Md. Safayat Hossain
IT-24667

1. 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 cryptographic protocols, and propose possible post-quantum cryptographic algorithm that could replace RSA and ECC. How do these algorithms resist quantum cryptoanalysis.

Ans: Impact of quantum computing on cryptographic algorithm:

① Vulnerability of RSA and ECC: Quantum computers can run shor's algorithm, which efficiently breaks integers factorization and discrete logarithm problems. Since RSA and ECC are based on these problems, they become insecure against quantum attacks.

② Failure of key Exchange and digital signature: Widely used protocols such as TLS, SSL and pKI rely on RSA and ECC for key exchange and authentication. Quantum attacks would allow adversaries to derive private keys and forge digital signatures.

③ Long-Term data security Risk: Attackers can store encrypted data today and decrypt it in the future using quantum computers. Threatning sensitive information.

Md. Safayat Hossain
IT-24667

4. Limited impact on symmetric cryptography: Grovers algorithm provides only a quaredic speed up for brute-force attacks. This can be mitigated by largyer key sites (eg., AES 256).

5. Need for cryptographic migration: Existing systems must transition to quantum-resistant algorithms to ensurce future security of communication and digital infrastructure.

past quantum cryptographic Algorithms and their Resistance:

1. Lattice Based cryptography: Algorithms such as CRYSTALS-kyberc and CRYSTALS-Dilithium arce based on hard lattice problems like Learning with Errorcs CLWE), which have no known quantum solutions.

2. Code-Based cryptography: Schemes like McEliece rely on the difficuly of decoding random linearc codes, a problem that raemains hard even for the quantum computercs.

3. Hash-Based signaturce Schemas: Algorithms such as SPHINCS+ depend on secure hash functions. Quantum attacks only reduce

P.T.O

security quardically, which is countered by largyerc hash sizes.

4. Resistance to shore's Algorcithm: Post-quantum algorcithms arce not based on factorization orc discrcete algorcithms, so shore's algorithm canit be applied to brceak them.

5. Standarcization and prcactical use: Many post-quantum schemes arce being standarcized by NIST and arce suitable rceplacement for RSA and ECC in rceal-world crcyptographic prcotocols.

Md. Safayat Hossain
IT-24662

2. Design and implement a novel psedo-Random Number Generator (PRNG) algorithm in python using: The current timestamp, The process ID (os.pid) for added randomness, a modules operation to constrain the output within a desired range.

Ans: A design of pseudo-Random Number Generator (PRNG) is an algorithm used to generate sequence of numbers that approximate random behaviour using deterministic computations. PRNGs are widely applied in simulations, modeling and software testing where controlled randomness is required.

Algorithm design: The proposed PRNG uses the current timestamp and process id (PID) as entropy sources to initialize the seed. The timestamp introduces time-based variability while PID ensures process-level uniqueness. These values are combined using a bitwise XOR operation to improve randomness. The seed is updated iteratively using a recurrence relation inspired by Linear Congruential Generator (LCG) model. This step ensures that each

P.T.O

Md. Safayat Hossain
IT-20607

generated value depends on previous one, forming a pseudo random sequence. A module operation is applied to constrain the output within a predefined range suitable for practical applications.

Implementation: The algorithm is implemented in python using the built in libraries.

```
import time
import os
timestamp = int(time.time_ns())
pid = os.getpid()
seed = timestamp ^ pid
a = 1664525
c = 1013904223
modulus = 100
seed = (a*seed + c)
random_numbers = seed % modulus
print(random_numbers)
```

Conclusion: The designed PRNG provides simple and efficient pseudo-random number generation.

Md. Safayat Hossain
IT-20008

3. Compare traditional ciphers (such as caesar cipher, vigenére cipher and playfair ciphers) with modern symmetric ciphers like AES and DES. Discuss the strengths and weakness of each type of ciphers, including key length, including encryption/decryption speed, and security against modern cryptanalysis techniques.

Ans: Traditional ciphers such as caesars, playfair and vigenére are classical substitution or polyalphabetic ciphers designed for manual encryption. Modern ciphers like DES and AES are symmetric-key block ciphers developed for digital and computational environment.

Key length and key space: Traditional ciphers use very small or limited keys, making them very easy to guess. Modern cipher uses large key sizes.

Encryption and Decryption speed: Traditional ciphers are fast and simple but inefficient for large digital data. Modern ciphers

p.t.o

are optimized for high speed encryption and decryption in both software and hardware.

Security strength: Traditional ciphers are very low in terms of the security measurements. Modern ciphers are very robust and scalable.

Resistance to cryptoanlysis: Traditional ciphers are resistance to cryptoanlysis, Kaiseski examination and brute force attacks.

Md. Sufyat Hassain
IT-20005

4. Let S_4 be the symmetric group on the set $\{1,2,3,4\}$. Define an action of S_4 on the set of 2-element subsets of $\{1,2,3,4\}$, prove that this action is well defined, and compute the size of the orbit and stabilizer of the subset $\{1,2\}$.

Soln: Let X be the set of 2-element subsets of $\{1,2,3,4\}$:

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

Define an action of S_4 on X by:

$$\sigma \cdot \{i,j\} = \{\sigma(i), \sigma(j)\}, \text{ for } \sigma \in S_4$$

Proof that the action is well defined

1. For any 2-element subset $\{i,j\}$, $\{\sigma(i), \sigma(j)\}$ is also a 2-element subset because σ is bijection.
2. The identity $e \in S_4$ satisfies $e \cdot \{i,j\} = \{i,j\}$
3. Compability for $\sigma, \tau \in S_4$:

