LESSON 1: HISTORY OF CRYPTOGRAPHY AND ITS EARLY STAGES IN EUROPE

AUTHOR: Arturo Ribagorda Garnacho
Carlos III University of Madrid, Spain

BOB
Hello and welcome to Intypedia. Today we are presenting the first subject of the encyclopedia: a walkthrough of the History of Cryptography, from its first steps till World War I. Come with us!

1. THE BEGINNING

ALICE
Nowadays, cryptography can be found everywhere in our world. Everyday actions like receiving or making a call from a mobile telephone, paying with a credit or debit card, withdrawing money from an ATM or logging on to a computer with a password, for example, use techniques based on this science.

BOB
When did mankind invent these techniques and when did societies begin to use them? How were they first used? I recall that the answer is found in the origin of writing.

ALICE
That’s right, Bob. Writing is, according to many, the most important invention of Humankind. Writing renders proof of events, opinions, ideas and so on, across time and space, while helping knowledge to progress and civilizations to advance. However, when writing developed
and had become generalized, the danger of others reading the texts was acknowledged. And thus, the first systems to protect writing were invented.

**BOB**

Right. Usually, the information that is being protected is referred to as “plaintext” and when the information has been encrypted, we talk about “ciphertext”. Only the recipient, who possesses the information called “cryptographic key” or “key” can reveal the encrypted information.

**ALICE**

We would have to go back to the 5th century BC, to Sparta, to see the first methodical ciphered system. It consisted of a cylinder with a strip of leather wound around it, like a bandage and a message written on it. The unwound strip would look like a long string of letters without any meaning. But when the recipient wound the strip around a cylinder of the same size as the first one, the message would be decrypted. The diameter of the cylinder, therefore, was the key.

### 2. **MONOALPHABETIC METHODS**

**ALICE**

The scytale method was used by the government officials of Sparta to communicate with their military officers. It was not until a couple of centuries later that another popular encryption method arises: the Caesar cipher, named after Julius Caesar. It consisted in replacing each letter in the text by another letter, 3 positions down the alphabet. That is, replacing the A with a D, the B would become an E, and so on, until the end of the alphabet where “X”, “Y” and “Z” would be replaced by “A”, “B” and “C” respectively.

Both methods, the scytale and the Caesar, are examples of the two main cipher methods: transposition and substitution. The transposition technique consists of shifting the position of the letters in the text following a certain pattern. This way, the ciphertext has the same letters as the plaintext, but with permuted positions. These encryption methods are called transposition or permutation ciphers and the previously described scytale would be an example of this.

The substitution methods, on the other hand, maintain the position of the letters in the text, but their appearance changes. That is, each letter is replaced by another letter, a number or a symbol. If each letter is replaced by only one cipher symbol, the method is considered monoalphabetic, like the Caesar method.

**BOB**

Oh, I see. But nowadays, this method isn’t very appropriate, is it?

**ALICE**
No, this method isn’t very secure. The answer can be found within cryptanalysis.

BOB

Excuse me, Alice, I don’t quite understand. What is cryptanalysis?

ALICE

Allow me to explain. Over the years, many people have tried to reveal the protected secrets without knowing the key with which they are encrypted. This field of study is called cryptanalysis and the people who perform them are cryptanalysts.

Cryptology is the name of the science enclosing both cryptography and cryptanalysis.

From the decline of the Roman Empire up to the Renaissance, cryptology only advanced significantly within the Islamic caliphates, especially with the Abbasids. In their capital, Baghdad, modern cryptanalysis was born in the 9th century when they discovered that in each language, letters appeared with a different frequency. This way, they only had to count the number of times a symbol, letter or number appeared in a text, to know which letter it represented, regardless of its appearance.

BOB

Now I understand why they say that monoalphabetic cipher isn’t secure.

3. POLYALPHABETIC METHODS

ALICE

Obviously, from that moment on, monoalphabetic ciphers were broken and cryptanalysts had won the battle over cryptographs.

