Criptografia — 2011/12

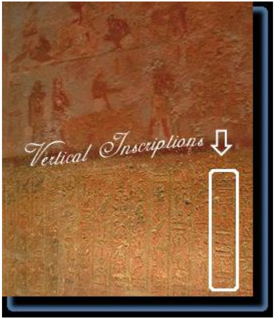
Introduction

Cryptology is made up of two Greek words: kryptos, meaning “hidden”, and ology, meaning “science”. It may be defined as the science concerned with communications in secure and usually secret form. It encompasses both cryptography (from the Greek *graphia* meaning “writing”) and cryptanalysis, or the art of extracting the meaning of a cryptogram.

Criptografia — 2011/12

Introduction

Cryptography has a history that is almost as long as the history of the written word. Some four millennia ago an Egyptian scribe recorded in stone **the first known hieroglyphic symbol substitution in the tomb of Khnumhotep II**, a nobleman of the time.



Criptografia — 2011/12

Introduction

machine
sense
machine
sense

Although the intention in this case was to exalt the virtues of the person, rather than to send a secret message, the scribe used for the first time one of the fundamental elements used by cryptographers throughout the ages, namely, substitution.

He used unusual hieroglyphic symbols, known perhaps only to the elite, in place of the more common ones.

Criptografia — 2011/12

Introduction

NATIONAL CRYPTOLOGIC MUSEUM
A B C D E F G H I J K L M N O P Q R S T U V W X Y Z
A Z Y X W V U T S R Q P O N M L K J I H G F E D C B

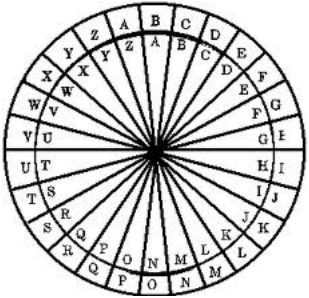
A CIPHER DISK
courtesy National Cryptologic Museum / NSA

In **substitution**, the sender replaces each letter of a word in a message by a new letter (or sequence of letters or symbols) before sending the message. The recipient, knowing the formula used for the substitution — the secret key — is able to reconstruct the message from the scrambled text that is received. It is assumed that only the recipient and the sender know the secret key.

Criptografia — 2011/12

Introduction

The Roman general Julius Caesar was the first attested user of substitution (shift) ciphers for military purposes. In the cipher form used by Caesar, the first letter of the alphabet "A" was replaced by the fourth letter "D", the second letter "B" by the fifth, "E", and so on. In other words, each original letter was replaced by the letter three steps further along in the alphabet.


A B C D E F G E I J K L M N O P Q R S T U V W X Y Z
Z A B C D E F G H I J K L M N O P Q R S T U V W X Y

More about shift

Criptografia — 2011/12

Introduction

The other main cryptographic technique used is transposition (or permutation), in which the letters of the message are simply rearranged according to some prescribed formula that would be the secret key in this case.

Criptografia — 2011/12

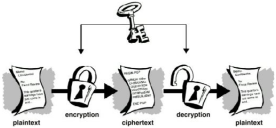
Introduction

The Greeks were the inventors of the first transposition cipher. The Spartans in the fifth century b.C. were the first recorded users of cryptography for correspondence. They used a secret device called a scytale consisting of a tapered baton around which was spirally wrapped a strip of either parchment or leather on which the message was written.

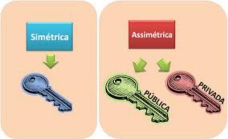
When unwrapped, the letters were scrambled, and only when the strip was wrapped around an identically sized rod could the message be read.

Criptografia — 2011/12

Introduction



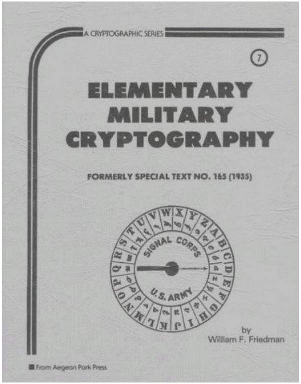
Today, even with the advent of high-speed computers, the principles of substitution and transposition form fundamental building blocks of ciphers used in symmetric cryptography.



To put it in a historical perspective, asymmetric or public key cryptography was not invented until the 1970s. Exactly when it was invented, or who should take the most of the credit, is an issue still in dispute. Both the NSA (United States National Security Agency) and the CESG (Britain's Communications Electronics Security Group) have claimed priority in the invention of public key cryptography.