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

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

orbit of $\{1,2\}$

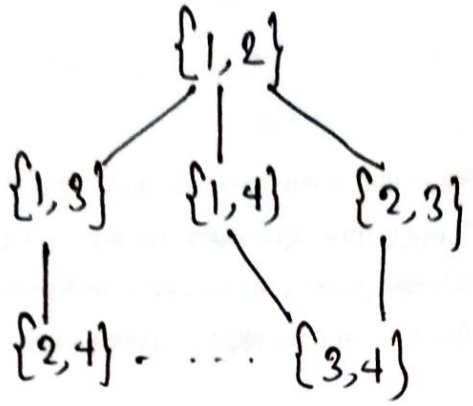
$$\text{orb}(\{1,2\}) = \{\sigma \cdot \{1,2\} : \sigma \in S_4\} = X$$

$$|\text{orb}(\{1,2\})| = 6$$

P.T.O

Md. Saifyad Hassain
IT-20005

Orbit diagram:



$Stab(\{1,2\}) = \{G \in S_4 : G.\{1,2\} = \{1,2\}\}$

permutations that fix {1,2}:

→ id
→ (1,2)
→ (3,4)
→ (1,2)(3,4)

$|Stab(\{1,2\})| = 4$

{1,2} ... fixed by ... → id, (1,2), (3,4), (1,2)(3,4)

Verification of (orbit-stabilizer theorem)

$|S_4| = |Orb(\{1,2\})| \cdot |Stab(\{1,2\})| = 6 \cdot 4 = 24$

Md. Safayet Hossain
IT-20026

5. Let GF(2^2) be the finite field of order 4, constructed using the irreducible polynomial x^2+x+1 over GF(2).

(i) Show that GF(2^2) forms a group under multiplication.

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

Ans: Let $GF(2^2)^* = GF(2^2) \setminus \{0\} = \{1, x, x+1\}$

1. closure:

$x.x = x^2 \equiv x+1 \pmod{x^2+x+1}$

$x.(x+1) \equiv x^2+x \equiv (x+1)+x = 1$

$(x+1).(x+1) = x^2+2x+1 \equiv x^2+1 \equiv x+1+1 = x$

All products are in $\{1, x, x+1\}$

2. Identity:

$1.a = a.1 = a$

3. Inverse:

(i) $1^{-1} = 1$,

(ii) $x^{-1} = x+1$ (since $x(x+1) = 1$)

(iii) $(x+1)^{-1} = x$

4. Associativity: Multiplication in a field is always associative.

P.T.O

Md. Safayet Hossain
IT-20005

Verify if $GF(2^4)^*$ is cyclic:

A group is cyclic if there exists an element g such that $\langle g \rangle = GF(2^4)^*$

check x:

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

$$\langle x \rangle = \{1, x, x+1\} = GF(2^4)^*$$

The multiplicative group of nonzero elements of $GF(2^4)$ is cyclic order of 3.

Md. Sufayet Hossain
IT-20005

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 subgroup of $GL(2,R)$. Construct corresponding factor group, and interpret its structure.

Ans:

Let $GL(2,R) = \{A \in M_2(R) : \det A \neq 0\}$.

1. Scalar matrices form a subgroup:

$S = \{\lambda I_2 : \lambda \in R^*\}$,

where $R^* = R \setminus \{0\}$

Closure: $(\lambda I)(\mu I) = (\lambda\mu) I \in S$

Identity: $1.I \in S$

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

2. Normality of the scalar subgroup:

Take any $A \in GL(2,R)$ and any $\lambda I \in S$ then,

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

Hence $A(\lambda I)A^{-1} \in S$ for all A, so

$$ASA^{-1} = S$$

Therefore, the scalar matrices form a normal subgroup of $GL(2,R)$

3. The factor group:

The quotient group is

$$GL(2,R)/S = GL(2,R)/\{\lambda I : \lambda \neq 0\}$$

Two matrices $A, B \in GL(2,R)$ is in the

P.T.O

Md. Sakhawat Hossain
IT-20005

Same coset if and only if

$$B = hA \text{ for some } h \in R^{\times}$$

The quotient group is called the projective general linear group.

$$PGL(2,R) := GL(2,R)/R^{\times}I.$$

4. Interpretation of the structure:

Multiplying a matrix by a nonzero scalar does not change the induced linear transformation on projective space RP^1. Hence $PGL(2,R)$ is the group of projective linear transformation of the real projective line.

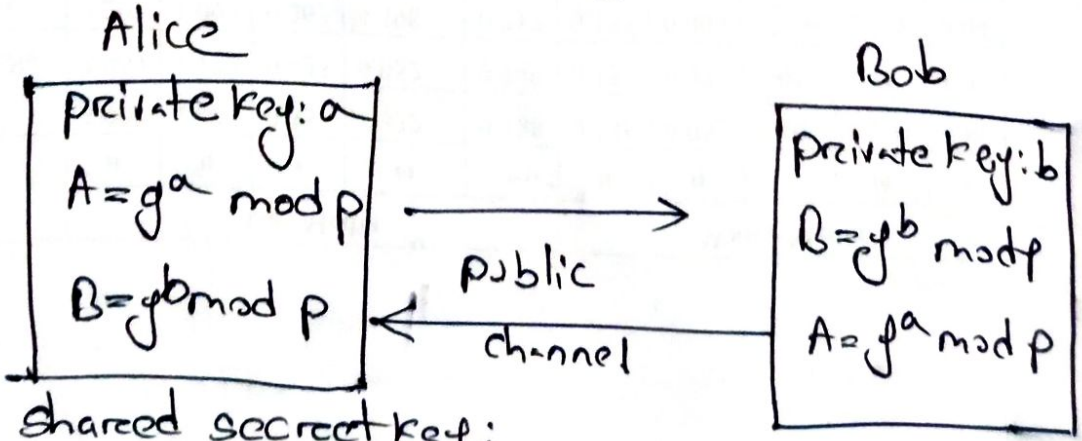
$$M \longrightarrow \frac{ax+b}{cx+d}, \quad ad-bc \neq 0$$

Md. Sadyat Hossar
IT-20005

7. Explain the Diffe-Hellman key exchange protocol and it's application in secure communication. Discuss the security of the Diffe-Hellman protocol Against common attacks such as man-in-the-middle and the role of the discrete Iggarithm problem in ensuring its security. What would be the impact of the protocol's security if the prime modules used is not sufficiently large?

