Discuss the implications of quantum computing on the security of cryptographic protocols, and propose possible post-quantum cryptography algorithms that could replace RSA and ECC.

⇒ Implications of quantum computing on Cryptography

① Breaking public-key Encryption:

⇒ RSA, ECC and DSA rely on the difficulty of factorizing large numbers or solving discrete logarithm, problems that classical computers struggle with.

⇒ Shor's Algorithm runs in polynomial time on a quantum computer, making it feasible to break RSA and ECC encryption in minutes or hours, compared to billions of years on a classical computer.

Q5 With the advent of quantum computing, traditional public key cryptosystems such as RSA and ECC are potentially vulnerable to shors algorithm

=> Traditional public key cryptosystems like RSA and ECC rely on mathmatical problems that are computationally hard for classical computers but can be efficiently solved using shors algorithm on a sufficiently powerful quantum computer.

① RSA Vulnerable

→ RSA security is based on the difficulty of factoring large number (integer factorization problem)

→ shors algorithm can factor an n-bit RSA modulus ($N = p \times q$) in $O(n^3)$ time on a quantum computer, breaking RSA encryption

② ECC vulnerable :-

→ ECC security relies on the difficulty of solving the Elliptic Curve Discrete Logarithm problem.

→ shors algorithm can solve this problem efficiently breaking ECC-based encryption and signatures

(b) Threat to Digital signature

-> Many Authentical mechanisms depend on digital signatures using RSA or ECC.

(c) Impact on symmetric cryptography

-> Symmetric Algorithms are relatively more resistant to quantum attacks

Here some promising alternatives that could replace RSA and ECC.

(1) Lattice - Based cryptography

Example → Kyber, Dilithium.

why? - Lattice problems are believed to be hard even for quantum computers.

Pros: High sec' security, relatively efficient

cons: Largers key sizes compared to RSA and ECC.

(2) Code - Based cryptography:

Ex: classic McEliece

why? Based on the difficulty of decoding random linear codes, which is a well-studied hard problem.

Pros: Very strong security.
cons: Very large public keys

③ Multivariate polynomial cryptography :-

Example :- Rainbow
Why? Based on solving systems of multivariate quadratic equations and a problem known to be NP-hard.
Pros: Fast signature generation.
cons: Some variants have been broken.

④ Hash-Based Crypto graph :-

Example : SPHINCS
Why? Security is based on well-understood hash functions rather than number-theoretic problems
Pros: Simple, strong security.
cons: Larger signatures, not suitable for general encryption.

⑤ Isogeny-Based cryptography :-

Example → SIKE
Why? Uses the mathematical properties of elliptic curve isogenies.

Pros : Small key sizes

cons : Recent breakthrough have shown weaknesses in some schemes.

Q2 How do these algorithms resist quantum cryptanalysis?

=> (i) Lattice-Based Cryptography :-

→ Quantum-resistant due to the hardness of problems like the Learning with Errors and shortest vector problem.

→ Shor's algorithm which efficiently breaks RSA and ECC, does not provide an advantage for solving Lattice problems.

Example : Kyber, Dilithium, Falcon

(2) Code-Based cryptography :

→ Relies on the hardness of decoding random linear codes, a problem still hard for quantum computers

Example : Classic McEliece.

(3) Multivariate polynomial :- Based on solving systems of multivariate quadratic equations which remains difficult for quantum computers.

Ex : Rainbow.

Pros : Small key sizes

cons : Recent breakthrough have shown weaknesses is some schemes.

Q2 How do these algorithms resist quantum cryptanalysis?

⇒ (1) Lattice-Based Cryptography :-

→ Quantum-resistant due to the hardness of problems like the Learning with Errors and shortest vector problem.

→ Shor's algorithm which efficiently breaks RSA and Ecc, does not provide an advantage for solving Lattice problems.

Example : Kyber, Dilithium, Falcon

(2) Code-Based cryptography :

→ Relies on the hardness of decoding random linear codes, a problem still hard for quantum computers

Example : classic McEliece.

(3) Multivariate polynomial :- Based on solving systems of multivariate quadratic equations which remains difficult for quantum computers.

Ex : Rainbow.

(4) Hash-Based cryptography :-

→ Utilizes cryptographic hash functions for secure digital signature.

Example → SPHINCS+

(5) Isogeny-Based cryptography:

→ Based on the hardness of finding isogenies between elliptic curves.

