The Affine Cipher

Modular Arithmetics

Prof Hans Georg Schaathun

Høgskolen i Ålesund

Autumn 2013 – Video 3/3
Recorded: September 30, 2013

Another problem

- Cæsar's cipher is insecure because it has no key
- The generalised cipher $e_k(x) = x + k \mod 26$
    - is insecure because the key space is small
- We shall see another generalisation

Another Monoalphabetic Cipher

Definition

A monoalphabetic cipher is a permutation $e_k : \mathcal{A} \rightarrow \mathcal{A}$ on the alphabet, which is applied independently on every letter of the plaintext.

- Remember the modular ring $\mathbb{Z}_{26}$
- We have four arithmetic operations $+, \cdot, -, /$
- Any bijection on $\mathbb{Z}_{26}$ will do as a monoalphabetic ciper.
- Cæsar is additive $x + k$
- How about multiplicative $x \cdot k$?

Some examples

A B C D E F G H I J K L M N O P Q R S T U V W X Y Z

The Affine Cipher

$$e_{k_1,k_2}(x) = k_1 \cdot x + k_2 \mod 26$$

- This is an affine function (map)
- Gives us the affine cipher
- Combines a multiplicative and an additive key.

The Affine Cipher

$$e_{k_1,k_2}(x) = k_1 \cdot x + k_2 \mod 26$$

Exercises

Exercise

Encrypt the string Hello world using the affine cipher

$$e_{k_1,k_2}(x) = k_1 \cdot x + k_2 \mod 26$$

with key $(k_1, k_2) = (12, 3)$.