Lecture 1

from which you will learn about the oldest methods of concealing information. You will find out what the basic methods of cryptology are, as well as attempt at breaking your first cipher.

INTRODUCTION

Poland, the late twenties of the 20th century. The Cipher Agency of the Polish military intelligence are working out a new mysterious cipher that the Germans have begun to use. On the surface, the puzzle is unsolvable - long strings of characters that do not exhibit any characteristics similar to the available methods for covering up messages. The officers working for the Agency decide to involve mathematicians to help them break the code. They suspect that, in that particular case, this discipline of science may play an important part. It becomes obvious that for a task of such a gravity new personnel need to be recruited from mathematics students. The students should first be trained and educated on a special course presenting the basics of cryptology.

This is how the cipher adventure of three maths students, Marian Rejewski, Jerzy Różycki and Henryk Zygalski, begins. After completing the course they then become the Polish CODE BREAKERS. The work is difficult and demanding but rewarding at the same time. Particularly in 1932 when the German machine cipher ENIGMA (until then considered unbreakable) gets broken for the first time, only two months after having received the orders concerning deciphering the code...

Marian Rejewski

Jerzy Różycki

Henryk Zygalski

In 1939, in the face of the expected outbreak of war, the Poles decide to share their secret with the Allies. The allied services are surprised as well as delighted to accept this unexpected present. The famous British intelligence cetre, Bletchley Park, takes over the crusade against ENIGMA.

Maksymilian Ciężki

Today, several decades since those events we can still see their far-reaching influence. The possibility of regularly breaking of the German cipher by the British aided the victorious ending to World War II and to the suffering of millions of people. This undoubtedly would not have been possible without the pre-war achievements of Polish cryptologists.

The present game has been created to bring tomind these events of the past. And the game has taken the form of a cryptology course, of course. Imagine you are now in 1929, together with Rejewski, Różycki and Zygalski you take your seats at the student desks. In front of you, there are the tutors: Maksymilian Ciężki, Gwido Langer, Antoni Palluth, supported by the authority of Zdzisław Krygowski. You begin your cipher adventure...

THE EARLY METHODS OF CONCEALING INFORMATION

We will start our course with a short introduction to the history of cryptology. Although it was only in the 20th century that cryptology was given its name, it nevertheless occupied an important place in human culture already in the ancient times.

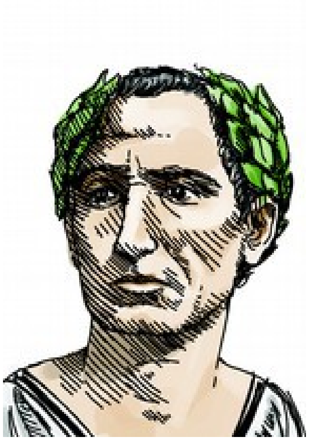
The oldest sources of texts in which some information was hidden from an unwelcome eye come from ancient Egypt, from the period of about 1900 BC. In one of the books of Old Testament, the Book of Jeremiah, some concepts were encrypted with a code called Atbash. The code utilised the letters of the Hebrew alphabet in such a way that the fist letter of the alphabet was replaced by the last, the second by the penultimate and so on. The name of the code derives directly from the method used in the encryption (A changes to T, Ba to Sh and so on). This simple cipher was easily broken by Bible experts who guessed that a strange word 'Sheshakh' appearing in some Biblical sources refered to 'Babilon'.

Ancient Spartans, on the other hand, would hide their messages by winding spirally narrow strips of leather around a wooden stick called 'skytale', and then writing the message down along the stick. After unwinding of the leather strip, the characters appeared to be random. The addressee read the message by winding it around the stick of the same diameter. You can say that the skytale's diameter was the key to the code.

Skytale - www.wikipedia.com

A Greek named Histiayos, serving at the court of the great king of Persia, decided once to send to his cousin in Miletus a message about a convenient moment to stir the uprising against the Persian rulers. He summoned one of his slaves, shaved his head and tattooed the text of warning on it. When the hair on the messenger's head grew back, he sent him to his country.

Later on, Julius Caesar, running a campaign in Gaul, used to coordinate operations of several military units by sending out couriers with the orders to their commanders. Being aware of the risk of the courier falling into the hands of the enemy, he encrypted the letters in the messages by replacing each character of the Latin alphabet with a character situated three positions further.



Gajusz Juliusz Cezar

His own name, IULIUS CAESAR, thus became LXNLXV FDHVDU. By doing so he used encryption, the essence of which is to replace each letter of the plaintext with a letter of the ciphertext. By sending encrypted messages, Caesar could feel confident as literacy was rare among the Celtic tribes fighting against him. If, however, a Roman deserter had found his way to the opponents, additionally aware of the Caesar's tricks, he would not have had many problems with breaking his cipher.

VARIOUS METHODS OF CONCEALING INFORMATION

It can easily be seen that the methods of concealing information described above differ slightly from one another. What is interesting is that (...)

Have you enjoyed it?

If yes, register your team and read the follow-up of the lecture in your team panel. We are happy to invite you to join in the adventure with cryptology and history.

- If you are not sure for which category to register your team, you have three options:
- if you don't know anything about ciphers, or know very little - choose the basic category
- if you can tell the difference between the substitution and transposition ciphers, and you know the methods of breaking them - choose the advanced category
- you can, naturally, play in both categories. However, if at least one member of your team took part in any of the previous editions of the game, you will not be allowed to take the first, second or third place in the basic category in the final.

Feel free to register at any time!