IT24640

1

Quantum computers running "Shor's algorithm" can efficiently factor integers and compute discrete logarithms, breaking RSA, DSA and ECC. This threatens confidentiality, authentication and digital signatures.

Post quantum alternatives:

- Lattice-based (CRYSTALS-kyber, Dilithium): secure via LWS/SVP Problems.
- Code-based (McEliece): relies on decoding random linear codes.
- Hash-based (SPHINCS+): Security from hash functions.
- Multivariate Polynomial Schemes.

Resistance to Quantum Attacks:

These schemes rely on mathematical problems for which no efficient quantum algorithms are known, unlike factorization and DLP.

IT24640

2

A Pseudo-Random Number Generator (PRNG) Produces deterministic sequences that approximate randomness.

Design Principles:

- Use current timestamp for entropy.
- Use Process ID (PID) for uniqueness.
- Apply modulus to constrain output.

Python Implementation:

Python

```
import time
import os
def custom_prng(modulus = 1000):
    seed = int(time.time()) ^ os.getpid()
    a = 1664525
    c = 1013904223
    return (a * seed + c) % modulus
print(custom_prng())
```

IT24640

3

Classical Vs Modern Symmetric Ciphers

Traditional Ciphers:

- Caesar cipher : Shift substitution
- Vigenere cipher : Polyalphabetic
- Playfair cipher : digraph substitution.

Modern Ciphers:

- DES : 56-bit key block cipher
- AES : 128/192/256 bit block cipher

Feature	Classical	Modern
Key Length	Small	Large
Security	Weak	Strong
Speed	manual	Optimized
Attacks	Frequency Analysis	Resistant

Classical ciphers are educational; modern ciphers are secure and practical.

IT24640

4

Action of S_4 on 2-Element Subsets.

Lets S_4 act on subsets of size 2 by:

$$\sigma(\{i,j\}) = \{\sigma(i), \sigma(j)\}$$

Well-Defined:

- Order innelevant
- Closure presenved

Orbit of (1,2):

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

Orbit size = 6

Stabilizen:

Permutations fixing $\{1,2\} \rightarrow$ size = 4

By Orbit-Stabilizen Theorem:

$$|S_4| = 24 = 6 \times 4$$

IT24640

Finite Field $GF(2^2)$ 5

Constructed using irreducible polynomial:

$$x^2+x+1$$

Elements:

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

i) Multiplicative Group:

- closed
- Identity = 1
- Inverses exist
- Associative

ii) Cyclic Nature:

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

Thus nonzero elements from a cyclic group.

α generates all nonzero elements $\Rightarrow$ cyclic of order 3.

IT24640

6

Scalar matrices in $GL(2,\mathbb{R})$

Scalar matrices:

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

Properties:

- Subgroup under multiplication
- Normal since λI commutes with all matrices.

Factor group:

$$GL(2,\mathbb{R}) / \{\lambda I\} \cong PGL(2,\mathbb{R})$$

- Form a subgroup
- Normal since they communicate with all.

Represents linear transformation up to scaling.

Linear transformations modulo scaling.

IT24640

7

Diffie-Hellman Key exchange:

Steps:

1. Public Parameters : g, P.
2. Exchange : g^a, g^b
3. Shared key : $g^{ab} \bmod p$.

Security:

- Based on discrete logarithm problem.
- Vulnerable to MITM without authentication.
- MITM attack:
  Possible without authentication.

Small P : Vulnerable to brute-force / logarithm attacks.

Small Prime Risk:

- Enables brute-force or Index calculus attacks.

IT24640

8

Intersection of subgroups :

Let $H_1, H_2 \leq G$

- Identity exists
- Closed under operation
- Closed under inverses

Thus $H_1 \cap H_2$ is a subgroup.

Example :

$2\mathbb{Z} \cap 3\mathbb{Z} = 6\mathbb{Z}$

Since $H_1 \cap H_2$ is non-empty, closed under the group operation, and closed under inverses, it is a subgroup of G.

$H_1 \cap H_2 \leq G$

The intersection of any two subgroups of a group is always a subgroup of that group, and this result extends to the intersection of any collection of subgroups.

