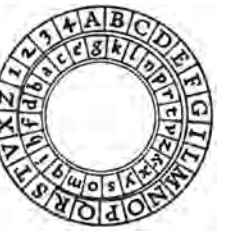
CRITTOGRAFIA

Book Series

I

CRITTOGRAFIA

Book Series



It is impossible to agree beforehand about things
of which one cannot be aware before they happen

— Polibyus (150 BC)

La collana raccoglie le opere scientifiche che riguardano e approfondiscono l'affascinante, enigmatico e complesso campo crittografico.
La Crittografia è una materia molto ampia, che comprende tanto la progettazione di algoritmi, quanto lo sviluppo di tecniche crittoanalitiche. L'intento è quello di raccogliere opere che presentino e analizzino sia gli aspetti più teorici, tra cui le basi matematiche, sia quelli più pratici, tra cui gli aspetti protocollari. In questa ottica, inoltre, è interessante e necessario fornire visibilità alle innovazioni più promettenti, come la crittografia *postquantum*, la tecnologia blockchain e la cifratura nel cloud.
La collana ospita volumi che trattano ogni ambito della Crittografia, interessando e raggiungendo trasversalmente differenti contesti scientifici e divulgativi: note di lezioni universitarie per favorire la comprensione e la diffusione di tale disciplina; atti di convegni specializzati, per incrementare la consapevolezza della comunità scientifica nazionale e internazionale; monografie, che comprendono anche tesi di laurea e di dottorato, per divulgare ricerche e sperimentazioni.

The book series collects cryptographic works with ample scope.
Cryptography is a wide discipline, encompassing algorithm design and the investigation of cryptonalytic techniques. The book series aims at presenting both theoretical aspects, in particular the mathematical bases, and practical aspects, e.g. protocols. Along this line, we want to highlight the most promising innovations, such as *postquantum* cryptography, blockchain technology and cloud encryption.
The book series hosts lecture notes, to help spreading the knowledge of this fascinating subjecto, as well as workshop proceedings, to help the Italian scientific community collaborate, as well as specialized monographs, including Master's theses and PHD theses.

Go to the multimedia content

Michele Elia

An introduction to Classic Cryptography

With an exposition of the mathematics of private and public key ciphers

Aracne editrice

www.aracneeditrice.it
info@aracneeditrice.it

www.gioacchinoonoratieditore.it
info@gioacchinoonoratieditore.it

via Vittorio Veneto, 20
00020 Canterano (RM)
(06) 45551463

ISBN 978-88-255-1073-7

I edition: February 2018

To my parents Luigi and Cristina

Contents

Preface

Cryptography concerns the principles, protocols, and methods for protecting information against deliberate or accidental alterations.

The protection is achieved by means of transformations, called enciphering, whose aim is to conceal the information, and by inverse transformations, called deciphering, to re-obtain the useful information.

In the sixteen century, Sir Francis Bacon, Viscount St. Alban, defined cryptography as « this art of ciphering, hath for relative an art of deciphering, by supposition unprofitable, but as things are, of great use ».

As Bacon's fine irony points out, the entire set of procedures is nonsense but, as things stand in this world, it is very useful.

For millennia, cryptography was mainly used in diplomacy and military affairs, but cryptographic techniques have recently also been introduced into the bureaucratic, managerial, and economic sides of civil life.

Cryptographic techniques can be applied in data transmission, computation and storage systems. The design of any information protection system may be seen as the engineering way to solve the philosophically insoluble conflict between security and the resources needed to achieve it. Therefore, any cryptographic system is a compromise between functional requirements, scientific knowledge, logistics, technological possibilities and economic costs. The evaluation of an information protection system must relate to the combination of these resources, taking a pragmatic view that excludes both the ingenuity and the presumption typical of factual knowledge and improvisation.

In this scenario, cryptography is only one component, although an indispensable one, of any information protection system. A knowledge of it, even if limited to basic techniques, is an absolute requisite for professionally and successfully managing any system that needs security.

Chapter I

Cryptography from Art to Science

> Some people are so busy learning the tricks of the trade that they never learn the trade.
>
> V. Law

1.1. Introduction

It is a fact of recent history that, in the last two decades of the twentieth century, a scientific, technological, and cultural revolution swept through the communication systems of high–technology countries. Satellite telecommunications, cellular telephony, digital television, the Internet and personal computers show that the convergence of telecommunications and computer technology has overturned the entire world order of Information Technology. This atypical revolution has had unforeseeable repercussions also on the traditional methods of knowledge production and transmission. However, the effects in these fields will only be fully observed in the coming decades, and will probably turn out to be much more far–reaching than the highly visible modifications already produced on the economy and on the world of finance. Commerce is increasingly based on the Internet, with sometimes disturbing effects on the consolidated systems of trading and handling goods. In the banking world, thanks to the Internet, the traditional branch has expanded to enter into the homes of customers, modifying both the way users relate to the banking system and the inner organization of the banks themselves.

