Advance Cryptography Assignment

ID = IT24612

(1) With the advent of quantum computing, traditional public-key cryptosystems such as RSA and Ecc are potentially vulnerable to Shor's algorithms. Discuss the implications of quantum computing on the security of cryptographic protocols, and propose possible post-quantum cryptographic algorithms that could replace RSA and Ecc. How do these algorithms resist quantum cryptoanalysis?

Ans:

Quantum computing threatens traditional public-key cryptosystems such as RSA and ECC because shor's algorithms can efficiently solve integer factorization and discrete logarithm problems. This means encrypted data, digital signatures, and secure communication protocols can be broken once large-scale quantum computers became available.

To address this, Post-Quantum Cryptography (PQC) proposes quantum-resistant algorithms

ID = IT24612

such as:

↳ Lattice-based cryptography (e.g., Kyber, Dilithium) - secure due to hardness of Learning with Errors (LWE) problems.

↳ Hash-based cryptography (e.g., XMSS, SPHINCS+) - Resists quantum attacks since Grover's algorithm offers only limited speedup.

↳ code-based cryptography (e.g., McEliece) - relies on hard error-correcting code decoding problems.

These algorithms resist quantum cryptanalysis because no efficient quantum algorithms are known to solve their underlying mathematical problems.

ID = IT24612

(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 constrain the output within a desired range.

Ans:

```
import time
import os

def simple_prng(modulus = 10000):
    timestamp = int(time.time_ns())
    pid = os.getpid()
    seed = (timestamp ^ pid) % modulus
    return seed

# Example output
print(simple_prng())
```

ID=IT24612

Explanation :

The PRNG uses the current timestamp and process ID as entropy sources, combines them using XOR, and applies a modulus operation to constrain the output rang. This PRNG is suitable for learning and simulation purposes but not for cryptographic security.

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

ID = IT24612

Ans:

Traditional ciphers such as the ceasar cipher, vigenere cipher and playfair cipher are classical encryption techniques mainly used for educational purposes. The ceasar cipher uses a very small key space (shift value) making it extremely vulnerable to brute-force attacks. The vigenere cipher improves security by using a repeating keyword, but it is still vulnerable to frequency analysis (e.g. kasiski examination). The playfair cipher encrypts digraphs instead of single letters, which slightly improves security but remain weak against modern cryptanalysis.

Modern symmetric ciphers such as DES and AES are designed for high security and efficiency. DES uses a 56-bit key, which is now considered insecure due to brute-force attacks. AES, on the other hand, supports key sizes of 128, 192, and

ID = IT24612

256 bits, providing strong resistance against modern cryptanalysis. Modern ciphers are much faster, mathematically complex and secure against known attacks, making them suitable for real-world applications.

(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 the stabilizer of the subset $\{1, 2\}$.

Ans:

Let S_4 be the symmetric group on the set $\{1, 2, 3, 4\}$. Consider the set X of all 2 element subsets of $\{1, 2, 3, 4\}$.

Definition of the Action.

For $\sigma \in S_4$ and a 2 element subset $\{a, b\} \subseteq \{1, 2, 3, 4\}$, define

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

ID=IT24612

well-defined

since permutations map elements of the set $\{1,2,3,4\}$ to itself, the image of a 2-element subset is again a 2 element subset. Hence the action is well defined.

orbit of $\{1,2\}$

All 2 element subsets can be reached by permuting elements, so the orbit of $\{1,2\}$ consists of all such subsets;

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

Thus, the orbit size is 6.

stabilizer of $\{1,2\}$.

The stabilizer consists of permutations that keep the set $\{1,2\}$ fixed (possibly swapping 1 and 2, and permuting 3 and 4).

There are 4 such permutations, so the stabilizer size is 4.

There are 4 such permutations, so the stabilizer size is 4.

This satisfies the orbit-stabilizer Theorem:

$$|S4| = |\text{orbit}| \times |\text{stabilizer}| = 6 \times 4 = 24.$$

ID = IT24612

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 non-zero elements of GF(2^2) is cyclic.

Ans:

Let

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

where $q^2 + q + 1 = 0 \Rightarrow q^2 = q + 1$

i) Group under multiplication

consider the set of nonzero elements:

$$GF(2^2)^* = \{1, q, q+1\}$$

→ closure: multiplication of any two nonzero elements stays within the set.

