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

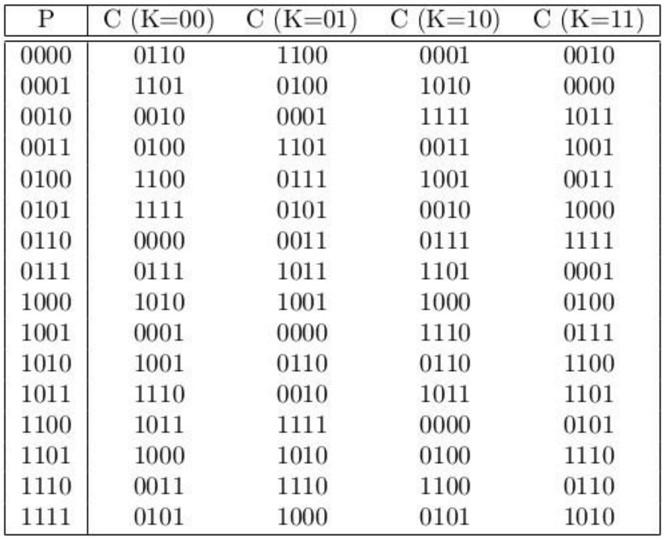
CSEN1001: Computer and Network Security

Spring Term 2019

Tutorial 5

Problem 1 – 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/nonce/counter 1100) using the following modes of operation: CFB, OFB, Counter.

Answer

CFB:

- E(IV,K) = 1011, C1 = 0111
- E(C1,K) = 0111, C2 = 1101
- E(C2,K) = 1000, C3 = 0100
- E(C3,K) = 1100, C4 = 0011

OFB:

- E(IV,K) = 1011, C1 = 0111
- E(E1, K) = 1110, C2 = 0100
- E(E2, K) = 0011, C3 = 1111
- E(E3, K) = 0100, C4 = 1011

CTR:

- E(IV,K) = 1011, C1 = 0111
- E(CTR+1, K) = 1000, C2 = 0010
- E(CTR+2, K) = 0011, C3 = 1111
- E(CTR+3, K) = 0101, C4 = 1010

Problem 2 - Predictability of Pseudo-Random Number Generators (PRNGs)

Consider the case when an attacker intercepts a ciphertext block $C = 11100001$ which is a result of a stream cipher. Assuming the attacker knows that the plaintext belongs to a protocol where each message is highly likely to be prefixed with: 010. Additionally from a PRNG algorithm weakness he was able to predict the next bit in the keystream K such that:

$$b_j = \begin{cases} 0 & \sum_{i=0}^{j-1} 1|b_i = 1 > \sum_{i=0}^{j-1} 1|b_i = 0 \\ 1 & otherwise \end{cases} \qquad where\ b_j \in K.$$

Obtain the plaintext. Assume that the ciphertext is the product of XORing every bit in the plaintext with the corresponding bit in the “pseudo” random key.

Answer

By computing the XOR of the known portion of the plaintext with the ciphertext, one could know the first 3 bits of the pseudo randomly generated keystream K. So,

$$C_{0,1,2} \oplus P_{0,1,2} = 111 \oplus 010 = 101.$$

Next, exploiting the weakness in the PRG one could recursively predict the next bit in the key stream. So, $K_{3,4,5,6,7} = 01010$. Thus, the full key $K = 10101010$ and the plaintext is simply computed as

$$K \oplus C = 10101010 \oplus 11100001 = 01001011$$

Problem 3

When a communication link is subject to monitoring, what is the advantage for using an end-to-end encryption solution over link encryption solution?

a) Clear text is only available to the sending and receiving entities.
b) Routing information is included in the message transmission protocol.
c) Routing information is encrypted by the originator.
d) Each message has a unique encryption key.

Answer

a) Clear text is only available to the sending and receiving entities.