The modulo operator

Introduction to Cryptography

Prof Hans Georg Schaathun

Høgskolen i Ålesund

Autumn 2013 – Video 1/2
Recorded: September 18, 2013

Cæsar's cipher

- Substitute each letter by jumping three letters in the alphabet.
  - $A \mapsto D$, $B \mapsto E$, $C \mapsto F$
- Wrap around:
  - $X \mapsto A$, $Y \mapsto B$, $Z \mapsto C$

HØGSKOLEN I ÅLESUND
Aalesund University College

Cæsar the Mathematician

How do we automate the encryption?

Step 1 Translating letters into numbers

- A bijection from the alphabet to a set of numbers.

Step 2 Encryption on a set of numbers

- A permutation on our set of numbers.

Step 3 Putting it all together

HØGSKOLEN I ÅLESUND
Aalesund University College

Cæsar the Mathematician

Step 1: Abstraction into a mathematical form

- Let $\mathcal{A}$ be the 26-letter alphabet
- Encryption is a permutation $e : \mathcal{A} \to \mathcal{A}$
- Bijection $z : \mathcal{A} \to \mathbb{Z}_{26}$, where $Z_{26} = \{0, 1, 2, \ldots, 25\}$

$$z(A) = 0, z(B) = 1, \ldots, z(Z) = 25$$

Working with e' on $\mathbb{Z}_{26}$ in lieu of $\mathcal{A}$ gives access to general theory.

HØGSKOLEN I ÅLESUND
Aalesund University College

Cæsar the Mathematician

Step 2: Encrypting in numbers

- Encryption is a permutation $e : \mathcal{A} \to \mathcal{A}$
  - or $e' : \mathbb{Z}_{26} \to \mathbb{Z}_{26}$
- e' jumps three places
  - i.e. $e'(x) = x + 3$
- but what if $x + 3 > 25$?
  - we need to wrap around.
- The wrap around operator in mathematics is known as modulus
  - and we write $e'(x) = x + 3 \mod 26$

If $(x + 3) \geq 26$, $\mod 26$ *tells us to subtract 26 (or a multiple thereof) to get* $e'(x) \in \mathbb{Z}_{26}$

HØGSKOLEN I ÅLESUND
Aalesund University College

Cæsar the Mathematician

Step 2: Encrypting in numbers

- Encryption is a permutation $e : \mathcal{A} \to \mathcal{A}$
  - or $e' : \mathbb{Z}_{26} \to \mathbb{Z}_{26}$
- e' jumps three places
  - i.e. $e'(x) = x + 3$
- but what if $x + 3 > 25$?
  - we need to wrap around.
- The wrap around operator in mathematics is known as modulus
  - and we write $e'(x) = x + 3 \mod 26$

If $(x + 3) \geq 26$, $\mod 26$ *tells us to subtract 26 (or a multiple thereof) to get* $e'(x) \in \mathbb{Z}_{26}$

HØGSKOLEN I ÅLESUND
Aalesund University College

Cæsar the Mathematician

Step 2: Encrypting in numbers

- Encryption is a permutation $e : \mathcal{A} \to \mathcal{A}$
  - or $e' : \mathbb{Z}_{26} \to \mathbb{Z}_{26}$
- e' jumps three places
  - i.e. $e'(x) = x + 3$
- but what if $x + 3 > 25$?
  - we need to wrap around.
- The wrap around operator in mathematics is known as modulus
  - and we write $e'(x) = x + 3 \mod 26$

If $(x + 3) \geq 26$, $\mod 26$ *tells us to subtract 26 (or a multiple thereof) to get* $e'(x) \in \mathbb{Z}_{26}$

HØGSKOLEN I ÅLESUND
Aalesund University College

Cæsar the Mathematician

Step 2: Encrypting in numbers

- Encryption is a permutation $e : \mathcal{A} \to \mathcal{A}$
  - or $e' : \mathbb{Z}_{26} \to \mathbb{Z}_{26}$
- e' jumps three places
  - i.e. $e'(x) = x + 3$
- but what if $x + 3 > 25$?
  - we need to wrap around.
- The wrap around operator in mathematics is known as modulus
  - and we write $e'(x) = x + 3 \mod 26$

If $(x + 3) \geq 26$, $\mod 26$ *tells us to subtract 26 (or a multiple thereof) to get* $e'(x) \in \mathbb{Z}_{26}$

HØGSKOLEN I ÅLESUND
Aalesund University College

Cæsar the Mathematician

Step 1 Bijection

$$z : \mathcal{A} \to \mathbb{Z}_{26}$$

Step 2 Encryption is a permutation

$$e' : \mathbb{Z}_{26} \to \mathbb{Z}_{26}$$

Step 3 We put it together

$$e : \mathcal{A} \to \mathcal{A}$$
$$e = z^{-1} \circ e' \circ z$$

A monoalphabetic cipher is a permutation $e : \mathcal{A} \to \mathcal{A}$ on the alphabet $\mathcal{A}$.

We call e the encryption function.

HØGSKOLEN I ÅLESUND
Aalesund University College

Modulus

Theorem (Euclid's Division Theorem)

Let n be a positive integer. Then for every integer m, there exist unique integers q and r so that $m = nq + r$ and $0 \leq r < n$.

- The theorem essentially concerns integer division
- You will recall the remainder r from primary school.
- This is used as the definition for modulus
  - $m \mod n = r$
  - To calculate $\mod n$ you divide by n and take the remainder

HØGSKOLEN I ÅLESUND
Aalesund University College

Exercise

Exercise

Consider the plaintext `peculiar` *to be encrypted using Cæsar's cipher. Show how you encrypt the message step by step, mapping to integers, using modular arithmetrics, and then mapping back to the alphabet.*

Exercise

Calculate the following expressions

- $2 + 3 \mod 4$
- $2 \cdot 3 \mod 6$
- $4 \cdot 3 - 1 \mod 10$

HØGSKOLEN I ÅLESUND
Aalesund University College