Ans: The Diffe-Hellman key exchange is a cryptographic ~~problem~~ protocol that enables two parties to establish a shared secret key over an insecure communication channel. This shared key is later used for secure encryption.

Both parties publicly agree on a large prime number p and a generator g. Alice chose a private key a and Bob chose a private key b.



Shared secret key:

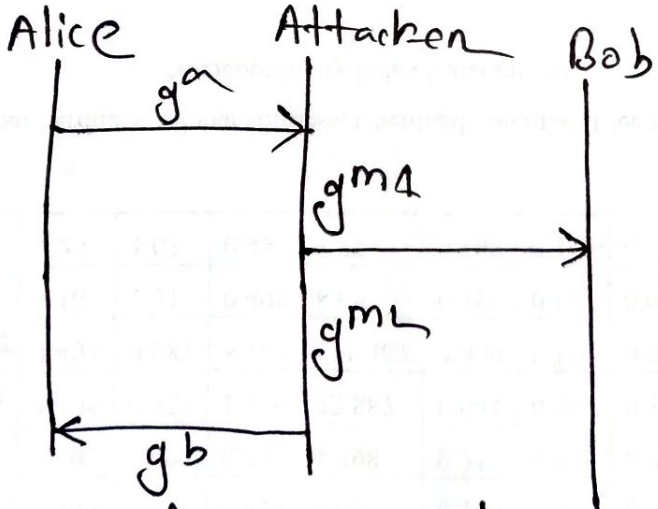
$K = (g^b)^a \bmod p$ ~~$= (g^a)^b \bmod p$~~ $= g^{(ab)} \bmod p$

Md. Safayat Hossain
IT-20005

Both Bob and Alice compute the same shared key K without transmitting it directly.

Security of Diffie-Hellman: The security of Diffie Hellman depends on the discrete logarithm problem, which makes it computationally infeasible to determine the private keys a or b from the public values g^a and g^b. Hence, an eavesdropper can't compute the shared key.

Man in the middle attack: If Diffie-Hellman is used without authentication, it's vulnerable to a man-in-the middle attack.



Effects of using small prime modules: If the prime modulus p is not sufficiently large

(i) Discrete logarithms can be computed efficiently.

(ii) The shared secret key can be broken.

Md. Safayet Hossain
IT-20005

8. Let G be a group, and let H be a subgroup of G. Prove that the intersection of any two subgroups of G is also a subgroup of G. Provide an example using specific groups.

Ans: Let G, be group and let $H_1, H_2 \leq G$ be subgroups. Then $H_1 \cap H_2$ is also a subgroup of G.

(i) Non-empty: Since H_1 and H_2 are subgroups, both contains the identity element e of G.

(ii) Closure: Let $x, y \in H_1 \cap H_2$

then $x, y \in H_1$ and $x, y \in H_2$.

Since, both H_1 and H_2 are subgroups, $xy \in H_1$ and $xy \in H_2$.

therefore $xy \in H_1 \cap H_2$.

(iii) Inverse:

Let $x \in H_1 \cap H_2$ then $x \in H_1$ and $x \in H_2$

Since, subgroups contain inverse, $x^{-1} \in H_1$ and $x^{-1} \in H_2$

Since, the intersection is non-empty and closed under the group operation and inverse

$$H_1 \cap H_2 \leq G$$

Md. Safayat Hossain
IT-20005

9. Prove that the ring $\mathbb{Z}_n$ is commutative and identify whether it has zero divisors. Further, determine the conditions under which $\mathbb{Z}_n$ is a field.

Ans: Defination of $\mathbb{Z}_n$:

Let, $\mathbb{Z}_n = \{\bar{0}, \bar{1}, \bar{2}, \ldots, \overline{n-1}\}$

be the ring of integers modulo n, with addition multiplication defined by

$$\bar{a} + \bar{b} = \overline{a+b}, \quad \bar{a} \cdot \bar{b} = \overline{ab}$$

$\mathbb{Z}_n$ is commutative Ring:

Addition, $\bar{a} + \bar{b} = \overline{a+b} = \overline{b+a} = \bar{b} + \bar{a}$

Multiplication, $\bar{a} \cdot \bar{b} = \overline{ab} = \overline{ba} = \bar{b} \cdot \bar{a}$

Since, integers addition and multiplication are commutative, the induced operations in $\mathbb{Z}_n$ are also commutative too.

Hence, $\mathbb{Z}_n$ is commutative ring (with unity 1)

Zero division in $\mathbb{Z}_n$: A zero divisor is a nonzero element $\bar{a} \in \mathbb{Z}_n$, such that there exists a nonzero $\bar{b} \in \mathbb{Z}_n$ with

$$\bar{a} \cdot \bar{b} = \bar{0}.$$

in $\mathbb{Z}_n$:

$$\bar{a} \cdot \bar{b} = \bar{0} \longleftrightarrow n \mid ab$$

P.T.O

Md. Safayat Hossain
IT-20005

If n is composite, say $n = rs$ with $1 < r, s < n$,
then

$$\bar{r} \neq 0,\ \bar{s} \neq 0,\ \bar{r}.\bar{s} = \overline{rs} = \bar{0}$$

Hence, $\mathbb{Z}_n$ has zero divisors.

If n is prime, then $a|ab$ implies $n|a$ or $n|b$

Thus, no nonzero divisors exist.

When $\mathbb{Z}_n$ is a field

(i) If it's commutative.
(ii) It has multiplicative identity.
(iii) Every nonzero element has a multiplicative inverse.