→ Associativity: Inherited from polynomial multiplication.

→ Identity: 1 is the multiplication identity.

→ Inverse: $q(q+1) = q^2 + q = (q+1) + q = 1$

so $q' = q+1$ and vice versa.

Hence, $GF(2^2)^*$ forms a group under multiplication.

ii) cyclic nature:

compute power of q:

$$q^1 = q, \quad q^2 = q+1, \quad q^3 = q(q+1) = 1$$

Thus,

$$\langle q \rangle = \{1, q, q+1\}$$

Therefore, the multiplicative group of nonzero elements of $GF(2^2)$ is cyclic of order 3.

(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 the corresponding factor group, and interpret its structure.

Ans:

Let $GL(2,R) = \{A \in M_{2\times 2}(R) \mid \det(A) \neq 0\}$.

Define the set of scalar matrices:

$$S = \{\lambda I \mid \lambda \in R^*\}.$$

subgroup

ID = IT24612

Subgroup

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

→ Identity : $I = 1 \cdot I \in S$

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

Thus, S is a subgroup of $GL(2, R)$

Normality

For any $A \in GL(2, R)$ and $\lambda I \in S$.

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

Hence, $S \triangleleft GL(2, R)$ (normal subgroup)

4. Factor Group and Interpretation

the factor group is:

$$GL(2, R) / S.$$

It identifies matrices that differ only by a nonzero scalar multiple.

This group represets linear transformations up to scaling and is known as the projective general linear group:

$$PGL(2, R).$$

SIDPSTT = 01 ID = IT24612

(7) Explain the Diffie-Hellman key exchange protocol and its application in secure communication. 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. what would be the impact on the protocol's security if the prime modulus used is not sufficiently large?

Ans:

The Diffie-Hellman (DH) key exchange protocol allows two parties to establish a shared secret over an insecure communication channel. Let p be a large prime and g a generator of a cyclic group modulo p. One party chooses a secret integer a and send $g^a \bmod p$, while the other chooses a secret integer b and sends $g^b \bmod p$. Both compute the shared key as $g^{ab} \bmod p$. which is identical for both parties.

The security of Diffie-Hellman relies on the Discrete Logarithm problem (DLP): given

ID = IT29612

a and $g^a \bmod p$, it is computationally infeasible to determine a when p is sufficiently large. This ensures that an eavesdropper cannot compute the shared secret.

However, the basic DH protocol is vulnerable to a man-in-the-middle (MITM) attack, where an attacker intercepts and replaces public values, establishing separate keys with each party. This attack is prevented in practice by authentication mechanism such as digital signatures and certificates.

If the prime modulus p is not sufficiently large, discrete logarithms can be computed efficiently using modern algorithms, making the shared key vulnerable to brute force or index calculus attacks. Thus large prime (e.g. 2048 bits or more) are essential for security.

ID = IT24612

(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. provides an example using specific groups.

Ans:
Let G be a group and Let H_1 and H_2 be subgroups of G. we show that $H_1 \cap H_2$ is also a subgroup of G.

poof
→ Non-empty: Since both H_1 and H_2 are subgroups they contain the identify element e. Hence, $e \in H_1 \cap H_2$

→ closure: If $x, y \in H_1 \cap H_2$, then $x, y \in H_1$ and $x, y \in H_2$, Since both are subgroups $xy^{-1} \in H_1$ and $xy^{-1} \in H_2$. Thus, $xy^{-1} \in H_1 \cap H_2$

→ Inverse: The inverse of any element in the Intersection belongs to both subgroups.

Therefore, $H_1 \cap H_2$ satisfies the subgroup test and is a subgroup of G.

Example:
Let $G = \mathbb{Z}$ (Integers under addition).
$H_1 = 2\mathbb{Z}$ (even integers),
$H_2 = 3\mathbb{Z}$ (multiples of 3).

Then,

$$H_1 \cap H_2 = 6\mathbb{Z},$$

which is a subgroup of $\mathbb{Z}$.

(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: Properties of the ring $\mathbb{Z}_n$

The ring $\mathbb{Z}_n$ consists of integers modulo n with addition and multiplication defined modulo n.

Commutativity

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

$$a+b = b+a \pmod{n}, \quad ab = ba \pmod{n}$$

Since integer addition and multiplication are commutative $\mathbb{Z}_n$ is a commutative ring.

