Prof. Dr. Rudolf Mathar, Dr. Michael Reyer

Tutorial 2
- Proposed Solution -

Friday, April 26, 2019

Solution of Problem 1

a) Claim:

$$c_l = m \prod_{i=1}^{l} a_i + \sum_{i=1}^{l} b_i \left(\prod_{j=i+1}^{l} a_j \right) \mod q \qquad \forall\, l \in \mathbb{N}$$

Proof by induction.

Basic step

$$c_1 = a_1 m + b_1 \mod q = m \prod_{i=1}^{1} a_i + \sum_{i=1}^{1} b_i \left(\prod_{j=i+1}^{1} a_j \right) \mod q$$

Inductive step $l \to l+1$

$$\begin{aligned} c_{l+1} &\equiv a_{l+1} c_l + b_{l+1} \equiv a_{l+1} \left(m \prod_{i=1}^{l} a_i + \sum_{i=1}^{l} b_i \left(\prod_{j=i+1}^{l} a_j \right) \right) + b_{l+1} \\ &\equiv m \prod_{i=1}^{l+1} a_i + \sum_{i=1}^{l+1} b_i \left(\prod_{j=i+1}^{l+1} a_j \right) \pmod q \end{aligned}$$

Obviously, it holds $c = c_n$.

b) We obtain an effective key:

$$k = (a = \textstyle\prod_{i=1}^{n} a_i \mod q, b = \sum_{i=1}^{n} b_i \left(\prod_{j=i+1}^{n} a_j \right) \mod q)$$

Therefore, successively encrypting with two different affine functions is the same as encrypting with only one effective key $k = (a, b)$.

Solution of Problem 2

a) The explicit encryption function is given as:

$$\begin{aligned} c_{ik+1} &= m_{ik+1} + m_{ik+2} + m_{ik+3} \\ c_{ik+2} &= m_{ik+1} + m_{ik+2} \\ c_{ik+3} &= m_{ik+1} \qquad\qquad\quad + m_{ik+3} \end{aligned}$$

b) To derive the encryption function, calculate the inverse of matrix A (in $\mathbb{F}_2$). You may first make sure that A^{-1} exists.

$$\det A = 1 \cdot 1 \cdot 1 + 1 \cdot 0 \cdot 1 + 1 \cdot 1 \cdot 0 - 1 \cdot 1 \cdot 1 - 1 \cdot 1 \cdot 1 - 1 \cdot 0 \cdot 0 = -1 = 1 \neq 0$$

$$\begin{array}{ccc@{\quad}ccc@{\quad}l}
1 & 1 & 1 & 1 & 0 & 0 & + \\
1 & 1 & 0 & 0 & 1 & 0 & + \\
1 & 0 & 1 & 0 & 0 & 1 &
\end{array}$$

$$\begin{array}{ccc@{\quad}ccc@{\quad}l}
1 & 1 & 1 & 1 & 0 & 0 & + \\
0 & 0 & 1 & 1 & 1 & 0 & \\
0 & 1 & 0 & 1 & 0 & 1 &
\end{array}$$

$$\begin{array}{ccc@{\quad}ccc@{\quad}l}
1 & 1 & 0 & 0 & 1 & 0 & + \\
0 & 1 & 0 & 1 & 0 & 1 & \\
0 & 0 & 1 & 1 & 1 & 0 &
\end{array}$$

$$\begin{array}{ccc@{\quad}ccc}
1 & 0 & 0 & 1 & 1 & 1 \\
0 & 1 & 0 & 1 & 0 & 1 \\
0 & 0 & 1 & 1 & 1 & 0
\end{array}$$

The explicit decryption function becomes:

$$\begin{aligned}
m_{ik+1} &= c_{ik+1} + c_{ik+2} + c_{ik+3} \\
m_{ik+2} &= c_{ik+1} \qquad\qquad\; + c_{ik+3} \\
m_{ik+3} &= c_{ik+1} + c_{ik+2}
\end{aligned}$$

Solution of Problem 3

a) Substitution cipher: Keys are permutations over the symbol alphabet $\Sigma = \{x_0, ..., x_{l-1}\}$.
$\Rightarrow$ As known from combinatorics, there are $l!$ permutations, i.e., $l!$ possible keys.

b) Affine cipher with key (b, a) and with symbols in alphabet $\mathbb{Z}_{26}$:

$$c_i = (a \cdot m_i + b) \bmod 26$$

$$m_i = a^{-1} \cdot (c_i - b) \bmod 26$$

For a valid decryption a^{-1} must exist. a^{-1} exists if $\gcd(a, 26) = 1$ holds
$\Rightarrow a \in \mathbb{Z}_{26}^*$. 26 has only 2 dividers as $26 = 13 \cdot 2$ is its prime factorization.

$$\mathbb{Z}_{26}^* = \{a \in \mathbb{Z}_{26} \mid \gcd(a, 26) = 1\} = \{1, 3, 5, 7, 9, 11, 15, 17, 19, 21, 23, 25\} \subset \mathbb{Z}_{26}$$

$\Rightarrow |\mathbb{Z}_{26}^*| = 12$ possible keys for a.
There is no restriction on $b \in \mathbb{Z}_{26}$, i.e., $|\mathbb{Z}_{26}| = 26$ possible keys for b.
Altogether, we have $|\mathbb{Z}_{26} \times \mathbb{Z}_{26}^*| = |\mathbb{Z}_{26}| \cdot |\mathbb{Z}_{26}^*| = 26 \cdot 12 = 312$ possible keys (a, b).

c) Permutation cipher with block length $L \Rightarrow L!$ permutations $\Rightarrow L!$ possible keys.