IT-23609

Question: 01

With the advancement of quantum computing, traditional public key cryptosystems like RSA and ECC are at risk due to Shor's Algorithm, which can efficiently factor large numbers and compute discrete algorithms in polynomial time. This presents significants security threats to modern cryptographic systems, particularly those used in secure communication financial transactions and digital signatures.

Let discuss how Quantum Computing threatens cryptography

Shor's algorithm can break widely used encryption schemes:

① RSA: RSA relies on factoring large numbers, which Shor's algorithm solves in polynomial time.

② ECC : ECC is based on elliptic curve discrete logarithm problem, which quantum computers can solve efficiently.

Impact of these threates:

① Future quantum computers could decrypt stored encrypted data.

② Digital signature can be forced, enabling identity theft.

③ HTTPs, VPNs and blockchain security will be compromised.

To counteract quantum attacks, new encryption methods are being developed, we can say them post-quantum cryptographic algorithms. The PQC algorithms include:

IT-23609

① Lattice-Based Cryptography: Kyber, Dilithium, NTRU, FrodoKEM are some example of this type of algorithm. They are secure because, hard lattice problems remain difficult for quantum computers.

② Code-Based Cryptography: includes McEliece, this is secure because no known quantum algorithm efficiently decodes random linear codes.

③ Hash-Based Cryptography: includes SPHINCST, XMSS which are secure because they are resistant to Shor's algorithm, larger hashes mitigate Grovers attack.

these algorithms resist quantum attacks by:
i) Mathematical Hardness.
ii) Lack of quantum speed up.
iii) Diversity of approaches.

IT-23609

Question:02 → PRNG Generation

A Pseudo-Random Number Generation (PRNG) is an algorithm that generates a sequence of numbers that appear to be random but are actually deterministic and generated using an initial value called a seed.

Here, A PRNG algorithm using python and considering the current timestamp, the process ID (os.pid) for added randomness, a modulus operation to contain the output.

```
import random
from datetime import datetime
import time
import os
random.seed((time.time.ns() + os.getpid())
            % 10)
for i in range(5):
    print(random.randint(0,100), end = "\t")
```

Question: 03 → Comparison of traditional ciphers and Modern symmetric cipher.

Here a concise comparison table of traditional cipher like caesar, vibinere, playfair and modern symmetric cipher like AES, DES:

features	Traditional Cipher			Modern symmetric cipher	
	caesar	Vibinere	playfair	AES	DES
key length	1 integer (tiny)	Variable (short)	keywords based	56-bits	128, 192, 25-bits.
speed	very fast	Fast	Moderate	Moderate	Fast
security	very weak	weak (if key reused)	Moderate	weak (56-bit key)	very strong
Vulnerabilities	Brute force, frequency analysis	kasiski, frequency analysis	known-plain text, digraph analysis	Brute force, differential cryptoanalysis	Resists all known attack.
Use case	Historical Education	Historical Basic	Historical, Basic	Legacy system	Modern encryption.

IT-23609

Question:04 → Well defined Action, Orbit and Stabilizer Proved

1.) **Well defined Action:** Define the action of S_4 on 2-element subset $\{a,b\}$

And the action σ on $\{a,b\}$

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

identity : The identity permutation e act as identity set:

$$e.\{a,b\} = \{e(a), e(b)\}$$
$$= \{a,b\}$$

Compatibility : for any two permutation.

$\sigma, \tau \in S_4$.

$$(\sigma\tau).\{a,b\} = \{\sigma\tau(a), \sigma\tau(b)\}$$
$$= \sigma.(\tau.\{a,b\})$$

On the other hand,

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

2). Orbits of $\{1,2\}$

S_4 acts transitively on-2-element subset, so the orbits is all 6 subsets.

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

The orbit size is 6.

3) Stabilizer of $\{1,2\}$:

The stabilizer consists of permutation fixing & swapping $\{1,2\}$ and $\{3,4\}$;

Subgroup of $\{1,2\} = \{e, (12), (34), (12)(34)\}$

The stabilizer has size 4.

Question: 05 →

i) Define GF(2^2) elements

Step 1:

GF(2^2) is constructed using the irreducible polynomial x^2+x+1 over GF(2).

The elements of GF(2^2) can be represented as:

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

where 'α' is the root of $x^2+x+1=0$;

meaning $\alpha^2 = \alpha+1$;

Step 02: Multiplication table

Lets construct the multiplication table for GF(2^2)

	0	1	α	$\alpha+1$
0	0	0	0	0
1	0	1	α	$\alpha+1$
α	0	α	$\alpha^2=\alpha+1$	$\alpha(\alpha+1)=\alpha^2+\alpha=(\alpha+1)+\alpha=1$
$\alpha+1$	0	$\alpha+1$	1	$(\alpha+1)^2=\alpha^2+2\alpha+1=(\alpha+1)+0+1=$

Step 03: Verify Group axioms

Closure: From the multiplication table, all products are with in $\{0, 1, \alpha, \alpha+1\}$; so closure are satisfies.

