Presentation Title: The Structure of Groups

Course Title: Advanced Cryptography

Course Code: ICT-6115

Presented by :

Md. Ahosanul Hasan Roki
IT-23608
Dept. of ICT,
MBSTU

Supervised By:

Mr. Ziaur Rahman
Associate Professor
Dept. of ICT,
MBSTU

Question-01:- With the advent of quantum computing, traditional public key cryptosystems such as RSA and Ecc are potentially vulnerable to shor's algorithm. Discuss the implications of quantum computing on the security of the cryptographic protocols and process possible post-quantum cryptographic algorithm that could replace RSA and Ecc. How do these algorithms resist quantum cryptanalysis.?

Answer:- quantum computing poses a singnificant threat to traditional public-key cryptograpsystems like RSA and Elliptic curve cryptography (Ecc). These systems rely on the difficulty of mathmatical problem such as integer factorization (for RSA) and the descrete logarithm problem (For Ecc). Howeven, shor's algorithm when run on a sufficiently powerful quantum competen, can solve these problem efficiently, rendering RSA and Ecc insecure, This has profound implications for cryptographic protocols and data security.

IT-23608 (Roki)

Implication Quantum Computing on Cryptography:-

1. **Breakdown of current cryptosystems:-** Shor's algorithm can break RSA and ECC, computing, compromising widely, used protocols like TLS/SSL, SSH, and digital signature.

2. **Long-Term Data Vulnerability:-** Encrypted data secured today could be decrypted in the future using quantum computer, a threat known as "harvest now, decrypt later".

3. **Urgent Need for Quantum-Resistant Algorithms:**

The cryptographic community must transition to post quantum cryptographic algorithm that are scure aganist both classical and quantum attack.

Post Quantum Cryptographic Algorithms:-

post quantum cryptography focuses on developing algorithms based on mathematical problems that are believed to be hard for quantum computers. Some of leading candidates include:-

1. **Lattice-Based Cryptography:**

   * Example: NTRU, Learning with Error, Ring LWE.
   * Security Basis:- The hardness of problems like the shortest Vector problem and Closest vector prob in lattice structure.
   * Resistance to Quantum Attack:- No known quantu Algorithm can efficient solve these lattice problem

2. **Hash-Based cryptography:**

   Ex. SPHINCS+, Merkle signature.
   Usess collision-resistant hash function.

3. **Code-Based Cryptography:-** (e.g: McEliece): Based on decoding random linear codes.

4. **Mutrivarte polynomial Cryptography: (Rainbow):**

Solves system of multivariate equations.

5. Isogeny-Based Cryptography (SIKE). Uses supersingular elliptic curve isogenies.

How these Algorithm Resist Quantum Cryptanalysis:-

Mathmatical Hardness:- post quantum algorithms are based on problems that are believed to be hard for both classical and quantum computer.

Lack of Quantum speedup:- Unlike factoring and discrete Logarithms. the problem underlying post-quantum do not currently have efficient quantum algorithms that provide exponential speedup.

Larger key size. post-Quantum-alogorithms often require Langer key size compared to classical algorithms to achieve compirable security levels. attack.

~~It-62308~~

It-23608 (Roki)

Question No-2:- Design and implement a novel Pseudo-Random Number Generator (PRNG) algorithm in python using. The current timestamp, the process ID(os.pid) for added randomness, a modulus operation to constain the output with in desired range.

Ans: currently : Bellow is a python implementation of a novel PRNG that uses the current timestamp, ID - and a modular number with in a specified range.

python code:

```
import time
import os

class TimestampPIDPRNG:

    def __init__(self, seed=None):
        if seed is None:
            self.seed = int(time.time() * 1000) + os.getpid()

        else
            self.seed = seed

    def generate(self, min_range, max_range):

        self.seed = (self.seed * 1103515245+12345) & 0x7
                                                    fffffff
random_number = min_range + (self.seed % (max_range - min_range+1))
return random number
```

Ex

```
if __name__ == "__main__":
    prng = TimestampPIDPRNG()
    for _ in range(10):
        random_number = prng.generate(1,100)
        print(random_number)
```

output:-
42
87
15
63
29
91
37
78
51
10

IT-23608 (Roki)

