

Cryptography Assingment 3

Exercise 1

a) Given the recursive sequence/LFSR defined by

$$z_{i+4} = z_i + z_{i+1} + z_{i+2} + z_{i+3}(\text{mod } 2)$$

What are the periods using the keys

1 $K = 1000$?

2 $K = 0011$?

3 $K = 1111$?

b) What are the periods with the same keys using the following LFSR?

$$z_{i+4} = z_i + z_{i+3}(\text{mod } 2)$$

Exercise 2

Vi define a HMAC as follows:

- Key $K = 1001$
- ipad = 0011
- opad = 0101
- h is the midsquare-hasing, calculationg $x^2(\text{mod } 2^8)$ and retrieving the middle four binary digits. Eg. $1011^2 = 01111001$ (with leading 0), giving us 1110 as hash value.

- a) Find the HMAC for the message 0110
- b) You receive the message 0111, with HMAC 0100. Is it reason to believe that the message is authentic?

Oppgave 3

Use the Cæsar cipher, with encryption $e_3(x) = x + 3 \pmod{2^8}$ and find the CBC-MAC to the following two messages:

$$x = 1101\ 1111\ 1010\ 0001$$

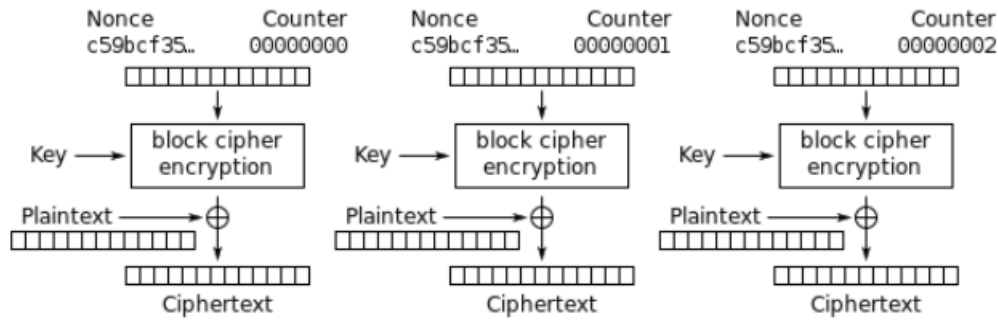
$$x' = 0010\ 1100\ 0001\ 1111$$

Exercise 4

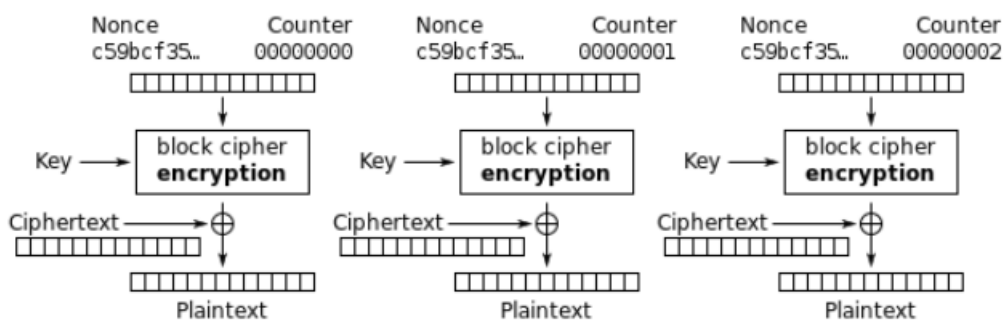
We can construct a key-stream by using a block cipher in CTR-mode, by simply encrypting a sequence of values with a block cipher. It will use a *nonce* (initial value) combined with a counter. Here we will use addition modulo $2^8 = 256$ as the operation combining the nonce and the counter. The counter starts at 0, and add 1 to it for each round.

For the block cipher in parts a)-c) below, we use the SUBBYTES of the AES cipher, which substitutes a byte (8 bits) for another byte using a table lookup (actually a calculation in a certain Galois field, but its not in the curriculum).

Write programs to do the calculations.



Counter (CTR) mode encryption



Counter (CTR) mode decryption

- Using the nonce = 01100101, write down the first 4 bytes produced with counter values 0,1,2,3.
- What is the period of the key-stream?
- Can the computation of the keystream be easily parallelized?
- You intercept a message which is encrypted by XOR-ing a key-stream generated by CTR, as described above, but with an unknown block cipher (not the one above). How could information about known plaintexts-ciphertext pairs be used to infer information about the key used?