Prof. Dr. Rudolf Mathar, Dr. Arash Behboodi, Markus Rothe

Exercise 2
- Proposed Solution -

Friday, April 27, 2018

Solution of Problem 1

a)

$$A = \begin{pmatrix} a_{11} & \dots & a_{1m} \\ \vdots & \ddots & \vdots \\ a_{m1} & \dots & a_{mm} \end{pmatrix} \in \mathbb{Z}_n^{m\times m}$$

It holds

$$A^{-1} = \begin{pmatrix} b_{11} & \dots & b_{1m} \\ \vdots & \ddots & \vdots \\ b_{m1} & \dots & b_{mm} \end{pmatrix} = \frac{\operatorname{adj} A}{\det A} = \frac{1}{\det A} \begin{pmatrix} \tilde{a}_{11} & \dots & \tilde{a}_{1m} \\ \vdots & \ddots & \vdots \\ \tilde{a}_{m1} & \dots & \tilde{a}_{mm} \end{pmatrix},$$

with

$$\tilde{a}_{ij} = (-1)^{i+j} \cdot M_{ij} = (-1)^{i+j} \cdot \det \begin{pmatrix} a_{1,1} & \cdots & a_{1,j-1} & a_{1,j+1} & \cdots & a_{1,n} \\ \vdots & \ddots & \vdots & \vdots & \ddots & \vdots \\ a_{i-1,1} & \cdots & a_{i-1,j-1} & a_{i-1,j+1} & \cdots & a_{i-1,n} \\ a_{i+1,1} & \cdots & a_{i+1,j-1} & a_{i+1,j+1} & \cdots & a_{i+1,n} \\ \vdots & \ddots & \vdots & \vdots & \ddots & \vdots \\ a_{n,1} & \cdots & a_{n,j-1} & a_{n,j+1} & \cdots & a_{n,n} \end{pmatrix}.$$

Note: $\operatorname{adj} A$ denotes the adjugate matrix or classical adjoint matrix, but *not* the conjugate transpose.

$$\begin{aligned} &\Rightarrow \quad b_{ij} = \frac{1}{\det A}\tilde{a}_{ji} \mod n, \ \tilde{a}_{ij} \in \mathbb{Z}_n \\ &\Rightarrow \quad b_{ij} \text{ exists if } (\det A)^{-1} \text{ exists} \quad \Leftrightarrow \quad \gcd(n, \det(A)) = 1\,. \end{aligned}$$

b)

$$M = \begin{pmatrix} 7 & 1 \\ 9 & 2 \end{pmatrix} = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathbb{Z}_{26}^{2\times 2}$$

$$\det(M) = ad - cb = 7 \cdot 2 - 1 \cdot 9 = 5$$

$$\gcd(n, \det(M)) = \gcd(26, 5) = 1$$

$\Rightarrow$ the inverse exists, it is computed by:

$$M^{-1} = \frac{1}{\det M} \cdot \begin{pmatrix} d & -b \\ -c & a \end{pmatrix} = 5^{-1} \begin{pmatrix} 2 & -1 \\ -9 & 7 \end{pmatrix} \equiv 21 \cdot \begin{pmatrix} 2 & -1 \\ -9 & 7 \end{pmatrix} \equiv \begin{pmatrix} 16 & 5 \\ 19 & 17 \end{pmatrix} \mod 26$$

Solution of Problem 2

a) Applying the n encryption functions successively results in:

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

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.