Tutorial 6

P2/ Given: Alphabet A, blocklength $n \in \mathbb{N}$, $\mathcal{M} = A^n = \mathcal{C}$

a) An encryption function is an injective function $e_K : \mathcal{M} \to \mathcal{C}$, with $K \in \mathcal{K}$

injective function f: $f(x_1) = f(x_2) \Rightarrow x_1 = x_2$

$|\{e_K(M) \mid M \in \mathcal{M}\}| = |\mathcal{M}|$

$\{e_K(M) \mid M \in \mathcal{M}\} \subseteq \mathcal{C} \Rightarrow e_K(\mathcal{M}) = \mathcal{C}$

$\Rightarrow e_K$ is also surjective $\Rightarrow e_K$ is a bijective

A permutation π is a bijective function $\pi : X \to X$

$\Rightarrow \forall K \in \mathcal{K}$, the encryption e_K is a permutation with $X = A^n$

b) $A = \{0,1\}$, $n = 6$, there are $N = 2^6 = 64$ elements

$\Rightarrow$ there are $64! \approx 1.2689 \cdot 10^{89}$ different block ciphers.

P3/ a) The bit error occurs in block C_i, $i > 0$, with blocksize BS

mode	M_i	max # errors	Remark
ECB	$E_k^{-1}(C_i)$	BS	Only block C_i is affected
CBC	$E_k^{-1}(C_i) \oplus C_{i-1}$	BS + 1	M_i and one bit in M_{i+1} is affected
OFB	$C_i \oplus z_i$	1	$z_0 = C_0, z_i = E_k(z_{i-1})$
CFB	$C_i \oplus E_k(C_{i-1})$	BS + 1	M_{i+1} and one bit in M_i
CTR	$C_i \oplus E_k(z_i)$	1	$z_0 = C_0, z_i = z_{i-1} + 1$

b) One bit is last one added at block C_i at position j, $i > 0$

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

In ECB and CBC all bits of all blocks C_{i+k}, $k \in \mathbb{N}_0$ may be corrupt.

In OFB, CFB, CTR all bits beginning at position j in block i may be corrupt.

P1) $k = (2D\ 61\ 72\ 69 \mid 65\ 00\ 76\ 61 \mid 6E\ 00\ 43\ 6C \mid 65\ 65\ 6666)$

$= (w_0\ w_1\ w_2\ w_3)$

a) $K_0 = K = (w_0\ w_1\ w_2\ w_3)$

b) $K_1 = (w_4\ w_5\ w_6\ w_7)$

Follow flg 1 to calculate w_4 which are the first 4 Bytes of K_1

$tmp \leftarrow w_3 = (65\ 65\ 6666)$

1) Evaluate SubBytes(RotByte(tmp)) $\oplus$ Rcon($i/4$)

1.1 $i/4 = 1$; $Rcon(1) = (RC(1), 00, 00, 00) = (01, 00, 00, 00)$

1.2 RotByte(tmp) $= (65\ 66\ 66\ 65)$ // cyclic left-shift of bytes

1.3 SubBytes$(65\ 66\ 66\ 65) = (4D\ 33\ 33\ 4D)$

$\Rightarrow tmp = (4C\ 33\ 33\ 4D)$ // 1.3 + 1.1

2) $w_4 \leftarrow w_0 \oplus tmp$

	2	D	6	1	7	2	6	9
w_0	0010	1101	0110	0001	0111	0010	0110	1001
tmp	0100	1100	0011	0011	0011	0011	0100	1101
Result	0110	0001	0101	0010	0100	0001	0010	0100
	6	1	5	2	4	1	2	4
tmp	4	C	3	3	3	3	4	D