1. Quantum computing threatens RSA and ECC because Shor's algorithm can break the math problems they depend on. This means current encryption and digital signature may become insecure.

Post-quantum cryptography offers safer alternatives such as lattice-based algorithms (Kyber, Dilithium), hash-based schemes, and code-based cryptography. These methods are secure because their underlying problems cannot be efficiently solved by known quantum algorithms, making them resistant to quantum attacks.

2. simple custom PRNG design and its python implementation is explained below -

→ Use the current time stamp for time-based randomness.

→ Use the process ID (PID) to add system-level randomness.

→ Mix them using arithmetic operations.

→ Apply modulus to keep numbers within a fixed range.

Python Code :

```
import time
import os

class SimplePRNG:
    def __init__(self, seed = none):
        if seed is None:
            seed = int(time.time() * 1000) ^ os.
                                        getpid()
        self.state = seed

    def random(self, modulus = 1000):
        self.state = (self.state * 1103515245 +
                        12345) ^ os.getpid()
        return self.state % modulus

prng = SimplePRNG()

for _ in range(5):
    print(prng.random(100))
```

3. Traditional ciphers like the Caesar, Vigenère, and Playfair ciphers are simple and easy to understand. They use small keys and basic rules for encryption and decryption, so they are fast to compute. However, their security is weak. Caesar cipher can be broken by trying all possible shifts, Vigenere can be cracked using frequency analysis, and playfair is vulnerable to known-plaintext attacks. These ciphers are not safe against modern crypto-analysis.

Modern symmetric ciphers such as DES and AES are much stronger. They use larger key sizes and complex mathematical operations, which provide high security. DES uses a 56-bit key and is now considered due to brute-force attacks, while AES supports 128, 192, and 256-bit keys and is currently secure. AES is also very fast and efficient in both hardware and software. Overall, traditional ciphers are mainly useful for learning while modern ciphers are designed to protect real-world data against advanced attacks.

IT24644

4. Let S_4 act on the set of all 2-element subsets of $\{1,2,3,4\}$ as follows:

for $\sigma \in S_4$ and a subset $\{a,b\}$, define

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

Since σ is a bijection, $\sigma(a) \neq \sigma(b)$ when $a \neq b$. Hence $\{\sigma(a), \sigma(b)\}$ is again a 2-element subsets of $\{1,2,3,4\}$. The identity acts trivially, and composition is preserved, so this is a valid group action.

orbit of $\{1,2\}$:

All 2-element subsets can be obtained from $\{1,2\}$ by some permutation in S_4. There are

$$\binom{4}{2} = 6, \text{ such subsets.}$$

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

The stabilizer consists of permutations that map the set $\{1,2\}$ to itself. These can either fix 1 and 2 or swap them, and independently permute 3 and 4. Hence, $|\text{Stab}(\{1,2\})| = 2 \times 2 = 4$. This also agrees with the orbit-stabilizer theorem: $|S_4| = 24 = 6 \times 4$.

IT24644

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

where $\alpha^2 + \alpha + 1 = 0$ so, $\alpha^2 = \alpha + 1$

i) Consider the nonzero-elements $\{1, \alpha, \alpha+1\}$

closure : using $\alpha^2 = \alpha + 1$ all products stay inside the set.

Associativity : comes from polynomial multiplication

Identity : 1 is the multiplicative identity.

Inverse : $\alpha(\alpha+1) = 1$ so each nonzero element has an inverse.

Hence, the nonzero elements of $GF(2^2)$ form a group under multiplication.

ii) Compute powers of α :

$\alpha^2 = \alpha$, $\alpha^2 = \alpha + 1$, $\alpha^3 = 1$

thus $\{1, \alpha, \alpha+1\} = \langle \alpha \rangle$

so the set of all nonzero elements of of $GF(2^2)$ is cyclic.

6. The set of scaler matrix

$$S = \{\lambda I \mid \lambda \in \mathbb{R}^*, \lambda \neq 0\}$$

is a subgroup of $GL(2, \mathbb{R})$. It is normal because for any $A \in GL(2, \mathbb{R})$.

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

The factor group $GL(2, \mathbb{R})/S$ consists of matrices up to nonzero scaler multiples. This group is called the projective general linear group $PGL(2, \mathbb{R})$. It represents linear transformations where scaling is ignored, describing transformation of the real projective line.

7. Diffie-Hellman key exchange is a method that allows two parties to create a shared secret over an insecure network. Both sides agree on a public prime number p and a generator g. Each party chooses a private secret to compute the same shared key. This key is later used for symmetric encryption to secure communication.

The security of diffie-hellman relies on the discrete logarithm problem, which is hard to solve for large primes. An attacker can't easily find the private keys from the public values. However, Diffie-hellman is vulnerable to a man-in-the-middle attack if the exchanged public values are not authenticated. This is why it is usually combined with digital signatures or certificates.

If the prime modulus is not large enough, the discrete logarithm problem becomes easier to solve, allowing attackers to compute the shared secret. This would break the security of protocol, making encrypted communication ~~vul~~ vulnerable to attacks.