IT24640

9

Ring $\mathbb{Z}_n$

- Commutative under addition and multiplication.
- Zero divisors exist if n is composite.

Field condition:

$\mathbb{Z}_n$ is a field iff n is Prime.

$\mathbb{Z}_n$ is a Commutative Ring:

Addition:

For any $a, b \in \mathbb{Z}_n$,

$$a+b \equiv b+a \pmod{n}$$

Since integer addition is commutative

Thus, addition in $\mathbb{Z}_n$ is commutative.

multiplication: for any, $a, b \in \mathbb{Z}_n$,

$$ab \equiv ba \pmod{n}.$$

Since integer multiplication is commutative.

Thus, multiplication in $\mathbb{Z}_n$ is also commutative.

IT24640

10

DES Vulnerabilities and AES Improvements.

DES Weknesses:

- 56-bit key → brute-force feasible.
- Vulnerable to Linear/differential cryptanalysis.

AES Advantages:

- Key sizes: 128-256 bits
- Strong non-Linear transformations.
- Efficient and secure.

The Data Encryption Standard (DES) is a symmetric block cipher adopted in the 1970s. Although it was widely used for decades, DES is now considered insecure for modern cryptographic applications due to several fundamental vulnerabilities

- SubBytes (non-linearity)
- ShiftRows (diffusion)
- Mix Columns (strong mixing)

IT24640

11

Differential Cryptanalysis :

i) DES :-

feistel structure diffuses differences but is insufficient against advanced attacks.

ii) AES :-

- SubBytes → non-Linearity.
- MixColumns → diffusion.
- Resistant by design.

Differential cryptanalysis is a chosen-plaintext attack that studies how differences in plaintext pairs affect differences in ciphertext pairs. The goal is to exploit non-random behavior in a cipher to recover key information.

→ Diffusion of Differences.
→ Use of-Boxes.
→ Multiple Rounds

IT24640

12

Extended Euclidean Algorithm :

Find integers x, y:

$$ax + ny = \gcd(a, n)$$

if $\gcd = 1 \rightarrow x$ is inverse of $a \bmod n$.

RSA Use :

- Computes Private Key d
- Efficiency crucial for Large keys.
- RSA uses very Large numbers (2048 - 4096) bits.
- EEA runs in Polynomial time $O(\log n)$, making it Practical even for Large integers.
- Efficient modular inverse computation ensures:
  - fast key generation.
  - secure real-time encryption
  - $ax \equiv 1 \pmod n$.
  - Scalability for large cryptographic systems.

IT24640

13

Modes of Operation :

i) ECB Insecurity :

$$E(P_i) = E(P_j) \Rightarrow P_i = P_j$$

Reveals Patterns.

ii) CBC Recurrence :

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

Error Propagation : Limited to two Blocks.

- ECB mode is insecure because it Preserves Plaintext Patterns due to its deterministic encryption.
- CBC mode introduces chaining, hiding Patterns and Providing better security.
- During decryption, CBC limites error Propagation making it Practical and robust for secure communications.

IT24640

14

Vulnerability of LFSRs Due to Linearity and its mitigation :

A Linear Feedback shift Register (LFSR) is a commonly used component is stream ciphers for generating keystream sequences. Its operation is defined by a linear recurrence relation over GF(2). which makes it efficient but also introduces serious security weaknesses.

An LFSR of Length m generates a keystrem $\{k_t\}$ using:

$$k_t = c_1 k_{t-1} \oplus c_2 k_{t-2} \oplus \cdots\cdots \oplus c_m k_{t-m}$$

where, $c_i \in \{0,1\}$

This relation is Linear over GF(2).

$$C_t = P_t \oplus K_t$$

$$K_t = P_t \oplus C_t$$

IT29640

15

Perfect Secrecy and the One-time Pad.

Let,

- M be the set of Plaintexts
- K be the set of keys, and
- C be the set of ciphertexts in a cryptographic system.

