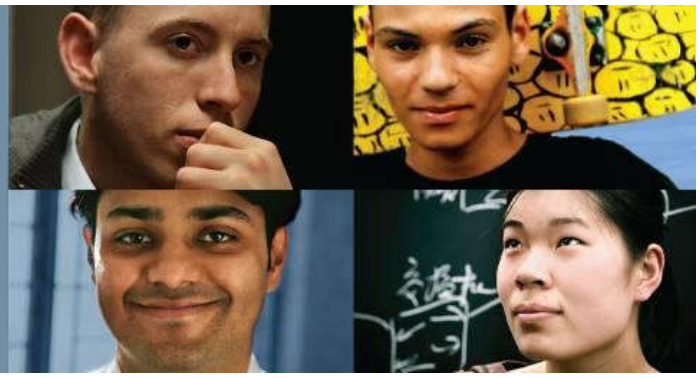
Chapter 4: The Art of Protecting Secrets



Cybersecurity Essentials v1.1

Cisco Networking Academy®
Mind Wide Open™

Chapter 4 - Sections & Objectives

4.1 Cryptography

Explain how encryption techniques protect confidentiality.

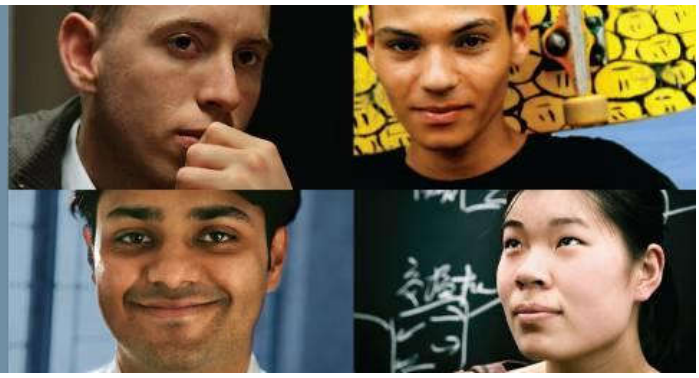
4.2 Access Control

Describe access control techniques used to protect confidentiality.

4.3 Obscuring Data

Describe the concept of obscuring data.

4.1 Cryptography



Cisco Networking Academy®
Mind Wide Open™

Cryptography
Overview

Cryptology is the science of making and breaking secret codes. Cryptography is a way to store and transmit data so only the intended recipient can read or process it. Modern cryptography uses computationally secure algorithms to make sure that cyber criminals cannot easily compromise protected information.

The history of cryptography started in diplomatic circles thousands of years ago. Messengers from a king's court took encrypted messages to other courts. Occasionally, other courts not involved in the communication, attempted to steal messages sent to a kingdom they considered an adversary. Not long after, military commanders started using encryption to secure messages.

Each encryption method uses a specific algorithm, called a cipher, to encrypt and decrypt messages. A cipher is a series of well-defined steps used to encrypt and decrypt messages. There are several methods of creating ciphertext:

- Transposition（rail fence cipher ,…）
- Substitution (Caesar – monoalphabetic - …. ）
- One-time pad (OTP)

Overview (Cont.)

Two Types of Encryption

There are two classes of encryption algorithms:

- **Symmetric algorithms** - These algorithms use the same pre-shared key, sometimes called a secret key pair, to encrypt and decrypt data. Both the sender and receiver know the pre-shared key before any encrypted communication begins. (AES – DES - …)
- **Asymmetric algorithms** - Asymmetrical encryption algorithms use one key to encrypt data and a different key to decrypt data. One key is public and the other is private. In a public-key encryption system, any person can encrypt a message using the public key of the receiver, and the receiver is the only one that can decrypt it using his private key. Parties exchange secure messages without needing a pre-shared key. Asymmetric algorithms are more complex. These algorithms are resource intensive and slower to execute. (RSA – ELGamal - ….)