Criptografia — 2011/12

Introduction



A CRYPTOGRAPHIC SERIES

7

ELEMENTARY MILITARY CRYPTOGRAPHY

FORMERLY SPECIAL TEXT NO. 165 (1935)

by
William F. Friedman

From Aegean Park Press

Cryptography has had several reincarnations in almost all cultures. Because of the necessity of keeping certain messages secret (i.e. totally unknown to potential enemies) governments, armies, ecclesiastics, and economic powers of all kinds have been associated throughout history with the development of cryptography. This trend continues today.

Criptografia — 2011/12

Introduction — Extra information

The invention and development of **radio communication around 1900** caused an even more striking change in the cryptographic landscape, especially in urgent military and political situations. A general could now instantaneously communicate with all of his troops, but unfortunately the enemy could listen in on all of his broadcasts.

The need of secure and efficient ciphers became paramount and led to the invention of machine ciphers, such as Germany's **Enigma machine**.

Criptografia — 2011/12

Introduction — Extra information

This was a device containing a number of rotors, each of which had many wires running through its center. Before a letter was encrypted, the rotors would spin in a predetermined way, thereby altering the paths of the wires and the resultant output. This created an immensely complicated polyalphabetic cipher in which the number of cipher alphabets was enormous. Further, the rotors could be removed and replaced in a vast number of different starting configurations, so breaking the system involved knowing both the circuits through the rotors and figuring out that day's initial rotor configuration.

Criptografia — 2011/12

Introduction — Extra information

Despite these difficulties, during World War II the British managed to decipher a large number of messages encrypted on Enigma machines. They were aided in this endeavor by Polish cryptographers who, just before hostilities commenced, shared with Britain and France the methods that they had developed for attacking Enigma. But determining daily rotor configurations and analyzing rotor replacements was still an immensely difficult task, especially after Germany introduced an improved Enigma machine having an extra rotor. The existence of Britain's ULTRA project to decrypt Enigma remained secret until 1974, but there are now several popular accounts. Militaty intelligence derived from ULTRA was of vital importance in the Allied war effort.

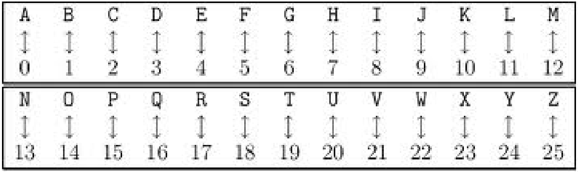
Criptografia — 2011/12

Introduction — Extra information

Another WWII cryptanalytic success was obtained by United States cryptographers against Japanese cipher machine that they code-named Purple. This machine uses switches, rather than rotors, but again the effect was to create an incredibly complicated polyalphabetic cipher. A team of cryptographers, led by William Friedman, managed to reconstruct the design of the Purple machine purely by analyzing intercepted encrypted messages. They then built they own machine and proceeded to decrypt many important diplomatic messages.

Modular arithmetic and shift ciphers

The Caesar (or shift) cipher works by shifting each letter in the alphabet a fixed number of letters. We can describe a shift cipher mathematically by assigning a number to each letter as below.



A	B	C	D	E	F	G	H	I	J	K	L	M
↕	↕	↕	↕	↕	↕	↕	↕	↕	↕	↕	↕	↕
0	1	2	3	4	5	6	7	8	9	10	11	12

N	O	P	Q	R	S	T	U	V	W	X	Y	Z
↕	↕	↕	↕	↕	↕	↕	↕	↕	↕	↕	↕	↕
13	14	15	16	17	18	19	20	21	22	23	24	25

Table 2: Encoding English capital letters using integers from $\mathbb{Z}_{26}$.

Then a shift cipher with shift k takes a plaintext letter corresponding to the number p and assigns it to the ciphertext letter corresponding to the number $p + k \bmod 26$. Notice how the use of modular arithmetic, in this case modulo 26, simplifies the description of the shift cipher.

Modular arithmetic and shift ciphers

The shift amount serves as both the encryption key and the decryption key. Let

$$p = \text{Plaintext Letter} \quad c = \text{Ciphertext Letter} \quad k = \text{Secret Key}$$

then

$$\underbrace{c \equiv p + k \pmod{26}}_{\text{Encryption}} \quad \textit{and} \quad \underbrace{p \equiv c - k \pmod{26}}_{\text{Decryption}}.$$

Modular arithmetic and shift ciphers

In general we write

$$\mathbb{Z}/m\mathbb{Z} = \{0, 1, 2, \cdots, m-1\}$$

and call $\mathbb{Z}/m\mathbb{Z}$ the *ring of integers modulo m*. Note that whenever we perform anaddition or multiplication in $\mathbb{Z}/m\mathbb{Z}$, we always divide the result by m and take the remainder in order to obtain an element in $\mathbb{Z}/m\mathbb{Z}$.

Go back