Chapter XI
Introduction to Cryptography

Rajeeva Laxman Karandikar
Indian Statistical Institute, India

ABSTRACT

The chapter introduces the reader to various key ideas in cryptography without going into technicalities. It brings out the need for use of cryptography in electronic communications, and describes the symmetric key techniques as well as public key cryptosystems. Digital signatures are also discussed. Data integrity and data authentication are also discussed.

INTRODUCTION

With a many-fold increase in digital communication in the recent past, cryptography has become important not only for the armed forces, who have been using it for a long time, but for all the aspects of life where Internet and digital communications have entered. *Secure and authenticated communications* are needed not only by the defense forces but, for example, in banking, in communicating with customers over the phone, automated teller machines (ATM), or the Internet.

Cryptography has a very long history. Kahn (1967) describes early use of cryptography by the Egyptians some 4,000 years ago. Military historians generally agree that the outcomes of the two world wars critically depended on breaking the codes of secret messages. In World War II, the breaking of the Enigma code turned the tide of the war against Germany. The term cryptography comes from the Greek words kryptós, meaning "hidden," and gráphein, meaning "to write." The first recorded usage of the word "cryptography" appears in Sir Thomas Browne's Discourse of 1658 entitled "The Garden of Cyrus," where he describes "the strange Cryptography of Gaffarel in his Starrie Booke of Heaven."

This chapter provides an introduction to the basic elements of cryptography. In the next section, we discuss the need for cryptography. The following four sections describe the four pillars of cryptology: confidentiality, digital signature, data integrity, and authentication. The final section concludes the chapter.

WHY WE NEED CRYPTOLOGY

First, if a company that has offices in different locations (perhaps around the globe) would like to set up a link between its offices that guarantees secure communications, they could also need it. It would be very expensive to set up a separate secure communication link. It would be preferable if secure communication can be achieved even when using public (phone/Internet) links.

Second, e-commerce depends crucially on secure and authenticated transactions–after all the customers and the vendors only communicate electronically, so here too secure and secret communication is a must (customers may send their credit card numbers or bank account numbers). The vendor (for example, a bank or a merchant), while dealing with a customer, also needs to be convinced of the identity of the customer before it can carry out instructions received (say the purchase of goods to be shipped or transfer of funds). Thus, authenticated transactions are required. Moreover, if necessary, it should be able to prove to a third party (say a court of law) that the instructions were indeed given by said customer. This would require what has come to be called a *digital signature*. Several countries have enacted laws that recognize digital signatures. An excellent source for definitions, description of algorithms, and other issues on cryptography is the book by Menezes, van Oorschot, & Vanstone (1996). Different accounts can be found in Schneier (1996), and Davies and Price (1989).

Thus, the objectives of cryptography are:

1. **Confidentiality-secrecy-privacy:** To devise a scheme that will keep the content of a transaction secret from all but those authorized to have it (even if others intercept the transcript of the communication, which is often sent over an insecure medium).
2. **Digital signature:** Requires a mechanism whereby a person can sign a communication. It should be such that at a later date, the person cannot deny that it (a communication signed by him) was indeed sent by him.
3. **Data integrity:** Requires a method that will be able to detect insertion, substitution, or deletion of data (other than by the owner). (Say on a Web server or in a bank's database containing the information such as the balance in various accounts.)
4. **Authentication:** Two parties entering into a communication identify each other. This requires a mechanism whereby both parties can be assured of the identity of the other.

CONFIDENTIALITY-SECRECY-PRIVACY: ENCRYPTION

Encryption is necessary to secure confidentiality or secrecy or privacy. This requires an understanding of the encryption process. Most of such encryption in the past involved linguistic processes.

Consider the following example. Suppose two persons, A and B, would like to exchange information that may be intercepted by someone else. Yet A and B desire that even if a transmitted message is intercepted, anyone (other than A and B) should not be able to read it or make out what it says. Two friends may be gossiping or two senior executives in a large company may be exchanging commercially sensitive information about their company. This may be executed via e-mail (which can be intercepted rather easily). The most widespread use of secure communication is in the armed forces, where strategic commands are exchanged between various officers in such a fashion that the adversary should not be able to understand the meaning, even if they intercept the entire transcript of communication.

Let us first see how this objective could be achieved. Consider a *permutation* of the 26 letters of the Roman alphabet:

abcdefghijklmnopqrstuvwxyz
sqwtynbhgzkopcrvxdfjazeilm

Suppose that A and B both have this permutation (generated randomly). Now when A would