COMP 417 INTRODUCTION TO CRYPTOGRAPHY

QUIZ 1-SOLUTION

(Total=100 points Duration:1 Hour)

DATE: 02.11.2023 2:00 pm

1.RSA
Choose p = 3 and q = 11

- Compute n = p * q = 3 * 11 = 33
- Compute ϕ(n) = (p - 1) * (q - 1) = 2 * 10 = 20
- Choose e such that 1 < e < ϕ(n) and e and ϕ (n) are coprime. Let e = 7
- Compute a value for d such that (d * e) % ϕ(n) = 1. One solution is d = 3 [(3 * 7) % 20 = 1]
- Public key is (e, n) => (7, 33)
- Private key is (d, n) => (3, 33)
- The encryption of $m = 2$ is $c = 2^7 \% 33 = 29$
- The decryption of $c = 29$ is $m = 29^3 \% 33 = 2$
- *RSA depends on factoring problem because for long numbers it is hard to factor them. 2048 is the key length is the min key length considered secure.*

2. Diffie-Hellman Key exchange

a.5^4 mod 17=13 public key of Bob 5^2 mod 17=8 public key of Alice.
b. 8^4 mod 17=13^2 mod 17=16
c.They can use one symmetric encryprtion scheme for example Ceaser when k=16 means C=m+16 mod 26.
d. Diffie-Hellman Key exchange depends on dicreete logarithm problem because for large number q, even if we know q and g it is hard to find a from g^a mod q or it is hard to find g^(ab) from g^a mod q and g^b mod q.

3. 1. Differences between Symmetric and Asymmetric Cryptography:

a. Key Usage:

- Symmetric Cryptography: Uses a single shared key for both encryption and decryption.
- Asymmetric Cryptography: Uses a pair of public and private keys for encryption and decryption, where the public key is used for encryption, and the private key is used for decryption.

b. Key Distribution:

- Symmetric Cryptography: Requires a secure mechanism to share the secret key between communicating parties.
- Asymmetric Cryptography: Eliminates the need for secure key distribution as each user has their own private key and a public key for encryption.

c. Computational Complexity:

- Symmetric Cryptography: Generally faster and more efficient for bulk data encryption due to its simpler operations.
- Asymmetric Cryptography: Slower and computationally intensive, making it suitable for key exchange and digital signatures but less efficient for large data encryption.