Crypto 1 GÜ 8.)

09. JUNI 2011

Ex 22) Correction:

$$c = \min\{k \in \mathbb{N} \mid \exists i_0 \in \mathbb{N}, \forall i \geq i_0, i \in \mathbb{N}, z_{i+k} = z_i\}$$

HW 8

E23) Weak keys in DES: $E_k(E_k(m)) = m \quad \forall m \in M$

Recall: DES^{-1} means to execute DES with round keys in reverse order

$K_1 = K_{16}, \; K_2 = K_{15}, \ldots, \; K_8 = K_9$

This holds in particular, if $K_1 = K_2 = \ldots = K_{16}$

We know $K_n = (C_n, D_n)$

In table S. 1: - First three bits of first 4 bytes are used for C_0

- First 4 bits of last 4 bytes used for C_0
- "Rest" is used for D_0

Choose $k = xxxxyyyy$

$x = bbbccccd$ $\qquad b, c \in \{0, 1\}$

$y = bbbbcccc e$

$C_0 = bb \ldots b \Rightarrow C_n = C_0 \quad \forall 0 \leq n \leq 16$

$D_0 = cc \ldots c \Rightarrow D_n = D_0 \quad \forall 0 \leq n \leq 16$

$\Rightarrow K_1 = K_2 = \ldots = K_{16}$

(b.) $b = c = 0, \; K = 0101010101010101 \quad d = e = 1$

$b = 1, c = 0, \; K = E0E0E0E0F1F1F1F1 \quad d = 0, e = 1$

$b=0, c=1$, $k = 1F1F1F1F0E0E0E0E$ $\quad d=1, e=0 \Leftrightarrow$ (a.)

$b=1, c=1$, $k = FEFEFEFEFEFEFEFE$ $\quad d=1, e=1$

E24) Alphabet A, $n \in \mathbb{N}$ Block length

$\Rightarrow \mathcal{M} = A^n = [redacted] \; C$

(a) Fix key $K \in \mathcal{K}$, as $e(\cdot, k)$ is injective it holds

$|\mathcal{M}| = |e(\mathcal{M}, K)| = |C| \Rightarrow e(\mathcal{M}, K) = C = \mathcal{M}$

$\Rightarrow e(\cdot, k)$ is a permutation

(b.) $A = \{0,1\}$ and block length $n = 6$

so there are $N = 2^6 = 64$ elements

It follows $64! \approx 1.2689 \cdot 10^{89}$ different block ciphers

E26)

$\underline{r} = \underline{I} \cdot \underline{c}$

$$\begin{pmatrix} r_0 \\ r_1 \\ r_2 \\ r_3 \end{pmatrix} = \begin{pmatrix} x & x+1 & 1 & 1 \\ 1 & x & x+1 & 1 \\ 1 & 1 & x & x+1 \\ x+1 & 1 & 1 & x \end{pmatrix} \begin{pmatrix} c_0 \\ c_1 \\ c_2 \\ c_3 \end{pmatrix} \in F_{2^8}^4 \qquad (*)$$

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

$= r_3 u^3 + r_2 u^2 + r_1 u + r_0 \mod u^4+1$

$= c_3(x+1)u^6 + (c_3 + (x+1)c_2)u^5 + (c_3 + c_2 + (x+1)c_1)u^4$

$+ (x c_3 + c_2 + c_1 + (x+1)c_0)u^3$

$+ (x c_2 + c_1 + c_0)u^2 + (x c_1 + c_0)u + x c_0$

$= c_3(x+1)u^6 + \underline{c_3(x+1)u^2} \equiv 0 \mod u^4+1$

$$+ (c_3 + (x+1)c_2)u^5 + (c_3 + (x+1)c_2)u \equiv 0 \mod u^4+1$$
$$+ (c_3 + c_2 + (x+1)c_1)u^4 + c_3 + c_2 + (x+1)c_1 \equiv 0 \mod u^4+1$$
$$+ (x c_3 + c_2 + c_1 + (x+1)c_0)u^3$$
$$+ ((x+1)c_3 + x c_2 + c_1 + c_0)u^2$$
$$+ (c_3 + (x+1)c_2 + x c_1 + c_0)u$$
$$+ c_3 + c_2 + (x+1)c_1 + x c_0$$

$$= r_3 u^3 + r_2 u^2 + r_1 u + r_0 \pmod{u^4+1}$$

E2.5)

subbyte (65 66 66 65) = (4D 33 33 4D)