Symmetric Encryption

Overview

Symmetric encryption, or secret-key encryption, is a fundamental cryptographic method where the same key (the secret key) is used for both encryption (converting plaintext to ciphertext) and decryption (recovering the plaintext from the ciphertext). The communication parties must agree upon and securely exchange this secret key beforehand.

Key Information

Terminology:

- **Cryptographic Algorithm or Cipher** This algorithm defines the encryption and decryption processes.
- **Key** The cryptographic algorithm needs a key to convert the plaintext into ciphertext and vice versa.
- **plaintext** is the original message that we want to encrypt
- **ciphertext** is the message in its encrypted form

A symmetric encryption algorithm uses the same key for encryption and decryption.

Encryption Algorithm	Notes
AES, AES192, and AES256	AES with a key size of 128, 192, and 256 bits
IDEA	International Data Encryption Algorithm (IDEA)
3DES	Triple DES (Data Encryption Standard) and is based on DES. We should note that 3DES will be deprecated in 2023 and disallowed in 2024.
CAST5	Also known as CAST-128. Some sources state that CAST stands for the names of its authors: Carlisle Adams and Stafford Tavares.

Encryption Algorithm	Notes
BLOWFISH	Designed by Bruce Schneier
TWOFISH	Designed by Bruce Schneier and derived from Blowfish
CAMELLIA128, CAMELLIA192, and CAMELLIA256	Designed by Mitsubishi Electric and NTT in Japan. Its name is derived from the flower camellia japonica.

Notes

Popular tools for symmetric encryption:

1. **GNU Priacy Guard**: The GNU Privacy Guard, also known as GnuPG or GPG, implements the OpenPGP standard.
2. **OpenSSL Project**: The OpenSSL Project maintains the OpenSSL software.

GNU Privacy Guard

- Command to ecnrypt `gpg --symmetric --cipher-algo CIPHER message.txt`
- Ascii armorded output `gpg --armor --symmetric --cipher-algo CIPHER message.tx`
- command to decryp `gpg --output original_message.txt --decrypt message.gpg`

OpenSSL Project

- command to encrypt `openssl aes-256-cbc -e -in message.txt -out encrypted_message`
- command to decrypt `openssl aes-256-cbc -d -in encrypted_message -out original_message.txt`
- Password-Based Key Derivation Function 2 `openssl aes-256-cbc -pbkdf2 -iter 10000 -e -in message.txt -out encrypted_message`

Task

1. Decrypt the file `quote01` encrypted (using AES256) with the key `s!kR3T55` using `gpg`.
   What is the third word in the file?
   1. `gpg --output quote1.txt --decrypt quote01.txt.gpg`

    2. Third Word `waste`
2. Decrypt the file `quote02` encrypted (using AES256-CBC) with the key `s!kR3T55` using `openssl`. What is the third word in the file?
    1. `openssl aes-256-cbc -d -in quote02 -out quote2`
    2. Third Word `science`
3. Decrypt the file `quote03` encrypted (using CAMELLIA256) with the key `s!kR3T55` using `gpg`. What is the third word in the file?
    1. `gpg --output quote3.txt --decrypt quote03.txt.gpg`
    2. Third Word `understand`

Conclusion

Symmetric encryption is a cryptographic method where a single secret key is used to encrypt plaintext into ciphertext and decrypt it back. While historical algorithms like DES (56-bit key) were broken, modern standards like AES (128/192/256-bit keys) remain secure and provide confidentiality, integrity, and authenticity. Popular implementations include GnuPG (GPG) and OpenSSL. Despite its security benefits, symmetric encryption suffers from a scalability problem because the number of required keys grows quadratically with the number of users, making it impractical for large-scale key distribution.

Resources

- **TryHackMe**: Intro to Cryptography
- **OpenSSL Project**: OpenSSL
- **GNU Privacy Guard**: GPG

Revision #4
Created 2025-11-25 18:38:41 UTC by David Rizzo
Updated 2025-11-25 19:18:26 UTC by David Rizzo