Proof: fix the plaintext $m \in M$ and ciphertext $c \in C$

$$c = m \oplus K \Rightarrow K = m \oplus c$$

- Keys are chosen uniformly at random,
- Each key is equally likely.

$$P(C = c \mid M = m) = P(K = m \oplus c) = \frac{1}{|K|}$$

$$P(M = m \mid C = c) = \frac{P(C = c \mid M = m)\, P(M = m)}{P(C = c)}$$

Since, $P(C = c \mid M = m)$ is constant for all m,

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

The one time Pad achieves Perfect Secrecy.

IT24640

16

The general formula for an LCG is:

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

where,

- x_0 = initial seed.
- a = multiplier
- c = increment
- m = modulus.

Lets take an bitrary example:-

$a = 5, \quad c = 3, \quad m = 16, \quad x_0 = 7.$

① $x_1 = (5.7 + 3) \bmod 16 = (35 + 3) \bmod 16 = 38 \bmod 16 = 6$

② $x_2 = (5.6 + 3) \bmod 16 = (30 + 3) \bmod 16 = 33 \bmod 16 = 1$

③ $x_3 = (5.1 + 3) \bmod 16 = (5 + 3) \bmod 16 = 8 \bmod 16 = 8$

④ $x_4 = (5.8 + 3) \bmod 16 = (40 + 3) \bmod 16 = 43 \bmod 16 = 11$

⑤ $x_5 = (5.11 + 3) \bmod 16 = (55 + 3) \bmod 16 = 58 \bmod 16 = 10$

The final 5 numbers of the LCG sequence are: **6, 1, 8, 11, 10**

IT24640

17

Ring and Abstract Algebra:

A Ring R is a set equipped with two binary operation, addition (+) and multiplication (·), satisfying the following properties:

Addition Properties:

1. Closure: $(a+b) \in R$ for all $a, b \in R$.
2. Associativity: $(a+b)+c = a+(b+c)$
3. Identity element: $0 \in R$ such that $a+0=a$.
4. Inverse element: for each $a \in R$, there exists $-a \in R$ such that $a+(-a)=0$.
5. Commutativity: $a+b = b+a$

Multiplication Properties:

- Multiplication is associative:

$$(a \cdot b) \cdot c = a \cdot (b \cdot c).$$

- Distributive Laws hold:

$$a \cdot (b+c) = a \cdot b + a \cdot c$$
$$(a+b) \cdot c = a \cdot c + b \cdot c.$$

IT24640

18

RSA example:

$P=5,\ q=11 \rightarrow n = 55, \phi(n) = 40.$

- Public key $(e, n) = (3, 55)$
- Private key $d = 27$
- message $m = 2$

$$C = m^e \bmod n.$$

$$C = 2^3 \bmod 55 = 8.$$

Plaintext $m = 2$

↓ Enenypt using Public key $(e=3, n=55)$

Ciphertext $C = 8$

$$m = C^d \bmod n = 8^{27} \bmod 55 = 2$$

Ciphertext $C = 8$

↓ Deenxpt using Private key $d = 27$

recovered $m = 2$.

message successfully recovered → confidentiality maintained.

IT24640

10

Elliptic Curve operations step by step :-

we are given,

$E : y^2 = x^3 + ax + b \bmod p, \quad a = 1, b = 1, P = 23$

$\therefore P = (3, 10), Q = (9, 7)$

if $y^2 \equiv x^3 + ax + b \bmod 23$.

$x = 3, y = 10$.

Compute LHS :-

$y^2 \bmod 23 = 10^2 \bmod 23 = 100 \bmod 23$

compute $100 \bmod 23$:

$23 \cdot 4 = 92, \quad 100 - 92 = 8$

$y^2 \equiv 8 \bmod 23$

Compute RHS :

$x^3 + ax + b \bmod 23 = 3^3 + 1 \cdot 3 + 1 \bmod 23 = 27 + 3 + 1 = 31$

$\bmod 23,$

$31 \bmod 23 = 8$.

LHS = RHS = 8 $\rightarrow$ P = (3, 10) lies on the curve.

