③ Mix Columns: MixColums applies matrix multiplicat in GF(2^8), which spreads small.

④ AddRoundKey

⑤ More Round and stronger Non-linearity.

I723611

Q12. Finding the modular Inverse using the Extended Euclidean Algorithm

The modular inverse of an integer a modulo n is an integer x such that:

$$a.x \equiv 1 \pmod{n}$$

This are comprime ($\gcd(a,n) = 1$) The Extended Euclidean Algorithm is used to compute this inverse efficiently.

steps to find the modular Inverse

compute gcd (a,n)

to express $\gcd(a,n) = 1$ as a linier combination

$$ax + ny = 1$$

for some integer x and y.

$3^{-1} \bmod 26$

we need to find x such that

$$3x \equiv 1 \pmod{26}$$

Apply to Euclidean Algorithm to compute gcd(3

$$26 = 3(8) + 2$$
$$3 = 2(1) + 1$$
$$2 = 1(2) + 0$$

since $\gcd(3, 26) = 1$

Back-substituting to express 1 as linear combination of 3 and 26

from $3 = 2(1) + 1$

$1 = 3 - 1(2)$

Subbtining $2 = 26 - 3(8)$

$1 = 3 - 1(26 - 3(8))$

$1 = 3 + 1(26) + 1(3(8))$

$1 = 3(9) - 26(1)$

So $x = 9$ and the modular inverse is $3^{-1} = 9 \pmod{26}$

RSA Key Generation

1. choosing Large Prime Numbers
2. choosing a Public key Exponente
3. computing the Private key Exponent d:

Important of Effeiency in large-scale cryptographic System.

1. RSA uses very large Numbers
2. key generation speed
3. Security considerations.

Q.13 insecurity of ECB mode for highly Redundant Data.

in electronic codebook (ECB) mode into fixed blocks (of size n) and encrypted independently the same key.

IT23&4

$c_i = E_k(P_i)$

Why ECB is insecure for Redundant data

The identical Plaintext blocks will always produce identical ciphertext blocks under the same key:

$$P_i = P_j = c_i = c_j$$

This leads to a significant security weakness:

(i) Pattern Leakage.
(ii) No diffusion.
(iii) Lack of semantic security

(ii) CBC mode Encryption and Decryption Recurrence Relation:

In cipher Block chainning (CBC) mode, each Plaintext block is xored encryption history.

Encryption Process

Let P_i be the plaintext block, c_i be the ciphertext block and IV be the initialization vector

$$c_i = E_k(P_i \oplus C_{i-1})$$

IT23611

Decryption Process

To retrieve P_i, we use:

$$P_i = D_K(C_i) \oplus C_{i-1}$$

since xoring twice with the same value cancels out:

$$P_i = (P_i \oplus C_{i-1}) \oplus C_{i-1} = P_i$$

Thus, the original plaintext is recovered.

Error Propagation in CBC Decryption.

(i) Effect on current Block

(ii) Effect on Next Block P_{i+1}

(iii) Effect on subsequent Blocks.

Q.15.

(i) Shannon's Definition of Perfect Secrecy

Shannon's definition of Perfect Secrecy states that knowing the ciphertext provides no additional information about the plaintext.

$$P(P|C) = P(P)$$

(ii) Definition of the One-time Pad (OTP)

The OTP encryption schema is defined as

① Each plaintext P is encrypted using key K

② the ciphertext is computed as

$$C = P \oplus K$$

show that $P(C|P) = P(C)$

for OTP to achieve perfect we must have

$$P(P|C) = P(P)$$

This can be rewritten using Bayes' Theorem:

$$P(P|C) = \frac{P(C|P)\,P(P)}{P(C)}$$

$$C = P \oplus K$$

$$P(K) = \frac{1}{|K|}$$

$$P(C|P) = P(K = C \oplus P) = \frac{1}{|K|}$$

$$P(C) = \sum_{P'} P(C|P')\,P(P')$$

since $P(C|P') = \frac{1}{|K|}$

$$P(C) = \frac{|M|}{|K|}$$

since $|K| \geq |M|$.

$$P(P|C) = \frac{P(C|P)\,P(P)}{P(C)} = \frac{\frac{1}{|K|}\,P(P)}{\frac{|M|}{|K|}} = P(P)$$

Thus $P(P|C) = P(P)$, having perfect secrecy.

IT23611

(iii) Why perfect secrecy is impractical for large scale communication.

(i) Key length Requirement
(ii) Key distribution Problem
(iii) Key Reuse Destroys security
(iv) Lack of Integrity Protection
(v) High Entropy Requirment.

