Homework 1 in Advanced Methods of Cryptography - Proposal for Solution -

Prof. Dr. Rudolf Mathar, Michael Reyer, Henning Maier
16.10.2012

Solution to Exercise 3.

A bijective function $\pi : M \mapsto M$ over a finite set M is called *permutation*.

(a) It holds:

i) $\pi(1) \in M$ has n different possibilities

ii) $\pi(2) \in M \setminus \{\pi(1)\}$ has $n-1$ different possibilities, $\pi(1)$ has to be taken out, otherwise π is not bijective.

iii) $\pi(3) \in M \setminus \{\pi(1), \pi(2)\}$ has $n-2$ different possibilities.

iv) $\vdots$

Overall, there are $n \cdot (n-1) \cdot (n-2) \cdot \ldots \cdot 1 = n!$ different permutations possible.

(b) Let π_1, π_2, π_3 be permutations over M and $m \in M$.

i) **Associativity**: $((\pi_1 \circ \pi_2) \circ \pi_3)(m) = (\pi_1 \circ \pi_2)(\pi_3(m)) = \pi_1(\pi_2(\pi_3(m))) = \pi_1((\pi_2 \circ \pi_3)(m)) = \pi_1 \circ (\pi_2 \circ \pi_3)(m)$

ii) **Neutral element**: $\pi_0(m) = m, \forall m \in M$ is the neutral element, it holds for a permutation π and $m \in M$:
$(\pi \circ \pi_0)(m) = (\pi(\pi_0(m)) = \pi(m) = \pi_0(\pi(m)) = (\pi_0 \circ \pi)(m)$

iii) **Inverse element**: Each permutation π has an inverse element as it is a bijective function, it holds $\pi \circ \pi^{-1} = \pi^{-1} \circ \pi = \pi_0$.

With i), ii), and iii) the permutations form a group together with the composition of functions.

For $n = 1, 2$ this group is commutative. However, for $n \geq 3$ it is not. Given a permutation π it can be fully described by

$$(1, 2, \ldots, n) \mapsto (\pi(1), \pi(2), \ldots, \pi(n)).$$

Define π_1 by $(1, 2, 3, \ldots, n) \mapsto (1, 3, 2, \ldots)$ and π_2 by $(1, 2, 3, \ldots, n) \mapsto (2, 1, 3, \ldots)$, then it holds $(\pi_1 \circ \pi_2)(1) = \pi_1(\pi_2(1)) = \pi_1(2) = 3$ and
$(\pi_2 \circ \pi_1)(1) = \pi_2(\pi_1(1)) = \pi_2(1) = 2$ which shows that the group is not commutative.

There are two applications of using permutations for cryptography.

- In 2.2 of the script the substitition cipher is introduced, where the permutation is defined over the alphabet, i.e., each character m of the message is encrypted as $c = \pi(m)$. This is a generalization of the Caesar cipher.
- In 2.3 of the script permutation ciphers are introduced, where the order of characters is permutated in message blocks of length $k \in \mathbb{N}$, i.e., π is a permutation over $\{1, \ldots, k\}$, and for $l \in \mathbb{N}_0, 1 \leq i \leq k$ the message $(m_1, m_2, \ldots)$ is ecnrypted as $c_{lk+i} = m_{lk+\pi(i)}$.