

Name: Nguyễn Việt Hoàng

Student's ID: B22DCVT214

CLASS PREP

Directions. After reading the section 2.2 and 2.5, please answer the following questions (either directly on the template or on separate paper). This class prep assignment will be graded on effort. Please do not leave any questions blank – if you are stuck, either formulate a question that you believe will help you get unstuck or write down some preliminary ideas.

1. As for the DES algorithm, please answer the following questions:

- What is the size of plaintext? The plaintext are 64 bit long. Longer message are processed in 64 bit block
- What is the size of key? The key is 56 bit long
- How about the number of rounds? DES has 16 round of processing.

2. Have a comparison between Electronic Codebook (ECB) Mode and Cipher Block Chaining (CBC) Mode.

ECB:

- How it works: Each plaintext block is encrypted independently with the same key.
- Pro: Very fast, easy to implement, fully parallelizable for both encryption and decryption.
- Con: Identical plaintext blocks produce identical ciphertext blocks, so it is possible for attacker to exploit patterns, vulnerable to replay and frequency attacks.

CBC:

- How it works: Each plaintext block is XOR with the previous ciphertext block before encryption. The first block uses a random IV.
- Pro: Hides patterns, provides much better confidentiality, resistant to known-plaintext attacks if IV is unique.
- Con: Slightly slower, encryption cannot be parallelized, requires secure random IV.

3. In the CBC mode, should we protect the initialization vector (IV)? And why?

The initialization vector should be protected because if the attacker can manipulate the IV, the plaintext after decryption can be alter without the need of knowing the IV from the attacker, which made the communication unreliable