Q.16. Lets compute the first numbers of an LCG sequence using the recurrence relation:

$$x_{n+1} = (ax_n + c) \bmod m$$

$a = 5,\ c = 3,\ m = 16,\ x_0 = 7$

$x_1 = (5 \times 7 + 3) \bmod 16$

$x_1 = (35 + 3) \bmod 16 = 38 \bmod 16 = 6$

$x_2 = (5 \times 6 + 3) \bmod 16$

$x_2 = (30 + 3) \bmod 16 = 33 \bmod 11 = 1$

$x_3 = (5 \times 1 + 3) \bmod 16$

$= 5 + 3 \bmod 16 = 8$

$x_4 = (5 \times 8 + 3) \bmod 16$

$= (40 + 3) \bmod 16 = 43 \bmod 16 = 11$

$\mathbb{Z}_{23}^{11}$

$x_5 = (5 \times 11 + 3) \bmod 16$

$= (55 + 3) \bmod 16 = 58 \bmod 16 = 10$

final Lcg sequence

7, 6, 1, 8, 11, 10.

Q.18. $p = 5,\ q = 11$

$n = p \times q$

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

$M = 2 \quad c = m^e \bmod n$

$c = c^d \bmod n$

$n = 5 \times 11 = 55$

$\phi(n) = (p-1)(q-1) = (5-1)(11-1) = 4 \times 10 = 40$

$1 < e < \phi(n)$

$\gcd(e, \phi(n)) = 1$

$e = 3$

$\gcd(3, 40) = 1$

~~$e = 3$~~ since 3 and 40 are coprime we select

$e = 3$

d satisfies

$d \times e = 1 \pmod{\phi(n)}$

$d \times 3 = 1 \pmod{40}$

$d = 3^{-1} \bmod 40$

$40 = 3(13) + 1$

Rearranging $1 = 40 - 3(13)$, so $d = -13 \pmod{40}$

$d = 27$ (since $-13 + 40 = 27$)

$d = 27$

$M = 2$

$c = M^e \bmod n$

$c = 2^3 \bmod 55 = 8 \bmod 55$

$c = 8$

$M = c^d \bmod n$

$M = 8^{27} \bmod 55$

$8^2 \bmod 55 = 64 \bmod 55 = 9$

$8^4 \bmod 55 = 81 \bmod 55 = 26$

$8^8 \bmod 55 = 21^2 \bmod 55 = 16$

$8^{16} \bmod 55 = 16^2 = 256 \bmod 55 = 36$

$8^{27} = 8^{16} \times 8^8 \times 8^2 \times 8^1 \bmod 55$

$M = (36 \times 16 \times 9 \times 8) \bmod 55$

$= 168 \bmod 55 = 2$

$M = 2$

$e, n = (3, 55)$

$d = 27$

$M = 2, \ c = 8$

$c = 8, \ M = 2$

Q.19. Elliptic curve cryptography (ECC)