Associativity: Multiplication in a field is associative, so this holds.

Identity: 1 is multiplication identity.
[$\alpha = \alpha \cdot 1 = \alpha$; for any a in $GF(2^4)$].

Inverse: Each nonzero element has an inverse.

Since four axioms are satisfied.

ii) Verify whether the set of all nonzero elements of $GF(2^4)$ is cyclic

IT-2360g

Step:01 :→ Identify nonzero elements

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

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

Step:02 → Check the Generation:

We need to find any element Generate all non zero elements through its power.

1. Element 1:

* $1^1 = 1$
* $1^\alpha = 1$
  * Only Generate $\{1\}$

2. Element α:

$\alpha^1 = \alpha$

$\alpha^2 = \alpha+1$

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

Generate $\{1, \alpha, \alpha+1\}$ ω

3. Element $\alpha+1$,

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

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

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

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

Step:3 : Both α and $\alpha+1$ Generate multiplicative number element of $GF(2^2)$. Though, the set of all nonzero elements of $GF(2^2)$ is cyclic.

Question:06 → $GL(2,R)$ be the general linear group of 2×2 invertible matrices over R.

Step:01: Define the set of scalar matrix

A scalar matrix in $GL(2,R)$ is a matrix of form, $\begin{pmatrix} a & 0 \\ 0 & a \end{pmatrix}$, when, $a \in R$, $a \neq 0$

$$\therefore S = \left\{ \begin{pmatrix} a & 0 \\ 0 & a \end{pmatrix} \mid a \in R,\ a \neq 0 \right\}$$

Step:02 Show that 'S' is subgroup of $GL(2,R)$.

to verify that S is subgroup $GL(2,R)$

1. Closure: if $A = \begin{pmatrix} a & 0 \\ 0 & a \end{pmatrix}$ and

$B = \begin{pmatrix} b & 0 \\ 0 & b \end{pmatrix}$

S is their Product.

$AB = \begin{pmatrix} ab & 0 \\ 0 & ab \end{pmatrix}$; where is also S.

2. Identity: The identity matrix $I, = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$

3. Inverse: if $A = \begin{pmatrix} a & 0 \\ 0 & a \end{pmatrix}$; thus.

$A^{-1} = \begin{pmatrix} \frac{1}{1} & 0 \\ 0 & \frac{1}{1} \end{pmatrix}$

Step:03 Show that S is normal subgroup

A subgroup S is normal if for every $g \in GL(2,R)$ and $s \in S$, the conjugate gsg^{-1} is in S.

Let, $g \in GL(2,R)$ and $s = \begin{pmatrix} a & 0 \\ 0 & a \end{pmatrix} \in S$, thus

$$gsg^{-1} = g \cdot \begin{pmatrix} a & 0 \\ 0 & a \end{pmatrix} \cdot g^{-1}$$
$$= \begin{pmatrix} a & 0 \\ 0 & a \end{pmatrix} \cdot g \cdot g^{-1}$$
$$= \begin{pmatrix} a & 0 \\ 0 & a \end{pmatrix}$$

Thus $gsg^{-1} \in S$ and S is a normal subgroup of $GL(2,R)$.

Step 04 → Construct the factor group :

The factor group $GL(2,R)/S$ consist of the cosets S in $GL(2,R)$. Each coset of the form :

$$gS = \{gs \mid s \in S\}$$

when, $g \in GL(2,R)$

The group operation in $GL(2,R)/S$ is defined by,

$$(g_1 S)(g_2 S) = (g_1 g_2) S.$$

Step 05 The factor Group is isomorphic to the projective general line. Group PGL(2,R); which represents projective transformation of the real projective line.

Question:16

Let's choose specific values for the parameters:

Multiplier $a = 5$, modulus $m = 16$

increament $c = 3$, seed $x_0 = 7$

Using the recurrence relation:

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

we compute the first five values:

1. $x_1 = (5.7 + 3) \mod 16 = 38 \mod 16 = 6$
2. $x_2 = (5.6 + 3) \mod 16 = 33 \mod 16 = 1$
3. $x_3 = (5.1 + 3) \mod 16 = 8 \mod 16 = 8$
4. $x_4 = (5.8 + 3) \mod 16 = 43 \mod 16 = 11$
5. $x_5 = (5.11 + 3) \mod 16 = 58 \mod 16 = 10$

So, Resulting LCG sequence :

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

Question: 18

Public → {e, n}
Private → {d, n}

i) Given that,

$p = 5, \quad q = 11$

$n = p \times q = 5 \times 11 = 55$

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

Choosing public key e.