Example → SIDH, SIKE

Design and implement a novel Pseudo-Random Number Generator algorithms in python using: The current timestamp, The process ID for added randomness, a modulus operation to constrain the output within a desired range.

Design:

(1) Seed Generation : Use the current timestamp and the process ID to create a seed.

(2) Hashing for Entropy : Use a hash function to increase entropy.

(3) XOR Operations: Introduce non-linearity by XOR-ing parts of the seed.

(4) Modulus Operation: Ensure the number is within the desired range.

03 Compare traditional ciphers (such as the Caesar cipher, vigenere cipher, and playfair cipher) with modern symmetric ciphers like AES and DES.

Feature	Traditional ciphers (caesar, vigenere playfair	Modern Symmetric ciphers (AES, DES)
Encryption principle	Based on simple substitution transposition or poly-alphabetic techniques	Uses complex mathematical operations like substitution permutation networks, feistel structures and modular arithmetic
Security Level	Weak by modern standards easily broken using frequency analysis and brute force	Highly secure
key Length	short keys	Longer keys
key management	simple key distribution but vulnerable to attacks if intercepted	Requires robust key exchange mechanisms like Diffie - Hellman or public key cryptography

IT23619

Cryptanalysis Resistance	Vulnerable to known plaintext attacks frequency analysis and brute force	Resistant to known cryptanalytic attacks
Computational Efficiency	simple and fast but impractical for securing modern digital communication	Optimized for fast computation in hardware and software suitable for large-scale data encryption.

Q4 Discuss the strengths and weaknesses of each type of cipher, including key length, encryption/decryption speed and security against modern cryptanalysis techniques.

=> Below is a discussion of different encryption types including their key length description speed and security against modern cryptanalysis techniques

① Symmetric Encryption :-

Key Lenght →: 56 bit (DES) 112/168-bit (3DES) 128/192/256 bit (AES)

Description → uses a single key for encryption and decryption. Fast and efficient for bulk data

speed →: Very fast, suitable for real time applications

strenght →: Fast encryption and decryption

Weaknesses → key distribution problem.

Security Against cryptanalysis →: AES-256 is secure against brute force attacks.

I123619

(2) Asymmetric Encryption

Key Length →: 1024 / 2048 / 4096 bit (RSA). 160-521 bit (ECC)

Decription →: Uses a public key for encryption and a private key for decryption.

speed → slower than symmetric encryption

strength → No key distribution problem, secure authentication and digital signature.

weaknesses → much slower than symmetric encryption.

Security against cryptanalysis →: RSA is secure with large key sizes but it is vulnerable

(3) Hash Function :-

key length →: No key

Decription → One way function that converts data into a unique hash.

speed → Very fast

strengths → Provides data integrity verification. Used in digital signature and authentication.

weaknesses → Cannot be reversed but susceptible to collision attacks.

Security against cryptanalysis → MD5 and SHA-1 are broken.

(4) Post-Quantum cryptography:

key length → Variable depends on the algorithm.

Description → Uses mathematical problem that are hard quantum computers to solve

speed → typically slower than classical cryptography methods

strengths → Resistant to quantum attacks. Future proof encryption methods being developed.

IT-23619

Weaknesses → Some post quantum algorithm require large keys etc. computational resources.

Security Against cryptanalysis → Design to withstand attacks from both classical and quantum computers.

05 (E) Explain the Diffie-Hellman key exchange protocol and its application in secure communication.

⇒ The Diffie-Hellman key Exchange is a cryptographic protocol that allows two parties to securely establish a shared secret key over an insecure communication channel without transmitting the key itself.

How the Diffie-Hellman protocol works

(i) Public parameters :-

⇒ Two parties (Alice & Bob) agree on a large prime number p and a generator g. This values are public.

(ii) Private key selection :

→ Alice selects a private key a (a randomly chosen integer) and keeps it secret.

→ Bob selects a private key b and keeps it secret.

8) Public key computation:

→ Alice computes her public key:

$A = g^a \bmod p$

$B = g^b \bmod p$

→ Exchange of public keys

Alice sends A to Bob

Bob sends B to Alice

→ Shared secret computation

→ Alice computes the shared secret using Bob's public key.