Private-Key Encryption

Symmetrical Encryption Process - Symmetric algorithms use pre-shared key to encrypt and decrypt data, a method also known as private-key encryption. Numerous encryption systems use symmetric encryption. Some of the common encryption standards that use symmetric encryption include the following:

- **3DES (Triple DES):** Digital Encryption Standard (DES) is a symmetric block cipher with 64-bit block size that uses a 56-bit key. Triple DES encrypts data three times and uses a different key for at least one of the three passes, giving it a cumulative key size of 112-168 bits.
- **IDEA:** The International Data Encryption Algorithm (IDEA) uses 64-bit blocks and 128-bit keys. IDEA performs eight rounds of transformations on each of the 16 blocks that results from dividing each 64-bit block. IDEA was the replacement for DES.
- **AES:** The Advanced Encryption Standard (AES) has a fixed block size of 128-bits with a key size of 128, 192, or 256 bits.

Public-Key Encryption

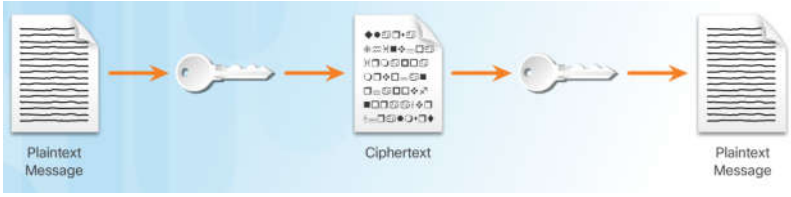
Asymmetrical Encryption Process - Asymmetric encryption, also called public-key encryption, uses one key for encryption that is different from the key used for decryption. A criminal cannot calculate the decryption key based on knowledge of the encryption key, and vice versa, in any reasonable amount of time. The asymmetric algorithms include:

- **RSA (Rivest_Shamir-Adleman)** - uses the product of two very large prime numbers with an equal length of between 100 and 200 digits. Browsers use RSA to establish a secure connection.
- **Diffie-Hellman** - provides an electronic exchange method to share the secret key. Secure protocols, such as Secure Sockets Layer (SSL), Transport Layer Security (TLS), Secure Shell (SSH), and Internet Protocol Security (IPsec), use Diffie-Hellman.
- **ElGamal** - uses the U.S. government standard for digital signatures. This algorithm is free to use because no one holds the patent.
- **Elliptic Curve Cryptography (ECC)** - uses elliptic curves as part of the algorithm. In the U.S., the National Security Agency uses ECC for digital signature generation and key exchange.

Symmetrical versus Asymmetrical Encryption

Comparing Encryption Types

- It is important to understand the differences between symmetric and asymmetric encryption methods. Symmetric encryption systems are more efficient and can handle more data. However, key management with symmetric encryption systems is more problematic and harder to manage.
- Asymmetric cryptography is more efficient at protecting the confidentiality of small amounts of data, and its size and speed make it more secure for tasks such as electronic key exchange which is a small amount of data rather than encrypting large blocks of data.



Symmetrical versus Asymmetrical Encryption

Application

There are many applications for both symmetric and asymmetric algorithms. A one-time password-generating token is a hardware device that uses cryptography to generate a one-time password. A one-time password is an automatically generated numeric or alphanumeric string of characters that authenticates a user for one transaction of one session only. The number changes every 30 seconds or so. The session password appears on a display and the user enters the password.

- The electronic payment industry uses 3DES.
- Operating systems use DES to protect user files and system data with passwords.
- Most encrypting file systems, such as NTFS, use AES.

Symmetrical versus Asymmetrical Encryption

Application

Four protocols use asymmetric key algorithms:

- Internet Key Exchange (IKE), which is a fundamental component of IPsec Virtual Private Networks (VPNs).
- Secure Socket Layer (SSL), which is a means of implementing cryptography into a web browser.
- Secure Shell (SSH), which is a protocol that provides a secure remote access connection to network devices.
- Pretty Good Privacy (PGP), which is a computer program that provides cryptographic privacy and authentication to increase the security of email communications.

Symmetrical versus Asymmetrical Encryption

Application

A VPN is a private network that uses a public network, usually the Internet, to create a secure communication channel. A VPN connects two endpoints such as two remote offices over the Internet to form the connection.

- VPNs use IPsec. IPsec is a suite of protocols developed to achieve secure services over networks.
- IPsec services allow for authentication, integrity, access control, and confidentiality.
- With IPsec, remote sites can exchange encrypted and verified information.
- Data in use is a growing concern to many organizations. When in use, data no longer has any protection because the user needs to open and change the data.
- System memory holds data in use and it can contain sensitive data such as the encryption key.
- If criminals compromise data in use, they will have access to data at rest and data in motion.