'e' should be coprime to $\phi(n) = 40$ and $1 < e < 40$

A common choice is $e = 3$ [since $gcd(3, 40) = 1$]

Computing private key d,

'd' is the modulan multiplicative inverse of e modulo $\phi(n)$. i.e.

$d \times e = 1 \mod \phi(n)$

solving for d,

using extended Euclidian Algorithm

$\therefore d = 27$

Encryption: Given, message, $M = 2$

we know, $C = M^e \mod n$

$\Rightarrow C = 2^3 \mod 55$

$\Rightarrow C = 8 \mod 55$

So, ciphertext $C = 8$

Decryption:

we know, $M = C^d \mod n$

$\Rightarrow M = 8^{27} \mod 55$

Using modular exponention,

$M = 2$

So, we successfully recovered the original message

ii) Digital signature

Given, $p = 7, q = 3$.

$n = 7 \times 3 = 21$.

$\phi(n) = 6 \times 2 = 12$

Choosing public key e should be coprime to $\phi(n)$ and $1 < e < 12$

So, the value of e is 5 [$\gcd(5, 12) = 1$]

Compute private key 'd', such that

$d \times e = 1 \mod \phi(n)$

$d \times 5 = 1 \mod 12$

using extended eucledian Algorithm,

we get, $d = 5$

Given, signing the Hash $H(m) = 3$

signature s is computed as:

$$s = H(m)^d \mod n$$

$$\Rightarrow s = 3^5 \mod 21$$

$$\Rightarrow s = 243 \mod 21$$

So, $s = 12$

Verifying the signature,

Compute as: $H'(m) = s^e \mod n$

$\Rightarrow H'(m) = 12^5 \mod 21$

Using modular exponentiation

$H'(m) = 3$

Since, $H'(m) = H(m)$; the signature is vali

Explaining how the signature ensur the integrity and authenticity of the message:

1) Integrity: The hash function ensures that any modification to the message changes the hash, leading to a failed signature verification.

2) Authenticity: Since only the private key can generate a valid signature, verifying it with the public key, confirms that it was signed by the legitimate sender.

3) Non-repudiation: The sender can't deny signing the message because only their private key could have generated the valid signature.

Question: 19

a) Given that,

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

where: $p = 23$, $a = 1$, $b = 1$

Substituting, $a=1$, $b=1$, $p=23$ in the equation, it becomes,

$$y^2 = x^3 + x + 1 \pmod{23}$$

For the point $P(3,10)$

$$10^2 = 3^3 + 3 + 1 \pmod{23}$$

$$\Rightarrow 100 = 27 + 3 + 1 \pmod{23}$$

$$\Rightarrow 100 = 31 \pmod{23}$$

Since, $31 \pmod{23} = 8$

$100 \pmod{23} = 8$

both sides are equal. Thus P lies on the curve.

b) Doubling the point P (Computing 2P)

IT-23609

The formula for point doubling is:

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

$$x_2 = \lambda^2 - 2x_1 \mod p$$

$$y_2 = \lambda(x_1 - x_2) - y_1 \mod p$$

substituting $P(3,10)$

$$\lambda = \frac{3(3)^2 + 1}{2(10)} \mod 23$$

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

$$= 28 \times 20^{-1} \mod 23$$

here, $20^{-1} = 7 \mod 23$

so, $\lambda = 28 \times 7 \mod 23$

$= 196 \mod 23$

$\therefore \lambda = 12$

now,

$x_2 = \lambda^2 - 2x_1 \mod p$

$= (12)^2 - (2 \times 3)$

$= 144 - 6 \mod 23$

$= 138 \mod 23$

$= 0$

$y_2 = \lambda(x_1 - x_2) - y_1 \mod p$

$= 12(3 - 0) - 10 \mod 23$

$= 26 \mod 23$

$= 3$

$\therefore$ so, $P(0,3)$

c) The formula for adding two distinct points, $P(x_1, y_1)$ and $Q(x_2, y_2)$ on a elliptic curve is,

$$\lambda = \frac{y_2 - y_1}{x_2 - x_1} \bmod p$$

$$x_3 = \lambda^2 - x_1 - x_2 \bmod p$$

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

here, $P(3,10)$ and $Q(9,7)$

$$\therefore \lambda = \frac{y_2 - y_1}{x_2 - x_1} \equiv \frac{7-10}{9-3} = \frac{-3}{6} \bmod 23$$

$$= (-3)(6^{-1}) \bmod 23$$

$-3 \bmod 23 = 20$

$6^{-1} \bmod 23 = 4$

$$\lambda = 20 \times 4 \bmod 23$$

$$= 80 \bmod 23$$

$$\equiv 11$$

$x_3 = \lambda^2 x_1 - x_2 \mod p$

$= 11^2 - 3 - 9 \mod 23$

$= 109 \mod 23$

$= 17$

$y_3 = \lambda(x_1 - x_3) - y_1 \mod p$

$= 11(3-17) - 10 \mod 23$

$= -164 \mod 23$

$= 20$

Thus the sum of the points $P(3,10)$, $Q(9,7)$ is $R = (x_3, y_3) = (17, 20)$.