Whereas in one respect these perhaps irreversible phenomena have improved the quality of life, they have conversely made the system as a whole more fragile and more sensitive to any recession. Adversaries of all types, compatriots or foreigners, governmental or private bodies, can order and scan plain text they have intercepted and selected, based on details of your address, or on convenient key words present in the message. This improper monitoring activity has been going on for decades, obviously even before the computer made the job so much easier. The novelty comes from the proportions and the number of customers who entrust their personal transactions and secrets to fiber optics, to copper cables or to the ether. The

more technologically advanced a country is, the more will it be susceptible to the interception of electronic traffic. Therefore, protection of information is becoming an unavoidable necessity to assure a society's operative life. The technologies for protecting information have been developed in the discipline known as cryptology. For millennia, cryptology had as main objective the confidentiality of information, but in recent times, technological evolution, together with the creation of a world–wide society with integrated services and global systems of communication, has given much more extensive, wider–ranging and more complex objectives to cryptology. Specifically, the number of services that need some form of information protection is continually growing. No list could ever be complete, but would be headed by the telephone, e–mail, e–commerce, tele–working, remote monitoring, tele–medicine, and could continue almost indefinitely.

1.2. Information Protection

It is unlikely that authoritative statements can be definitively formulated to systems protecting information. Rather, security comes from the concurrence of needs, situations, and purposes that contribute to defining the scenario in which information plays the role of principal actor.

A system for the protection of information depends on:

a) accuracy of the principles;
b) robustness of the mathematical procedure used to transform the information;
c) physical security of the technological equipment that processes the information and the environments where such devices reside;
d) discipline of employees, where "discipline" means the mental attitude and the behavioral attention to details that could make even the most technically–secure system vulnerable.

As just noted, security systems bring together many components of a human and technical nature. Among these, an important role is played by cryptology and the related mathematical techniques.

1.2.1. *The goals of Information Protection*

The objectives for protecting information against deliberate manipulation should in general respond to four basic questions:

a) what information to protect?:

- — the message as such, keeping it confidential;
- — the integrity of the message, that is guaranteeing it is received correctly by the recipient, whether privately or not;
- — the authenticity of the message, that is reassuring the recipient about the identity of the message's author;
- — the very existence of the message;

b) why protect the information?:

- — to ensure integrity: the Information should be preserved in its original form. It must not be fraudulently altered and passed off as authentic;
- — to ensure availability: the Information should be usable when required, without delay or uncertainty;
- — to ensure confidentiality: the information must be kept as private as the owner wants. Only authorized persons or entities can have access;
- — to ensure privacy: It should not be possible to trace the source of the information;

c) against whom to protect the information?:

- — against opponents determined to steal it;
- — against accidental or deliberate destruction;
- — against improper or unauthorized use;

d) how to protect the information?:

- — physically, i.e. endowing physical locations or equipment with defenses difficult to violate;
- — logically, that is by transforming the information so that it cannot be stolen, understood, or manipulated by any opponent;
- — virtually, namely by preventing persons from locating the information in real terms.

Although these statements may sound authoritative, it is not in any way possible to give definite and final answers to the above four questions, if such responses even exist. Rather, these questions and their partial answers guide the presentation of cryptography and related mathematical techniques, to give security managers the most valuable tools that are available at the current state of knowledge. With reference to how to protect the information, the techniques developed to hide the very existence of the message have had a somehow more exoteric development than cryptographic techniques proper, and fell into the discipline known as steganography (a word

of Greek origin that means "covered writing"). The first recorded use of steganography is in the title of a book by Johannes Trithemius (1462–1516). Steganography has recently experienced a great revival, mainly thanks to the Internet, and a short overview will be given in the last chapter of these Notes.

1.2.2. *Aims*

The situation that pits the defender against the attacker has dual aspects, that characterize the two main branches into which Cryptology is partitioned: cryptography / steganography and cryptanalysis.

Cryptography / steganography pursue five main goals:

a) to protect against intruders, ensuring that access to the information is reserved to authorized persons, entities, or devices;
b) to protect from deliberate destruction or alteration, ensuring the data's integrity, both logical (meaning of the texts) and physical (supporting paper, magnetic tapes, CD–ROMs, etc.);
c) to prevent shadowing (authenticity), namely to ensure recognition of the source of information;
d) to prevent repudiation (signature), to ensure the impossibility of denying the origin of a message;
e) to prevent tracking, ensuring anonymity of the source and route of messages, objects or people.

The purposes of cryptanalysis are operations that may be the converse of above aims, namely:

a) to determine the contents of a message;
b) to destroy a message, i.e. to deliberately prevent communication between two parties;
c) to falsify a message, that is to send it as if it were from another author, e.g. launching a communication with a party and being accepted as a legitimate counterpart;
d) to deny being the author of one's own message;
e) to trace the origin and path of messages, objects, or people.

