COMP 417 INTRODUCTION TO CRYPTOGRAPHY
HOMEWORK 1- SOLUTION

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.

2. Constructing a Secure Block Cipher:

A secure block cipher is typically constructed using a Feistel network or a substitution-permutation network (SPN). The following components are used to ensure security:

- Substitution Box (S-Box): Non-linear substitution that provides confusion.
- Permutation Box (P-Box): Rearranges the bits for diffusion.
- Key Schedule: Generates round keys from the main encryption key.
- Multiple Rounds: The more rounds applied, the greater the security.

These tools should provide secure PRP conditions.

3. AES-128 vs. AES-256 Quantum Resistance:

AES-128 is not quantum-resistant because Grover's algorithm can be used to perform a brute-force search of the key space in 2^64 operations, which is faster than classical brute-force but still feasible. AES-256, on the other hand, is considered quantum-resistant because Grover's algorithm reduces the search time to 2^128 operations, which remains infeasible even with quantum computers.

4. a. Modes of Operation for Block Ciphers:

- ECB (Electronic Codebook): Each block is encrypted independently. Identical plaintext blocks result in identical ciphertext blocks.
- CBC (Cipher Block Chaining): XORs each plaintext block with the previous ciphertext block before encryption, introducing diffusion.
- CFB (Cipher Feedback): Uses the ciphertext from previous blocks to create a keystream, which is XORed with plaintext.

- OFB (Output Feedback): Similar to CFB but encrypts the output of the block cipher, creating a keystream.
- CTR (Counter): Encrypts a counter value to generate a keystream that is XORed with plaintext.

b. Applications:
- ECB: Rarely used in practice due to security issues, but can be used for single block data encryption.
- CBC: Commonly used for disk encryption and secure data transmission.
- CFB: Suitable for real-time data encryption, like streaming video.
- OFB: Used in applications that require data synchronization, such as encrypted telecommunication.
- CTR: Well-suited for disk encryption and secure communication over unreliable networks.

5. Differences between Stream Ciphers and Block Ciphers:

a. Stream Ciphers:
  - Operate on a bit-by-bit or byte-by-byte basis.
  - Typically faster for real-time data streaming.
  - Generally simpler and require less computational overhead.

b. Block Ciphers:
  - Process data in fixed-size blocks (e.g., 128 bits).
  - Better suited for bulk data encryption.
  - Provide better security for data at rest.

6. Perfect Secrecy vs. Computational Secrecy:
- Perfect Secrecy: The ciphertext reveals no information about the plaintext, regardless of computational resources. Achieved with a one-time pad (OTP).
- Computational Secrecy: Provides security against computationally bounded adversaries but may not be perfectly secure. Achieved in practical encryption systems, including block ciphers and stream ciphers.

7. OTP (One-Time Pad) and Perfect Secrecy:
- OTP provides perfect secrecy because:
  1. The key is as long as the message.
  2. Each key bit is used only once.
  3. There are two equally likely keys for any ciphertext.

- Perfect secrecy is provided when the key is truly random and used only once for a single message.

8. Constructing a Stream Cipher from a Block Cipher:

A stream cipher can be constructed by using a block cipher in a mode of operation like Counter (CTR) mode. In CTR mode, a counter value is encrypted to generate a keystream, which is then XORed with the plaintext to produce the ciphertext.

Example:

- Use a block cipher like AES in CTR mode.
- Initialize a counter value.
- Encrypt the counter value to generate the keystream.
- XOR the keystream with the plaintext to obtain the ciphertext.

9. Calculating 7^123 mod 145:

   - Using the modular exponentiation algorithm, you can calculate this value using the number theory as follows:

$7^{123} \bmod 145 = 7^{(123 \bmod \phi(145))} \bmod 145$

$145= 5 * 29$ so; $\phi(145)=(5-1)(29-1)= 4*28=112$

$7^{123} \bmod 145 = 7^{(123 \bmod 112)} \bmod 145 =7^{11} \bmod 145$

$=7^3*7^3*7^3*7^2 \bmod 145$
$=343*343*343*49 \bmod 145$
$= 53*53*53*49 \bmod 145$
$=2809*53*49 \bmod 145$
$=54*53*49 \bmod 145$
$=2862*49 \bmod 145$
$=107*49 \bmod 145$
$= 5243 \bmod 145$
$= 23$

10. Euler's Totient Function (ϕ) and Coprime Numbers:

   The total number of positive numbers less than 2436 and coprime to 2436 can be calculated using Euler's Totient function $\phi(n)$. $\phi(n)$ is the count of positive integers coprime to n.

   $\phi(2436) = \phi(2^2 * 3 * 7 * 29)=2^{(2-1)}*(2-1)*(3-1)*(7-1)*(29-1)=2*1*2*6*28=672$

   So, there are 672 positive numbers less than 2436 that are coprime to 2436. These numbers do not share any common factors with 2436 except for 1.