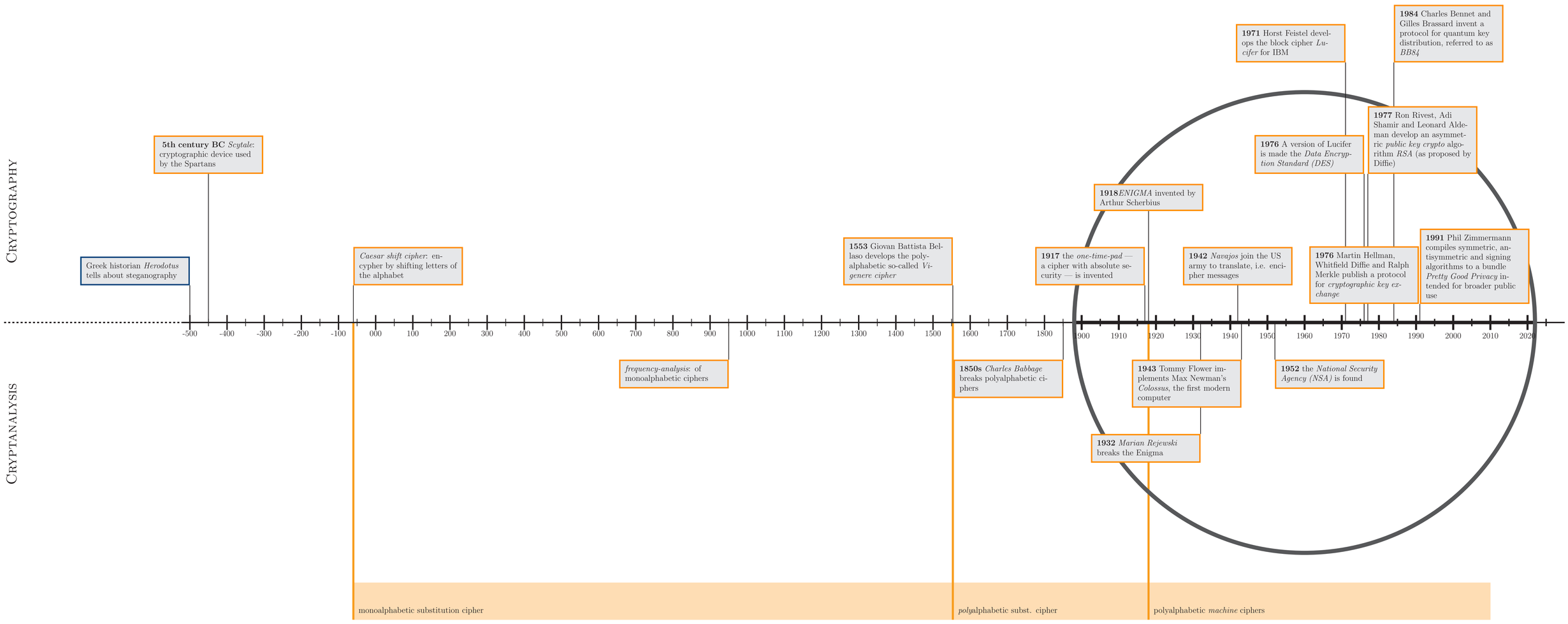
Universität della Svizzera italiana

C&QI Cryptography & Quantum Information

The History of Cryptography

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

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.

A secret history

Having particular information can be a great advantage, just as not having certain information can be of 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 in particular 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. Monoalphabetic ciphers like the Caesar Cipher turned insecure as frequency analysis were developed. Cryptographers therefore introduced polyalphabetic ciphers, like the Vigenere Cipher. Consequently frequency analysis were refined until cryptanalysts got access to the information again. And so on and so forth ...

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. These ways of hiding messages physically are called steganography (Greek *steganos* "concealed, covered").

The Caesar Shift Cipher: monoalphabetic ciphers

The first documented military use of cryptography is attributed to Caesar. In order to secure a message to the besieged Cicero against being read by his enemies, Caesar replaced the Roman letters by Greek ones. Ever since cryptography and cryptanalysis have played a crucial role in wars. The military and secret services have focussed on developing both, ciphers and methods to break them.
Caesar also used substitution ciphers without introducing new symbols by simply replacing Roman letters by others. The permutation scheme was the key for these ciphers and had be kept secret.

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 (re-)invented 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 keys as long as the message 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 research on cryptography.