No-3 Here a concise comparison table of traditional ciphers (Caesar, Vigenere, playfair) and modern symmetric ciphers (AES, DES):

Feature	Traditional ciphers			Modern symmetric ciphers	
	caesar cipher	Vigenere cipher	playfair cipher	DES	AES
Key length	1 integer (tiny)	Variable (short)	keyword-based	56 bits	128, 192, 256 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 crypto-analysis	Resists all known attack.
Use case	Historical education	Historical, Basic	Historical, Basic	Legacy, system	modern encryption.

It-23608 (Roki)

* Traditional ciphers (caesar, Vigenere, playfair)

* Strengths: simple, fast easy to implement.

* Weakness: small key space., vulnerable to brute force and freequency analysis, insecure by modern standends.

* Modern Symentric Ciphers (DES, AES):

* Strengths: Large key space, resistant to modern attacks. fast with hardware support.

* Weakness: More complex to implement, computationally heavier that traditional chipher. (but still efficient).

No-4

Ans: 1. Well-defined Action:-

Define the action of S_4 on 2-element subset as $\sigma \cdot \{a,b\}$

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

* identity $e \cdot \{a,b\} = \{a,b\}$

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

The action is well-defined.

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 swaping $\{1,2\}$ and $\{3,4\}$:,

$\{e, (12), (34), (14), (37)\}$.

The stabilizer has size 4.

4. Orbit-stabilizer Theorem:

$$|\text{orbit}| = \frac{|S_4|}{|\text{stabilizer}|} = \frac{24}{4} = 6, \text{ match the orbit size}$$

✓.

No-05 Let GF(2^{12}) be the finite field of order 4, constructed using the irreducible polynomial x^2+x+1 over GF(2).

(i) show that GF(2^{12}) forms a groups under multiplication.

Ans To demonstrate that GF(2^{12}) forms a group under multiplication, we need to verify four group axioms.

1. Closure: For any two ~~group~~ elements a, b in GF(2^4), the product a.b must be also in GF(2^4)

2. Associativity: For any a, b, c in GF(2^4)

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

3. Identity: There exists an element e in GF(2^2) such that for any a in GF(2^2), $e \cdot a = a \cdot e = a$.

4. Inverse: For every a in GF(2^2), there exists an element a^{-1} in GF(2^2) such that $a \cdot a^{-1} = a^{-1} \cdot a = e$.

Step 1: Define GF(2^2) Elements:

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 a root of $x^2+x+1=0$, meaning $\alpha^2 = \alpha+1$.

Step 2: 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	$\alpha^2 = \alpha^0+1$	$\alpha(\alpha+1) = \alpha^2+\alpha = (\alpha+1)+\alpha = 1$
$\alpha+1$	0	$\alpha+1$	1	$(\alpha+1)^2 = \alpha^2+2\alpha+1 = (\alpha+1)+0+1 = \alpha$

Step 2 Verify Group Axioms.

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

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

Identity: $1 \cdot \alpha = \alpha \cdot 1 = \alpha$ for any α in $GF(2^4)$.

Inverse Each nonzero element has an inverse.

- $1^{-1} = 1$
- $\alpha^{-1} = \alpha+1$ because $\alpha \cdot (\alpha+1) = 1$
- $(\alpha+1)^{-1} = \alpha$ because $(\alpha+1) \cdot \alpha = 1$

Since Four axioms are satisfied.

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

A **Step 1:** Identity Nonzero elements

The nonzero elements of $(GF)(2^4)$ are.

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

step 2: check the Generation.

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

1. Element 1:
   - $1^1 = 1$
   - $1^2 = 1$
   - only Generate $\{1\}$.

2. Element α

$\alpha^1 = \alpha$

$\alpha^2 = \alpha + 1$

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

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

Both α and $\alpha+1$ Generate the multiplicative group non-zero of $GF(2^2)$. Therefore, the set of all nonzero elements of $GF(2^2)$ is cyclic.

