1 INTRODUCTION

1.1 Preamble

In 1988, the *New Encyclopædia Britannica* defined *cryptology* as:

> The science concerned with communications in secure and usually secret form. It encompasses both cryptography and cryptanalysis. The former involves the study and application of the principles and techniques by which information is rendered unintelligible to all but the intended receiver, while the latter is the science and art of solving cryptosystems to recover such information.

Today this definition needs to be extended as modern cryptology focuses its attention on the design and evaluation of a wide range of methods and techniques for information protection. Information protection covers not only secrecy (a traditional protection against eavesdropping) but also authentication, integrity, verifiability, nonrepudiation and other more specific security goals. The part of cryptology that deals with the design of algorithms, protocols and systems which are used to protect information against specific threats is called *cryptography*.

To incorporate information protection into a system, protocol, or service, the designer needs to know:

- a detailed specification of the environment in which the system (protocol or service) is going to work, including a collection of security goals,
- a list of threats together with the description of places in the system where adverse tampering with the information flow can occur,
- the level of protection required or amount of power (in term of accessible computing resources) that is expected from an attacker (or adversary), and
- the projected life span of the system.

Cryptography provides our designer with tools to implement the information protection requested or in other words, to achieve the security goals expected. The collection of basic tools includes encryption algorithms, authentication codes, one-way functions, hashing functions, secret sharing schemes, signature schemes, pseudorandom bit generators, zero-knowledge proof systems, etc. From these elementary tools, it is possible to create more complex tools and services, such as threshold encryption algorithms, authentication protocols, key establishment protocols, and a variety of application-oriented protocols including, electronic payment systems, electronic election, and electronic commerce protocols. Each tool is characterized by its security specification which usually indicates the recommended configuration, its strength against specific threats, such as eavesdropping and illegal modification of information. The designer can use all the tools provided by cryptography to combine them into a single solution. Finally, the designer has to verify the quality of the solution including, a careful analysis of the overall security achieved.

The second part of cryptology is *cryptanalysis*. Cryptanalysis uses mathematical methods to prove that the design (an implementation of information protection) does not achieve a security goal or that it cannot withstand an attack from the list of threats given in the security specification of the design. This may be possible if the claimed security parameters are grossly overestimated or more often, if the interrelations among different threats are not well understood.

An attentive reader could argue that cryptography includes cryptanalysis as the designer always applies some sort of analysis of the information protection achieved. To clarify this point, note that the aim of cryptography is the design of new (hopefully) secure algorithms, protocols, systems, schemes, and services, while cryptanalysis concentrates on finding new *attacks*. Attacks (which are a part of cryptanalysis) are translated into the so-called *design criteria* or *design properties* (which are a part of cryptography). The design criteria obtained from an attack allow us to design a system that is immune against the attack.

Cryptography tries to prove that the obtained designs are secure, using all available knowledge about possible attacks. Cryptanalysis carefully examines possible and realistic threats to find new attacks and to prove that the designs are not secure (are breakable). In general, it is impossible to prove that information protection designs are unbreakable, while the opposite is possible – it is enough to show an attack.