Homework 3 in Cryptography I

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

28.04.2011

Exercise 8. The permutation[1] $\pi = (1)(2, 11, 5, 8)(3, 6, 7, 4)(9, 10)$ 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.

Exercise 9. Show the following properties for the greatest common divisor:

(a) Prove that: $a \in \mathbb{Z}_m$ invertible $\Leftrightarrow \gcd(a, m) = 1$.

(b) Let $a, b \in \mathbb{Z}$ with $b \neq 0$ and $q, r \in \mathbb{Z}$ and $a = bq + r$ and $0 \leq r < b$.
Prove that: $\gcd(a, b) = \gcd(b, r)$.

(c) Give a sufficient condition on $a, b \in \mathbb{Z}$ such that:
$\gcd(a \cdot b, m) = \gcd(a, m) \cdot \gcd(b, m)$.

(d) Show that $\mathbb{Z}_m^* = \{b \in \mathbb{Z}_m \mid \gcd(b, m) = 1\}$ is a multiplicative group.

(e) Is 221 invertible modulo 2310?

Hint: For any $a, b \in \mathbb{Z}$, there exist $x, y \in \mathbb{Z}$ such that $\gcd(a, b) = ax + by$.

Exercise 10. The plaintext hidden in the following ciphertext is part of a famous English play:

```
KPJDLCGS PVHQKWRK KCKRBKPJ DLCWILKR BGSKORKO VCVCNVEW OVQDLCIL YFIRRIGB
IVSXQKRB DLCSVCXX PKRAOWYX HMXIKKRG XLGCXGWI NVEWCQYX CNKVRC
```

(a) Determine the index of coincidence I_C. What can you derive from it[2]?

[1] $(2, 11, 5, 8)$ means that position 2 is moved to position 11, 11 to 5, 5 to 8 and 8 to 2.

[2] $I_C \approx 0.0385$: polyalphabetic and uniformly distributed; $I_C \approx 0.0668$: monoalphabetic and English