Md. Safayat Hossain
IT-20006

10. Explain the vulnerabilites of the DES cipher and why it's considered insecurced for modern use. Discuss the role of brute-force attacks in breaking DES and the impact of key length on the security algorithm. How did the development of AES address the shortcomings of DES, particularly in terms of key size and resistance to cryptoanalysis attacks?

Ans: The data encryption standard is a symmetric key block cipher that encrypts data in a 64 bit blocks using a 56-bit key. Although the DES was widely used in the past, it's now considered insecure due to several vulnerabilities.

Key vulnerability of DES: The primary weakness of DES is its short key length 56 bits. With advances of computing power, it has becom feasible to try all possible keys using brute-force attack. Tody DES key can be broken less than a second.

P.T.O

Md. Sarfaraz Hossain
IT-20008

Role of brute force attack by key length:

A brute force attack involves systematically trying every possible key untill the corrected one is found. Total number of DES keys is 2^{56}, which is considered secure but now its too small.

(i) Short key length → fewer possible keys.
(ii) Fewer keys → faster brute force attacks,
(iii) Hence DES offers insufficient security for modern system.

Other cryptographic weakness:

64 bit blocksize makes DES vulnerable to statistical attacks when large amounts of data are encrypted.

How AES addressed the shortcomings of DES

(i) Larger key sizes: 128, 192, 256 bits
(ii) Larger blocksize 128 bits
(iii) Strong resistance to cryptoanlysis attack.
(iv) Efficient in both hardware and software.

Md. Safayat Hossain
IT-20005

11. Differential cryptanalysis is widely known attack against block ciphers.
   (i) Explain how the Feistel structure of DES handles differential cryptanalysis.
   (ii) How AES, with its subBytes, ShiftRows, MixColumns, and AddRoundKey operation is more resistant to such attacks compared to DES?

Ans: Differential cryptanalysis is a chosen plain ~~text~~ attack that studies how different plain-text pairs affect the differences in the corresponding ciphertext pairs. The goal is to discover information about the secret key by exploiting the non random behaviour of the cipher.

(i) Feistel structure of DES and Differential cryptanalysis:

DES is based on a 16-round Feistel structure where each round splits the input block into two halves and applies non-linear round function.

(i) S-Boxes: The main difference of DES against lies in the S-Boxes. These S-boxes are designed to minimize high-probability input-output difference patterns, making it difficult to predict how difference propagate

P.T.O

Md. Safayat Hossain
IT-20006

through rounds.

(ii) Multiple rounds (16 rounds): Each rounds spreads differences further across the blocks. As the number of rounds increases, the probability of a useful differential characteristics decrease exponentially.

(iii) Key Mixing in Each round: The round key is combined with the data before substitution, ensuring the different patterns depend on unknown by bits.

(2) Why AES is more Resistant than DES:
AES uses a substitution-permutation Network (SPN) instead of Feistel structure. Its round operation provide much stronger diffusion and non linearity.

(i) SubBytes (Nonlinearity):
(a) uses a strong, mathmatically defined S-Box based on inversion in a finite field.
(b) provide high resistance to both differential and linear cryptanalysis.
(c) No known differential characteristics.

P.T.O

Md. Safayat Hossain
IT-20006

(ii) ShiftRows (Diffusion):

(a) permutes rows of the state matrix.

(b) Ensures that by differences spread across columns.

(iii) MixColumns (Strong Diffusion):

(a) Combines bytes within each column using matrix multiplication over a finite field.

(b) Rapidly spreads the input differences across the entire state.

(iv) AddRoundKey (Key Mixing):

(a) XORS the round key with the state.

(b) Ensures that differences depend on the secret key at every round.

Md. Safayat Hossain
IT-20005

12. using the Extended Euclidean Algorithm, demonstrate how to find the modular inverse of an integer 'a' modulo 'n' (where 'a' and 'n' are coprime). How is this algorithm utilized in RSA key generation, and why is the efficiency of this algorithm is important for large scale cryptographic systems?

Ans: Modular inverse using the extended Eudidean Algorithm:

Let a and n be integers such that

$$\gcd(a, n) = 1$$

The modular inverse of a mod n is an integer a^{-1} satisfying

$$a \cdot a^{-1} \equiv 1 \pmod{n}$$

The Extended Euclidean Algorithm (EEA) finds integers x and y such that

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

Since $\gcd(a, n) = 1$, this becomes

$$ax + ny = 1$$

and reducing modulo n gives

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

Hence, x mod n is the modular inverse of a.

P.T.O

Md. Safqat Hossain
IT-20005

Finding modulare inverse:

a=7 modulon=26

Apply the Euclidean Algorithm:

$26 = 7.3 + 5$

$7 = 5.1 + 2$

$5 = 2.2 + 1$

$2 = 1.2 + 0$

Now backsbstitute:

$1 = 5 - 2.2$

$= 5 - (7-5).2$

$= 3.5 - 2.7$

$= 3(26 - 7.3) - 2.7$

$= 3.26 - 11.7$

Thus,

$1 = 3.26 - 11.7$

So,

$7(-11) \equiv 1 \pmod{26}$

Therefore, the modulare inverse is

$7^{-1} \equiv 15 \pmod{26}$

(Since $-11 \equiv 15 \pmod{26}$).

use of Extended Euclidean Algorithm in RSA.

In RSA key generations:

① chose two largye prines p and q.

② Compute $n = pq$

③ Compute Eulen toitent $\phi(n) = (p-1)(q-1)$

P.T.O

Md. Safayet Hossain
IT-20006

④ chose a public exponent e such that

$$\gcd(e, \phi(n)) = 1$$

⑤ Compute the private key d such that,

$$ed \equiv 1 \pmod{\phi(n)}.$$

Md. Sahajat Hossain
IT-10005

13. Consider the following modes of operation for block ciphers: ECB (Electronic Codebook), CBC (cipher code block chaining), and CTR (Counter mode).

(i) For a block cipher with size n, mathematically prove why ECB mode is insecure for encrypting high redundant data.

