Q.1 IT-24620

Quantum Computing and Post Quantum Cryptography?

Quantum Computers can break RSA and ECC using Shor's algorithm, which efficiently solves factoring and discrete logarithm problems. To replace them post-quantum algorithm like lattice-based, hash-based and code-based cryptography are proposed. They resist quantum attacks because they rely on problems like learning with Errors (LWE) which remain hard even for quantum computers.

Q2

2. PRNG code in python IT24620

```
import time, os

def prng(mod = 1000):
    seed = int(time.time() * 1000)
           + os.getpid()
    return ((seed * 1103515245
           + 12345) % mod)
print(prng())
```

(Q3)

IT-24620

3. Traditional vs Modern Symmetric cipher

Ans: Traditional ciphers (Caesar, vigenere) use simple substitution and are easily broken by frequency analysis. Modern ciphers like AES and DES use complex, large key sizes and resist modern cryptoanalysis. AES is highly secure, while DES is weak today due to its short 56-bit key.

(Q-4) IT-24620

4. Action on S_4 on 2-element subset

Ans: $\sigma(\{a,b\}) = \{\sigma(a), \sigma(b)\}$

This is well defined because permutation map elements uniquely.

orbit of $\{1,2\}$: all 2-subset → size

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

Stabilizer: permutation fixing the set $\{1,2\}$

→ size 4

$$|\text{orbit}| \cdot |\text{Stabilizer}| = 6 \cdot 4 = 24 = |S_4|$$

2. (10-5) IT-24820

Field GF (2^2) using x^2+x+1

i) Multiplicative Group

GF(2^2) has elements:

$\{0, 1, \alpha, \alpha+1\}$

The nonzero element from a group under multi-plication because they have inverses.

ii) Cyclic Nature

The nonzero set has 3 elements:

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

A group of order 3 is always cyclic, so GF(2^2) is cyclic.

(Q-6) IT-24620

Scalar matrices Normal subgroup in $GL(2,R)$

Ans: Scalar Matrices are of the form

$$\lambda I, \quad \lambda \neq 0$$

They form a subgroup since:

Closed: $(\lambda I)(\mu I) = (\lambda\mu) I$

Inverse: $(\lambda I)^{-1} = \lambda^{-1} I$

Normality: for an $A \in GL(2,R)$

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

Scalar matrices from a normal

subgroup.

factor Group: $GL(2,R) / \{\lambda I\}$

This is called projective linear group $PGL(2,R)$.

(Q.7)

Diffie - Hellman key exchange

Ans: Public: prime p, generator g

Alice picks secret a, sends $g^a \bmod p$

Bob picks secret b, sends $g^b \bmod p$

Shared key: $K = g^{ab} \bmod p$

Security relies on the Discrete logarithmic problem.

Man-in-the-middle attack: Attacker intercepts and replaces keys → solved using authentication.

(Q-8)

Intersection of subgroups

Let $H_1, H_2 \leq G$

Then $H_1 \cap H_2$ is non empty.

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

$ab^{-1} \in H_1$ and $ab^{-1} \in H_2$

$ab^{-1} \in H_1 \cap H_2$

Thus intersection is a subgroup

(Q.9) IT-20620

Ring Z_n ~~commutation~~ commutative and Zero Divisors.

Addition and multiplication mod n are commutative:

$$a+b = b+a$$

$$ab = ba$$

Z_n is commutative

Zero divisors exists if n is composite.

Example in Z_6: $2.3 = 0 \bmod 6$

Z_n is a field if n is prime.

(Q10) IT-2420

DES and AES

Ans: DES is insecure because:

→ Key size only 56 bits.

→ Vulnerable to brute force search.

AES solved with:

→ Larger keys: 128/ 192/ 256 bits

→ Stronger structure against cryptanalysis.

So,

AES is modern secure replacement.

(Q-11) IT-24620

Differential ~~Cryptog~~ Cryptoanalysis Resistance

i) DES Feistel Structure: DES feistal rounds provide diffusion but limited. S-box size makes it vulnerable.

ii) AES Resistance: AES uses:

→ Sub Bytes
→ ShiftRows + MixColumns
→ AddRoundKey.

(Q-12) IT-24620

Modular Inverse via Extended Euclidean Algo:

Ans: If $gcd(a, n) = 1$ then

$$ax + ny = 1$$

So, $a^{-1} \equiv x \bmod n$

RSA uses this to compute private key:

$$d \equiv e^{-1} \bmod \phi(n)$$

Efficiency is crucial since RSA uses very large primes.

(Q-13) IT-24620

Block cipher Modes;

i) ECB insecurity: ECB encrypts blocks independently $c_i = E_K(P_i)$

So, identical plaintext block → identical ciphertext blocks.

ii) CBC Recurrence Relation

Encryption: $C_i = E_K(P_i \oplus C_{i-1})$

Decryption: $P_i = D_K(c_i) \oplus C_{i-1}$

(Q-14) IT-24L20

LFSR vulnerability

Ans: LFSR are linear:

$S_{t+k} \geq$ Exist $+1$

known plaintext allows solving linear equations → key recovery.

Mitigation → use non-linear combining functions or filter generators.

(Q-15)

One Time Pad:

i) shannon Perfect secrecy

$$P(M = m \mid C = c) = P(M = m)$$

ciphertext gives no information.

ii) OTP proof:

OTP encryption $= c = M \oplus K$

With uniform randomly key:

$$P(C = c / M = m) = 2^{-n}$$

iii) Impractically:

OTP requires:

→ key as long as message.

