

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 significant 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 threats:

- ① Future quantum computers could decrypt stored encrypted data.
- ② Digital signature can be forged, 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:

- Lattice-based
- Multivariate polynomial
- Code-based

① Lattice-Based Cryptography: Kyber, Dilithium, NTRU, FrodoKEM

Dilithium, NTRU, FrodoKEM are some examples of this type of algorithm. They are secure because, hard lattice problems remain difficult for quantum computers.

② Code-Based Cryptography: includes McEliece

McEliece, this is secure because no known quantum algorithm efficiently decodes random linear codes.

③ Hash-Based Cryptography: includes SPHINCST, XMSS

SPHINCST, XMSS which are secure because they are resistant to Shor's algorithm; longer hashes mitigate Grover's attack.

These algorithms resist quantum attacks by:

- i) Mathematical Hardness
- ii) Lack of quantum speed up.
- iii) Diversity of approaches.

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 constrain the output.

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

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

Here a concise comparison table of traditional cipher like Caesar, Vigenere, Playfair and modern symmetric cipher like AES, DES.

features	Traditional Cipher	Modern Symmetric Cipher	
key length	Caesar 1 integer (tiny)	Vigenere Variable (short) based	Playfair Keywords
			AES 56-bits 128, 192, 256-bits.
speed	Very fast	Fast	Moderate
security	Very weak weak (if key reused)	Moderate	weak (56-bit key)
vulnerability	Brute force, frequency analysis	Known-plain text, digraph analysis	Brute force, differential crypto analysis
use case	Historical Education	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 $\{a, b\}$

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

identity: The identity permutation e act as identity set.

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

$$\{e\} = \{a, b\}$$

Compatibility: for any two permutations,

$$\sigma, \tau \in S_4$$

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

on the other hand,

$$\begin{aligned}\sigma(\tau \cdot \{a, b\}) &= \sigma\{\tau(a), \tau(b)\} \\ &= \{\sigma(\tau(a)), \sigma(\tau(b))\} \\ &= \{\sigma \tau(a), \sigma \tau(b)\}\end{aligned}$$

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

S_4 acts transitively on 2-element

subset, so the orbits are 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 $\{1, 2\}$ and $\{3, 4\}$:

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

The stabilizer has size 4.

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

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

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

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

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

Question: 05

i) Define $GF(2^2)$ elements

Step 01:

$GF(2^2)$ 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

Let's construct the multiplication table for $GF(2^2)$

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

Step 103: Verify group axioms

Closure: From the multiplication table, all products are either in $\{0, 1, \alpha, \alpha + \beta\}$; so closure is satisfied.

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

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

Inverse: Each nonzero element has an inverse.

Since four axioms are satisfied.

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

$$\omega = \text{root}(H) \rightarrow \omega^{\infty} = (1+\alpha)^{\infty} \rightarrow \omega^{\infty} = \infty$$

$$\omega^{\infty} = \text{root}(1+\alpha) = \text{root}(\alpha^3 + \alpha) = \alpha^2(1+\alpha)$$

ω	0	α	$\alpha + \beta$
α	ω	0	$\alpha + \beta$
$\alpha + \beta$	α	ω	0
0	$\alpha + \beta$	β	ω

Step 01: → Identity nonzero elements

The nonzero elements of $\text{GF}(2^n)$ 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:

$$* 1^1 = 1$$

$$* 1^\infty = 1$$

+ Only generate. $\{1\}$

2. Element α :

$$\alpha^1 = \alpha$$

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

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

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

3. Element $\alpha+1$,

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

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

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

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 66 $\rightarrow GL(2, R)$ 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, $a \in R$, $a \neq 0$

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

$(1+x) + (1+y) = 2$

$$(1+x) = f(1+x)$$

$$y = f^{-1}(1+x)$$

$$(1+x) \cdot (1+y) = f((1+x))$$

$$\{(1+x, y)\} \text{ is closed}$$

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.

Now $AB = \begin{pmatrix} ab & 0 \\ 0 & ab \end{pmatrix}$ such that is also S .