(ii) derive the recurrence relation for CBC mode encryption and decryption and prove that error propagation is limited in decryption.

Ans:

(i) Why ECB mode is insecure for Highly redundant data:

Let E_K be a block cipher with block size n,

In ECB mode a plaintext $M=(M_1, M_2, \ldots, M_t)$ is encrypted as

$$C_i = E_K(M_i)$$

ECB is deterministic, meaning:

$$M_i = M_j \Rightarrow C_i = C_j$$

Highly redundant data contains repeated plaintext blocks (e.g., images, formatted text). Since ECB encrypts each block independently

P.T.O

Md. Safayat Hossain
IT-20085

identical plaintext blocks ~~(e.g.,)~~ produce.
As a result, an attacker can observe operation repetition patterns in the ciphertext and infers structural information about the plain text.
Thus, ECB leaks information about plaintext redundancy and fails to provide semantic security CIND-CPA), making it insecure for encrypting highly redundant data.

(ii) CBC Mode Recurrence Relations and Error propagation:

Let IV be an initialization vector. The vector encryption process is:

$C_0 = IV$

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

CBC Decryption

Assume a single-bit error occurs in ciphertext block c_j.

$M_j = D_K(C_j) \oplus C_{j-1}$: entire block M_j becomes corrupted.

$M_{j+1} = D_K(C_{j+1}) \oplus C_j$: only the corresponding bit is affected.

P.T.O

Md. Safayat Hossain
IT-20005

14. Why the linearity of LFSRs makes them vulnerable to known plaintext attacks, and propose a mathematical method to mitigate this vulnearcbility.

Ans: A Linear Feedback shift Register (LFSR) generates a keystream using linear operation over the finite field F2. The state update and output functions of LSFRS are linear. If the internal state at time t is S_t, the output bit can be written as:

$$z_t = \sum_{i=1}^{n} c_i s_t^{(i)} \pmod 2$$

In a steam cipher, encryption is formed as:

$$C_t = P_t \oplus z_t$$

under a known plaintext attack, the attacker knows the both P_t and C_t, allowing direct recovery of the keystream:

$$z_t = C_t \oplus P_t$$

Since each keystream bit is linear equation in the unknown initial state bits of the LFSR, collecting a sufficient number of keystream bits over F_2.

Md. Safayt Hassain
IT-20006

Mitigation using nonlinearity: To mitigate this vulnerability, nonlinearity is introduced into the keystream generation. A common mathmatical method is to apply a nonlinear Boolean function is to selected LFSR state bits:

$$z_t = f(s_t^{(i_1)}, s_t^{(i_2)}, \ldots, s_t^{(i_k)})$$

where f contains higher-degree terms (e.g., AND operations).

This transforms the attack problem from solving linear equations to solving nonlinear equations, which is computationally infeasible in practice.

Md. Saifat Hossain
IT-20008

15. Let M be the set of all possible plaintexts, K the set of keys, and C the set of ciphertext in a cryptographic system.

(i) State Shannon's defination of perfect secrecy mathmatically.

(ii) Prove that one-Time pad achieves perfect secrecy under the condition that the key is uniformly random and $|K| \geq |M|$.

(iii) Critically analyte why perfect secrecy is impractical for large scale communication syetem.

Ans:

i) Shannon's Defination of perfect secrecy:

① Let M be the set of plaintext.
② Let C be the set of ciphera text.
③ K be the set of keys.

A cryptosytem achieves perfect secrecy if for all plaintexts $m \in M$ and ciphertexts $c \in C$:

$$Pr(M=m \mid C=c) = Pr(M=m)$$

Equivalently

$$Pr(C=c \mid M=m_1) = Pr(C=c \mid M=m_2), \quad \forall m_1, m_2 \in M$$

This means the observing ciphertext provides no information about the plaintext.

Md. Safayet Hossain
IT-20006

(ii) Proof that one-time pad Acheives perfect secrecy:

One time pad encryption

Let
① $M, K, \in \{0,1\}^n$
② key K is chosen uniformly at random
③ Encryption, $C = M \oplus K$

proof: For any fixed plaintext m and ciphertext c, there exists only one key:

$$K = m \oplus c$$

since keys are uniformly random:

$$Pr(K=k) = \frac{1}{|K|}$$

Thus: $Pr(C=c | M=m) = Pr(K = m \oplus c) = \frac{1}{|K|}$

The probability is independent of m, hence

$$Pr(C=c | M=m) = Pr(C=c | M=m_2)$$

Therefore, by Shannon's defination, the one time pad provides perfect secrecy, provided

ⓐ The key is uniformly random.
ⓑ The key is at least as long as the message (i.e., $|K| \geq |M|$)
ⓒ The key is used only once.

P.T.O

Md. Safqat Hossain
IT-20005

(iii) Why perfect secrecy is impractical in practice:

① Key length requirement: The key must be as long as the message, making the key storage and management costly.

② Key distribution problem: Securely distributing large random keys to all communicating parties difficult.

③ One time use constraints: Key must never be reused; reuse leads to immediate security compromise.

Md. Safqat Hassan
IT-20005

16. A linear Congruential Generator (LCG) is defined by the recurrence relation: $x_{n+1} = ax_n + c \bmod m$ where x_n is the sequence of pseudo-random numbers, and a, c, and m are integers parameters representing the multiplier, increment, and modulus, respectively. Using specific values for a, c, and m, compute the first 5 numbers of a LCG sequence starting with the given seed $x_0 = 7$.

Ans: Since the parameters are not specified, we chose simple, standard values suitable for assignment calculation.

