Laboratory_02: DES encryption using OpenSSL

This laboratory covers OpenSSL tool applicability for DES encryption.

Installation

- sudo apt update
- sudo apt-get install openssl -y
- openssl version

OpenSSL for symmetric encryption using DES-CBC

1. Create a file to encrypt:
    a. echo "lab for fun, hands-on learning." > secret.txt
2. Review the created file:
    a. cat secret.txt
3. List DES cipher algorithm:
    a. openssl list -cipher-algorithms | grep -i des
4. Generate a random key:
    a. openssl rand -hex 8 > des.key
    b. KEY=$(cat des.key)
5. Generate a random number:
    a. openssl rand -hex 8 > des.iv
    b. IV=$(cat des.iv)
6. Encrypt the file using DES:
    a. openssl enc -des-cbc -e -in secret.txt -out secret.enc -K $KEY -iv $IV
7. Display the encrypted content:
    a. xxd -p secret.enc
8. Decrypting file using DES-CBC
    a. openssl enc -des-cbc -d -in secret.enc -out secret.dec -K $KEY -iv $IV
9. Verify decryption was successful:
    a. cat secret.dec
10. Increase the size key:

a. openssl rand -hex 24 > des.key
b. KEY=$(cat des.key)

11. Try to encrypt again the file using DES:
    a. openssl enc -des-cbc -e -in secret.txt -out secret.enc -K $KEY -iv $IV
    b. Explain the obtained error

OpenSSL for symmetric encryption using 3DES-CBC

12. Create a file to encrypt:
    a. echo "lab for fun, hands-on learning." > secret.txt
13. Review the created file:
    a. cat secret.txt
14. List DES cipher algorithm:
    a. openssl list -cipher-algorithms | grep -i des
15. Generate a random key:
    a. openssl rand -hex 24 > des3.key
    b. KEY=$(cat des3.key)
16. Generate a random number:
    a. openssl rand -hex 8 > des3.iv
    b. IV=$(cat des3.iv)
17. Encrypt the file using DES-EDES3:
    a. openssl enc -des-ede3-cbc -e -in secret.txt -out secret.enc -K $KEY -iv $IV
18. Display the encrypted content:
    a. xxd -p secret.enc
19. Decrypting file using 3DES-CBC
    a. openssl enc -des-ede3-cbc -d -in secret.enc -out secret.dec -K $KEY -iv $IV
20. Verify decryption was successful:
    a. cat secret.dec