



Chapter II

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:

15 more pages are available in the full version of this document, which may be purchased using the "Add to Cart" button on the publisher's webpage: www.igi-global.com/chapter/introduction-cryptography/8708

Related Content

Light-Weight Semantic Integration of Generic Behavioral Component Descriptions

Jens Lemcke (2010). *Semantic Enterprise Application Integration for Business Processes: Service-Oriented Frameworks* (pp. 131-171).

www.irma-international.org/chapter/light-weight-semantic-integration-generic/37936

A Multivariate Statistical Assessment of the Level of Use of Information Systems in the Public Sector Services in Greece in Order to Oppose Bureaucracy

Odysseas Moschidis and Jason Papathanasiou (2014). *International Journal of Operations Research and Information Systems* (pp. 19-31).

www.irma-international.org/article/a-multivariate-statistical-assessment-of-the-level-of-use-of-information-systems-in-the-public-sector-services-in-greece-in-order-to-oppose-bureaucracy/108109

A Heuristic Algorithm for Optimizing Business Matchmaking Scheduling

Yingping Huang, Xihui Zhang and Paulette S. Alexander (2012). *International Journal of Operations Research and Information Systems* (pp. 59-73).

www.irma-international.org/article/heuristic-algorithm-optimizing-business-matchmaking/73023

Evaluating the Effectiveness of Pre-Positioning Policies in Response to Natural Disasters

Jarrett Chapman, Lauren B. Davis, Funda Samanlioglu and Xiuli Qu (2014). *International Journal of Operations Research and Information Systems* (pp. 86-100).

www.irma-international.org/article/evaluating-the-effectiveness-of-pre-positioning-policies-in-response-to-natural-disasters/114937

Revised Weighted Fuzzy C-Means and Fortified Weiszfeld Hybrid Method for Uncapacitated Multi-Facility Location Problems

Isik Guzelgoz, Sakir Esnaf and Tarik Kucukdeniz (2019). *International Journal of Operations Research and Information Systems* (pp. 53-71).

www.irma-international.org/article/revised-weighted-fuzzy-c-means-and-fortified-weiszfeld-hybrid-method-for-uncapacitated-multi-facility-location-problems/236646