Lecture 15. Network Security Exercises ANS

CSC175

Block Cipher

- Consider the 3-bit block cipher in the Table below

Plain	000	001	010	011	100	101	110	111
Cipher	111	110	101	100	011	010	000	001

- Suppose the plaintext is 100101100.

(a) Initially assume that CBC is not used. What is the resulting ciphertext?

(b) Suppose Trudy sniffs the ciphertext. Assuming she knows that a 3-bit block cipher without CBC is being employed (but doesn't know the specific cipher), what can she infer?

(c) Now, suppose that CBC is used with IV-111. What is the resulting ciphertext?

Block Cipher ANS

Plain	000	001	010	011	100	101	110	111
Cipher	111	110	101	100	011	010	000	001

(a) Initially assume that CBC is not used. What is the resulting ciphertext?

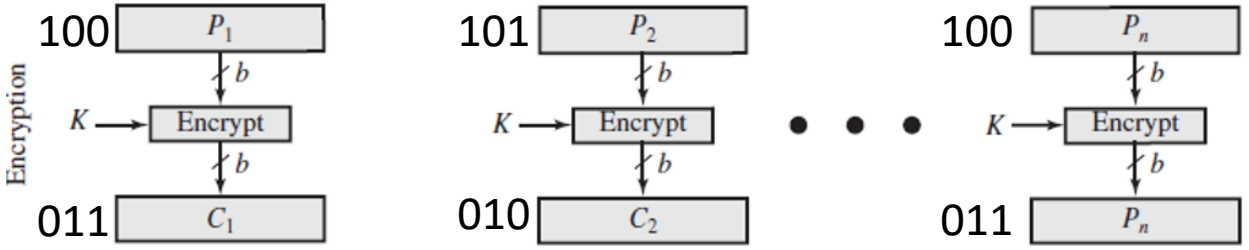
ANS: Ciphertext for plaintext 100101100 is 011010011, since 100 maps to 011, 101 maps to 010, 100 maps to 011

(b) Suppose Trudy sniffs the ciphertext. Assuming she knows that a 3-bit block cipher without CBC is being employed (but doesn't know the specific cipher), what can she infer?

ANS: Without CBC, each identical plaintext block will always map to the same ciphertext block. This makes it easier for Trudy to recognize patterns in repeated blocks of data. If Trudy intercepts enough ciphertexts, she could perform frequency analysis on the blocks. For example, if certain ciphertext blocks appear more frequently, she might guess that they correspond to more common plaintext blocks (like spaces or common letters in text). Or if it is known that the message always starts out with certain predefined fields, then the cryptanalyst may have a number of known plaintext-ciphertext pairs to work with.

(c) Now, suppose that CBC is used with IV=111. What is the resulting ciphertext?

ANS: With CBC and IV = 111, resulting ciphertext for plaintext 100101100 is 100110101. (See next page.)

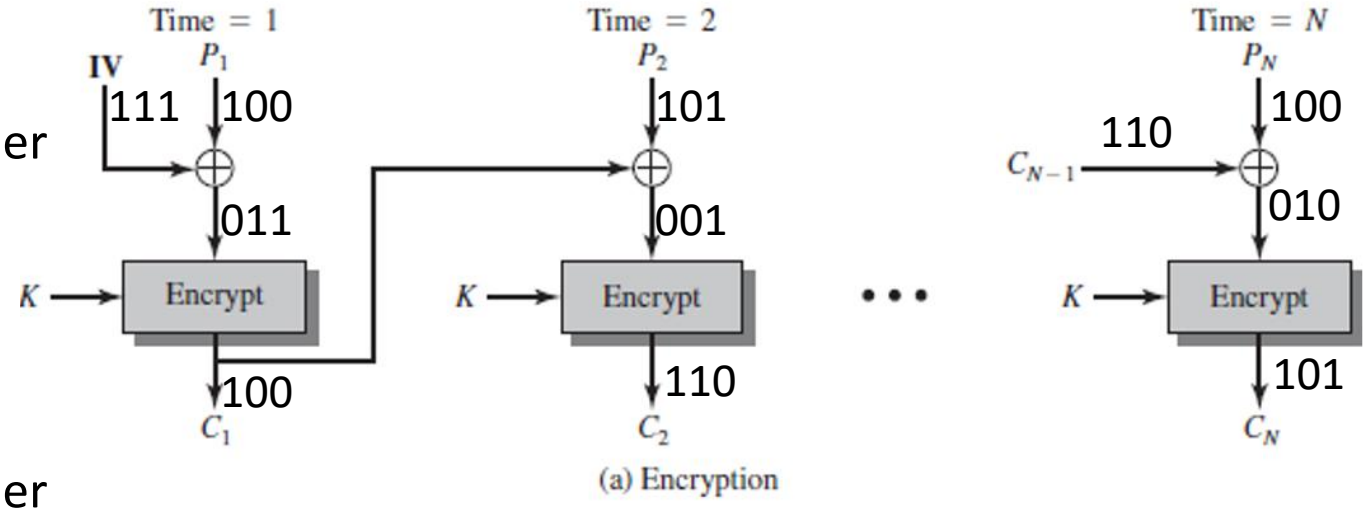


The same plaintext 100 is encrypted into the same cyphertext (011) at different positions in the input, making it possible to attacker to perform frequency analysis.

Block Cipher ANS

Plain	000	001	010	011	100	101	110	111
Cipher	111	110	101	100	011	010	000	001

- Plaintext 100101100
- The first step is to XOR the first plaintext block with IV = 111
  - First plaintext block: 100, so 100⊕111=011
  - Now we encrypt this result (011) using our cipher table: 011 maps to 100.
- Second Block: Now we XOR the second plaintext block with the first ciphertext block:
  - Second plaintext block: 101, so 101⊕100=001
  - Now we encrypt this result (001) using our cipher table: 001 maps to 110.
- Third Block: Finally, we XOR the third plaintext block with the second ciphertext block:
  - Third plaintext block: 100, so 100⊕110=010
  - Now we encrypt this result (010) using our cipher table: 010 maps to 101.
- Resulting ciphertext for plaintext 100101100 is 100110101.



(a) Encryption

The same plaintext 100 is encrypted into different cyphertexts (100 or 101) at different positions in the input, thanks to CBC.

Diffie-Hellman

- Suppose Alice and Bob wish to do Diffie-Hellman key exchange. Alice and Bob have agreed upon a prime p = 13, and a generator g = 2. Alice has chosen her secret number (private exponent) to be a = 5, while Bob has chosen his private exponent to be b = 4.
- Show the intermediate quantities that both Alice and Bob calculate, as well as the final (shared) secret that Diffie-Hellman produces.

Diffie-Hellman ANS

- Suppose Alice and Bob wish to do Diffie-Hellman key exchange. Alice and Bob have agreed upon a prime p = 13, and a generator g = 2. Alice has chosen her secret number (private exponent) to be a = 5, while Bob has chosen his private exponent to be b = 4.
- Show the intermediate quantities that both Alice and Bob calculate, as well as the final (shared) secret that Diffie-Hellman produces.
- ANS: Alice sends to Bob: A=g^a mod p= 2^5 mod 13 = 6.
- Bob computes the secret: S=A^b mod p = 6^4 mod 13 = 1296 mod 13 = 9.
- Bob sends to Alice B=g^b mod p = 2^4 mod 13 = 3.
- Alice computes the secret: S=B^a mod p = 3^5 mod 13 = 243 mod 13 = 9.