Prof. Dr. Rudolf Mathar, Dr. Arash Behboodi, Jose Leon

Exercise 2
- Proposed Solution -

Friday, April 29, 2016

Solution of Problem 1

It is helpful to organize the plaintext $\boldsymbol{m} = (m_1, m_2, m_3, ..., m_{kl})$ in a matrix with l rows and k columns as shown on the left hand side. The second matrix on the right hand side describes the mapping of the positions to the ciphertext.

$$
\begin{array}{cccc|cccc}
m_1 & m_{l+1} & \cdots & m_{(k-1)l+1} & 1 & 2 & \cdots & k \\
m_2 & \cdots & \cdots & \vdots & k+1 & \cdots & \cdots & \vdots \\
\vdots & \cdots & \cdots & \vdots & \vdots & \cdots & \cdots & \vdots \\
\vdots & \cdots & \cdots & m_{kl-1} & \vdots & \cdots & \cdots & (l-1)k \\
m_l & \cdots & \cdots & m_{kl} & (l-1)k+1 & \cdots & \cdots & kl
\end{array}
$$

From this the encryption of the Scytale is described by a permutation $\boldsymbol{\pi}$ with:

$$
\boldsymbol{\pi} = \begin{pmatrix} 1 & 2 & \dots & l & l+1 & \dots & (k-1)l+1 & \dots & kl-1 & kl \\ 1 & k+1 & \dots & (l-1)k+1 & 2 & \dots & k & \dots & (l-1)k & kl \end{pmatrix}
$$

Solution of Problem 2

a) Applying the n encryption functions successively results in:

$$
\begin{aligned}
c_1 &\equiv a_1 m + b_1 \mod q \\
c_2 &\equiv a_2 c_1 + b_2 \equiv a_2(a_1 m + b_1) + b_2 \\
&\equiv a_2 a_1 m + a_2 b_1 + b_2 \mod q \\
c_3 &\equiv a_3 c_2 + b_3 \\
&\equiv a_3(a_2 a_1 m + a_2 b_1 + b_2) + b_3 \\
&\equiv a_3 a_2 a_1 m + a_3 a_2 b_1 + a_3 b_2 + b_3 \mod q \\
&\vdots \\
c_n &\equiv \prod_{i=1}^{n} a_i m + \sum_{i=1}^{n-1} b_i \left(\prod_{j=i+1}^{n-1} a_j\right) + b_n \mod q \\
&\equiv \prod_{i=1}^{n} a_i m + \sum_{i=1}^{n} b_i \left(\prod_{j=i+1}^{n} a_j\right) \mod q
\end{aligned}
$$

using the definition of the empty product in the last step.

Note: A complete mathematical proof would involve the induction $n \to n+1$:

$$\begin{aligned} c_{n+1} &\equiv \prod_{i=1}^{n+1} a_i m + \sum_{i=1}^{n+1} b_i \prod_{j=i+1}^{n+1} a_j \\ &\equiv a_{n+1} \prod_{i=1}^{n} a_i m + a_{n+1} \sum_{i=1}^{n} b_i \prod_{j=i+1}^{n} a_j + b_{n+1} \\ &\equiv a_{n+1} c_n + b_{n+1} \quad \square \end{aligned}$$

b) We obtain an effective key:

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

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

Solution of Problem 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.

Solution of Problem 4

The message space of a finite sequence of length $k = 11$ is:

$$\mathcal{M} = \{(m_1, ..., m_{11}) \mid m_i \in \mathcal{X}\}$$

with the alphabet $\mathcal{X} = \{a, b, ..., z\} = \{0, 1, ..., 25\}$, and $|\mathcal{X}| = 26$.

In the given task, there are 4 blocks with cyclic permutations. These blocks are not changed if the letters are the same inside each individual block. Unchanged sequences are subsumed by:

$$\begin{aligned} \hat{\mathcal{M}} = \{&(m_1, ..., m_{11}) | m_1 \in \mathcal{X}, m_2 = m_{11} = m_5 = m_8 \in \mathcal{X}, m_3 = m_6 = m_7 = m_4 \in \mathcal{X}, \\ &m_9 = m_{10} \in \mathcal{X}\} \end{aligned}$$

The total number of such sequences is $|\hat{\mathcal{M}}| = |\mathcal{X}|^4 = 456976$.

Remark: However, compared to $|\mathcal{M}| = |\mathcal{X}|^{11} \approx 3.6 \cdot 10^{15}$, this is only a minor restriction.

(An unchanged plaintext in English is 'MISSISSIPPI'.)