Naturally, cryptographs couldn’t disregard substitution methods making all cryptography rely only on transposition, so they developed the polyalphabetic ciphers.

BOB

Does this mean that a more secure cryptographic method could be made using many different alphabets to hide the frequency in which the letters appear?

ALICE

That’s it! And it really isn’t all that difficult. In polyalphabetic methods, each time a plain letter appears, it is replaced by an encrypted character -be it a letter, a number or a symbol- from a limited range of characters. This way, a plain letter like “a”, is sometimes replaced by “x”, but other times by “y” or by the number 10. And always following a strict pattern so there aren’t any errors when deciphering. This way, the number of times a symbol appears in the text can’t give any useful information to the cryptanalyst.
BOB

So, which were the most popular polyalphabetic systems?

ALICE

The methods that use this system were conceived by one of the most important figures of the Renaissance: Leone Battista Alberti, inventor of the first cipher device: the Alberti cipher disk, also called formula. It was made up of two concentric disks. The inner disk had a lowercase mixed alphabet for ciphertext and was fixed, while the outer disk had one uppercase alphabet for plaintext and could move around its centre point. This way, each letter of the plaintext alphabet corresponds to another letter of the ciphertext alphabet, while being able to change this correspondence by sliding the outer ring. Therefore, it was a polyalphabetic method.

Another popular system was the one created by Blaise de Vigenère based on a table in which you could read the intersection letter of the plaintext with a key indicating which alphabet was being used.

4. EXTENDED USE OF CRYPTOGRAPHY

BOB

Alice, is it true, then, that the consolidation of secret writing was an essential instrument of power in the creation of modern countries, communication between armies and the presence of permanent embassies?

ALICE

Certainly. Cipher secretaries were established and they were responsible for ciphering the correspondence between kings, ministers and ambassadors, as well as cryptanalysing the correspondence intervened to other countries.

In Spain, for example, the first known Cipher Secretary was Pérez de Almazán, appointed by the Catholic Monarchs. But Philip II of Spain was the one to renew and greatly boost ciphering techniques, by putting the Cipher Secretary Luis Valle de la Cerda in charge. He established a General Cipher for communication between his secretaries, ambassadors, army officers and himself; and a Personal Cipher for communication between some of the afore-mentioned dignitaries and himself. Furthermore, for extra security, he would change frequently these ciphers.

BOB

Did they use these methods of protection in other countries as well?

ALICE
Of course they did. They followed these methods in the other European kingdoms. For example, Walsingham with Elizabeth I of England and Viêtè with Henry III and Henry IV of France both made cryptology an essential matter in European royal courts and embassies.

BOB

I know there was a famous ciphering machine. When did the first ones appear?

ALICE

Although cryptology continued developing throughout Modern and Contemporary Age, it isn’t until the 20th century that we find substantial advances in ciphering techniques. So it is considered, in fact, the machine century. Being the Enigma machine the one that captured most of the attention, more than any of the other machines from past or present.

Enigma was a cipher machine patented by Arthur Scherbius in 1918. It was used by the German Army in 1923, which had several thousands of them during World War II, where it played a very important role.

BOB

That sounds familiar. The Germans tried out how the machine worked in battle during the Spanish Civil War, providing the Nationalists with some devices.

ALICE

That’s right. The history of this machine and its use is fascinating. We’ll study it in detail later on. In fact, it is after World War II, when the most significant theoretical advances in the history of cryptology take place. For example, in 1948, Claude Shannon establishes the theoretical basics of cryptology, but that’s another subject.

BOB

Well, Alice. I think this is enough for today.

ALICE

Yes, you’re right Bob. We better continue this some other time. On the intypedia website you can find a document with additional information on this enthralling subject.

See you at our next video... Good-bye!

BOB

See you later!
Script adapted from original. Dr. Arturo Ribagorda Garnacho, Carlos III University of Madrid, Spain.

Madrid, Spain, September 2010

http://www.intypedia.com

http://twitter.com/intypedia