$y^2 \equiv x^3 + ax + b \mod p$

$p = 23, \ a = 1, \ b = 1$

The elliptic curve equation is

$y^2 = x^3 + x + 1 \mod 23$

$P(3, 10)$

A point $P(x, y)$ lies on the curve

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

$P = (3, 10)$

$10^2 \equiv 3^3 + 1(3) + 1 \mod 23$

$100 \equiv 27 + 3 + 1 \mod 23$

$100 \equiv 31 \mod 23$

$100 \equiv 31 - 23 = 8 \mod 23$

Q.20. ECDSA calculation on the elliptic curve

$y^2 = x^3 + 7x + 10 \mod 37$

$G = (2, 5), \ n = 19, \ d = 7, \ H(M) = 8, \ k = 3$

$Q = dG$

The public key

$Q = dG = 7G$

IT23611

for two identical points $P = (x_1, y_1)$

$$\lambda = \frac{3x_1^2 + a}{2y_1} \bmod p$$

$a = 7$, $P = (2, 7)$

$$\lambda = \frac{3(2^2) + 7}{2(7)} \bmod 37$$

$$\lambda = \frac{3(4) + 7}{14} \bmod 37$$

$$\lambda = \frac{12+7}{14} \bmod 37 = \frac{19}{14} \bmod 37$$

$14^{-1} \equiv 26 \bmod 37$

$\lambda = (19 \times 26) \bmod 37$

$\lambda = 494 \bmod 37 = 494 - (37 \times 13) = 494 - 481 =$

$x_3 = \lambda^2 - 2x_1$ and 37

$x_3 = 13^2 - 2(2) \bmod 37$

$x_3 = 169 - 4 \bmod 37 \equiv 165 \bmod 37 = 165 - (37$

$= 165 - 148 = 17$

$y_3 = \lambda(x_1 - x_3) - y_1 \bmod 37$

$= 13(2-17) - 7 \bmod 37$

$= 13(-15) - 7 \bmod 37$

$= -195 - 7 \bmod 37$

$= -200 \bmod 37 = (-200 + 5 \times 37) = (-20$

$= -15 \equiv 22 \bmod 37$

Thus $2Q = (17, 22)$

IT23611

Compute $4a = 2(2a)$

$$\lambda = \frac{3(17^2)+7}{2(22)} \bmod 37$$

$$= \frac{3(289)+7}{44} \bmod 37$$

$$= \frac{867+7}{44} \bmod 37$$

$$= \frac{874}{44} \bmod 37$$

Computing modular inverse of $44 \bmod 37$

$$44 = 7 \bmod 37$$

$$7^{-1} \equiv 16 \bmod 37$$

$$\lambda \equiv (874 \times 16) \bmod 37$$

$$= 13984 \bmod 37$$

Computing modulo 37,

$$\lambda = 13984 - (37 \times 378) \equiv 13984 - 13986 =$$

$$-2 \equiv 35 \bmod 37$$

$$x_4 = \lambda^2 - 2x_2 \bmod 37$$

$$y_4 = \lambda(x_2 - x_4) - y_2 \bmod 37$$

[redacted]

[redacted]

Q21.

① Essential characteristics of a secure Hash function.

1. Pre-image (one-way property)
2. Second Pre-image Resistance.
3. Collision Resistance
4. Avalanche Effect
5. Deterministic and fast computation

⑪ Impact of Hash output Length on security.

The length of the hash output directly impacts the security level

1. Resistance to Brute force Attacks
2. Collision Resistance and Attacks Probability
3. Trade-off Between Security and Performance

⑪ Real-world Application of SHA

① Digital signatures
② Blockchain and Cryptocurrencies
③ Password Hashing & Storage.
④ Integrity Verification
⑤ Menage Authentication code

IT23611

Q23.

① Shortest vector problem (SVP) and its Role in Lattice-Based cryptography

The shortest vector problem (SVP) is a fundamental problem in lattice-based cryptography.

1. Why is SVP Hard?

finding the shortest vector is computationally hard. The best known classical algorithms for SVP.

2. Role in cryptographic security

Lattice-based cryptographic schemes derive their security from approximate versions.

② Lattice Based cryptography vs. Traditional cryptography (RSA & ECC)

cryptosystem	Security Assumption	Impact
RSA	factoring large integers	Shor's algorithm in polynomial
ECC	solving the Discrete Logarithm Problem	Shor algorithm in polynomial
Lattice-Based	Hardness of SVP, LWE and other lattice problems	No known algorithm there

IT23611

(iii) Quantum cryptography vs. Lattice-Based cryptography.

Lattic-Based cryptography —— Quantum cryptography

① Computational complexity problem. — ① Laws of quantum mechanics theorem.

(ii) Develop classical cryptographic systems that resist quantum attacks — (iv) use quantum hardware photo, quantum key.

(v) Post-quantum encryption — (vi) Quantum key Distribution protocol.

Q25.

① Process of signing menage using and LWM-Based signature scheme

1. Key Generation: Generate a secret key S_K and corresponding public key P_K.

2. Signing: Given a menage M, generate a sig σ that proves knowledge of the S_K key S_K without revealing it.

3. Verification: The verifier uses the public key to check whether σ is a valid signature on M.

(ii) signing a message M using and LWE Ba... Schema.

Step 1: Key Generation

Public matrix $A \in Z_2^{n \times m}$

Secret key $Su \in Z_2^m$

error vector $e \in Z_2^n$

Public key is

$$Pu = A \cdot Su + e \pmod 2$$

The public key (A, Pu) is published.

Step 2: signing the message M

(i) Hash the message

(ii) Generate a Random Mask r:

(iii) Computer a commitment $r \in Z_2^m$

(iv) Generan a challage C

$$c = H(t, M)$$

(v) Computer the Response z:

$$z = r + c \cdot Su \pmod 2$$

(vi) Output the signature

$$\sigma = (z, c)$$

Step 3 Verification

(i) Recompute commitment t':

IT2364

$$H' = H.z - e.P_k \pmod 2$$

(iv) check Hash consistency of $H(H', m)$

Role of LWB in Ensuring security

(i) Unforgeability

(ii) zero-knowledge property.

(iii) collision Resistance.

IT23611