$s = B^a \bmod p = (g^b \bmod p)^a \bmod p$

$s = A^b \bmod = (g^a \bmod p)^b \bmod p$

Since S is the same for both Alice and Bob they now share a common secret key without ever transmitting it directly.

IT23619

Application in Secure Communication.

(1) Secure Communication (TLS/SSL):

→ Used in TLS and SSL protocols for establishing secure web connections.

(2) Vpns

→ Used in protocols like IPsec to establish a secure tunnel between clients and servers.

(3) End to end Encryption

(4) Wireless security

(5) Blockchain and cryptocurrencies

06 Discuss the security of the Diffie-Hellman protocol against common attacks such as man-in-the middle and the role of the discrete logarithm problem in ensuring its security.

⇒

(1) Man-in-the middle Attack :-

⇒ The classic MITM attack is a significant vulnerability of the Diffie-Hellman protocol when used with authentication.

→ Suppose Alice and Bob want to exchange a secret key using Diffie-Hellman

→ An attacker, Eve intercepts their communications.

→ Eve establishes two separate Diffie-Hellman key exchange.

* One with Alice pretending to be Bob
* One with Bob pretending to be Alice

→ Now Eve has two shared secrets: one with Alice and one with Bob.

07 Defining the Action of S_4 on 2-Element subset

⇒ The symmetric group S_4 consist of all permutation of the set $X=\{1,2,3,4\}$, we define an action of S_4 on the set of 2-element subset of X as follows—

For any $G \in S_4$, and any subset $\{a,b\}$ where $a,b \in X$ and $a \neq b$ define.

$$G.\{a.b\} = \{G(a).a(a)\}$$

Proving the action is well Defined

To show that this action is well define we must verify :-

(1) The image of a 2 element subset under any permutation is still a 2-element subset

(2) The identity element of S_4 acts trivially

(3) The composition of two permutation as expected.

closure : If $\{a,b\}$ is a 2-element subset of X then for any $\sigma \in S_4$ $\sigma(a) \neq \sigma(b)$ because σ is a bijection. Hence $\sigma \cdot \{a,b\} = \{\sigma(a), \sigma(b)\}$ is still a 2 element subset.

Identity Actions: The identity permutation e satisfies

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

Thus the action is well-defined

Computing the orbit of $\{1,2\}$

The orbit of $\{1,2\}$ under the action consists of all 2-element subsets that can be reached by applying some permutation in S_4

Since S_4 acts transitively on the 2-element subsets of the orbit of $\{1,2\}$ includes all possible 2-elements subsets of X, namely There are $\binom{4}{2} = 6$ such subsets meaning the size of the orbit of $\{1,2\}$ is 6.

08 We are given the finite field $GF(2^2)$ which is constructed using the irreducible polynomial

$$x^2+x+1$$

Constructing $GF(2^2)$

⇒ Since $GF(2^2)$ is a degree 2 extension of $GF(2)$ we define an element α as a root of the irreducible polynomial.

$$\alpha^2+\alpha+1=0$$

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

Since $GF(2)=\{0,1\}$ we construct the elements of $GF(2^2)$ as

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

We know consider the non zero elements

$$E=\{1,\alpha,\alpha+1\}$$

IT-2361g

(i) showing that E forms a Group under multiplication :-

⇒ To verify that E forms a group under multiplication. We check the group properties :-

(i) closure : We compute the product

→ $1.\alpha = \alpha, 1 \cdot (\alpha+1) = \alpha+1$ and $1.1 = 1$

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

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

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

since all products remain in E closure holds.

(2) Associativity :

→ since $GF(2^2)$ is a field multiplication is associative

(3) Indentity elements :-

⇒ The indentity element in multiplication is 1. since for all $x \in E$

$$x \cdot 1 = x.$$

Thus $E = \{1, \alpha, \alpha+1\}$ forms a group under multiplication.

(i) Verifying if E is cyclic :-

A group is cyclic if there exists an element $g \in E$ such that all elements of E can be written as powers of g.

We check if α can generate all elements.

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

Thus the powers of α cycle through all elements meaning α is a generator of E. E is cyclic.

