

Encryption Question

A symmetric encryption system consists of three main components: A key generator K , An encryption algorithm E and a decryption algorithm D .

For two users Alice and Bob, the generator K generates a shared secret key K_{ab} . Then one of the two users takes a plaintext message P and with the use of this shared key produces an encrypted ciphertext message $C = E(K_{ab}, P)$. The message can now be sent over an insecure channel. The recipient can retrieve the original message $P = D(K_{ab}, C)$.

What are the three basic requirements to make the system secure?

Modes of Operation Problem

An AES encryption system uses a 128-bit key K to encrypt a message M that consists of n 128-bit blocks (M_1, M_2, \dots, M_n) and produces n 128-bit blocks of ciphertext (C_1, C_2, \dots, C_n)

The encryption process is as follows.

The sender first chooses a random 128-bit string to be used as C_0

Then for all $i > 0$, the i^{th} cipher text block is given as

$$C_i = C_{i-1} \text{ EXOR } E(K, M_i)$$

The ciphertext would then be the concatenation of $C_1 || C_2 || \dots || C_n$

- a- Draw a sketch of this mode of operation showing M_1, M_2, \dots, M_n and their corresponding ciphertext blocks.
- b- What is the purpose of using C_0 ?
- c- Is this mode of operation secure? If so why so and if not give a reason.
- d- What change would you make to this scheme to improve security?