Enigma: a first machine cipher

In 1918 the German Arthur Scherbius invented the cipher machine Enigma. First the Enigma did not sell well, mostly due to the high costs. But in 1923 Churchhill published how the German encryption during WWI was regularly broken revealing vital information without the Germans taking note that they had been compromised. (As a consequence from information from deciphered telegrams the Americans had finally entered the war.) Realising how bad their communication had been secured in WWI the Germans turned to the Enigma thereby obtaining one of the most advanced crypto systems. But even the Enigma was proven not be unbreakable. In 1932 the Polish mathematician Marian Rejewski managed to decipher message encrypted with the Enigma. From a spy he obtain information about how the Enigma functioned. Further he knew that the message key transmitted at the beginning of each message was always sent twice in order to prevent transmission errors. This revealed finally enough information for Rejewski to beak into the Enigma. In 1939 — just before the German attack on Poland — the German increased the security of the enigma. Rejewski could not access their information any longer. In August, just one month before the outbreak of WWII, the Polish smuggled their knowledge about the Enigma to the French and the British who still assumed the Enigma was unbreakable.
In the following years the British built up a group of cryptanalysists, including Alan Turing, who achieved to regularly decipher the German communication. Again withouth them having a clue that their communication was not secure. The acquired information proved to be of high strategic importance and a crucial advantage to the allied forces.

Navajo Code: an unbroken 'linguistic' code

During WWII machine ciphers like the Enigma were commonly used. 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 receiving the radio signal. 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.

Lucifer: The Beginning of Block Ciphers

In 1934 Horst Feistel had come from Germany to the US. During the war he was put under house arrest. After the war when entering research on cryptography NSA did not approve of his work as it might deprive the organization from access to information. Indeed in the 70s while working for IBM he developed the Lucifer algorithm — a block cipher held to be strongest product on the commercial market. Therefore Lucifer was the core of the Data Encryption Standard (DES) adopted in 1976. Again rumours say NSA interfered the adoption of the standard in order to weaken it. Until today block ciphers are the working horses of cryptography used to encrypt the bulk of data.

Diffie-Hellman: Key Exchange Protocol

So far we have always assumed that the parties wanting to communicate with one another securely already share a key. We have not wondered how they could agree on a key, that as to be secret on any account. Otherwise all subsequent encryption is compromised. Martin Hellman, Whitfield Diffie and Ralph Merkle worked on the issue of how to agree on a secret key using a public transmission line (called channel). In 1976 they publish a protocol based on so-called one-way functions.

RSA: asymmetric encryption

In 1977 Ron Rivest, Adi Shamir and Leonard Aldeman developed a protocol for public key encryption, implementing an idea sketched before by Diffie. Say Alice wants to secretly send a message to Bob. So she'd take a Bob's public key, that is known to everybody, and use it to encrypt her message. Then she sends the encrypted message to Bob. He'd then use his private key to decrypt the message. Thus Alice and Bob do not have to share a common key before. Alice merely has to get Bob's public key from a trusted database.
The usual crypto setup today is an asymmetric cipher for the key exchange followed by a block cipher to encrypt larger amounts of data. Thanks to Phil Zimmermann encryption algorithms are now publicly available. Before he could release his crypto bundle *Pretty Good Privacy* he faced issues with the US American legislation that forbids the export of cryptographic products. The GNU Privacy Guard offers an open source implementation with interfaces for a range of current email and chat clients as well as tools to encrypt data on disk.

Bennet and Brassard: Quantum Key Distribution

The algorithms mentioned so far can be run on a computer or a smartphone. The security stems from the variety of substitution schemes one would need to check, superceding currently available computational power. Modern ciphers rely on mathematical functions that are hard to compute.
Charles Bennet and Gilles Brassard went a step beyond classical computers and developed in 1984 a key distribution protocol for a quantum computer. The protocol allows Alice and Bob to agree on a key secretely and even determine whether their wire was tapped or not. The protocol fundamentally relies on quantum mechanics. Measuring a quantum systems inevitably induces a change of the system. An eavesdropper therefore would leave traces behind.
Thus Alice and Bob could exchange a key using the *BB84* protocol and then encrypt their messages with a one-time pad to be entirely secure, independent of the computational power available to an eavesdropper.
Quantum Computers could not only increase the security of cryptography but also break common ciphers today. The so-called classical protocols mentioned above rely on particular mathematical functions with the property that they can hardly be inverted. For some of these functions there exists quantum protocols to compute the inverse efficiently. So far efficient quantum computers are not in sight and no encryption, wrong implementations, side channel attacks or leaked keys remain far greater threads.

http://www-i6.informatik.rwth-aachen.de {dreuw,deselaers}@cs.rwth-aachen.de