6 Let $GL(2,R)$ be the general linear group of 2×2 invertible matrices over R. show that the set of scalar matrices forms a normal subgrou. of $GL(2,R)$. construct the corresponding factor Group and interpret its structure.

An To show that the set of scalar matrices

$S = \{ \begin{pmatrix} a & 0 \\ 0 & a \end{pmatrix} \mid a \in R, a \neq 0 \}$ is a normal subgroup.

$GL(2,R)$

1. subgroup: S is closed under multiplication, contains the identity, and has inverses.
2. Normal: For any $g \in GL(2,R)$ and $s \in S$, the conjugate $gsg^{-1} = s \in S$.

The factor group $GL(2,R)/S$ consists of cosets gS, with group operation $(g_1S)(g_2S) = (g_1g_2)S$. The factor group is isomorphic to the projective general linear group $PGL(2,R)$ which represent projective transformation of real projective line.

Q 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, Provide an example using specific group.

Ans To prove that the intersection of two subgroup H and K of group 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,

$e \in H \cap K$.

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.

Ex In $G = \mathbb{Z}$, let, $H = 2\mathbb{Z}$ $K = 3\mathbb{Z}$, then, $H \cap K = 6\mathbb{Z}$ Which subgroup.

JT-2368 Poki

2 Prove that the ring Z_n is a commutative ring identify whether it has zero divisors. Further, determine the condition under which Z_n is a field.

Ans prove:

1. commutativity of Z_n:—

* The ring Z_n is commutative because both addition and multiplication modulo n are commutative operation. for any $a, b \in Z_n$, $a+b \equiv b+a \pmod{n}$ and $a \cdot b \equiv b \cdot a \pmod{n}$

2. Zero divisor Z_n:

* Z_n has zero divisor if n is a composite number. ex. if $n = k \times m$ when $1 < k, m < n$.

3 When is Z_n is field:

* Z_n is a field if and only if n is prime number. This is beacuse.

IT-23608

No-10

Ans Vulnerabilities of the DES Ciphen:-

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

(i) short key Attacks,

(ii) encryption weakness.

(iii) ~~encryption weak~~ Bruteforce Attacks.

(iv) small block size.

Brute force Attack. Break DES:

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

Pto.

IT-2308

→ With 56-bit key, there are $2^{56} \approx 72 \times 10^{15}$ possible keys.

→ modern hardware, such as ASICs, FPGAs and cloud based parallel processing can exhusted this key space quickly.

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

AES Addressed in the shortcomming are DES:

The Advanced Encryption standard AES was introduced in 200 to replace DES and overcome is weakness.

→ Increased the key size.

→ Resistance to encryption Attack.

→ Large block size.

It - 23608

No. - 11

Ans (i) Differential cryptoanalysis is a chosen plaintext attack that analyze how difference in plain text propagate through a cipher to predict difference in ciphertext.

Defense Mechanism in DES Against DC:

1. S-Box Design to resist DC.

The S-boxes in DES were carefully design to minimize different probabilities

2. Feistal structure provide;

In this feistal network as DES, the right half of the block is expanded, mixed with round key, and substituted via S-based.

(ii) Unlike DES, AES is not Feistel ciphers but follows a substitution permutation structure to DC.

Key feature that improve DC Registrer

(1) sub_bites (Non linear substitution using S-boxes)

(2) shiftroows (Row-wise Permutation)

(3) Add round key.

(4) mix column for strong Diffusion.

(5) more round in AES - 128 has rounds.

12 Ans:

Finding the modular Inverse using the Extended

Euclidean Algorithm:- The modular inverse of an integer a modulo n is an integer x such that

$$a \cdot x \equiv 1 \pmod{n}$$

This means that x is the multiplicative inverse of a modulo n, provided that a and n are coprime.

We used the extended Euclidean Algorithm to compute x.

Step 1: Apply the euclidian Algorithm. the eletlidean Algorithm. find the GCD of a and n using the division algorithm:

$$gcd(a,n) = gcd(n, a \bmod n)$$

We continue until we reach gcd = 1.

Step 2: Apply the Extended Euclidean algorithm.