IT-23619

09 Define the General linear group $GL(2,\mathbb{R})$

⇒ The general linear group $GL(2,\mathbb{R})$ consists of all 2×2 invertible matrices over $\mathbb{R}$ i.e.

$$GL(2,\mathbb{R}) = \{A \in M_{2\times2}(\mathbb{R}) \mid \det(A) \neq 0\}$$

This is a group under matrix multiplication

Define the set of scalar matrices :-

A scalar matrix is a multiple of the identity matrix :-

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

since λI is invertible for all $\lambda \neq 0$

10 Ans:

Proof:

Let G be a group and Let H and K be two subgroups of G. We want to show the intersection $H \cap K$ is also a subgroup.

step-1: show $H \cap K$ is Non-Empty. Since H and K are subgroups they both contain the identity element e of G.

$$e \in H \quad \text{and} \quad e \in K$$

Thus $e \in H \cap K$, meaning $H \cap K$ is non-empty

step-2: closure under multiplication Let

$$a, b \in H \cap K.$$

Since $H \cap K$ consists of element

$$a, b \in H \quad \text{and} \quad a, b \in K$$

Since both H and K are subgroups they are closed under multiplication, So

$a, b \in H$ and $ab \notin K$

Thus $ab \in H \cap K$ proving closure under multiplication. So we conclude that $H \cap K$ is a subgroup of G.

10 ~~[illegible]~~

Ans:

⇒ Finding the modulers Inverse using the Extended Euclidean Algorithm :-

Euclidean algorithm:

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

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

This means that 'x' is the multiplicative inverse of a modulo n, provided that a and n are coprime (i.e. $\gcd(a, n) = 1$)

We use the Extended Euclidean Algorithm (EEA) to compute x.

IT-23619

step-1 : Apply the Euclidean algorithm.

The Euclidian algorithm finds the greatest common divisor (gcd) of a and n using the division algorithm:

gcd (a,n) = gcd (n, a mod n)

we continue until we reach gcd = 1

step-2 : Apply the Extended Euclidean algorithm.

The EEA express gcd (a,n) as a linear combination:

gcd (a,n) = ax + ay

since gcd (a,n) = 1 we can rewrite this as 1 = ax + ny

Reducing modulo n:

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

Thus x is the modular inverse of a modulo n.

12 Use of the Extended Euclidean algorithm in RSA key generation :-

⇒ In RSA encryption, two large prime numbers p and q are chosen to form :

$$n = p \times q$$

The Euler totient function is computed as :-

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

A public exponent e is chosen such that

$$\gcd(e, \phi \cdot a) = 1 :$$

To find the private key d, we compute :

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

The requires finding the modulus inverse of e modulo $\phi(n)$ which is efficient computed using the Extended Euclidean algorithm.

Importance of the algorithms efficiencies is cryptography is:

→ Large prime modulii

→ Polynomial the complexity of layer

→ Avoiding Brute-force methods.

12) ECB mode is inverse for highly Redundant Data :-

⇒ In Electronic codebook (ECB) mode a plaint message p is divided into fixed size block and each block is independently encrypt using the same key K:

$$c_i = E_K(P_i)$$

Mathematical proof of ECB weakness :-

(i) Lack of Diffusion :-

⇒ Identical plaintext Blocks, produce identical 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 :-

$$C_i = E_K(P_i) = E_K(P_j) = C_j$$

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

14 Differential cryptanalysis is a chosen-plaintext attack that analyze how difference in plaintext propagate through a cipher to predict differences in ciphertext.

Defense mechanisms in DES Against DC:

1's Box Design to resist DC :-

⇒ The S-boxes in DES were carefully designed to minimize differential probabilites.

2. Feistal structure provides :

⇒ In this Feistal network of DES, the right half of the block is expanded mixed with the round key and substituted via - S-blocks.

3. key scheduling prevents simple DC attacks

⇒ The key schedule in DES ensure that

subkeys change across rounds making it harder for an attacker to track.

(i) Unlike DES, AES is not a Feistal cipher but follows a substitution - permutation vector structure to DE.

Key features that improve DC resistance

(i) Subbites (Non linear substitution using S-boxes

(ii) Shift rows (Row-wise permutation for Diffie

(iii) Mix colum for strong Diffusion

(iv) Addroundkey.

(v) More rounds in AES as AES-128 has 1. rounds

15. Define a ring in abstract algebbra and explain its key properties :

⇒

(i) Additive structure

(i) closure under addition : For all $a, b \in R$, ther sum $a+b$ is in R.

