College of Engineering Department of Electrical Engineering

Assignment 2

CMPS 485 Computer Security

L51

Instructor: Abdelkarim Erradi.

TA: Eng. Naveed Nawaz.

Student Name : Alanoud Alyafei

IDNumber :201300537

Date Submitted: Sunday, November 18, 2018

Fall 2018

- Command used:

1. (RC4)

- Encryption time:

  time openssl enc -rc4 -k secret -a -in TenDaysBook.txt -out rc4Enc.txt

- Decryption time:

  time openssl enc -d -rc4 -k secret -a -p -in rc4Enc.txt -out rc4Dec.txt

- Finding the size of the encryption file:

  Stat rc4Enc.txt

2. AES 128 (ECB)

- Encryption time:

  time openssl enc -aes-128-ecb -k secret -a -in TenDaysBook.txt -out aes128-ecbEnc.txt

- Decryption time:

  time openssl enc -d -aes-128-ecb -k secret -a -p -in aes128-ecbEnc.txt -out aes128-ecbDec.txt

- Finding the size of the encryption file:

  Stat aes128-ecbEnc.txt

3. AES 128 (CBC)

- Encryption time:

  time openssl enc -aes-128-cbc -k secret -a -in TenDaysBook.txt -out aes128-cbcEnc.txt

- Decryption time:

  time openssl enc -d -aes-128-cbc -k secret -a -p -in aes128-cbcEnc.txt -out aes128-cbcDec.txt

- Finding the size of the encryption file:

  Stat aes128-cbcEnc.txt

4. AES 128 (OFB)

- Encryption time:

  time openssl enc -aes-128-ofb -k secret -a -in TenDaysBook.txt -out aes128-ofbEnc.txt

- Decryption time:

  time openssl enc -d -aes-128-ofb -k secret -a -p -in aes128-ofbEnc.txt -out aes128-ofbDec.txt

- Finding the size of the encryption file:

  Stat aes128-ofbEnc.txt

5. AES 128 (CFB)

- Encryption time:

  time openssl enc -aes-128-cfb -k secret -a -in TenDaysBook.txt -out aes128-cfbEnc.txt

- Decryption time:

  time openssl enc -d -aes-128-cfb -k secret -a -p -in aes128-cfbEnc.txt -out aes128-cfbDec.txt

- Finding the size of the encryption file:

  Stat aes128-cfbEnc.txt

6. AES 128 (CTR)

- Encryption time:

  time openssl enc -aes-128-ctr -k secret -a -in TenDaysBook.txt -out aes128-ctrEnc.txt

- Decryption time:

  time openssl enc -d -aes-128-ctr -k secret -a -p -in aes128-ctrEnc.txt -out aes128-ctrDec.txt

- Finding the size of the encryption file:

Stat aes128-ctrEnc.txt

7. AES 256 (ECB)

- Encryption time:
  time openssl enc -aes-256-ecb -k secret -a -in TenDaysBook.txt -out aes256-ecbEnc.txt

- Decryption time:
  time openssl enc -d -aes-256-ecb -k secret -a -p -in aes256-ecbEnc.txt -out aes256-ecbDec.txt

- Finding the size of the encryption file:
  Stat aes256-ecbEnc.txt

8. AES 256 (CBC)

- Encryption time:
  time openssl enc -aes-256-cbc -k secret -a -in TenDaysBook.txt -out aes256-cbcEnc.txt

- Decryption time:
  time openssl enc -d -aes-256-cbc -k secret -a -p -in aes256-cbcEnc.txt -out aes256-cbcDec.txt

- Finding the size of the encryption file:
  Stat aes256-cbcEnc.txt

9. AES 256 (OFB)

- Encryption time:
  time openssl enc -aes-256-ofb -k secret -a -in TenDaysBook.txt -out aes256-ofbEnc.txt

- Decryption time:
  time openssl enc -d -aes-256-ofb -k secret -a -p -in aes256-ofbEnc.txt -out aes256-ofbDec.txt

- Finding the size of the encryption file:

  Stat aes256-ofbEnc.txt

10. AES 256 (CFB)

- Encryption time:

  time openssl enc -aes-256-cfb -k secret -a -in TenDaysBook.txt -out aes256-cfbEnc.txt

- Decryption time:

  time openssl enc -d -aes-256-cfb -k secret -a -p -in aes256-cfbEnc.txt -out aes256-cfbDec.txt

- Finding the size of the encryption file:

  Stat aes256- cfbEnc.txt

11. AES 256 (CTR)

- Encryption time:

  time openssl enc -aes-256-ctr -k secret -a -in TenDaysBook.txt -out aes256-ctrEnc.txt

- Decryption time:

  time openssl enc -d -aes-256-ctr -k secret -a -p -in aes256-ctrEnc.txt -out aes256-ctrDec.txt

