Contribution ID: **74** Type: **Presentation**

Symmetric Cryptography: from Ancient World to Modern Ciphers.

Monday, 14 April 2014 14:20 (1 hour)

Contrary to what many people think, the desire to communicate in a secure manner has been around for a very long time. Already in ancient times Greeks practiced safeguarding of information. Over centuries those practices evolved from a curiosity to a whole scientific discipline.

The presentation shows numerous and increasingly complicated techniques used to protect communication. It starts with the illustration of the process used by Julius Cesar and moves forward in time to the Second World War introducing the audience to techniques widely utilized in many modern algorithms. The presentation illustrates the Data Encryption Standard (DES) - the most widely used encryption algorithm in the 20th century and its two successors 3DES and Rijndael (AES). The short discussion about proof of security concludes that the only one proven completely unbreakable cipher method, despite its simplicity, is not applicable in many situations.

Primary author: PATER, Lukasz Piotr (CERN)

Presenter: PATER, Lukasz Piotr (CERN)

Track Classification: Information Security