Exercies 2 . 26.04.2019.

Problema 1 : $m \in \mathbb{Z}_q$ $e_K(m) = am + b$

$a \in \mathbb{Z}_q^*$ $b \in \mathbb{Z}_q$

a) $e_{K_n}(\dots(e_{K_2}(e_{K_1}(m)))\dots)$

$K_i = (a_i, b_i)$ $i = 1, \dots, n$

b) n-fold encryption

$e_{K_1}(m) = a_1 m + b_1$

$e_{K_2}(e_{K_1}(m)) = a_2 a_1 m + (a_2 b_1 + b_2)$

$\vdots$

$$e_{K_n}(\dots e_{K_1}(m)\dots) = \left(\prod_{i=1}^{n} a_i\right) m + \sum_{i=1}^{n} b_i \left(\prod_{l=i+1}^{n} a_l\right) \bmod q.$$

(b) No advantage: we still have an affine cipher.

Problem 2: (Hill cipher) A is used to generate c from m using $c = Am$.

$$A = \begin{pmatrix} 1 & 1 & 1 \\ 1 & 1 & 0 \\ 1 & 0 & 1 \end{pmatrix} \in \mathbb{Z}_2^{3\times 3} = \mathbb{F}_2^{3\times 3}$$

a) $m = \begin{pmatrix} m_1 \\ m_2 \\ m_3 \end{pmatrix}$ $\quad Am = c$

$$c_1 = m_1 + m_2 + m_3$$

$$c_2 = m_1 + m_2$$

$$c_3 = m_1 + m_3$$

b) $c_1 + c_3 = 2m_1 + 2m_3 + m_2 = (0 + 0 + m_2) \mod 2$

$\Rightarrow (c_1 + c_3) \mod 2 = m_2 \mod 2$

$$(c_1 + c_2) \mod 2 = (2m_1 + 2m_2 + m_3) \mod 2$$

$$= m_3 \pmod 2$$

$$(c_1 + c_2 + c_3) \mod 2 = (3m_1 + 2m_2 + 2m_3) \mod 2$$

$$= m_1 \pmod 2$$

$$(C_1 + C_3) \bmod 2 = m_2$$

$$(C_1 + C_2) \bmod 2 = m_3$$

$$(C_1 + C_2 + C_3) \bmod 2 = m_1$$

Problem 3: Compute the possible keys:

a) Substitution $\mathbb{Z}_\ell = \{0, \dots, \ell - 1\}$

$0 \longrightarrow a_0$

$\vdots \longrightarrow a_1$ $\quad (a_0, \dots, a_{\ell-1})$

$\ell - 1 \longrightarrow a_{\ell-1}$ $\quad$ is a permutation of $(0, \dots, \ell - 1)$

$\ell!$

b) Affine cipher $\mathbb{Z}_{26} = \{0, \dots, 25\}$

$K = (a, b) \in \mathbb{Z}_{26}^* \times \mathbb{Z}_{26}$ $\quad am + b$

$|\mathbb{Z}_{26}^*| \times |\mathbb{Z}_{26}| = 12 \times 26 = 312$

c) Permutation cipher with a fixed blocklength

$2 \; 0 \to 2 \; 1$)

Z_n^* Z_n $a + x = c \mod n$

$\Rightarrow x = (c-a) \mod n$

$x + 2 = 3 \mod 4$

$x = 1 \mod 4$

$\Rightarrow \underline{2x = 1 \mod 4}$

$x + a = b \qquad x = b - a$

$x = b + a_+^{-1}$

inverse element of addition operation.

$a_+^{-1} + a = 0 \mod n$

$a^{-1} \times a = 1 \mod n.$

$2x = 1 \mod 4 \Rightarrow 4 | 2x - 1$ ✗

$Z_4^* = \{1, 3\} \qquad Z_4 = \{0, 1, 2, 3\}$

$1 \times 1 = 1 \mod 4$

$3 \times 3 = 9 = 1 \mod 4.$