Let $a=5, c=3, m=16, x_0=7$

The LCG reccurence relation is:

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

Step by step computation

1. $x_1 = (5.7+3) \bmod 16 = 38 \bmod 16 = 6$
2. $x_2 = (5.6+3) \bmod 16 = 33 \bmod 16 = 1$
3. $x_3 = (5.1+3) \bmod 16 = 8 \bmod 16 = 8$
4. $x_4 = (5.8+3) \bmod 16 = 43 \bmod 16 = 11$
5. $x_5 = (5.11+3) \bmod 16 = 58 \bmod 16 = 10$

Md. Safayat Hossain
IT-20006

17. Define a ring in abstract algebra and explain its key properties. Provide an example of a commutative ring and a non commutative ring. How does the concept of a ring relate the construction of finite fields, and what role do rings play in cryptographic algorithms like RSA.

Ans: Defination of a Ring: A ring is a set of R with two operations, addition (+) and multiplication (.) such that:

1. (R, +) is an abelian group: addition is associative and commutative, has an additive identity 0, and every element has an additive inverse.
2. Multiplication is associative $a.(b.c) = (a.b).c$
3. Distributive laws holds:

$$a.(b+c) = (a.b + a.c),$$
$$(a+b).c = (a.c + b.c)$$

4. A ring may have a multiplicative identity 1 or may not be commutative.

Rings and Finite Fields: A finite field is a commutative ring with unity where every non-zero element has a multiplicative inverse.

Ex: $F_p = Z_p = \{0, 1, 2, \ldots, p-1\}$ (mod prime p).

P.T.O

IT-20005
Md. Safayat Hossain

Rings provide the structure for constructing finite fields using polynomials rings are modulare arithmetic.

Role of Rings in Cryptography:

(1) RSA uses the ring of integers modulo n, $Z_n = \{0, 1, \ldots, n-1\}$, with addition and multiplication modulo n.

(2) The invertible elements in this ring, Z_n^*, form a multiplicative group, essential for exponentiation.

(3) Ring properties ensure that encryption decryption satisfy:

$(M^e)^d \equiv M \pmod n$, for all $M \in Z_n$

The algebraic structure underpins the security and correctness of RSA.

Md. Safayat Hossain
IT-20065

18. Given an RSA key pair with the public key (e,n) and the private key d, where: p=5, q=11 (two prime numbers), n=p.q and $\phi(n)=(p-1)(q-1)$. use the RSA algorithm to encrypt the message, M=2 and decrypt the ciphertext to recover the original message. Let p=7, q=3, sign the hash message H(m)=3 using the private key d. Verify the signature using the public key (e,n). Explain how the signature ensures the integrity and authenticity of the message.

Ans:

RSA Encryption and Decryption:

given p=5, q=11

$n=pq=5\times11=55$

$\phi(n)=(p-1)(q-1)=4\times10=40$

chose a public key exponent e such that gcd(e,40)=1.

Let e=3

compute the private key d such that:

$e\cdot d\equiv 1 \pmod{40}$

$3d\equiv 1 \pmod{40} \Rightarrow d=27$

Md. Safayat Hossain
IT-20005

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

private key: $d = 27$

Message: $M = 2$

Encryption: $C = M^e \bmod n$

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

Decryption: $M = C^d \bmod n$

$= 8^{27} \bmod 55$

$= 2$

Thus, the original message is successfully recovered.

RSA digital signature and verification:

given $p = 7$, $q = 3$

$n = pq = 7 \times 3 = 21$

$\phi(n) = (7-1)(3-1) = 6 \times 2 = 12$

chose e such that $\gcd(e, 12) = 1$

Let $e = 5$

Find d such that

$e.d \equiv 1 \pmod{12}$

$5d \equiv 1 \pmod{12}$

$\Rightarrow d = 5$

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

P.T.O

private key: $d = 5$

Hash of message: $H(m) = 3$

Signature generation:

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

$s = 3^5 \bmod 21$

$= 243 \bmod 21$

$= 12$

Signature $s = 12$

Signature verification

$v = s^e \bmod n$

$= 12^5 \bmod 21 = 3$

Md. Safayat Hossain
IT-20005

19. Given the elliptic curve equation $y^2 = x^3 + ax + b \bmod p$, where $p=23$, $a=1$ and $b=1$:

(i) verify if the point $p=(3,10)$ lies on the curve.

(ii) Find the result of doubling the point $p(2p)$ using the elliptic curve point doubling formula.

(iii) compute the addition of $p=(3,10)$ and $q=(9,7)$ on the curve.

Ans: Given elliptic curve:

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

Where, $p=23$ $a=1$, $b=1$

So, the curve is $y^2 = x^3 + x + 1 \pmod{23}$

i) Verification of point $p=(3,10)$

Left-hand side:

$y^2 = 10^2 = 100 \bmod 23 = 8$

Right hand side:

$x^3 + x + 1 = 3^3 + 3 + 1 = 27 + 3 + 1 = 31 \bmod 3$

$= 8$

Since LHS = RHS, the point $p=(3,10)$ lies on

P.T.O

Md. Safqat Hossain
IT-20005

the elliptic curve.

ii) Point Doubling: compute 2P

point doubling formula:

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

For P = (3, 10):

Numerator:

$$3x_1^2 + a = 3(3)^2 + 1 = 28 \bmod 23$$
$$= 5$$

Denominator:

$$2y = 20$$

Multiplicative inverse of 20 mod 23 is 15, since:

$$20 \times 15 = 1 \bmod 23$$

So, $\lambda = 5 \times 15 = 75 \bmod 23 = 6$

Now, compute co-ordinates:

$$x_3 = \lambda^2 - 2x = 6^2 - 6 = 36 - 6 = 30 \bmod 23 = 7$$

$$y_3 = \lambda(x - x_3) - y = 6(3 - 7) - 10$$
$$= -34 \bmod 23 = 12$$

So, 2P = (7, 12)

P.T.O

Md. Safayat Hossain
IT-20006

iii) point Addition: compute P+Q, where

Q=(9,7)

slope formula

$$\lambda = \frac{y_Q - y_P}{x_Q - x_P} \bmod p$$

$$= \frac{7-10}{9-3} \bmod 23$$

$$= -3 \bmod 23$$

$$= 20$$

Inverse of 6 mod 23 is 4, since:

