The History of Cryptography

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

Ways of Hiding Information

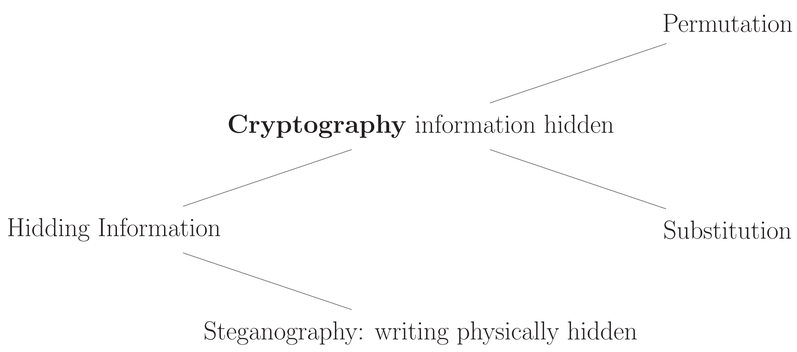
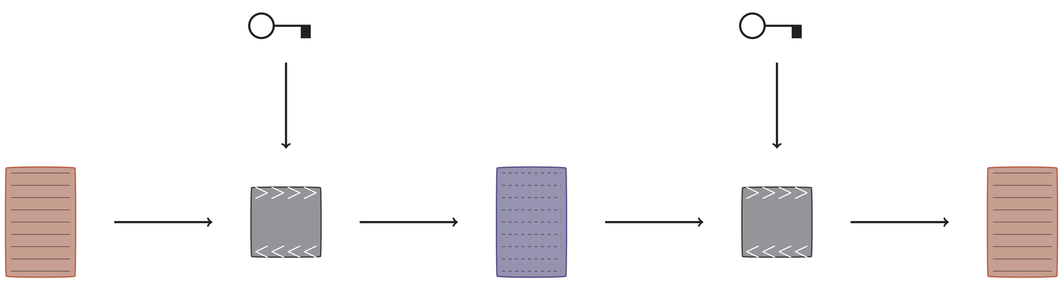


Figure : Categories of Secrecy

Cryptography hiding content of a message without hiding the writing itself.
Steganography physically hiding the message (invisible ink, . . .)

The Scheme of Cryptography

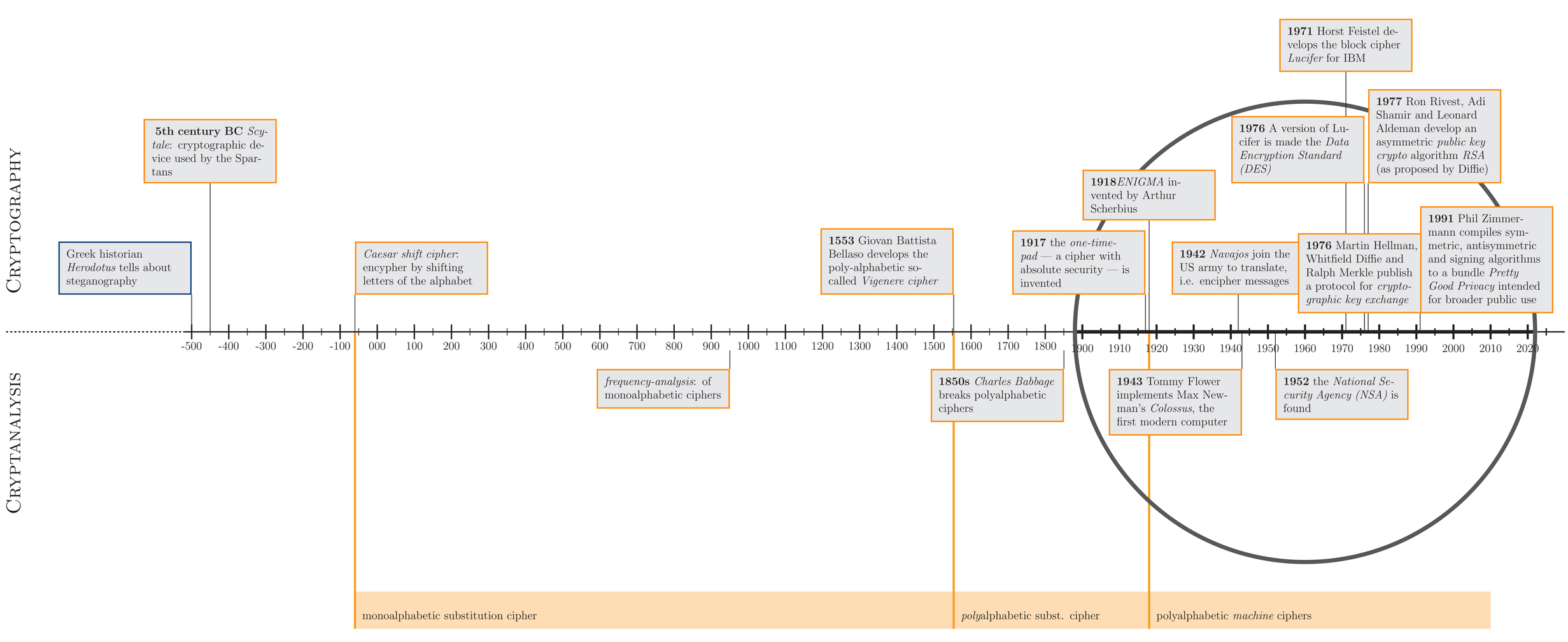


The plaintext is together with a key are given to an encryption algorithm generating the ciphertext. The ciphertext is then sent to another party. With the right key the message can be deciphered again.

The neverending competition between Cryptographers and Cryptanalysts

Cryptanalysts study cryptographic systems and try to break them. They search for ways to access the hidden information. In history the advantage alternated between cryptographers and cryptanalysists.
First cryptographic monoalphabetic substitution ciphers — i.e. ciphers built on replacing letters according to a fixed scheme like the Caesar cipher — were safe as long the substitution scheme was kept secret. The first cryptanalytic breakthrough stemmed from linguistic studies of the Koran in the 9^{th} century in the Arabic world. Theologians analyzed the structure of text in order to determine their origin, thereby counting letters and studying the frequencies with which they appeared. It turned out: some letters are used more often than others. In English for example the most frequent letter is “e”. Counting the frequencies of letters in a ciphertext makes it pretty easy to guess the replacement scheme used to encrypt a message. Once *frequency analysis* was developed cryptanalysists could basically break any message until cryptographic methods were developed further.
One might think, that after the one-time pad was shown to be absolutely secure, the competition might have been settled in favor of cryptographers. Unfortunately the one-time pad is not efficient as the key (that has to be destributed secretely) has to be as long as the message itself.

Timeline of Cryptography



The timeline shows the greatest achievements in the history of cryptography and cryptanalysis. On the bottom the evolution from monoalphabetic substitution ciphers to current computer based polyalphabetic substition ciphers is drawn.

Scytale: a transposition cipher

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

H	***E***	***L***	***P***	***M***
E	***I***	***A***	***M***	***U***
N	***D***	***E***	***R***	***A***
T	***T***	***A***	***C***	***K***

After unwinding the band it becomes scrambled to

HENTEIDTLAEAPMRCMUAK

Navajo Code: an unbroken ‘linguistic’ code

During WWII machine ciphers have been common among all parties. A major

The Caesar Shift Cipher

Frequency Analysis

The One-Time Pad

Enigma: a first machine cipher