IT24696

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 algorithm (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 a 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() * 10000) ^ 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, vigenere, 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.

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

for $\sigma \in S_4$ and a subset $a\{a,b\}$ 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 subset 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 is 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, $|Stab(\{1,2\})| = 2 \times 2 = 4$. This also agrees with the orbit stabilizer theorem: $|S_4| = 24 = 6 \times 4$.

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: Corners from polynomial multiplication

Identity: 1 is the multiplicative identity.

Inverse, $\alpha(\alpha+1) = 1$ so each non zero element has an inverse.

Hence, the non zero elements of $GF(2^2)$ from 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 $GF(2^2)$ is cycle.

6. The set of scaler matrix.

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

is a subgroup of $GL(2R)$ It is normal because for any $A \in GL(2R)$

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

The factor group $GL(2, R)/S$ consists of matrices up to nonzero scaler multiples.

The group $PGL(2, R)$. It represents linear transformations where scaling is ignored, describing transformation of the real projective line.

7. Diffie-Hellman key exchange is method that allows two parties to create a shared secret over 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 is vulnerable to man-in-the-middle attack if they exchanged public values are not authenticated. This is why it is usually combined with digital signature or certificates.

If the prime modulus is not large enough the distance logarithm problem becomes easier to solve, allowing attackers to compute the shared secret.

This would break the security of protocol, making encrypted communication vulnerable to attacks.

8. Let H_1 and H_2 be subgroups of a group G. The identity element 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. Z_n is commutative because addition and multiplication module n come from integer operations which are commutative.

Z_n has zero divisors when n is composit.

For example, in Z_6, $2 \cdot 3 \equiv 0 \pmod 6$

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 size and a stronger design, making brute force and Cryptoanalysis 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 $d = e^{-1} \bmod \varphi(n)$

Efficient for large keys → Partial 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 sequence under known plaintext attacks.

Mitigation - use non-linear combination of multiple LFSR.

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.

IT24646

16: Formula : $X_{n+1} = (aX_n + c) \bmod m$

Ex: $a=5$ $c=3$ $m=16$, $X_0=7 \rightarrow 6, 1, 8, 11, 10$

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 arithmetic for RSA, finite fields, ECC

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

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

Decrypt: $M = C^d \bmod n = 2$

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

Verify $S^e \bmod n = H(m) \rightarrow$ integrity/authenticity

20

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

check $P = (3, 10)$: verify $10^2 = 3^3 + 1 * 3 + 1$

$= 31 \rightarrow 100 \bmod 23 = 8$? 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~~ $G = (2, 5)$ $n = 19$ private $d = 9 \rightarrow Q = dG$

Sign $H(M) = 8$, random $k = 3 \rightarrow$ compute r, s)

verification: check r, s with $Q \Rightarrow$ 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, blockchain integrity verification.

23 GF(p): arithmatic mod prime P.

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

Field arithmatic ensures invertibility, diffusion and secure cryptographic operations.

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

ii) Security VS RSA / ECC: Resistant to shors algorithm RSA / ECC broken.

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

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

→ Ensures full utilization to all states except 0.

26 i) Key ~~or~~ Generation: lattice public/private key.

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