A history of cryptology

François Morain

LIX, École polytechnique

April 21, 1997

[summary by Pierrick Gaudry]

Abstract

Cryptology is very old but has got a renewal of interest. Until the end of the 80's, it was reserved to military people or diplomats, but it is now accessible to the general public. Cryptology contains the art of hiding information and the techniques to break a secret. This talk is a brief survey of the history of this art.

Introduction

First of all, one needs to recall the precise meaning of some terms. *Cryptography* is the art of communicating confidentially through an insecure channel. *Cryptanalysis* is the art of deciphering those communications when one is not the legitimate receiver. And *Cryptology* is the union of these two domains.

Two basic principles are known for cryptography: *substitution*, which consists in permuting the letters of the alphabet, and *transposition*, which permutes the letters of the text.

1. From prehistory to the modern era

During antiquity, writing was safe because only a few people could read. We can however note some simple substitutions in India and the use of special or rare symbols by scribes in Mesopotamia. In Greece and Rome, the use of cryptography increased for military purposes. In Sparta, in 475 B.C, was invented the *scytale*, which is a conic stick around which one encircles a strip of paper, and then writes the message vertically. Julius Caesar used a simple substitution system.

After this period and till the fifteenth century, the only valuable cryptographic activity was in the Arabic civilization. Qalqahandi wrote an encyclopedia with a section dedicated to cryptology, with the first appearance of cryptanalysis.

Cryptology came back in occident with the Renaissance (first in Italy). A lot of techniques appear at this time, notably polyalphabetical substitutions. The principle is to have a key (for example CADEAU), and to "add" the repeated key to the message we want to encrypt.

	c	r	y	p	t	o	g	r	a	p	h	e
+	c	a	d	e	a	u	c	a	d	e	a	u
=	E	R	A	T	T	I	I	R	D	T	H	W

In France, during the Renaissance, the monarchy used a system of nomenclator; there was a quite good security thanks to the frequent change of code and to the existence of spare codes.

2. From telegraph to radio

In the middle of the nineteenth century, the telegraph generated a new craze for cryptography and cryptanalysis. Kasiski in 1863 gave a method to attack polyalphabetical substitutions. Mathematics are introduced in cryptology, and Kerckhoffs gave a few laws that should be verified by a "good" cryptographic system. In particular he insists on the fact that the system has to be public, the only secret being a key.

During World War I, England decrypted a lot of German messages. A decisive one was the Zimmermann telegram which proved the double game played by Germany with Mexico and the USA. The publication of this telegram in the American press incited the USA to go to war.

In France, a remarkable cryptanalysis was achieved by Painvin. He broke the German system ADFGX in April 1918. Before they launched their last offensive, the Germans modified the system, and in a few days Painvin broke it once more. The French then discovered where Ludendorff wanted to attack, and could stop the offensive.

3. The automation of cryptology

The most important invention of the beginning of the twentieth century is the *one-time-pad* by Vernam. The principle is to "add" an infinite random sequence to the message. The problem is then to build a pseudo-random generator. That was done with the invention of the rotor which gives a polyalphabetical substitution with a huge period. All the machines used during World War II were based on this principle.

Japan first used the RED machine which was broken by classical spying, and then the PURPLE system which was cryptanalysed by Friedman in 1940. Germany used the famous ENIGMA machine, regularly improved by addition of cabling and a choice of three rotors between five. There was two great centers of cryptanalysis: the first in USA with Friedman, and the second in England with Turing and Welchman. In the latter, a lot of German messages where decrypted. The principle of the cryptanalysis was to take advantage of some weaknesses of the usage that Germans did of ENIGMA: they had a very strict format for the beginning of the messages, and some operators did not choose random keys.

4. The last fifty years

The key facts of the last years are the increasing development of computers, and the great interest of civilians for cryptography.

In the beginning of the 70's, the National Bureau of Standards decided to publish a cryptosystem which could be used by governmental agencies or banks; this was done in 1977, with the Data Encryption Standard (DES). Concurrently to this, Diffie invented in 1975 the concept of public-key cryptosystem, which was applied by Rivest, Shamir and Adleman (RSA) in 1977.

There is now a great link between cryptology and some branches of modern mathematics and computer science: probability theory, information theory, algorithmic number theory, or the theory of error correcting codes are useful tools.

Nowadays, some new applications of cryptography appear: electronic trade, money, or notarial deeds.

References

[1] Kahn (David). – *The codebreakers; the story of secret writing.* – Macmillan, New York, 1967.

[2] Schneier (Bruce). – *Applied cryptography: protocols, algorithms, and source code in C.* – Wiley, New York, 1996, 2nd edition.