1.2.3. *Summary*

The five situations considered above are at the core of modern cryptology, and can all be incorporated into a mathematical description in the framework of Shannon information theory. However, for practical purposes, it

has been preferred to develop a discipline that is apparently independent, referring to information theory only for the basic principles. This exposition will be the subject of the following chapters.

1.3. Historical glimpses

The long history of cryptology began in ancient Egypt at the Court of the Pharaohs where, between sphinxes, pyramids, and plots, for millennia the power game was played. But it was the warrior soul of Greece, with its oligarchic system, kingdoms, and ambitions of military and cultural domination, that first systematically applied a cryptographic method of which we have any certain knowledge. In the silent palaces of Sparta, King Agide encrypted messages directed to his distant generals in charge of controlling the eastern Mediterranean, by rolling up a string of papyri, helicoidally around a skytale (command baton) and writing his message along the length of the roll. The straightened string of papyri with the encrypted message looked like a chaotic set of symbols. To read his message, the general rolled the string around a baton of the same diameter. Today, these procedures for exchanging secret messages may move us to smile. Nevertheless, they solved the problem of private communication in an acceptable way, compatibly with the available technology.

1.3.1. *Cryptography from diplomacy to commerce*

From the Spartan hegemony on the Aegean sea, through the grandeur of the Roman Empire, the effervescent political and cultural milieu of the Italian Renaissance, down to the modern supra–national governments, cryptography has been variously, but almost exclusively, used in affairs of power. The impulse to its development was almost always given by the exigencies of war. The first scheme for sending concealed information over a public channel is cleverly described by Polybius (200–116 BC) in his *Histories*. Fast communications at long distances were achieved by means of fires located at the top of a chain of mutually visible hills. The letters were distinguished by the number of fires. The method that Polybius described, which he himself had perfected, consisted of translating the message into Greek and then encoding each letter in pairs of Roman numbers from one to five. Polybius does not mention the possibility of changing the correspondence to make it known only to the sender and legitimate recipient, but the idea seems so obvious that it was certainly adopted.

Surely, the complex needs of the Roman army to exchange secret messages at the time of Gaius Julius Caesar promoted the invention and dif-

fusion of a method for concealing information that was relatively secure, and at the same time operatively easy. The cryptographic method known as *Caesar's cipher* consisted in substituting each letter with a letter three positions onward (in the natural alphabetical order from A to Z of the letters). For example, the letter A is replaced by D, B by E, and so on, W being replaced by Z. The last three letters X, Y, and Z are substituted with A, B, and C, respectively. The rule was very easy and number 3 was the secret key for enciphering and deciphering the massage. The decryption operation to recover the original message from the encrypted text consisted of the inverse substitution. In technical jargon, this encryption rule is called mono–alphabetic, while its generalization is called polyalphabetic substitution.

This general and relatively strong encryption rule (i.e. polyalphabetic substitution) was perfected by Blaise de Vigenère (1523–1596) and reported in his *Traicté des chiffres, ou secrètes manierères d'écrire* published in 1586, where a square table that bears his name appeared for the first time with a certain emphasis. However, this table was invented by Giovan Battista Bellaso (1505–1580?), who worked as secretary and cryptographer for the Papal Court, and actually appeared for the first time in a booklet *La cifra del Sig. Giovan Battista Belaso, gentil'huomo bresciano, nuovamente da lui ridotta a grandissima breuitá & perfettione* that was published in 1553 with a mistake in the author surname. This book made public, for the first time, a table for encrypting, that was easy to build from a secret key (in truth, the idea of using tables for encrypting is likely due to Johannes Trithemius). Bellaso improved his encryption rule further in two papers (notebooks) published in 1555 and 1564, proposing schemes that are still difficult to break with cryptanalysis even with the help of today's computers.

Bellaso's table had already been reported in *De Furtivis Literarum Notis* by Giovanni Battista Della Porta (1535–1615), published in 1563, and this publication started a dispute over the priority of authorship. Actually, in his third booklet, dedicated to Cardinal Alessandro Farnese, published in 1564 in Brescia (Italy) by Giacomo Britannico il Giovane, with the title *Il vero modo di scrivere in Cifra con facilitá, prestezza, et securezza di Misser Giovan Battista Bellaso, gentil'huomo bresciano*. In this booklet, Bellaso inserted a gentle complaint that his table had been reproduced, fifteen years later, by Della Porta without mentioning its inventor.

The Vigenère polyalphabetic enciphering was long considered impossible to crack. In polyalphabetic encryption, the key consists of an ordered set of numbers (or letters). For example, if encrypting with a key consisting of the numbers 3 and 12, the letters of the text, starting from the first, are alternately transformed by mono–alphabetic substitution, as in the Caesar cipher, with keys 3 and 12.