German University in Cairo
Faculty of Media Engineering and Technology
Mervat Abu-Elkheir
Mohamed Abdelrazik
Ahmad Helmy

CSEN1001: Computer and Network Security

Spring Term 2019

Tutorial 4

Problem 1 - Stream & Block ciphers

Determine the type of the cipher used in the following:

a) A cipher encrypts bits by applying the XOR operator on the plain text bits and a string of alternating bits that starts with 0 (i.e. 010101...).

b) A cipher encrypts bits by applying the XOR operator on the first bit and 0, then for each remaining bit the operator is applied with the result of encrypting the previous bit.

c) A cipher reverses the order of every 4 consecutive letters (e.g. ABCDEFGH! DCBAHGFE).

Answer

a) Assume we are encrypting the string 01001110, the result would be: The cipher used is a synchronous stream cipher. Each bit is encrypted using a separate key, thus it is a stream cipher. And it is synchronous because the key stream is independent from both, the plain text and the cipher text. For example:

Bits stream	0	1	0	0	1	1	1	0
Key stream	0	1	0	1	0	1	0	1
Result	0	0	0	1	1	0	1	1

b) The cipher used is a self-synchronizing stream cipher. Each bit is encrypted using a separate key, thus it is a stream cipher. And it is self-synchronizing because the key stream depends on the result of encrypting the previous bit (the key depends on the cipher text).

Bits stream	M_0	M_1	M_2	M_3	M_4	M_5	M_6	M_7
Key stream	0	K_1	K_2	K_3	K_4	K_5	K_6	K_7
Result	C_0	C_1	C_2	C_3	C_4	C_5	C_6	C_7

Where $K_i = M_i$ **XOR** C_{i-1}

c) The cipher used is a block cipher, because the plain text is divided into blocks of 4 letters, and the same key is applied on each block (the key reverses the letters).

Problem 2

Which is the best defense against network sniffing (intercepting network packets on the transmission medium)?

a) Use of switches (over hubs)

b) Use of wired networks (not wireless)

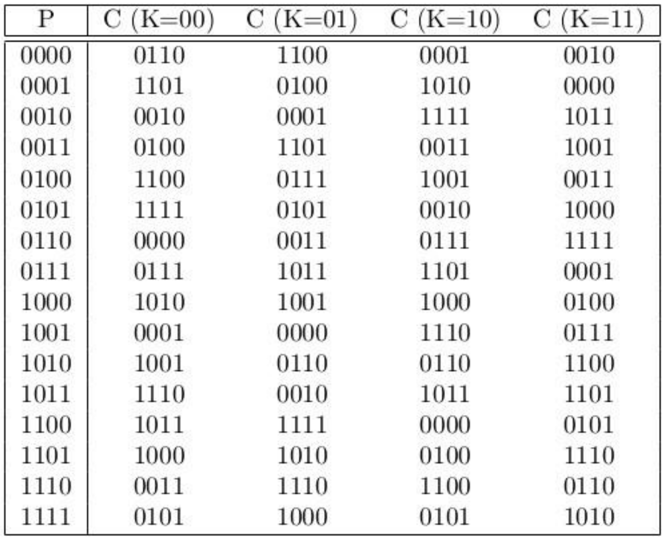
c) Use of gateway
d) Encryption

Answer

e) Encryption.

Problem 2 – Modes of Operation

Consider a 4-bit block cipher, called Steve’s Simple Cipher or SSC for short, shown in the table below. The table gives the ciphertext C produced when encrypting the plaintext P with one of the four keys.



P	C (K=00)	C (K=01)	C (K=10)	C (K=11)
0000	0110	1100	0001	0010
0001	1101	0100	1010	0000
0010	0010	0001	1111	1011
0011	0100	1101	0011	1001
0100	1100	0111	1001	0011
0101	1111	0101	0010	1000
0110	0000	0011	0111	1111
0111	0111	1011	1101	0001
1000	1010	1001	1000	0100
1001	0001	0000	1110	0111
1010	1001	0110	0110	1100
1011	1110	0010	1011	1101
1100	1011	1111	0000	0101
1101	1000	1010	0100	1110
1110	0011	1110	1100	0110
1111	0101	1000	0101	1010

Figure 1: Steve’s Simple Cipher

Encrypt the plaintext 1100101011001111 using SSC and key 00 (and where necessary use an IV 1100) using the following modes of operation: ECB, CBC.

Answer

The plaintext message is divided into 4 blocks, each block consisting of 4 bits.

ECB:

- P1 = 1100, C1 = 1011
- P2 = 1010, C2 = 1001
- P3 = 1100, C3 = 1011
- P4 = 1111, C4 = 0101

CBC:

- P1 XOR IV = 0000, C1 = 0110
- P2 XOR C1 = 1100, C2 = 1011
- P3 XOR C2 = 0111, C3 = 0111
- P4 XOR C3 = 1000, C4 = 1010