Exercise 2 in Cryptography

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

2015-04-23

Problem 4. *(decipher classical cryptosystem)* The following ciphertext is given:

```
rgneidvgpewn xh iwt hijsn du bpiwtbpixrpa itrwcxfjth gtapits id phetrih
du xcudgbpixdc htrjgxin hjrw ph rdcuxstcixpaxin, spip xcitvgxin, tcixin
pjiwtcixrpixdc, pcs spip dgxvxc pjiwtcixrpixdc.
```

a) Why is this ciphertext easy to decrypt?

b) Decipher the given ciphertext. What is the secret key?

Hint: The plaintext is an English text.

Problem 5. *(properties of the greatest common divisor)*
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 $0 \leq r < b$.
Show that: $\gcd(a, b) = \gcd(b, r)$.

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

Hint 1: For any $a, b \in \mathbb{Z}$, there exist $x, y \in \mathbb{Z}$ such that $\gcd(a, b) = ax + by$.
Hint 2: For any $a, b \in \mathbb{Z}$ with $\gcd(a, b) = 1 \Rightarrow \gcd(a \cdot b, m) = \gcd(a, m) \cdot \gcd(b, m)$.
Hint 3: The definition of a multiplicative group is given in Appendix A.1 of the script.

Problem 6. *(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