ID=IT24612

Zero Divisors.

An element $a \neq 0$ in Z_n is a zero divisor if there exists $b \neq 0$ such that

$$ab = 0 \pmod{n}$$

This occurs if and only if n is composite. Hence Z_n, has zero divisors when n is not prime

When is Z_n a Field?

A ring is a field if every nonzero element has a multiplicative inverse. Z_n is a field if and only if n is prime, because only then every nonzero element is relatively prime to n.

(10) Explain the vulnerabilities of the DES (Data Encryption standard) cipher and why it is considered insecure for modern use. Discuss the role of brute-force attacks in breaking DES and the impact of key length on the security of the algorithm. How did the development of AES address the shortcomings of DES - particularly in terms of key size and resistance to cryptanalytic attacks?

ID = ST24612

Ans:

Vulnerabilities of DES and Role of AES:

The Data Encryption standard (DES) is a symmetric block cipher that uses a 56 bit key. Its primary weakness is its short key length, which makes it vulnerable to brute-force attacks. Modern computers can try all possible keys in a feasible amount of time, making DES insecure.

DES also suffers from:

→ small block size (64 bits)

→ susceptibility to differential and linear cryptanalysis.

→ Inadequate security for modern applications

Brute force attacks became practical in the late 1990s when specialized hardware successfully broke DES keys in hours.

To overcome these weaknesses, the Advanced Encryption standard (AES) was introduced. AES supports larger key sizes (128, 192, and 256 bits), making brute-force attacks

computationally infeasible. AES also has a stronger mathematical structure and is resistant to known cryptanalysis attacks. As a result, AES is faster, more secure, and suitable for modern cryptography applications.

11. Differential cryptanalysis is a 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 operations, is more resistant to such attacks compared to DES?

Ans:

i) Feistel Structure of DES and Differential cryptanalysis

Differential cryptanalysis studies how differences in plaintext pairs affect differences in ciphertext pairs. DES uses a feistel structure with 16 rounds, where the input block is divided into left and right halves.

ID = IT24612

In each round, one half is processed through nonlinear s-boxes and mixed with the other half using XOR operations. The repeated application of s-boxes and permutations spreads input differences across many bits, reducing predictable patterns. Although DES was designed to resist differential cryptanalysis to some extent, its small block size and limited number of rounds makes it vulnerable to advanced differential attacks.

(ii) AES Resistance compared to DES

AES uses a substitution permutation network (SPN) instead of a Feistel structure. The subBytes operation introduces strong nonlinearity through s-boxes, shiftRows rearranges bytes to prevent local patterns, mixcolumns provide high diffusion across the state, and AddRoundKey ensures key dependency in every Round. This strong

ID = IT24612

combination of confusion and diffusion makes it extremely difficult for attackers to track input differences, giving AES much stronger resistance to differential cryptanalysis than DES.

(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 important for large-scale cryptographic systems?

Ans:
The Extended Euclidean Algorithm (EEA) is used to find integers x and y such that:

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

if $\gcd(a, n) = 1$, then:

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

so x is the modular inverse of a modulo n.

Example.
Find the inverse of $a = 7$ modulo $n = 26$

ID = IT24612

Using EEA:

$26 = 3 \times 7 + 5$, $7 = 1 \times 5 + 2$, $5 = 2 \times 2 + 1$

Back substituting gives:

$1 = 3 \times 26 - 11 \times 7$

Thus

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

Use in RSA.

In RSA the EEA is used to compute the private key exponent d, which is the modular inverse of the public exponent e modulo $\phi(n)$. Efficient computation is crutial because RSA uses very large integers (1024 - 4096 bits). The efficiency of the EEA ensures fast key generation and secure cryptographic operations in large scale systems.

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

ID = IT24612

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

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

Ans:

(i) Let $E_K(i)$ be a deterministic block cipher with block size n.

In ECB mode, encryption is defined as:

$$C_i = E_K(P_i)$$

For each plaintext block P_i.

If the plaintext is redundant, then there exist indicates $i \neq j$ such that

$$P_i = P_j$$

since the cipher is deterministic

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

Thus identical plaintext blocks produce identical ciphertext blocks, leaking structural information about the plaintext. This violates

ID = IT29612

Semantic security and allows pattern recognition (e.g. Image outlines) & providing ECB is insecure for redundant data.