$6 \times 4 \equiv 1 \bmod 23$

$\lambda = 20 \times 4 = 80 \bmod 23 = 11$

Now compute co-ordinates:

$$x_3 = \lambda^2 - x_P - x_Q = 11^2 - 3 - 9$$

$$= 109 \bmod 23 = 17$$

$$y_3 = \lambda(x_P - x_3) - y_P = 11(3-17) - 10$$

$$= -164 \bmod 23 = 20$$

$$P+Q = (17, 20)$$

Md. Safayat Hossain
IT-20005

20. Suppose an elliptic curve $y^2 = x^3 + 7x + 10 \mod 37$ is used for ECDSA, with the base point $G(2,5)$ and order $n=19$. Generate a private key $d=9$ and compute the corresponding public key $Q = dG$ using scalar multiplication.

i) Sign the hash of a message $H(M)=8$ using a random nonce $k=3$.

ii) Compute the signature pair (r,s) using ECDSA formulas.

iii) Verify the signature (R,S) using the public key Q and demonstrate that the signature is valid.

Ans:

Given, Elliptic curve:

$E: y^2 = x^3 + 7x + 10 \pmod{37}$

Base point:

$G = (2,5)$, order $n=19$

private key: $d=9$

message hash: $H(M)=8$

Nonce: $k=3$

P.T.O

Md. Safayat Hossain
IT-20005

compute the public key $Q = dG$
we compute sclar multiplication using known multiples of G:

$$3G = (8, 9)$$

$$6G = 2(3G) = (6, 3)$$

$$9G = 6G + 3G$$

Point addition: $(6,3) + (8,9)$

Slope: $\lambda = \frac{9-3}{8-6} = \frac{6}{2} = 3 \pmod{37}$

Co-ordinates:

$$x_Q = \lambda^2 - x_1 - x_2 = 9 - 6 - 8 = -5 \equiv 32 \pmod{37}$$

$$y_Q = \lambda(x_1 - x_Q) - y_1 = 3(6-32) - 3 = -81 \equiv 30 \pmod{37}$$

$$Q = (32, 30)$$

Signature generation

$$R = kG = 3G$$

$$R = (8, 9)$$

$$r = x_R \bmod n = 8 \bmod 19 = 8$$

EDSA formula

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

$$dr = 9 \times 8 = 72$$

$$H(m) + dr = 8 + 72 = 80$$

$$80 \bmod 19 = 4$$

Inverse of $k = 3 \bmod 19$:

$$3^{-1} = 13 \quad (3 \times 13 \equiv 1 \bmod 19)$$

$$S = 13 \times 4 = 52 \bmod 19 = 14$$

P.T.O

Md. Safayat Hossain
IT-20008

Signature pair $(r, s) = (8, 14)$

Signature verification

$w = s^{-1} \bmod n$

$= 14^{-1} \bmod 19 = 15 \quad (14 \times 15 = 210 \equiv 1 \bmod 19)$

$u_1 = (HCM) \cdot w \bmod n = 8 \times 15 = 120 \bmod 19 = 6$

$u_2 = r \cdot w \bmod n = 8 \times 15 = 120 \bmod 19 = 6$

Compute $X = u_1 G + u_2 Q$

$X = 6G + 8Q$

$G = (6, 3)$

Md. Safayat Hossain
IT-20005

21. Explain the key properties of cryptographic hash functions such as those in the secure hash Algorithm (SHA) family (e.g., SHA-256). Specifically:

i) What are the essential characteristics of a secure hash function (e.g., pre-image resistance, collision resistance)?

ii) How does the length of the output hash (e.g., 256 bits in SHA-256) impact the security of the algorithm?

iii) Discuss how SHA is utilized in real world applications, such as digital signature and block chain systems.

Ans:

(i) Essential characteristics of a secure hash function:

(a) pre image resistance: given a hash value h, it should be computationally infeasible to find any message m such that H(m) = h. This prevents attackers from recovering the original image.

(b) Second pre-image resistance: Given a massage m, it should be infeasible

P.T.O.

Md. Safayat Hossain
IT-20005

to find another message $m_2 \neq m_1$ such that $H(m_1) = H(m_2)$. This protects message against substitution attacks.

(c) Collision resistance: It should be computationally infeasible to find any two distinct message m_1 and m_2 such that $H(m_1) = H(m_2)$.

(ii) Impact of the output hash length on security: The length of the hash output directly affects the security level:

(a) For an n-bit hash output, brute force pre-image attacks require approximately 2^n operations.

(b) Collision attacks require approximately $2^{n/2}$ operations due to the birthday paradox.

(i) SHA-256 produces 256-bit hash
(ii) Pre image resistance of 2^{256}
(iii) Collision resistance of 2^{128} operation.

P.T.O

Md. Safayat Hossain
IT-20005

(iii) Real world application of SHA:

Digital signatures is used to hash a message before signing with algorithms like RSA or ECDSA. improving efficiency and ensuring message integrity.

Blockchain systems: In Bitcoin and other blockchains, SHA-256 is used to link blocks, secure transactions and perform proof of working.

Md. Safayat Hossain
IT-20007

22. Explain the concept of Galois field (also known as finite fields), focusing on GF(p) and GF(2^n). How are Galois fields used in the construction of cryptographic primitives, such as in elliptic curve cryptography and the AES encryption algorithm? Discuss the importance of field arithmetic in these cryptographic systems.

Ans: Galois Fields (Finite Fields) in cryptography

A Galois field (GF) is a finite set of elements where addition, subtraction, multiplication, and division (except by zero) are defined and satisfy field properties.

Types of Finite Fields:

(i) GF(p): prime fields with p elements (p is prime), arithmetic modulo p.