→ key must be truly random.

→ key cannot be reused.

(Q-16) IT-24620

LCG: First 5 numbers (seed $x_0 = 7$)

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

Examples values: $a = 5$, $c = 3$, $m = 16$

$x_0 = 7$

$x_1 = (5 \cdot 7 + 3) \bmod 16 = 6$

$x_2 = (5 \cdot 6 + 3) \bmod 16 = 1$

$x_3 = (5 \cdot 1 + 3) \bmod 16 = 8$

$x_4 = (5 \cdot 8 + 3) \bmod 16 = 11$

$x_5 = (5 \cdot 11 + 3) \bmod 16 = 10$

Five outputs are: 6, 1, 8, 11, 10

(Q-17) IT-24620

Ring defination:

A ring is a set R with two operations and such that:

→ (R+) is an abelian group.

→ Multiplication is associative.

→ Distributive laws hold.

Example; $\mathbb{Z}_n$

Rings build finite field using:

$GF(p^n) = Z_p[x] / f(x)$

RSA uses ring arthmatic $\mathbb{Z}_n$

Q-18) IT-24628

RSA encrypt / decrypt (p=5, q=11)

Ans: $n = pq = 55$

$\phi(n) = 4 \cdot 10 = 40$

$e = 3$

$3d \equiv 1 \bmod 40$

$d = 27$

$M = 2$

Encryption: $C = M^e \bmod n$

$= 2^3 \bmod 55$

$= 8$

Decryption: $M = C^d \bmod n$

$= 8^{27} \bmod 55$

$= 2$

RSA signature (p=7, q=3)

$n = 21 \quad \phi(n) = 12$

$e = 5, \quad 5d = 1 \bmod 12$

$d = 5$

Hash $H(m) = 3$

Signature : $S = H(m)^d \bmod n$

$= 3^5 \bmod 21$

$= 12$

verify $= S^e \bmod n$

$= 12^5 \bmod 11$

$= 3$

(9-19) IT-2016201

Elliptic Curve over $p = 23$

Curve $= y^2 = x^3 + x + 1$

i) $P(3, 10)$

L.H.S $= 10^2 = 100 \bmod 23 = 8$

R.H.S $= 3^3 + 3 + 1 = 27 + 4 \bmod 23 = 8$

So, P lies on curve.

ii) Doubling of P

slope: $\lambda = \frac{3x^2 + a}{2y} = \frac{3(3) + 1}{20}$

$= \frac{28}{20} \bmod 23$

$x_3 = \lambda^2 - 2x = 36 - 6 = 30 \bmod 23$

$= 7$

$y_3 = \lambda(x - x_3) = y = 6(3 - 7) = -10$

$= 12$

iii) $P+Q$

$$\lambda = \frac{7-10}{9-3} = \frac{-3}{6} \bmod 23$$

$$= 11$$

$$x_3 = 11^2 - 3 - 9 = 109 \bmod 23$$

$$= 17$$

$$y_3 = 11(3-17) = -10 = -164 \bmod 23$$

$$= 20$$

$$P+Q = (17, 20)$$

9(20) IT-21620

EC DSA example (mod 27, n = 19)

private key d = 9

public key : Q = dG = 9(2,5)

= (8, 12)

Hash : H(m) = 8, K = 3

r = (KG) x mod n

KG = 3G = (5, 9)

r = 5 mod 19 = 5

S = k^{-1} (H + dr) mod n

= 3^{-1} mod 19 = 13

S = 13 (8 + 9.5) = 13 . (53) = 689 mod 19

= 5

Signature: $(r, s) = (5, 5)$

verification uses $w = s^{-1}$, $u_1 = Hw$, $u_2 = rw$

Q(21) IT-29620

SHA hash properties:

i) Secure hash characteristics.

→ Preimage resistance

→ Second Preimage resistance.

→ Collision resistance

ii) Output length effect

SHA-256 gives:

→ Collision security $= 2^{128}$

→ Preimage security $= 2^{256}$

iii) Applications:

→ Digital signature

→ Blockchain integrity

→ Password hashing.

(Q-2 & 8) IT-24620

Galois Field in Cryptography

GF(p): intergers mod prime p

GF(2^n): Polynomials mod irreducible polynomial

used in

→ Ecc point arithmatic

→ AES uses GF(2^8) in MixColumns.

Field arthmatic ensures secure algebra opened.

(Q-23) IT-24620

i) SVP : It Finds shortest non-zero lattice vector → NP-hard security basis for lattice schemes.

ii) RSA / ECC

RSA / ECC broken by shor lattice problems remain hard for quantum computers.

iii) Quantum vs lattice crypto

Quantum crypto uses physics (QKD)

Lattices uses math's hardness assumptions.

(Q-24) IT-24620

LFSR maximum period: If characteristic polynomial is primitive, LFSR generates all non zero states.

Number of non zero states; $2^m - 1$

Thus maximum period; $T = 2^m - 1$

(Q-25) IT-24620

i) LWE - Based signature

Process

1. Key Gen: choose secret vector S

2. Public key: noisy equation As + e

3. Sign: Sample short vector + hash

4. Verify: Check lattice relation holds.

ii) Signing steps

1. Hash message $H(M)$
2. Compute signature :

$$Z = S \cdot H(M) + noise$$

3. verify : $A_2 = PK \cdot H(M)$