IT2960

Q20

ECDSA over a finite field -

$$E : y^2 = x^3 + 7x + 10 \mod 37$$

- Base Point $G = (2,5)$, order $n = 19$
- Private key $d = 9 \rightarrow$ compute Public key $Q = dG$
- message hash $H(M) = 8$, random nonce $k = 3$

① Public key : $Q = dG$

② $R = kG = (x_R, y_R)$, $r = x_R \mod n$

$$s = k^{-1}(H(M) + dr) \mod n$$

Signature = (r, s)

③ $w = s^{-1} \mod n$

$u_1 = H(M) \cdot w \mod n$, $u_2 = r \cdot w \mod n$.

compute $X = u_1 G + u_2 Q = (x_x, y_x)$

Signature valid if $r \equiv x_x \mod n$

IT24640

21

Cryptographic Hash Function :

i) Essential characteristics of a secure hash function :

A cryptographic hash function takes an arbitrary length input and produces a fixed-length output (hash). A secure hash function such as SHA-256 must satisfy :

① Pre-image resistance : $H(x) = h$.

② Second pre-image resistance :
$H(x_1) = H(x_2)$.

③ Collision resistance : $H(x_1) = H(x_2)$

④ Deterministic and fast computation.
→ Same input always produces the same hash.

⑤ Avalanche effect.
→ A small change in input (even 1 bit) should drastically change the hash output.

IT24640

22

Galois Fields (Finite Fields)

Concept of Galois fields: A Galois field (GF), also called a finite field, is a set of finite elements in which addition, substition, multiplication, subtraction, and division (except by zero) are defined and satisfy field axioms.

GF(p):

- A finite field with p elements, where p is prime.
- Elements: $\{0, 1, 2, \ldots p-1\}$.
- Arithmetic is done modulo p.
- Example: $GF(7) \rightarrow \{0, 1, 2, 3, 4, 5, 6\}$.

GF (2^n):

- A finite field with 2^n elements.
- Elements are represented as n-bit binary Polynomials.
- Example: $GF(2^3)$ with irreducible Polynomial $x^3 + x + 1$

IT24640

23

Lattice-Based Cryptography:

i) SVP → Find shortest vecton in Lattice.

ii) Companion: → RSA/ECC broken by Shor's algorithm.
→ Lattice problems remain hard.

iii) Quantum vs Lattice:

→ Physics-based vs computational hardness.

RSA/ECC	Lattice-Based
Integen factorization	Learning with errron.
Broken by Shor's algorithm	Resistant to knowen quantum attacks.
Hardness of factoring on discrete log	Hardness of SVP.
Smallen	generally Langen.

Quantum Cryptography: Achieve provable seeurity using quantum Physics.

IT24640

24

Maximum Period of an LFSR keystream.

LFSR definition:

A Linear feedback Shift Register (LFSR) of length m generates a keystream $k = (k_1, k_2, k_3 \ldots)$ over GF(2) using the recurrence relation:

$$k_t = c_1 k_{t-1} \oplus c_2 k_{t-2} \oplus \cdots \oplus c_m k_{t-m} \pmod 2$$

- Here, $c_1, c_2 \ldots c_m \in GF(2)$ are the feedback coefficients.
- $P(x) = 1 + c_1 x + c_2 x^2 + \cdots + c_m x^m$.

This is the characteristic Polynomial of an LFSR is Primitive, the keystream period is $2^m - 1$.

- This ensures long, Pseudo-random sequences for stream ciphers.

IT24640

25

Lattice-Based Digital Signatures using LWE.

i) Process of Signing a message using an LWE-Based Scheme.

Lattice Based Signature schemes rely on the Learning with Errors (LWE) Problem, which is considered hard even for quantum computers.

the process includes key Generation, Signing and Verification.

1. Key Generation.
   - Choose a Public matrix $A \in \mathbb{Z}_q^{n \times m}$
   - Sample a Secret vector, $s_k \in \mathbb{Z}_q^m$ (Private key).
   - Compute the public key:

$$P_k = A \cdot s_k + e \pmod q.$$

where e is a small error vector.

Security: Recovering s_k from P_k is equivalent to solving the LWE Problem, which is hard.