Chapter V

Confidentiality:
Asymmetric Encryption

Confidentiality: Asymmetric Encryption

Asymmetric encryption is a form of cryptography in which one key is used to encipher and the other to decipher. The two keys are mathematically related, and if it is possible to make one of the keys public and still maintain the algorithm security, then the system is called public-key.

The most used public-key ciphers, the Pohlig-Hellman algorithm, the RSA algorithm, the ElGamal algorithm, and Diffie-Hellman, are discussed in this chapter.

Objectives

- Learn the design theory of Pohlig-Hellman, RSA, ElGamal, and Diffie-Hellman public-key algorithms
- Understand how public-key algorithms can be used to exchange crypto keys

Copyright © 2008, IGI Global. Copying or distributing in print or electronic forms without written permission of IGI Global is prohibited.
Introduction

Originally, the security of crypto systems depended on the secrecy of the encryption algorithm. Eventually, however, crypto manufacturers started developing crypto equipment in which the encryption algorithm could be revealed, yet, the security would remain intact because of the secret key. When the security of a crypto system depends exclusively on the secrecy of the key, the key must be transmitted by means of a protected channel. In general, most crypto equipment implements a secret key that is known only to the sender and to the receiver.

If a number of individuals wish to send secure information, symmetric cryptosystems require that initial arrangements be made for the individuals to share a unique secret key. First the secret key must be agreed upon by the users; then the key must be distributed to the individuals via some secure means to ensure key confidentiality and integrity. Knowledge of the ciphering key implies knowledge of the deciphering key and vice versa. In order to establish the secure channel, it is necessary to deliver the secret key to the individuals using a protected medium such as a courier. Of course, transporting the key in this way is risky, troublesome, slow, and expensive.

In their paper “New Directions in Cryptography,” Diffie and Hellman (1976) proposed a new kind of cipher system in which the enciphering and deciphering keys are related but different: one is made public, while the other is kept private. This type of crypto system is called asymmetric, since it provides encryption in only one direction—a second pair of keys is needed to communicate in the other direction. Once the two mathematically related keys are calculated, there is no way to find out the private key from the public key. Asymmetric public cryptosystems allow two users to communicate securely over an insecure channel without any key prearrangement.

By definition, a public-key cryptosystem has the property that knowledge of the encryption algorithm and the encryption key does not imply knowledge of the decipherment key or vice versa because it is not computationally feasible to derive one key from the other. In mathematical terms, this implies that the enciphering algorithm must be a one-way function. However, the legitimate recipient with his private deciphering key should be able to decipher the message, implying that the enciphering algorithm should not only be a one-way function but a trapdoor one-way function as well. Being computationally infeasible depends on state-of-the-art computer technology; a trapdoor one-way enciphering transformation today may lose its one-way status in several years.

Figure 5-1. Public key cryptosystem
Related Content

Wild-Inspired Intrusion Detection System Framework for High Speed Networks (flp) IDS Framework
[www.igi-global.com/article/wild-inspired-intrusion-detection-system/62315?camid=4v1a](www.igi-global.com/article/wild-inspired-intrusion-detection-system/62315?camid=4v1a)

CITS: The Cost of IT Security Framework
[www.igi-global.com/article/cits-cost-security-framework/75324?camid=4v1a](www.igi-global.com/article/cits-cost-security-framework/75324?camid=4v1a)

Scenario and Robust Optimization in Risk Management
[www.igi-global.com/article/scenario-and-robust-optimization-in-risk-management/165971?camid=4v1a](www.igi-global.com/article/scenario-and-robust-optimization-in-risk-management/165971?camid=4v1a)
A Mutual Authentication Protocol with Resynchronisation Capability for Mobile Satellite Communications
www.igi-global.com/article/mutual-authentication-protocol-resynchronisation-capability/53014?camid=4v1a