Cybersecurity

Architecture and Design

2.8.5 Block Ciphers and Lightweight Cryptography

How does symmetric encryption differ from asymmetric encryption?

Overview

The student will summarize the basics of cryptographic concepts.

Grade Level(s)

10, 11, 12

Cyber Connections

- Threats & Vulnerabilities
- Networks & Internet
- Hardware & Software

This content is based upon work supported by the US Department of Homeland Security's Cybersecurity & Infrastructure Security Agency under the Cybersecurity Education Training and Assistance Program (CETAP).

Teacher Notes:

CompTIA SY0-601 Security+ Objectives

Objective 2.8

- Summarize the basics of cryptographic concepts.
    - Cipher suites
        - Stream
        - Block
    - Symmetric vs. asymmetric
    - Lightweight cryptography

Block Ciphers and Lightweight Cryptography

Sweet Ciphers

Stream ciphers are symmetric key ciphers that encrypt pseudorandom numbers with bits of plaintext in order to generate ciphertext. Pseudorandom numbers satisfy one or more statistical tests for randomness but are produced by an algorithm. As the name suggests, ***block ciphers*** are symmetric key ciphers that apply an algorithm to encrypt data in blocks of text.

Didn't You Just Write the Same Thing Twice?

Stream ciphers and block ciphers are very similar, so it is important to be able to know the differences between the two. Stream ciphers encrypt plaintext one ***byte*** at a time while block ciphers encrypt one ***block*** at a time (each block is of a fixed size). Stream ciphers are faster than block ciphers but more difficult to implement. Stream ciphers have lower ***diffusion*** than block ciphers. In cryptographic terms, diffusion refers to the property that repetition in the statistics of the plaintext disappears in the statistics of the ciphertext. In layman's terms, diffusion helps hide the "relationship" between plaintext and ciphertext.

Stream ciphers have a lower ***error propagation*** than block ciphers. Error propagation is an error in a ciphertext block that results in a deciphering error only in the corresponding plaintext block. One final difference between stream ciphers and block ciphers has to do with authentication protections. Stream ciphers do not provide any authentication while block ciphers allow for authentication.

Teacher Notes:

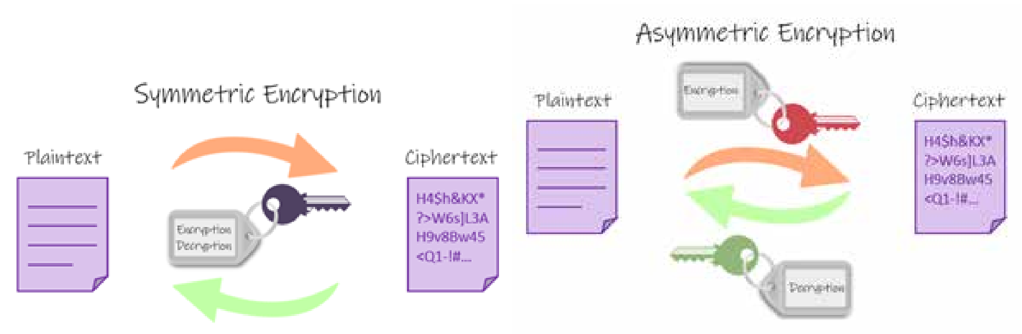
Examples

Here's a list of common stream and block ciphers.

Stream Ciphers	Block Ciphers
A53	DES
RC4	RC5
ISAAC	AES
SNOW	IDEA
Rabbit	Blowfish

Symmetric/Asymmetric Encryption

There are two general forms of encryption: symmetric and asymmetric. *Symmetric encryption* uses one key that must be shared among the people receiving a message. *Asymmetric encryption* uses a pair of keys, one public and one private, to encrypt and decrypt messages when communicating. The provided diagrams hopefully help give an understanding of the names.



Symmetric encryption is the older and simpler method of the two. The key used for both encryption and decryption would have been shared previously between the sender and receiver. The key is a secret algorithm that must be kept hidden from others. Symmetric encryption is a fast encryption method, which has little computational requirements.

Asymmetric encryption is newer and more complex. As mentioned, asymmetric encryption uses two keys. The public key is used to encrypt data. As the name suggests, this key is available to the public. The private key is used to decrypt data. As its name suggests, this key is kept private and cannot be decrypted using the public key.

Teacher Notes:

The Key to Creation

For asymmetric encryption, both keys are generated at the same time using extremely large, random (as random as can be) prime numbers. These keys are mathematical algorithms using modular arithmetic. The sender and the receiver are both able to generate a symmetric key using their private key and the public key.

Lightweight

Lightweight cryptography is an encryption method that requires low computational complexity. Although not useful for high powered devices, it is useful for constrained devices, and its related international standardization and guidelines compilation are currently being discussed.