(iv) Let 'Iv' be the initialization vector.

Encryption:

$$C_0 = Iv, \quad C_i = E_K(P_i \oplus C_{i-1})$$

Decryption

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

Error propagation proof

Assume a single bit error occurs in ciphertext block C_i.

→ During decryption of P_i:

$D_K(C_i)$ becomes corruption, entire block P_i is corrupted.

→ During decryption of P_{i-1}:

C_i is XORed with $D_i(C_{i-1})$. only one block is affected.

→ For P_{i+2} onward:

No effect since C_i is no longer used.

ID = IT24612

Thus, error propagation in CBC decryption is limited to two blocks, proving controlled damage.

(14) Why the linearity of LFSRs makes them vulnerable to known-plaintext attacks, and process propose a mathematical method to mitigate this vulnerability.

Ans:

An LFSR (Linear Feedback shift Register) generate sequences based on linear recurrence relations over GF(2):

$$B_1 = c_1 B_{t-1} \oplus c_2 B_{t-2} \oplus \cdots \oplus c_k B_{t-k}.$$

Because the system is linear, observing a sufficient number of output bits allows an attacker to:

→ Form linear equations.
→ Solve for the feedback coefficients and internal state using linear algebra
→ predict all future outputs.

This makes LFSRs vulnerable to known-plaintext and correlations attacks.

ID = IT29612

Mitigation method

A mathematical solution is to introduce nonlinearity, such as:

→ Nonlinear filter functions
→ combining multiple LFSRs using nonlinear Boolean functions.
→ using Nonlinear Feedback Shift Registers (NLFSRs)

These approaches prevent attackers from modeling the keystream as a solvable linear system, significantly improving resistance to cryptanalysis.

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

(i) State Shannon's definition of perfect secrecy mathematically.

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

(iii) critically analyze why perfect secrecy is impractical for large-scale communication systems.

Ans:

(i) A cryptosystem (M, K, C) achieves perfect secrecy if the ciphertext reveals no information about the plaintext. Mathematically:

$$P(M=m \mid C=c) = P(M=m) \quad \forall m \in M, \forall c \in C$$

Equivalently:

$$H(M \mid C) = H(M)$$

where H is is the entropy function

(ii) p

Let plaintext $m \in M$, key $K \in K$ uniformly random, and ciphertext:

$$C = m \oplus K$$

→ since K is uniform for any c

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

→ By Bayes theorem:

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

$$= P(M=m)$$

Thus, OTP provides perfect secrecy if the key is uniformly random and $|K| \geq |M|$

(iii) Impractically of perfect secrecy

→ Key length requirement: Each key must be as long as the message.

→ Key distribution: securely sharing large keys is difficult.

→ Key reuse is forbidden: Reuse compromises security.

→ storage: Requires massive key storage for large-scale communication.

Hence, OTP is secure but impractical for everyday, large-scale communication.

(16) A Linear congruential Generator (LCG) is defined by the recurrence relation:

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

ID = IT29612

Is the sequence of pseudo-random numbers, and a, c, and m are integer parameters representing the multiplier, increment, and modulus, respectively. Using specific values for a, c, and m compute the first 5 numbers of an LCG sequence starting with a given seed $x_0 = 7$.

Ans:

The LCG recurrence relation is:

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

Let's take example parameters:

→ $a = 5, c = 3, m = 16$, and seed: $x_0 = 7$

compute first 5 numbers:

1. $x_1 = (5 \cdot 7 + 3) \bmod 16 = (35 + 3) \bmod 16 = 38 \bmod 16 = 6$
2. $x_2 = (5 \cdot 6 + 3) \bmod 16 = (30 + 3) \bmod 16 = 33 \bmod 16 = 1$
3. $x_3 = (5 \cdot 1 + 3) \bmod 16 = (5 + 3) \bmod 16 = 8 \bmod 16 = 8$
4. $x_4 = (5 \cdot 8 + 3) \bmod 16 = (40 + 3) \bmod 16 = 43 \bmod 16 = 11$
5. $x_5 = (5 \cdot 11 + 3) \bmod 16 = (55 + 3) \bmod 16 = 58 \bmod 16 = 10$

First 5 numbers:

$x_1 = 6, x_2 = 1, x_3 = 8, x_4 = 11, x_5 = 10$