Università della Svizzera italiana

C&QI Cryptography & Quantum Information

The History of Cryptography

Arne Hansen and Prof Stefan Wolf
Cryptography and Quantum Information, USI Lugano

Hiding Information: A Definition of Cryptography

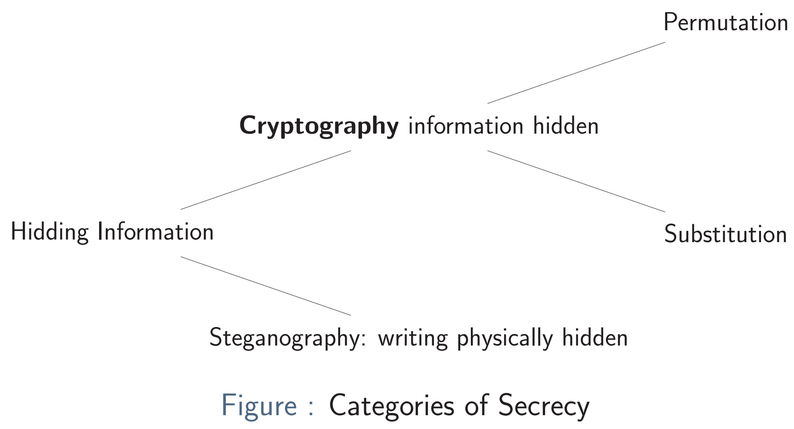
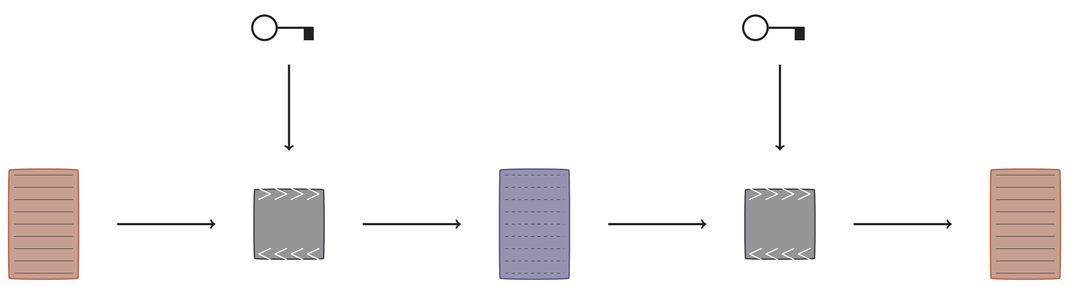


Figure : Categories of Secrecy

Cryptography hidding content of a message without hiding the writing itself.

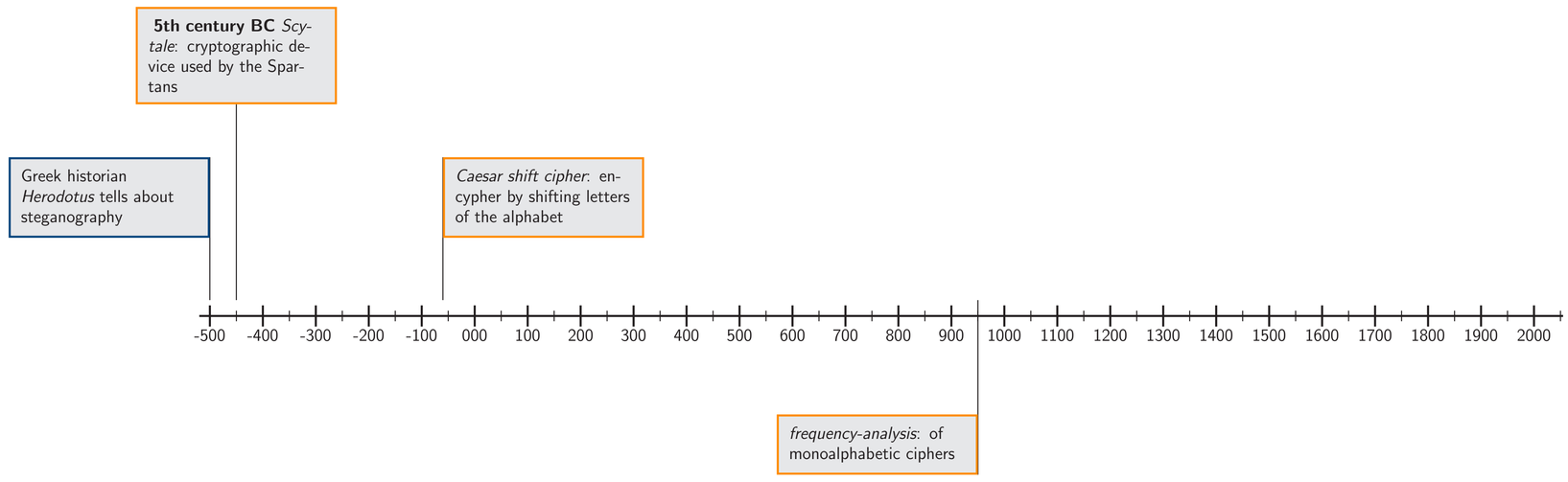
The Scheme of Cryptography



A battle between Cryptographers and Cryptoanalysts

An encrypted message remains only secret if the there is no way to break the restore the the

Timeline of Cryptography



Scytale: a transposition cipher

The message "Help me, I am under attack" is written on the scytale in rows

$$\begin{array}{|c|c|c|c|c|} \hline \boldsymbol{H} & \boldsymbol{E} & \boldsymbol{L} & \boldsymbol{P} & \boldsymbol{M} \\ \boldsymbol{E} & \boldsymbol{I} & \boldsymbol{A} & \boldsymbol{M} & \boldsymbol{U} \\ \boldsymbol{N} & \boldsymbol{D} & \boldsymbol{E} & \boldsymbol{R} & \boldsymbol{A} \\ \boldsymbol{T} & \boldsymbol{T} & \boldsymbol{A} & \boldsymbol{C} & \boldsymbol{K} \\ \hline \end{array} \tag{1}$$

After unwinding the band it becomes scrambled to

$$\boldsymbol{HENTEIDTLAEAPMRCMUAK} \tag{2}$$

Caesar Shift Cipher

- some items and $\alpha = \gamma, \sum_i$
- some items
- some items
- some items

$$\alpha = \gamma, \sum_i$$

Frequency Analysis

- some items
- some items
- some items
- some items

Introduction

- some items and $\alpha = \gamma, \sum_i$
- some items
- some items
- some items

$$\alpha = \gamma, \sum_i$$