8. Let H_1 and H_2 be subgroups of a group G. The identity element ~~of~~ e is in both H_1, and H_2 so $e \in H_1 \cap H_2$.

→ If $a, b, \in H_1 \cap H_2$. then $a, b \in H_1$ and $a, b \in H_2$. Since both are subgroups,

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

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

Hence, $H_1 \cap H_2$ is a subgroup of G.

Ex: Let $G = \mathbb{Z}$, $H_1 = 2\mathbb{Z}$ and $H_2 = 3\mathbb{Z}$

Then $H_1 \cap H_2 = 6\mathbb{Z}$, which is also a subgroup of $\mathbb{Z}$.

9. $\mathbb{Z}_n$ is commutative because addition and multiplication modulo n come from integer operations which are commutative.

$\mathbb{Z}_n$ has zero divisors when n is composite. For example, in $\mathbb{Z}_6$: $2 \cdot 3 \equiv 0 \pmod 6$.

$\mathbb{Z}_n$ is a field if and only if n is prime, since only then every nonzero element has a multiplicative inverse.

10. DES is insecure because it uses a 56-bit key, which is too short and can be broken by brute-force attacks with modern computers. Its small block size also makes

it vulnerable to attacks on large data.

AES was created to overcome these issues. It uses much larger key sizes and a stronger design, making brute-force and cryptoanalytic attacks impractical. Hence AES is secure while DES is obsolete.

11. i) DES Feistel structure :

spreads input differences → only partial exposure to each round.

ii) AES resistance :

→ SubBytes : non linear.

→ ShiftRows + MixColumns : diffusion.

→ AddRoundKey : key mixing.

→ Difficult to exploit differences.

12. Solve $ax \equiv 1 \bmod n$ for x

steps : compute gcd (a, n) recursively

RSA : Compute private key $d = e^{-1} \bmod \varphi(n)$

1T24644

Efficient for large keys → practical RSA encryption / decryption.

13. i) ECB insecurity:

Identical plaintext blocks → identical ciphertext → leaks patterns.

ii) CBC mode:

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

Decryption: $P_i = D_k(C_i) \oplus C_{i-1}$

Error propagation: only 1 block affected.

14. Linearity → Predictable sequences under known plaintext attacks.

Mitigation → use non-linear combination of multiple ~~LSI~~ LFSRs

IT24694

15 i) Shannon : $P(M|C) = P(M)$

ii) One-time pad :

key random, $|K| \geq |M|$ → perfect secrecy.

iii) Impracticality :

→ Requires large, truly random keys for each message.

→ key distribution is difficult.

16. Formula : $x_{n+1} = (a x_n + c) \bmod m$

Ex : $a = 5$, $c = 3$, $m = 16$, $x_0 = 7$ → 6, 1, 8, 11, 10

17. Ring definition : $(R, +, \cdot)$ with additive identity, inverses, associative + distributive

→ Commutative example : Z_n

Non-commutative example : $M_2(R)$

→ Use in cryptography : Provides modular arithmatic for RSA, finite fields, ECC

IT24644

18. $p=5,\ q=11 \rightarrow n=55,\ \varphi(n)=40,\ e=3.$

Encrypt M = 2 : $c = 2^3 \bmod 55 = 8$

Decrypt: M = c^d mod n = 2

19 Sign $H(m)=3,\ d=7 \rightarrow s = 3^7 \bmod 21 = 3$

verify s^e mod n = H(m) → integrity/ authencity.

20. Eqn : $y^2 = x^3 + ax + b \bmod p$

check $p=(3,10)$: verify $10^2 \equiv 3^3 + 1*3 + 1$

$= 31 \rightarrow 100 \bmod 23 = 8$? Not on curve

Doubling; $\lambda = (3x_1^2 + a)/(2y_1)$

Addition : $\lambda = (y_2 - y_1)/(x_2 - x_1), x_3$

$= \lambda^2 - x_1 - x_2,\ y_3 = \lambda(x_1 - x_3) - y_1$

21. Base G = (2,5) n = 19 private d = 9 → Q = dG

Sign H(M) = 8, random k = 3 → compute r, s

verification : check r, s with Q → signature valid.

22 i) Properties : Pre-image resistance, collision resistance, second pre-image resistance

ii) Output length : longer output → harder to find collisions.

iii) Application : Digital signature, block-chain, integrity verification.

23 GF(P) : arithmatic mod prime P

~~GF(2^n)~~

GF(2^n) : used in AES, ECC

Field arithmatic ensures invertibility, diffusion and secure cryptographic operations.

24. i) SVP : Finding shortest non zero vector in lattice → NP-hard.

ii) security vs RSA / ECC : Resistant to shor's algorithm. RSA / ECC broken.

IT2464

iii) Quantum cryptography: QKD ensures secure key exchange, different from lattice based encryption.

25. Max period = $2^m - 1$ if characteristic polynomial is primitive.

→ ensures full utilization of all states except 0.

26. i) key generation: lattic public/private key.

ii) signing: encode message as lattice vector, add small noise.