The EEA expresses gcd(a, n) as a linear combination,

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

Since gcd(a, n) = 1, we can rewrite this as

$$1 = ax + ny.$$

Reducing modulo n:-

$$ax = 1 \pmod{n}$$

Thus, x is the modular inverse of a modulo n.

No-13

Ans (i) ECB mode is inverse for highly Redundant Data:

In electronic codeblocks (ECB) mode, a plaintext message pis divided into fixed size blocks and each block is independently encrypt using the same key k.

$$e_i = E_k(P_i)$$

Mathmatical Proof of ECB weakness:

1. Lack of Diffusion:- Identical plaintext Blocks produce indentical ciphertext blocks. suppose we have two plaintext block P_i and P_j, such that.

$$P_i = P_j$$

Since encryption in ECB is deterministic:

$$e_i = E_k(P_i), E_k(P_j) = e_j$$

This means that identical plaintext block always produce identical ciphertext block which leaks information about the structure of the plaintext.

No-14

Ans A Linear Feedback shift register generates a repeating sequence of bits using a linear formula.

$$S_n = c_1 S_{n-1} \oplus c_2 S_{n-2} \oplus \cdots \oplus c_n S_{n-n}$$

Where,

→ S_n are the output bits.

→ C_i are fixed numbers.

→ $\oplus$ XOR.

The linear means as attackers can

pt.-

set up simple equation and solve them to find the LFSR's structure.

A hacker Breaks LFSR Encryption :-

A stream cipher using an LFSR encryption looks like this

$$C_i = P_i \oplus K_i$$

→ P_i = plaintext

K_i = LFSR-Generated key stream bit.

C_i = ciphertext bit.

if a hacker know that both p_i and c_i they can recover k_i,

$$K_i = C_i \oplus P_i$$

since the key stream follows a linear rule. the hacker can use math this to find all future k_i, This break the encryption.

It-23608

No. 15

Ans

(i) Claude Shannon defined perfect secrecy mathmatically as:-

$$P(m/c) = P(m)$$

for all plaintext means ciphertext c, where

→ P(m) is the probability of choosing as plaintext m.

→ P(m/c) is the probability of m given that we observe c.

This means that knowing the ciphertext given no additional information about the plaintext

using Bays theorem, we can rewrite the conditions as

$$P(c/m) = P(c)$$

IT-23608

(ii) Proof that the one-time pad (OTP):-

Difinition:

* Let m be a plaintext message from the set M.

* Let K be a key chosen uniformly at random from the keyspace K.

* Encryption is defined as

$$c = m \oplus k$$

* Decryption work as

$$m = c \oplus k.$$

The OTP satisfies shanon's Definition:-

We need to prove that knowing c does not requested any information about m.

1. Since k is chosen uniformely at random

for any given plaintext m, the ciphertext is $e = m \oplus k$.

2. The key is equally likely to be any value in k. and since $|k| \geq |m|$ · every plaintext has an equal chance of producing any ciphertext.

3. Thus, for any given ciphertext c, every plaintext m is equally probable

$$P(m/c) = P(m)$$

which statistic shannons definition of perfect secrecy.

No-16

Lets choose specific values for the LCG parameters

→ multiplier : $a = 5$.

→ Increment $c = 3$

→ modulus $m = 16$

→ seed $x_0 = 2$

The recurrence relation is

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

substituting our values.

$$x_{n+1} = (5 x_n + 3) \bmod 16$$

Now, we compute the first 5 values.

1. $x_1 = (5 \times 7 + 3) \bmod 16 = (35+3) \bmod 16 = 38 \bmod 16 = 6$.

2. $x_2 = (5 \times 6 + 3) \bmod 16 = (30+3) \bmod 16 = 33 \bmod 16 = 1$

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

P.T.O.

4. $x_4 = (5 \times 8 + 3) \bmod 16 = (40+3) \bmod 16$,

$43 \bmod 16 = 11$

5. $x_5 = (5 \times 11 + 3) \bmod 16 = (55+3) \bmod 16$

$58 \bmod 16 = 10$.

The sequence is : 6, 1, 8, 11, 10 ∆.