(ii) Associativity of addition :

⇒ For all $a, b, c \in R, (a+b)+c = a+(b+c)$

(iii) Additive identity :- There exists an elemen($0 \in R$ such that For all $a \in R$ $a+0=a$

(iv) Additive inverse; For every $a \in R$ there exists an element $-a \in R$ such that $a+(-a) = 0$

(v) Commutativity of addition :

For all $a, b \in R$, $a+b = b+a$

(2) multiplication structure :-

(i) closure under multiplication : For all $a, b \in R$, the product $a.b$ is in R

(ii) Associativity of multiplication : For all $a, b, c \in R$ $(a.b).c = a.(b.c)$

(3) Distributive properties :

(i) Left Distributivity

$a.(b+c) = a.b + a.c$ for all $a, b, c \in R$

(ii) Right Distributivity

$(a+b).c = a.c + b.c$ for all $a, b, c \in R$

16 Provide an example of a commutative ring and a non-commutative ring:

* Commutative ring example

⇒ The set of integers $\mathbb{Z}$ with addition and multiplication is a commutative ring. That is For all $a, b \in \mathbb{Z}$.

→ Addition : $a+b = b+a$

→ multiplication : $a \cdot b = b \cdot a$

→ It has a additive identity (0) and a multiplicative identity (1)

→ It satisfies the distributive property;

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

* Non-commutative Ring

⇒ The set of 2×2 matrices over R (the real numbers) denoted as $M_2(\mathbb{R})$ is a non-commutative ring under standard matrix addition and multiplication.

That is for some matrices $(A, B) \in M_2(R)$

→ Addition : $A+B = B+A$

→ Multiplication : $A \cdot B \neq B$.

→ It has an additive identity and a multiplication identity.

→ ~~It has an additive identity and~~ a

→ It satisfies the distributive property.

17 [H] How does the concept of a ring relate to the construction of finite fields

① Rings as a foundation :

→ A ring is an algebraic structure consisting of a set equipped with two operations that satisfy certain properties.

→ A ring can be commutative and with unity

(2) From Rings to Fields

→ A field is a special type of ring in which every nonzero element has a multiplicative inverse making division possible

→ Not all rings are fields, but every finite field must be a commutative ring with unity where every nonzero element is invertible.

(3) Constructing finite fields from Rings :-

→ The most basic finite fields is $\mathbb{Z}/p\mathbb{Z}$ the integers modulo a prime p, which forms a field, because every nonzero element has a multiplictive inverse.

~~Discuss the~~

16 Explain the vulnerabilities of the DES cipher ~~and~~

=> The data encryption standard cipher, while historically significant has several vulnerabilities that make it insecure for modern use. Here are its main weakness.

(1) short key length (Brute-Force vulnerabilities) :-

→ DES uses a 56 bit key, which is too short by modern standards.

(2) Weak and semi-weak keys :-

→ Certain keys in DES create identical encryption and decryption processes, reducing the number of unique keys available.

(3) key schedule weakness :-

→ DES uses a relatively simple key expansion process that does not sufficiently diffuse key bits.

IT 28619

~~Discuss the no~~

16. Explain the vulnerabilities of the DES cipher and

=> The data encryption standard cipher, while historically significant has several vulnerabilities that make it insecure for modern use. Here are its main weakness.

① short key length (Brute-Force vulnerabilities) :-

→ DES uses a 56 bit key, which is too short by modern standards.

② weak and semi-weak keys :-

→ Certain keys in DES create identical encryption and decryption processes reducing the number of unique keys available.

③ key schedule weakness :-

→ DES uses a relatively simple key expansion process that does not sufficiently diffuse key bits.

(4) Vulnerability to Differential and Linear cryptanalysis.

(5) Man-in-the middle attack on 2DES

(6) chosen-plaintext and known plaintext Attacks.

(7) Small block size

19 Why ~~vulnerabilities~~ DES is considered insecure for modern use.

⇒ Brute-force attacks can crack DES quickly due to its short 56-bit key

→ Cryptanalysis techniques have become more powerful

→ 64 bit block size makes it vulnerable to attacks on large datasets.

IT23619

Impact of key Length on security :-

→ DES : Vulnerable to brute force attacks as demonstrated by Deep crack.

→ Triple DED : Uses multiple rounds of DES encryptron to increase security making brute force attacks significantly harder.

→ AES : Designed as a replacement for DES, AES is resistant to brute force attacks due to its longer key lengths.

