The History of Cryptography

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

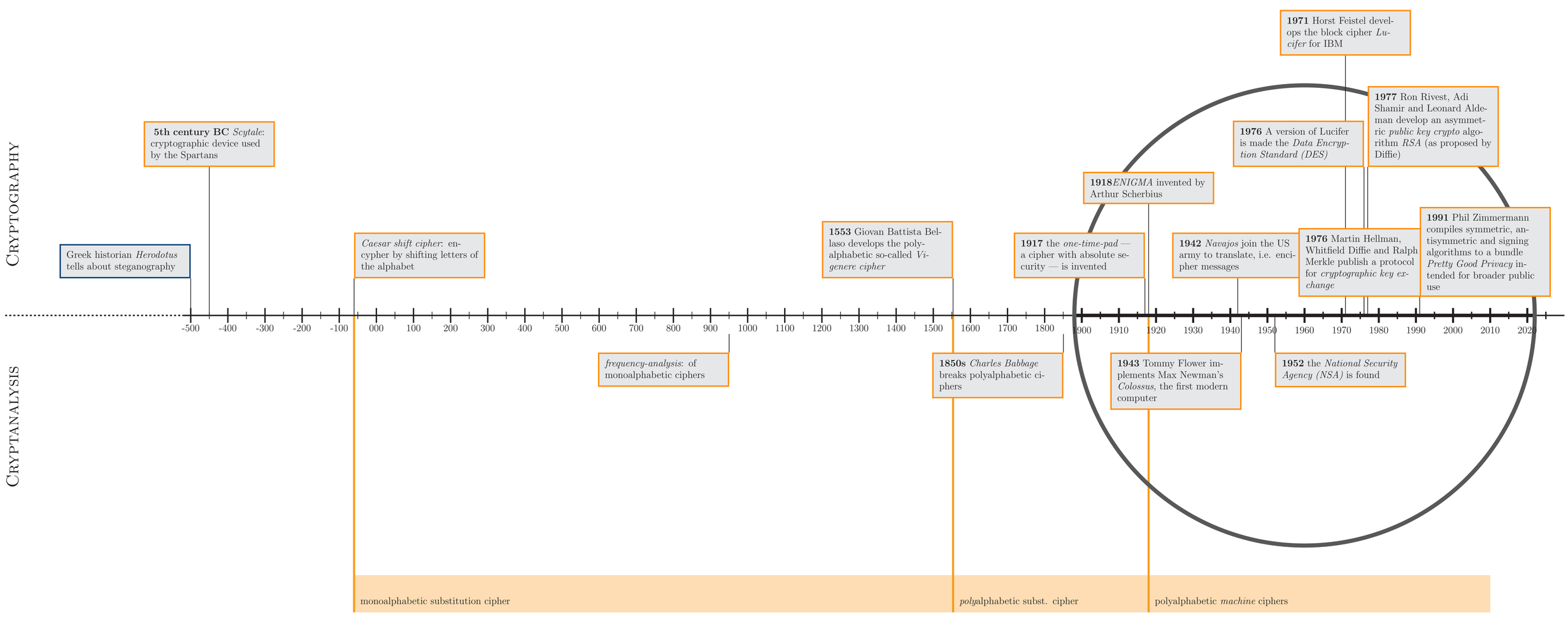
A secret history

Having particular information can be a great advantage, as well as not having some information can be a great disadvantage. This has a wide range of policital, economical and strategic implications. Intelligence services around the world gather information to support politicians and the army, plagiarism can cause severe economical losses. This has spurred attempts to hide information and on the contrary reveal hidden information.
As secret services try to maintain advantages in accessing or hiding information a good deal of information about cryptography itself is veiled. Discoveries are hidden, records are classified, the involved are sworn to silence. Therefore the history of cryptography remains shadowy at some points and occasionally had to be rewritten after discoveries were published belatedly.

The neverending competition between Cryptographers and Cryptanalysts

While cryptographers search for ways to hide information cryptanalysts study ciphers 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.
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.

Steganography in the ancient world

The Greek historian Herodotus has written about ways to conceal information. In the 5th century BC messages were covered with a layer of wax. In another instance the message was tattooed on the shaved head of a messenger. After the hair had grown again the message could finally be delivered. This way of hiding the message physically is called steganography.

Navajo Code: an unbroken 'linguistic' code

During WWII machine ciphers have been common among all parties. A major drawback was the time effort to encode and decode. In critical situations that required fast communication encryption was thus dropped revealing the content directly to the enemy. Therefore in 1942 Philip Johnston, a US American engineer, suggested to translate message to the tribal language of the Navajo before transmission. As its grammar and vocabulary was not related to neither European nor Asiatic languages it served as a very secure cipher. Therefore Navajos were recruited as translators and cryptographers. While machine ciphers were frequently broken, the Navajo language was never.

The Caesar Shift Cipher

Frequency Analysis

One of the first cryptanalytic breakthroughs 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. In 1553 the Italian Giovan Battista Bellaso suggested to use more then just one substitution scheme and switch among those. In the 19^{th} century the British Charles Babbage refined frequency analysis and broke into these polyalphabetic ciphers.

The One-Time Pad

The one-time pad — a cipher with an entirely random key as long as the meassage — was reinvented in 1917 (after having been described before in 1882). As long as the key is secret and the one-time pad is merely used once, as the name suggests, it is entirely secure as Shannon has shown in 1945. The major drawback though is that long keys have to be exchanged without being revealed or tampered.
The hotline between Moscow and Washington D.C. established after the Cuban Missle Crisis in 1963 was secured with a one-time pad.
Further it has theoretical significance in information theory and cryptography.

Enigma: a first machine cipher