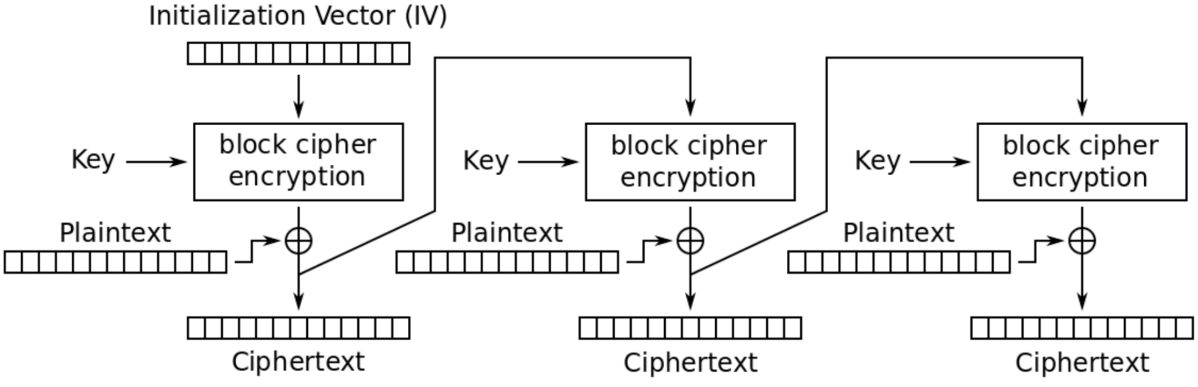
Week 7: Cryptography: Block Ciphers

Block Ciphers: Encryption Models



Cipher Feedback (CFB) mode encryption

Question 1: Above we have a diagram of the CFB mode or the Cipher Feedback Mode whose encryption is given as follows:

$$C_i = \begin{cases} \mathrm{IV}, i = 0 \\ E_k(C_{i-1}) \oplus P_i, \quad \text{Otherwise} \end{cases}$$

What is the decryption formula for this CFB mode?

Question 2: Select the true statements about CFB mode:

A. Encryption can be parallelized
B. Decryption can be paralellized
C. The scheme is CPA secure

Question 3: What happens if two messages are encrypted with the same key and IV? What can the attacker learn about the two messages just by looking at their ciphertexts? HINT: Think about how each block cipher transforms the corresponding plaintext block.

A. The attacker can determine if two messages have identical prefix up to the first block containing the difference.
B. The attacker can determine the entire plaintext by using the decryption formula on the available ciphertexts.
C. The attacker cannot determine any of the inputs, since CFB is CPA secure.

Question 4: If an attacker recovers the IV used for the CFB mode, but not the key, will they be able to decrypt a ciphertext encrypted with the recovered IV and a secret key?

Question 5: Message Padding
Assume we have a message being encrypted using a block cipher of block length L = 8. Which of the following are valid encoded messages? (select all that apply)

A. 0x F9 F4 92 16 04 04 04 04
B. 0x FF 04 54 04 04 04 04 04
C. 0x 01 02 03 04 05 06 07 01
D. 0x 01 02 03 04 05 06 01 01
E. 0x 01 02 03 04 05 06 09 10

Hash Functions: Integrity of communication.

Question 1: Let’s assume Alice and Bob are communicating over a public network, and they are playing a game where:

a. They both choose an integer number
b. Then, they each disclose this number to each other
c. If the sum of the two numbers is even Alice wins
d. If the sum of the two numbers is odd Bob wins .

If we don’t use hash functions, and there are no eavesdroppers on the network, who is guaranteed to win?

A. Alice
B. Bob
C. Whoever goes first wins
D. Whoever goes last wins

Question 2: Now, let’s have Alice and Bob play the same game but applying hash functions to their messages. This time the game proceeds as follows:

a. Alice and Bob each choose an integer number
b. Alice sends a hash of her number
c. Bob receives Alice’s hash and sends his number
d. Alice then sends her number over.

Assuming there are no eavesdroppers on the network, who is guaranteed to win?

A. Neither, its 50% chance
B. Alice
C. Bob
D. Whoever goes first
E. Whoever goes last

Question 3: We know that hash functions provide the following properties: collision resistance, and one-way or preimage resistance. Assume we play the same game as Question 2:

A. Which property protects Alice if Bob tries to cheat (i.e., change his response mid-way)? (collision resistance or pre-image resistance)
B. Which property protects Bob if Alice tries to cheat (i.e., change her response mid-way)? (collision resistance or pre-image resistance)

Question 4: Circle all possible applications of hash functions

A. Integrity verification of files
B. Time stamping files
C. Password Authentication
D. Proving Identity

Launching Attacks on Hash functions.

Question 1: We know that a hash computes a one-way function from an input string m to an output hash(m). If our input string is 4 bits long, and our hash has a fixed length, can you launch an attack that defeats pre-image resistance?

A. Yes
B. No

Question 2: We know that a hash computes a one-way function from an input string m to an output hash(m). If our input string is 60 bits long, and our hash has a fixed length, is it theoretically possible to launch an attack that defeats collision resistance?

A. Yes
B. No

Question 3: Alice comes up with a new scheme that she claims provides secure authentication. She first hashes her password, and sends it over the network and implements a hash checking function that compares the hashed password with the hash on file. Is this system more secure than sending passwords over the network using symmetric key encryption?

A. Yes
B. No