Secure and Dependable Systems
Jacobs University Bremen
Dr. Jürgen Schönwälder

Module: CO-566
Date: 2022-03-24
Due: 2022-03-31

SADS 2022 Problem Sheet #7

Problem 7.1: *block encryption modes of operation* (2+2+2+2+2 = 10 points)

Consider a simple symmetric block cipher with a block size and a key size of 4 bits. The encryption function $E(k, m)$ is defined as

$$E(k, m) = s(k \oplus m)$$

where k is the 4-bit key, m is a 4-bit cleartext block, $\oplus$ is the bitwise exclusive-or operation and the function s is a bijective substitution defined via the following table:

m	0000	0001	0010	0011	0100	0101	0110	0111
$s(m)$	0010	1010	0110	1100	1001	0000	1110	0101
m	1000	1001	1010	1011	1100	1101	1110	1111
$s(m)$	0001	1000	0100	1111	0111	1101	0011	1011

Hint: In your solution, you can write $+$ instead of $\oplus$ to refer to the exclusive-or operation.

a) Define the decryption function $D(k, c)$ and show that the decryption function is correct.

b) Encrypt the message $1010\ 0011\ 0101$ with the key $k = 1010$ using the Electronic Code Book (ECB) mode. Write the ciphertext in space-separated 4-bit blocks.

c) Encrypt the message $1010\ 0011\ 0101$ with the key $k = 1010$ using the Cipher Block Chaining (CBC) mode using the initialization vector $IV = 1001$. Write the ciphertext in space-separated 4-bit blocks.

d) Encrypt the message $1010\ 0011\ 0101$ with the key $k = 1010$ using the Output Feedback Mode (OFB) using the initialization vector $IV = 1001$. Write the ciphertext in space-separated 4-bit blocks.

e) Encrypt the message $1010\ 0011\ 0101$ with the key $k = 1010$ using the Counter Mode (CTR) using the two bit nonce $N = 11$ (in binary) and a two bit counter. Write the ciphertext in space-separated 4-bit blocks.