Question 07:

Diffie-Hellman key exchange Protocol:

→ is a cryptographic protocol that allows two parties to securely generate a shared secret over an insecure communication channel without directly transmitting the secret itself.

→ How it works

i) Public setup
ii) Secret choice
iii) key exchange
iv) unblock own layer.

Security of Diffy-Hellman against comm. attacks

i) Man-in-the middle attack
ii) Weak Prime numbers

→ impact of a small prime modulus p

i) if p small → brute force become feasible

ii) Precomputed attacks can quickly solve the DLP for small primes

iii) large well chosen primes (2048 bit) are required for security.

Question: 08 Let G be a group and let H be a subgroup of G. Prove that the intersection of any two subgroup of G is also subgroup of G, provides an example using specific group.

Soln: To prove that the intersection of ~~two~~ Hand K of group subgroup, G is also a subgroup

1. **Closure**: if $a, b \in H \cap K$, then $ab \in H$, and $ab \in K$
   So, $ab \in H \cap K$
2. **Identity**: The identity $e \in H$ and $e \in K$, so
   So, $e \in H \cap K$
3. **Inverse**: If $a \in H \cap K$, then $a^{-1} \in H$ and $a^{-1} \in K$
   So, $a^{-1} \in H \cap K$

Thus, $H \cap K$ is a subgroup of G.

Example: In $G, \mathbb{Z}$ let $H = 2\mathbb{Z}$, $K = 3\mathbb{Z}$, then

$H \cap K = 6\mathbb{Z}$, which is subgroup.

Question → 09

1. Commutivity of $\mathbb{Z}_n$:

* The ring $\mathbb{Z}_n$ is commutative because both addition and multiplication modulo n are commutative operation for any $a, b, \in \mathbb{Z}_n$, $a + b = \text{mod}(a)$ and $a \cdot b \equiv b \cdot a \pmod{n}$

2. Zero divison $\mathbb{Z}_n$: $\mathbb{Z}_n$ has zero divisor if n is a composite number. if $n = k$, where $1 < k, m < n$ then m and not non zero element is $\mathbb{Z}_n$

3. When $\mathbb{Z}$ is field: $\mathbb{Z}_n$ is a field if and only if n is a prime number.

Question 1

Vulnerabilities of the DES cipher:

The DES developing in the 1970 was one of the most widely used symmetric encyption algorithms. However, due to advancement in competing power and encryptanalysis, DES is now consider insecure for modern applied is the main vulnerabilities of DES includes:

i) Short key length
ii) encryption weakness
iii) Brute force attack
iv) small block size.

Brute force attack break DES:

A brute force attack systematically there as possible keys unit the correct is found.

→ with 56-bit key, there are $2^{56} \approx 7.2 \times 10^{16}$ possible keys.

→ modern hardware, such as ASICs, FPGA and cloud based Parallel processing can exhausted this key space quickly.

→ A modern high performance cluster with specialized can test handren of billions as key per sec.

AES addressed in the shortcomings are DES

The advanced encryption standard AES was introduced in 2000 to replace DES and overcome the weakness of the DES algorithm.

→ Increased the key size
→ Resistance to encryption attack
→ Large block size.

IT-23609

Question → 11

How DES handles different cryptanalysis in its feistal structure?

---

i) Complex S boxes

→ DES uses 8 substitution boxes (S box) designed to introduce non-linearity, making it harder to predict how input differences affect output differences.

↳ These S boxes were specialy optimized to resist different cryptanalysis making DES stronger than early block ciphers.

ii) 16 rounds of feistal structure

11

Subbytes (S-Box transformation)

→ AES uses a single, strong S-box based on inverse in $GF(2^8)$ offering better on non-linearity than DES's s boxes

Shift Rows (Byte transposition)

→ shift bytes within the block, increasing diffusion across multiple round.

Mixcolumns (Matrix multiplication)

→ Ensures that a small change in input affects all 128 bits after just a few rounds.

Add round key (key Mixing)

→ XOR's the state with a unique round key, ensuring that each round behaves unpredictability.