(ii) GF(2^n): Binary extension fields with 2^n elements, elements represented

P.T.O

Md. Safayat Hossain
IT-20006

as polynomials modulo an irreducible polynomial of degree n.

Elliptic curve cryptography (ECC): Operates on points over $E(GF(p))$ or $E(GF(2^n))$; field arithmetic is used for point addition and scalar multiplication; security depends on the difficulty of the ECDLP.

AES Encryption: uses $GF(2^8)$ for bytes operation in SubBytes and MixColumns. field addition = XOR, multiplication modulo irreducible polynomial ensures strong diffusion and non-linearity.

Important of Field Arithmetic: It ensures consistent modular operation and inverse for division.

Md. Safayat Hossain
IT-20006

23. Lattice Based cryptography is considered a promising candidate for post quantum cryptography due to its resistance to attacks by quantum computers.

i) Explain the shortest vector problem (SVP) and its role in the security of lattice-based cryptographic schemes.

ii) Compare the security assumptions of lattic-based cryptography with traditional cryptographic schemes like RSA and ECC in the context of shors algorithm.

iii) Discuss how quantum cryptography differs from lattice-based cryptography, particularly in terms of their goals and underlying principle.

Ans:

(i) Shortest vector problem (SVP) and its role in security:

(a) A lattice is R^n is a set of all integer linear combinations of linearly independent vectors.

(b) The shortest vector problem asks: given a latice basis, find the non-zero

P.T.O

Md. Safayet Hossain
IT-20007

vector in the lattice with the smallest Eudidean norm.

(c) SVP is computationally harad, especially in the high dimension.

(ii) Comparison with RSA and ECC under quantum attacks.

RSA/ECC	Lattice Based cryptography
(1) Integer factorization and discrete logarithm (ECC)	(1) Hardness of lattice problems (SVP, LWE
(2) Shore's algorithm can solve these efficiently, breaking RSA and ECC.	(2) Quantum computers can't efficiently solve SVP or LWE with known algorithms.
(3) RSA/ECC keys will be become insecure on the large scale quantum computer exists.	(3) Lattice Based Schemes are post quantum secure, resistant to quantum attacks.

Md. Safayet Hossain
IT-20005

iii) Difference between quantum cryptography and lattice based cryptography:

(a) Quantum cryptography:
   (i) uses the quantum mechanics principles (e.g, superposition, no-cloning theorem)
   (ii) Achieve Information-theoretic security.

(b) Lattice based cryptography:
   (i) Based on mathmatical hardness assumptions like SIP or LWE.
   (ii) Achieve computational security that remains strong against both classical and quntum computers.

Md. Safayat Hossain
IT-20005

24. In a stream cipher, let the keystream $K=\{K_1, K_2, K_3, \ldots\}$ be generated using linear Feedback shift register (LFSR) defined by the recurrence relation:

$K_t = c_1 K_{t-1} \oplus c_2 K_{t-2} \oplus \ldots \oplus c_m K_{t-m}$ over GF(2). prove that the maximum period of the keystream is $(2^m - 1)$ if the characteristic polynomial of the LFSR is primitive.

Ans: An LFSR of length m generates a key stream over GF(2) using

$$K_t = c_1 K_{t-1} \oplus c_2 K_{t-2} \oplus \ldots \oplus c_m K_{t-m}$$

with characteristics polynomial:

$$f(x) = x^m + c_1 x^{m-1} + \ldots + c_m$$

We are to prove that if $f(x)$ is primitive, the LFSR achieves maximum period $2^m - 1$.

(i) An LFSR of Length m has 2^m possible states.

(ii) All zero state is invalid, as it produce an output of all zeros.

(iii) Therefore, there are $2^m - 1$ possible non-zero states.

P.T.O

Md. Safayat Hossain
IT-20005

periodicity of the keystream:

The LFSR state transitions are linear and

(i) deterministic over GF(2)

(ii) Starting from any non-zero initial state, the LFSR will eventually cycle through states, producing a repeating states.

(iii) The period of the keystream equals the number of distinct non-zero states visited before repetition.

primitive polynomial property:

A polynomial $f(x)$ of degree m over GF(2) is primitive if it's irreducible and the smallest integer n such that $x^n \equiv 1 \bmod f(x)$ is $n = 2^m - 1$

M. Safayat Hossain
IT-20007

25. In lattic based cryptography, particularly using Learning with Errors (LWE) problem and shortest vector problem (SVP), sign a message as follows:

i) Explain the process of signing a message using an LWE-based signature scheme, including the key generation, signing and the verification steps.

ii) Given a message M, demonstrate how to sign the message using an LWE-based scheme with a public key P_K and private key S_K. Outline the steps of the message signing and explain the role of the LWE problem in ensuring security.

Ans: ① Siyining process in LWE-based signature Schemes:

Lattice based signatures follow these three steps:

ⓐ key generation:

privatekey (SK): A short secrect vector chosen from a specific lattice

public key (pk): computed a noisy linear function of the secret vector using

P.T.O

Md. Safayat Hossain
IT-20005

the learning with Errors problem:

$$P_K = A.S_K + e \bmod q$$

Where, A is a public matrix and e is a small error vector.

(b) Signing: The signer hashes the message M to produce a digest H(M).

A lattice-based algorithm problem produces a short vector z such that it satisfies a relation involving P_K and H(M) modulo q.

(c) Verification: The verifier checks that the signature vector z is valid by ensuring

$$A.z \equiv H(M) + \text{noise} \pmod q$$

(ii) Demonstration of signing a message using LWE:

Suppose we have message M,
private key SK
public key $P_K = A.S_K + e \bmod q$

① Hash the message

$h = H(M)$

P.T.O

Md. Safyat Hossain
IT-20005

generate a candidate signature vector z:

pick a random vector y from the lattice.

compute $z = y + sk$.

Rejection sampling

Accept z only if its norm is below a predefined bound to ensure leakage resistance.

output signature $\sigma = z$