2. Identity: The identity matrix $I_2 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$

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

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

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 .

$$\therefore gsg^{-1} = (g, g) (g, g)$$

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

$$\gamma s \gamma^{-1} = \gamma \cdot \begin{pmatrix} a & 0 \\ 0 & a \end{pmatrix} \cdot \gamma^{-1}$$

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

$$= \begin{pmatrix} a & 0 \\ 0 & a \end{pmatrix}$$

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

Step 04 → Construct the factor group:

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

$$gS = \{gs_1 | s_1 \in S\}$$

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

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 linear group $PGL(2, R)$; which represents projective transformation of the real projective line.

$$F = \text{ax base} \quad E = \text{dilatation}$$

rotation by θ around the origin

$$\text{in base } (\theta + \alpha x) = \alpha x$$

rotation by θ around the origin

$$F = \text{dilatation } \theta E = \text{dilatation } (\theta + F\alpha) = \theta x + \alpha$$

$$E = \text{dilatation } \theta F = \text{dilatation } (\theta + E\alpha) = \alpha x$$

$$F = \text{dilatation } \theta E = \text{dilatation } (\theta + F\alpha) = \alpha x$$

$$E = \text{dilatation } \theta F = \text{dilatation } (\theta + E\alpha) = \alpha x$$

$$F = \text{dilatation } \theta E = \text{dilatation } (\theta + F\alpha) = \alpha x$$

! Später PGL Rechnung

• GL, PL, PGL, PSL

Question: 16

Let's choose specific values for

the parameters: (a, c) = (5, 3)

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

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

Using the recurrence relation:

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

we compute the first five values:

$$1. x_1 = (5 \cdot 7 + 3) \bmod 16 = 38 \bmod 16 = 6$$

$$2. x_2 = (5 \cdot 6 + 3) \bmod 16 = 33 \bmod 16 = 1$$

$$3. x_3 = (5 \cdot 1 + 3) \bmod 16 = 28 \bmod 16 = 8$$

$$4. x_4 = (5 \cdot 8 + 3) \bmod 16 = 43 \bmod 16 = 9$$

$$5. x_5 = (5 \cdot 9 + 3) \bmod 16 = 58 \bmod 16 = 10$$

So, resulting LCG sequence :

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

Public \rightarrow se, n
Private \rightarrow d, nQuestion: 28

i) Given that,

$$p=5, q=11$$

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

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

Choosing public key e,

'e' should be coprime to $\phi(n) = 40$ and $1 < e < 40$ A common choice is $e = 3$ [since $\text{GCD}(3, 40) = 1$]

Computing private key d,

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

$$dxe = 1 \pmod{\phi(n)}$$

Solving for d,

using extended Euclidean Algorithm

$$\therefore d = 27$$

Encryption: Given, message, $M = 2$

we know,

$$c = M^e \mod n$$

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

$$\Rightarrow c = (2 \times 2 \times 2) \mod 55 = 8$$

$$\Rightarrow c = 8 \mod 55 = 8$$

so, ciphertext $c = 8$

OP = 2 \rightarrow 8 \rightarrow 8
OP = (add of binary sd bluwnk 'S')

[$S = (0, 1, 2)$ b/w 0 & 1] $\Rightarrow S = 2$ si ssions names A

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

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

using modular exponentiation,

$$M = 2^{(27) \mod 4} \times 2^3 = 2^3 = 8$$

so, we successfully recovered the original message \rightarrow b/w 0 & 1

$$FS = b$$

ii) Digital Signature

Given, $p=7, q=3 \Rightarrow n = pq = 21$ \rightarrow No. of digits

$$n = 7 \times 3 = 21$$

$$\phi(n) = (p-1)(q-1) = 12$$

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

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

compute private key 'd', such that

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

$$d \times 5 \equiv 1 \pmod{12}$$

using extended euclidean algorithm,

we get, $d = 5$ and private key

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

signature s is computed as:

$$s = H(m)^d \pmod{n}$$

$$\Rightarrow s = 3^5 \pmod{21}$$

$$\Rightarrow s = 243 \pmod{21}$$

$$\text{so, } s = 12$$

Verifying the signature,

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

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

$$= 2 \times 2 = (m)$$

→ Using modular exponentiation

$$H'(m) = 3^5 \mod (n)$$

Since, $H'(m) = H(m)$, the signature is valid.

■ Explaining how the signature ensures the integrity and authenticity of the message:

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

$$H(m) = 2$$

$$s = 3 \mod 2$$

$$s^e = 3^2 \mod 2$$

$$= 2 \mod 2$$

- 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.