- Finding the size of the encryption file:

  Stat aes256- ctrEnc.txt

12. DES (ECB)

- Encryption time:

  time openssl enc -des-ecb -k secret -a -in TenDaysBook.txt -out des-ecbEnc.txt

- Decryption time:

  time openssl enc -d -des-ecb -k secret -a -p -in des-ecbEnc.txt -out des-ecbDec.txt

- Finding the size of the encryption file:

Stat des-ecbEnc.txt

13. DES (CBC)

- Encryption time:

  time openssl enc -des-cbc -k secret -a -in TenDaysBook.txt -out des-cbcEnc.txt

- Decryption time:

  time openssl enc -d -des-cbc -k secret -a -p -in des-cbcEnc.txt -out des-cbcDec.txt

- Finding the size of the encryption file:

  Stat des-cbcEnc.txt

14. DES (OFB)

- Encryption time:

  time openssl enc -des-ofb -k secret -a -in TenDaysBook.txt -out des-ofbEnc.txt

- Decryption time:

  time openssl enc -d -des-ofb -k secret -a -p -in des-ofbEnc.txt -out des-ofbDec.txt

- Finding the size of the encryption file:

  Stat des-ofbEnc.txt

15. DES (CFB)

- Encryption time:

  time openssl enc -des-cfb -k secret -a -in TenDaysBook.txt -out des-cfbEnc.txt

- Decryption time:

  time openssl enc -d -des-cfb -k secret -a -p -in des-cfbEnc.txt -out des-cfbDec.txt

- Finding the size of the encryption file:

  Stat des-cfbEnc.txt

16. Triple DES (ECB)

- Encryption time:

time openssl enc -des-ede3 -k secret -a -in TenDaysBook.txt -out des-ede3Enc.txt

- Decryption time:

  time openssl enc -d -des-ede3 -k secret -a -p -in des-ede3Enc.txt -out des-ede3Dec.txt

- Finding the size of the encryption file:

  Stat des-ede3Enc.txt

17. Triple DES (CBC)

- Encryption time:

  time openssl enc -des-ede3-cbc -k secret -a -in TenDaysBook.txt -out des-ede3-cbcEnc.txt

- Decryption time:

  time openssl enc -d -des-ede3-cbc -k secret -a -p -in des-ede3-cbcEnc.txt -out des-ede3-cbcDec.txt

- Finding the size of the encryption file:

  Stat des-ede3-cbcEnc.txt

18. Triple DES (OFB)

- Encryption time:

  time openssl enc -des-ede3-ofb -k secret -a -in TenDaysBook.txt -out des-ede3-ofbEnc.txt

- Decryption time:

  time openssl enc -d -des-ede3-ofb -k secret -a -p -in des-ede3-ofbEnc.txt -out des-ede3-ofbDec.txt

- Finding the size of the encryption file:

  Stat des-ede3-ofbEnc.txt

19. Triple DES (CFB)

- Encryption time:

time openssl enc -des-ede3-cfb -k secret -a -in TenDaysBook.txt -out des-ede3-cfbEnc.txt

- Decryption time:

  time openssl enc -d -des-ede3-cfb -k secret -a -p -in des-ede3-cfbEnc.txt -out des-ede3-cfbDec.txt

- Finding the size of the encryption file:

  Stat des-ede3-cfbEnc.txt

- The result of command execution:

	Encryption time	Decryption time	size of the encryption file
RC4	0.545s	1.023s	52.4 MB
AES 128 (ECB)	0.594s	1.108s	131KB
AES 128 (CBC)	0.584s	1.099s	131KB
AES 128 (OFB)	0.637s	1.134s	131KB
AES 128 (CFB)	0.591s	1.107s	131KB
AES 128 (CTR)	0.663s	1.068s	131KB
AES 256 (ECB)	0.672s	1.203s	131KB
AES 256 (CBC)	0.692s	1.195s	131KB
AES 256 (OFB)	0.681s	1.180s	131KB
AES 256 (CFB)	0.687s	1.194s	131KB
AES 256 (CTR)	0.693s	1.465s	131KB
DES (ECB)	1.787s	2.279s	131KB
DES (CBC)	1.787s	2.348s	131KB
DES (OFB)	1.817s	2.356s	131KB
DES (CFB)	1.902s	2.480s	131KB
Triple DES (ECB)	4.082s	4.463s	131KB
Triple DES (CBC)	4.049s	4.499s	131KB
Triple DES (OFB)	4.093s	4.566s	131KB
Triple DES (CFB)	4.212s	4.687s	131KB

- Conclusion:

The best performing ciphers is RC4 because it has shortest encryption and decryption time.

The worst performing ciphers is Triple DES (CFB) because it has longest encryption and decryption time.

The biggest size of the encryption file is all types except RC4
The smallest size of the encryption file is RC4.