# Cryptography

Prof. Dr. Klaus Meer, Ameen Naif

Exercise Sheet 3
Version 10.05.2019

---

**Exercise 1.**

Let $n \in \mathbb{N}$ and $a \in \mathbb{Z}_n$ be fixed.

(a) Show that $ax = b \; mod \; n$ has a unique solution $x \in \mathbb{Z}_n$ for every $b \in \mathbb{Z}_n$ if and only if $gcd(a, n) = 1$.

(b) How many possible keys has the **Affine Cipher**?

**Exercise 2.**

Let $\mathbf{s} = s_1 s_2 \cdots s_r$ be a random string of $r \in \mathbb{N}$ characters from the alphabet $\mathbb{Z}_{26}$. Show that $I_c(\mathbf{s}) \simeq \sum_{i=0}^{25} p_i^2$, where $I_c$ is the **Index of Coincidence** and $p_i$ is the probability to have $i$ in the string $\mathbf{s}$.

**Exercise 3.**

Suppose that $\pi$ is the following permutation of $\{1, 2, ..., 8\}$: $\pi = \left(\begin{smallmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 4 & 1 & 6 & 2 & 7 & 3 & 8 & 5 \end{smallmatrix}\right)$.

i) Compute the permutation $\pi^{-1}$.

ii) Decrypt the following ciphertext, which was encrypted using the key $\pi$:

TGEEMNELNNTDROEOAAHDOETCSHAEIRLM.

**Exercise 4.**

Let $\mathcal{P} = \{a, b\}, \mathcal{C} = \{1, 2, 3, 4\}$ and $\mathcal{K} = \{K_1, K_2, K_3\}$ denote **random variables** with $\mathbf{Pr}(a) = 1/4$, $\mathbf{Pr}(b) = 3/4$ and $\mathbf{Pr}(K_1) = 1/2$, $\mathbf{Pr}(K_2) = \mathbf{Pr}(K_3) = 1/4$. Suppose the encryption functions defined to be $e_{K_1}(a) = 1$, $e_{K_1}(b) = 2$; $e_{K_2}(a) = 2$, $e_{K_2}(b) = 3$ and $e_{K_3}(a) = 3$, $e_{K_3}(b) = 4$.

(a) Compute the probability distribution on $\mathcal{C}$.

(b) Compute the conditional probability distributions on the ciphertext, given that a certain ciphertext has been observed.

(c) has the cryptosytem $(\mathcal{P}, \mathcal{C}, \mathcal{K})$ **perfect secrecy**?

**Exercise 5.**

Show that for any plaintext probability distribution the **Shift Cipher** has perfect secrecy, if the 26 keys are used with equal probability 1/26.

**Exercise 6.**

Prove that the Affine Cipher achieves perfect secrecy if every key is used with equal probalbility 1/312.

**Exercise 7.**

Suppose that $y, y' \in \mathcal{C} = \mathbb{Z}_2^n$ for some $n \in \mathbb{N}$ are two ciphertext elements in the **One-time Pad** that were obtained by encrypting plaintext elements $x, x' \in \mathcal{P} = \mathbb{Z}_2^n$, respectively, using the same key $k \in \mathcal{K} = \mathbb{Z}_2^n$. Prove that $x + x' = y + y' \; mod \; 2$.

**Exercise 8.**

Let $e(p, k)$ represent the encryption of plaintext $p$ with key $k$ using the **DES** cryptosystem. Suppose $c = e(p, k)$ and $c' = e(\sim (p), \sim (k))$, where $\sim$: $\{0,1\}^{64} \to \{0,1\}^{64}$ denotes the **bitwise complement operator** of its argument,i.e. $\sim$ converts every 1 to a 0 and vice versa. Prove that $c' = \sim (c)$.

**Note:** the actual structure of **S-boxes** and other components of the system are irrelevant for the above property.

**Exercise 9.**

Compute the following using the method of **Modular Exponentiation**:

a) $2^{71}$ *mod* 143 b) $16^{47}$ *mod* 143 c) $21^{19}$ *mod* 143

**Exercise 10.**

Bob wants to set up his own public and private keys. He chooses $p = 23$ and $q = 19$ with $e = 283$. Find the private key to decrypt the ciphertext $c = 14^{283}$ *mod* $p \cdot q$.

**Exercise 11.**

**Big $\mathcal{O}$ Notation**:

(a) Let $f(n) = 4n^2 + 3n + 5$. Is $f \in \mathcal{O}(n^3)$? Is there a function $h : \mathbb{N} \to \mathbb{N}$ such that $f \in \mathcal{O}(h)$, where $h \in \mathcal{O}(n^3)$?

(b) Show that $f$ is not an element of $\mathcal{O}(n)$.

**Recall:** Let $f, g : \mathbb{N} \to \mathbb{N}$ be functions. One writes $f \in \mathcal{O}(g)$ **iff** there exists an integer $N \geq 1$ and a real number $c > 0$ such that for all $n \geq N$, we have $f(n) \leq c \cdot g(n)$.

**Exercise 12.**

**Division Algorithm for Polynomials:** Let $p, q \in \mathbb{R}[x]$ such that $q(x) \neq 0$. Prove by induction over $deg(p)$ that there exist unique polynomials $k, r \in \mathbb{R}[x]$ such that $\forall x \in \mathbb{R} : p(x) = k(x) \cdot q(x) + r(x)$, $deg(r) < deg(q)$ or $r(x) = 0$.

**Exercise 13.**

**Polynomial greatest common divisor:** Let $p, q \in \mathbb{R}[x]$ such that $q(x) \neq 0$ and let $r \in \mathbb{R}[x]$ be the remainder of the polynomial division $p/q$.

(a) Show that $gcd(p, q) = gcd(q, r)$ (Euclidean algorithm).

(b) Find $gcd(x^4 - 7x^2 - 6x, x^3 - x^2 - 5x - 3)$.

**Recall:** The greatest common divisor of polynomials $p \in \mathbb{R}[x]$ and $q \in \mathbb{R}[x]$, denoted by $gcd(p, q)$, is a polynomial $d \in \mathbb{R}[x]$ that divides $p$ and $q$ and such that every common divisor of $p$ and $q$ also divides $d$.