21 How did the development of AES address the shortcoming of DES, particularly in terms of key size and resistance to cryptanalytic attacks?

⇒

(1) Ans : (1) Increased key size :-

(a) DES weakness : DES uses a 56-bit key which became vulnerable to brute force attacks as computing power increased.

(2) → stronger Resistance to cryptanalytic Allack.

→ DES weakness: DES is vulnerable to various cryptanalytic techniques such as—

(i) Differential Cryptanalysis

(ii) Linear cryptanalysis

(b) → AES improvement : Uses a substitution permutation network structure instead of DES's Feistel structure making it more resistant to known attacks.

(3) Elimination of weak and semi-weak keys :-

→ DES Weakness : Certain keys in DES lead to insecure encryption patterns.

→ AES Improvement : AES's key scheduling and design ensure that no such weak keys exist.

(4) Larger Block size

→ DES Weakness : DES operates on a 64-bit block size making it susceptible to birthday attacks, and b.

→ AES Improvement → AES uses a 128-bit block size, reducing the likelihood of such attacks and improving security for large datasets.

(5) Scalability and performance

→ AES is more efficient in both software and hardware implementations compared to DES.

→ It support parallel processing making it well-suited for modern computing architectures.

22 Differential cryptanalysis is a widely known attack against block ciphers.

Explain

22 Explain how the Feistel structure of DES handles differential cryptanalysis.

⇒ Here's how the Feistel structure helps DES defend against this attack.

① Understanding Differential cryptanalysis :

→

② Role of the Feistel structure in DES.

→ DES is a 16-round Feistel cipher, where each round applies.

* A key-dependent round function
* Bitwise XOR operations
* Swaps between left and right halves.

IT-23619

(3) How DES Resists Differential cryptanalysis

→ Avalanch effects

→ 16 rounds provide security

→ complex s-box Design

→ key mixing in Each Round.

(4) Impact of differential cryptanalysis on DES

→ DES is not immune but is resilient

→ Reduced-round DES is weaker

→ This attack influenced modern cryptography.

23 How AES with it subBytes, shiftRows MixColumns and addroundkey operations, is more resistant to such attacks compared to DES ?

⇒ Here is how these operations enhance AES's resistance to attacks particularly compared to DES.

① Resistance to differential and linear cryptanalysis.

→ AES : The subBytes operation provides strong non-linearity making it difficult to trace input-bit change to output-bit change

DES → DES has a weaker s-box design compared to AES and differential cryptanalysis was successfully applied to reduced-round DES, showing some vulnerabilities.

I.T. 23619

(2) Stronger key schedule

AES → Uses a sophisticated key expension Algorithm that ensures each round key is significantly different from the previous one

DES → The DES key schedule has weak and semi-weak keys making it susceptible to related-key and differential cryptanalysis.

(3) Larger Block size :-

AES → Uses a 128-bit block size which reduces the risk of birthday attacks and ensures stronger security against brute force attempts.

(4) Elimination of weaknesses in Feistel structure

(5) Increased Number of rounds

(6) Mix Columns Provides stronger Diffusion.

(7) Resistance to Brute Force Attacks.

24. Prove that the ring Z_n is commutative and identify whether it has zero divisors. Further determine the conditions under which Z_n is a field.

⇒ Let's analyze the ring Z_n also known as the ring of integers modulo n.

(1) Proving that Z_n is commutative

⇒ The ring Z_n consist of the set $0, 1, 2 \ldots n-1$ with addition and multiplication defined modulo n. To show it is commutative we need to verify that multiplication is commutative

$[a] \cdot [b] = [b] \cdot [a]$ for all $[a] \cdot [b] \in Z_n$

$a \cdot b = b \cdot a$

$[a] \cdot [b] = [a \cdot b] = [b \cdot a] = [b][a]$

2. Zero Divisors in Z_n

= A zero divisor Z_n is element $[a]$ such that there exist element $[b]$ with

$[a] \cdot [b] = [0]$

$ab \equiv 0 \pmod{n}$, where $a, b \neq 0$ in Z_n

Example: In Z_6

$[2][3] = [6] = [0]$

Thus Z_n has zero divisors if and only if n is not prime

(3) When is Z_n a field?