No-18

(i) RSA Encryption & Decryption :-

Given values:

$P = 5$, $q = 11$,

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

Compute Euler's totient function $\phi(n)$

$\phi(n) = (p-1)(q-1) = (5-1)(11-1) = 40$

Step-1: choose public key e.

e must be co prime to $\phi(n) = 40$

choose $e = 3$ (since $\gcd(3, 40) = 1$)

step2: compute private key d.

d is the modular inverse of e modulo $\phi(n)$, satisfying

$$d \times e = 1 \bmod 40.$$

Using the Extended euclidean Algorithm,

$d = 27$, since $(3 \times 27) \bmod 40 = 81 \bmod 40 = 1$

Thus, our RSA key pair

public key $(e, n) = (3, 55)$

private key $d = 27$

step3 Encrypt message $m = 2$

using RSA encryption formula.

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

$$c = 2^3 \bmod 55 = 8$$

The ciphertext $2^3 \bmod 55 = 8$.

It- 23608

The ciphertext is $c = 8$.

step 4: Decrypt ciphertext $c = 8$ using RSA decryption formula:

$$m = c^d \bmod n$$

$$m = 8^{77} \bmod 55$$

$$= 2$$

8.

(ii) **RSA Digital signature:**

Given values,

$$p = 7,\ q = 3,\ n = p \times q = 7 \times 3 = 21$$

compute $\varphi(n) = (p-1)(q-1) = (7-1)(3-1) = 12$

choose e such that $\gcd(e, 12) = 1$, let $e = 5$

compute private key d as the modular inverse of e modulo $\varphi(n)$

$$d \times 5 = 1 \bmod 12$$

Using the extended Euclidean Algorithm

$d = 5$

Thus our RSA key pair

public key $(e, n) = (5, 21)$

private key $d = 5$.

Step 1: sign hash of message $H(m) = 3$

Using RSA signature formula.

$$s = H(m)^d \bmod n.$$

$$s = 3^5 \bmod 21$$

computing, $3^5 = 243$.

$243 \bmod 21 = 243 - (21 \times 11) = 243 - 231 = 12$

The signature is $is = 12$

Step 2: Verify the signature:

to verify, we compute,

$$H'(m) = s^e \bmod n$$

$$H'(m) = 12^5 \bmod 7$$

$$= 3$$

Hence $H'(m) = H(m)$ the signature is verified.

IT-23608

No-19

(i) We are given the elliptic curve equation:

$$y^2 = x^3 + ax + b \mod p.$$

with parameter,

$$p = 23, \quad a = 1, \quad b = 1$$

(ii) Verify if $P = (3, 10)$ lies on the curve.

To check if the point $P = (3, 10)$ lies on the curve; substitute $x = 3$, $y = 10$ into the equation

$$10^2 = 3^3 + (3) + 1 \mod 23$$

$$100 = 27 + 3 + 1 \mod 23$$

$$= 31 \mod 23$$

Since $31 \mod 23 = 8$ and $100 \mod 23 = 8$.

both sides are equal. This p lies on the curve.

— 3 —

(i) Doubling the point P (computing 2P)

The formula for point doubling is:

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

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

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

substituting, $P = (3, 10)$

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

$$= \frac{3(9+1)}{20} \bmod 23$$

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

since division in modular arithmetic requires the modular inverse of 20 modulo 23, we compute

$$20^{-1} \bmod 23$$

Using the Extended Euclidean Algorithm we find,

$$20^{-1} = 7 \bmod 23$$ so,

IT-23608

$2^{-1} = 7 \mod 23$

$d = 28 \times 7 \mod 23$

$= 196 \mod 23 = 12$

Now compute x_2,

$x_2 = 12^2 - 2x1 \mod 23$

$= 12^2 - 2(3) \mod 23$

$= 144 - 6 \mod 23$

$= 138 \mod 23$

$= 138 - (23 \times 6)$

$= 138 - 138 = 0$.

Compute y_2;

$y_2 = d(x_1 - x_2) - y_1 \mod 23$

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

$= 26 \mod 23$

$= 3$

∴ Thus P(0,3) is

No: 20 | Ans

The curve equation is: $y^2 = x^3 + 7x + 10 \mod 37$.

