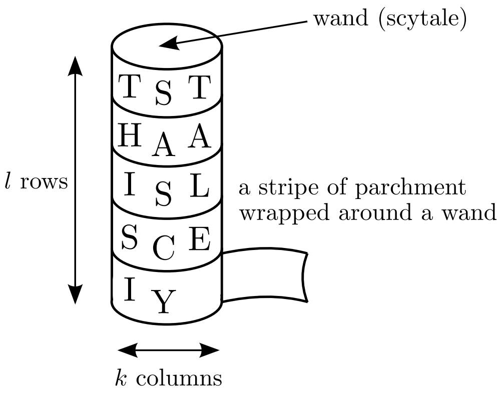
Prof. Dr. Rudolf Mathar, Dr. Arash Behboodi, Jose Leon

Exercise 2

Friday, April 29, 2016

Problem 1. *(Scytale)* For the encryption with an ancient Scytale, a parchment is wrapped around a wand such that there are $l \in \mathbb{N}$ rows and $k \in \mathbb{N}$ columns, cf. the conceptual figure. The letters of the plaintext $\boldsymbol{m} = (m_1, m_2, \ldots, m_{kl})$ are written columnwise on the parchment. After unwrapping, the cryptogram is given on the stripe of parchment.



a) Give the entries $\pi(i)$ for $i \in \{1, 2, l, l+1, (k-1)l+1, kl-1, kl\}$ for the permutation

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

which describes the encryption scheme of the Scytale with l rows and k columns.

Problem 2. *(sequence of affine ciphers)*

Suppose you encrypt a message $m \in \mathbb{Z}_q$ using an affine cipher $e_k(m)$ with key $k = (a, b) \in \mathbb{Z}_q^* \times \mathbb{Z}_q$.

a) Compute the n-fold encryption $c = e_{k_n}(...e_{k_2}(e_{k_1}(m))...)$ for different keys $k_i = (a_i, b_i)$ with $i = 1, ..., n$.

b) Is there an advantage using n subsequent encryptions, rather than using a single affine cipher? Substantiate your claim.

Problem 3. *(number of keys)* Compute the number of possible keys for the following cryptosystems:

a) Substitution cipher with the alphabet $\Sigma = \mathbb{Z}_l = \{0, \ldots, l-1\}$

b) Affine cipher with the alphabet $\Sigma = \mathbb{Z}_{26} = \{0, \ldots, 25\}$

c) Permutation cipher with a fixed blocklength L

Problem 4. *(weak permutations)* The permutation $\pi = (1)(2, 11, 5, 8)(3, 6, 7, 4)(9, 10)$ defines a permutation cipher with block length $k = 11$.

(a) Determine the number of character sequences of length 11 over the usual alphabet with 26 letters whose ciphertext is equal to the plaintext.

Hint: $(2, 11, 5, 8)$ means that position 2 is moved to position 11, 11 to 5, 5 to 8 and 8 to 2.