**ISQS 3360**

**Question 1**

Suppose that Alice and Bob use CBC mode encryption. What security problems arise if they always use a fixed initialization vector (IV), as opposed to choosing IVs at random?

Using a fixed initialization vector (IV) in CBC mode encryption can cause some big security issues:

1. Predictable encryption: If you use the same IV for different messages, identical parts of those messages will turn into the same jumbled-up text, making it easier for hackers to figure out what's being said.
2. Repeating problems: Repeating an IV lets hackers see if the same parts of different messages show up again. This leaks information and can mess with the secrecy of what's being said.
3. Spotting patterns: If a fixed IV is used over and over, hackers might start to notice repeating patterns in the jumbled-up text. This can give them clues about what the original message was, making the encryption less secure.
4. Trust issues: Using a fixed IV can also mess with how secure the encryption is overall. Hackers could change parts of the encrypted message without anyone noticing, which breaks the promise that the encryption will keep the message safe and unaltered.

**Question 2**

We know that the generic formula for encryption and decryption for block cipher is that , and .

Suppose we use a new block cipher, which looks similar but actually different from CBC mode, to encrypt plaintexts according to the following rules:

, ,

What are the corresponding decryption rules for , , ? Please write them out for , , , respectively.

To obtain the original plaintext blocks P0 ​, P1​, and P2​, the decryption process reverses the encryption operations using the decryption function with the key D and K the appropriate XOR operations. The presentation clarifies the general principles of block cipher encryption and decryption, emphasizing the reversible nature of encryption operations to ensure secure communication.

Therefore, following these principles, the decryption rules corresponding to the given encryption rules are as follows:

* To obtain P0​​, decrypt C0​ with K and then perform an XOR operation with IV.
* To obtain P1​, decrypt C1​​ with K and perform an XOR operation with C0​​.
* To obtain P2​, decrypt C2​​ with K and perform an XOR operation with C1​.

This is the result:

P0 ​= D (C0​⊕ IV, K) ⊕ IV

P1 = D (C1⊕ C0, K) P1​ = D (C1​ ⊕ C0, K)

P2 = D (C2⊕C1, K) P2= D (C2 ⊕ C1​, K)

**Question 3**

Recall that a MAC is given by the CBC residue, that is, the last ciphertext block when the data is encrypted in CBC mode. Now, suppose we calculate MAC by CTR (Counter Mode) residue, that is, the last ciphertext block when the data is encrypted in CTR mode.

Suppose Alice has three plaintext blocks, P0, P1 , and P2 , and she computes:

C0 = P0 ⊕ E(IV, K),

C1 = P1 ⊕ E(IV+1, K),

C2 = P2 ⊕ E(IV+2, K) = MAC

Then Alice sends IV, P0, P1 , P2 , and MAC to Bob.

Suppose Trudy intercepts these information and changes P0  to X, before Bob receives them. Bob, after receiving the information, verifies the data integrity by computing the MAC value himself. Assume the key K is pre-shared between Alice and Bob.

Can Bob detect the plaintext data has been tampered? Why or why not?

Bob can detect tampering of plaintext data by Trudy. In CTR mode, the MAC is computed using the last ciphertext block, which is a function of the last plaintext block (P2) and the key K. If Trudy alters P0​, the modified P0 (now X) doesn't directly impact the computation of C2​​ ​ because C2​​ ​ is derived from P2​ and not P0​. However, since Alice sends the plaintext blocks along with the MAC, Bob recalculates the MAC using the received plaintext blocks and the pre-shared key K. He computes C0​, C1​​​, and C2​​ from the received P0 (now altered to X), P1​, and P2​. If Trudy altered only P0​ and not the MAC, the recalculated C2​​ by Bob (considering it involves recalculating MAC based on the altered P0​) would not match the received MAC (which was based on the original P0​), indicating potential tampering.

When Bob verifies the data, he received by recalculating the MAC, any changes made to the data will result in a mismatch between the new MAC and the original MAC sent with the data. This discrepancy indicates to Bob that the data has been tampered with. The approach, which combines CTR mode encryption with MAC to verify data integrity, effectively ensures that any unauthorized alterations to the data can be detected.