$G = (2,5)$, $n = 19$, $d = 9$, $k = 3$, $H(m) = 8$.

Step 1: compute the public key $Q = dG$

since the public key is obtained by scalar multiplicative of the base point.

$$Q = d \cdot G = 9 \cdot (2,5)$$

We compute $9G$ using double and add.

Compute $2G$ (point doubling)

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

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

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

For $G = (2,5)$ we have.

$$\lambda = \frac{3(2)^2 + 7}{2(5)} \mod 37$$

$$= \frac{19}{10} \mod 37$$

IT-23608

We compute modular inverse to 19 mod 32.

$19^{-1} = 26 \bmod 32$

$\Rightarrow 19 \times 26 \bmod 32$

$= 494 \bmod 32$

$= 494 - (32 \times 13) = 0$

$= 494 - 481$

$= 13$

Now, $x_2 = 13^2 - (2)2 \bmod 32$

$= 165 \bmod 32$

$= 165 - (32 \times 4) = 165 - 128 = 12$

$y_2 = 13(2-12) - 5 \bmod 32$

$= -260 \bmod 32$

$= -260 + (32 \times 9) = -260 + 288 = 28$.

$2G = (12, 28)$

$\therefore$

IT-23608

No-22

Ans: A Galois field (GF(q)) is a finite set of element where arithmatic operation are defined.

Types of Gal. fields:

1. GF(P) (prime fields):

→ Elements : {0, 1, 2 .... p-1} where p is prime.

→ Used in Elliptic curve encryptography for secure encryption digital signature and key exchange.

2. GF(2^n) Binary fields:

→ Elements are binary polynomial modulo an irreducible polynomial.

→ Used in AES encryption, error correcti., and post quantum cryptography.

No. 23

Ans: (i) The shortest vector problem (SVP) is a fundamental hard problem in lattice based encryptography. Given a lattice, the SVP asks for the shortest nonzero vector in the lattice under a chosen norm. The problem computationally hard meaning even the best known algorithm requires exponential time for lattice.

Role in security:

→ many lattice-based cryptographic schemes rely on the difficulty of approximately SVP.

→ Learning with error and Ring-LWE key problem in the lattice. cryptography are used to SVP.

No 24|

Step 1: A Linear Feedback shift register is defined by the recurrence relation:

$$K_t = c_{K_t-1} \oplus e_{L k_{i-2}} \oplus \cdots c_{n k_{t-n}}$$

Where,

the coefficient $e_1, e_L \cdots e_n$ belong to GF(2)

→ The sequence of key stream bits $\{k_i\}$ is periodic meaning it eventually repeats.

This recurrence relation corresponds to a characteristics polynomial:

$$P(x) = x^m - e_1 x^{m-1} - e_2 x^{m-2} \cdots e_n.$$

Therefore the maximum possible non zero is $2^m - 1$

Thus the maximum possible period of the key stream is $2^m - 1$

No - 25

Ans

(i) An LWE - based signature scheme consists of three main step.

1. **key Generation.**

→ Generate a private key sk.

→ compute the public key Pk using a matrix A and the LWE problem structure.

2. **signing.**

→ Hash the message m to create a challenge.

→ Use the private key sk and a trapdoor function, to produce a short lattice vector.

3: Verification

→ use the public key Pk to check

→ if the verification equation holds, the signature is valid.

(ii) **step 1:**

→ choose a random matrix $A \in Z_q^{n \times n}$.

→ Generate a secret key sk (a short vector)

→ compute the public key

$$Pk = A \cdot sk + e$$

where, e is a small error vector sampled from a noise distribution.

step 2:

→ Hash the message to obtain a challenge

$$c = H(m) \in Z_q^n$$

→ Use a trapdoor function refind a short vector z such that,

$$A \cdot z \equiv H(m) \bmod q$$

→ The signature is the short vector z.

Step3.

→ The verifier checks if.

$$A \cdot z \equiv H(m) \bmod q$$

→ if z is a short vector, the signature is valid.