= A ring Z_n is a field if every nonzero element has a multiplicative inverse

An element $[a]$ has a inverse if only if

$\gcd(a, n) = 1$

Thus Z_n is a field if only if 2 is prime

(5) Scalability and performance

→ AES is more efficient in both software and hardware implementations compared to DES.

→ It support parallel processing making it well-suited for modern computing architectures.

22 Differential cryptanalysis is a widely known attack against block ciphers.

Explain

22 Explain how the Feistel structure of DES handles differential cryptanalysis.

⇒ Here's how the Feistel structure helps DES defend against this attack.

① Understanding Differential cryptanalysis :

→

② Role of the Feistel structure in DES.

→ DES is a 16-round Feistel cipher, where each round applies.

* A key-dependent round function
* Bitwise XOR operations
* Swaps between left and right halves.

IT-23619

(3) How DES Resists Differential cryptanalysis

→ Avalanch effects

→ 16 rounds provide security

→ complex s-box Design

→ key mixing in Each Round.

(4) Impact of differential cryptanalysis on DES

→ DES is not immune but is resilient

→ Reduced-round DES is weaker

→ This attack influenced modern cryptography.

23 How AES with it subBytes, shiftRows MixColumns and addroundkey operations, is more resistant to such attacks compared to DES ?

⇒ Here is how these operations enhance AES's resistance to attacks particularly compared to DES.

① Resistance to differential and linear cryptanalysis.

→ AES : The subBytes operation provides strong non-linearity making it difficult to trace input-bit change to output-bit change

DES → DES has a weaker s-box design compared to AES and differential cryptanalysis was successfully applied to reduced-round DES, showing some vulnerabilities.

I.T. 23619

(2) Stronger key schedule

AES → Uses a sophisticated key expension Algorithm that ensures each round key is significantly different from the previous one

DES → The DES key schedule has weak and semi-weak keys making it susceptible to related-key and differential cryptanalysis.

(3) Larger Block size :-

AES → Uses a 128-bit block size which reduces the risk of birthday attacks and ensures stronger security against brute force attempts.

(4) Elimination of weaknesses in Feistel structure

(5) Increased Number of rounds

(6) Mix Columns Provides stronger Diffusion.

(7) Resistance to Brute Force Attacks.

24. Prove that the ring Z_n is commutative and identify whether it has zero divisors. Further determine the conditions under which Z_n is a field.

⇒ Let's analyze the ring Z_n also known as the ring of integers modulo n.

(1) Proving that Z_n is commutative

⇒ The ring Z_n consist of the set $0, 1, 2 \ldots n-1$ with addition and multiplication defined modulo n. To show it is commutative we need to verify that multiplication is commutative

$[a] \cdot [b] = [b] \cdot [a]$ for all $[a] \cdot [b] \in Z_n$

$a \cdot b = b \cdot a$

$[a] \cdot [b] = [a \cdot b] = [b \cdot a] = [b][a]$

2. Zero Divisors in Z_n

= A zero divisor Z_n is element $[a]$ such that there exist element $[b]$ with

$[a] \cdot [b] = [0]$

$ab \equiv 0 \pmod{n}$, where $a, b \neq 0$ in Z_n

Example: In Z_6

$[2][3] = [6] = [0]$

Thus Z_n has zero divisors if and only if n is not prime

(3) When is Z_n a field?

= A ring Z_n is a field if every nonzero element has a multiplicative inverse

An element $[a]$ has a inverse if only if

$\gcd(a, n) = 1$

Thus Z_n is a field if only if 2 is prime

23 Why the linearity of LFSRs makes them vulnerable to known-plaintext attacks and porcopose a mathematical method to mitigate this vulnerability.

Ans:

⇒ The main reason is that LFSRs makes them vulnerable to know-plaintext

① Linear Recurrence Relations:

→ An LFSR of length n follows a linear recurrence relation:

$$S_{t+n} = C_0 S_t + C_1 S_{t+1} + \cdots + C_{n-1} S_{t+n-1}$$

② known plaintext Attack

→ if the attacker has access to plaintext and its corresponding ciphertext they can derive the key stream.

Mathematical Mitigation:

① Non-linear combining function

$$K_t = f(S_t^{(1)}, S_t^{(2)}, \ldots S_t^{(m)})$$

② Non-linear filter function

$$K_t = f(S_t, S_{t+1} \ldots S_{t+n-1})$$

③ clock controlled or irregular clocking LFSRs.