Information and Communication

Codebreaking for Traditional Cipher Systems

Abe Wiersma

Universiteit van Amsterdam

20 januari 2016

Inhoudsopgave

Introduction in Ciphers
- Modern Ciphers
- Traditional Ciphers

Breaking Traditional Ciphers
- Substitution Cipher

Modern Ciphers

- Private-key cryptography, where the same key is used for encryption and decryption.
- Public-key cryptography, where two different keys are used for encryption and decryption.

Ciphers can be distinguished into two types by the type of input data:

- block ciphers, which encrypt block of data of fixed size
- stream ciphers, which encrypt continuous streams of data

Traditional Ciphers

- Origin lies in ancient Egypt $\sim$ 4000 years ago.
- Ends after second world war with the emergence of the computers.

Uses

- War movement.
- Government Secrets.

Types: Traditional Ciphers

- Substitution Cipher
- Permutation Cipher
- Running key Cipher
- An Enigma-style periodic polyalphabetic Cipher

Substitution Cipher: Example

Example cipher

Substitution Cipher: Problem

Example cipher

Substitution Cipher: Solution

Example cipher

Stelling

Stelling (Massa-energierelatie)

$E = mc^2$

Conclusie

Belangrijkste conclusie