Homework 8 in Cryptography I

E23|

$$\begin{pmatrix} r_0 \\ r_1 \\ r_2 \\ r_3 \end{pmatrix} = \begin{pmatrix} x & x+1 & 1 & 1 \\ 1 & x & x+1 & 1 \\ 1 & 1 & x & x+1 \\ x+1 & 1 & 1 & x \end{pmatrix} \begin{pmatrix} c_0 \\ c_1 \\ c_2 \\ c_3 \end{pmatrix} \qquad (*)$$

Expand the left hand side, reduce it modulo $u^4+1 \in \mathbb{F}_{2^8}[u]$ and use the abbreviations $(r_0, r_1, r_2, r_3)'$ according to $(*)$.

$$\left(c_3 u^3 + c_2 u^2 + c_1 u + c_0\right)\left((x+1)u^3 + u^2 + u + x\right)$$

$$= (x+1)c_3 u^6 + \left[c_3 + (x+1)c_2\right]u^5 + \left[c_3 + c_2 + (x+1)c_1\right]u^4$$
$$+\left[x c_3 + c_2 + c_1 + (x+1)c_0\right]u^3 + \left[x c_2 + c_1 + c_0\right]u^2$$
$$+\left[x c_1 + c_0\right]u + x c_0$$

$$= (x+1)c_3 u^6 + \underline{(x+1)c_3 u^2}$$
$$+\left[c_3 + (x+1)c_2\right]u^5 + \underline{\left[c_3 + (x+1)c_2\right]u} \qquad \equiv 0 \pmod{u^4+1}$$
$$+\left[c_3 + c_2 + (x+1)c_1\right]u^4 + \underline{\left[c_3 + c_2 + (x+1)c_1\right]} \qquad \equiv 0 \pmod{u^4+1}$$
$$+\left[x c_3 + c_2 + c_1 + (x+1)c_0\right]u^3$$
$$+\underline{\left[(x+1)c_3 + x c_2 + c_1 + c_0\right]u^2} \qquad \equiv 0 \pmod{u^4+1}$$
$$+\left[\underline{c_3 + (x+1)c_2} + x c_1 + c_0\right]u$$
$$+\left[\underline{c_3 + c_2 + (x+1)c_1} + x c_0\right]$$

$$\overset{(*)}{\equiv} r_3 u^3 + r_2 u^2 + r_1 u + r_0 \pmod{u^4+1}$$

E24|

a)
- In mode ECB it holds $M_i = BC_k^{-1}(C_i)$. Therefore only the block containing the changed bit is affected. Hence, at maximum 128, 192 or 256 Bits are decrypted wrongly. (depending on the block size)
- In mode CBC it holds $M_i = BC_k^{-1}(C_i) \oplus C_{i-1}$. Therefore a changed bit in block i may change at maximum all bits of block i and one bit in block $(i+1)$.
- In mode OFB it holds $M_i = C_i \oplus Z_i$. As Z_i only depends on K and C_0 exactly one bit will be decrypted wrongly. $[Z_0 = C_0, Z_i = BC_k(Z_{i-1})]$
- In mode CFB it holds $M_i = C_i \oplus BC_k(C_{i-1})$. Consequently at most one block and one bit is affected.
- In mode CTR it holds $M_i = C_i \oplus BC_k(Z_i)$. As the second addend only depends on K and C_0 exactly one bit will be decrypted wrongly. $[Z_0 = C_0, Z_i = Z_{i-1} + 1]$

b) If one bit of the ciphertext is lost or an additional one is inserted in block i at position j all bits beginning with the following position may be corrupt

mode	block	position
ECB	i	1
CBC	i	1
OFB	i	j
CFB	i	j
CTR	i	j

In modes ECB and CBC all bits of blocks $i, i+1, \ldots$ may be corrupt, whereas in modes OFB, CFB and CTR all bits beginning at position j of block i may be corrupt.

Alternative representation of a) with blocksize BS

mode	M_i	wrong bits at maximum	commentary
ECB	$BC_k^{-1}(C_i)$	BS	
CBC	$BC_k^{-1}(C_i) \oplus C_{i-1}$	BS+1	
OFB	$C_i \oplus Z_i$	1	$Z_0 = C_0, Z_i = BC_k(Z_{i-1})$
CFB	$C_i \oplus BC_k(C_{i-1})$	BS+1	
CTR	$C_i \oplus BC_k(Z_i)$	1	$Z_0 = C_0, Z_i = Z_{i-1} + 1$