RWTH AACHEN UNIVERSITY Lehrstuhl für Theoretische Informationstechnik

Exercise 1 in Cryptography

Prof. Dr. Rudolf Mathar, Henning Maier, Jose Angel Leon Calvo

2015-04-16

Problem 1. *(Multiplicative Inverses)* Take a look at the appendix of the lecture notes and solve the following tasks.

a) Compute $1234 \mod 357$ using the standard long division with a remainder.

b) Compute the greatest common divisor of 357 and 1234, i.e., $\gcd(357, 1234)$, using the Euclidean algorithm.

c) Compute the multiplicative inverse of 357 modulo 1234, i.e., $357^{-1} \mod 1234$ using the extended Euclidean algorithm. Check if $357 \cdot 357^{-1} \equiv 1 \mod 1234$ holds.

Consider polynomials with the indeterminate x and coefficients in $\mathbb{Z}_2 = \{0, 1\}$.

d) A polynomial $a(x)$ is a multiplicative inverse of $b(x)$ modulo $m(x)$ if the product yields $b(x) \cdot a(x) \equiv 1 \bmod m(x)$. Compute $\gcd(b(x), m(x))$ and the multiplicative inverse of $b(x) = x^3 + x + 1$ modulo $m(x) = x^5 + x^3 + 1$.

Hint: *Addition of the coefficients is taken modulo 2.*

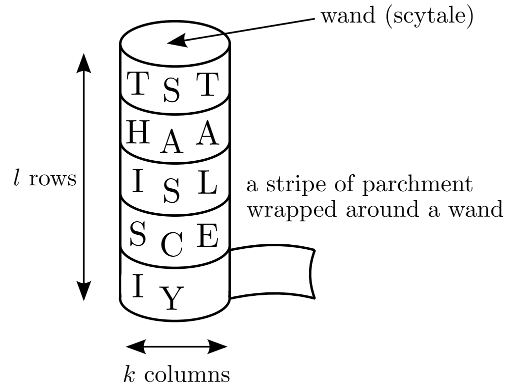
Problem 2. *(Dividers)* Let $a, b, c, d \in \mathbb{Z}$. The integer a divides b if and only if there exists a $k \in \mathbb{Z}$ such that $a \cdot k = b$. This property is denoted by $a \,|\, b$. Prove the following implications:

a) $a \,|\, b$ and $b \,|\, c \quad \Rightarrow \quad a \,|\, c.$

b) $a \,|\, b$ and $c \,|\, d \quad \Rightarrow \quad (ac) \,|\, (bd).$

c) $a \,|\, b$ and $a \,|\, c \quad \Rightarrow \quad a \,|\, (xb + yc) \;\; \forall\, x, y \in \mathbb{Z}.$

Problem 3. *(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.