Cairo University
Faculty of Engineering

Computer Engineering Department

Cryptography and Network Security- CMP 404**
Spring 2019

Security Project 2: DES Block Modes with Authentication

Project Objectives:

1. Apply security concepts you study in the course.
2. Enhance student's understanding of encryption algorithms.
3. Understand different block chaining modes of DES and compare them.
4. Practice message authentication.

Project Requirement:

Develop a network application where two parties are communicating, using DES algorithm, and using different DES block modes. Your application should support message authentication, by implementing any reasonable MAC algorithm.

Part 1:

Develop a network application which provides DES encryption and decryption of data, transmitted via network. Implement the following operation mode of DES

- Electronic Codebook (ECB)
- Cipher Block Chaining (CBC)
- Cipher Feedback (CFB)
- Output Feedback (OFB)
- Counter

Your application should provide interaction of two peers via network (send and receive data, their encryption and decryption, display of plaintext and sent ciphertext on sending side; display of received ciphertext and obtained plaintext on the receiving side).

At the start of communication, the block mode should be configured (sender sends a message of any suitable format to the receiver).

Part 2:

Implement any reasonable Message Authentication Code (MAC) generation algorithm of your choice, and integrate it with part 1 such that the sender sends the encrypted message, and its associated MAC. On the other side, the receiver should verify the MAC besides decrypting the message.

If the MAC verification outputs that the message is invalid, you should display a message of that at the receiver side.

Analysis Part:

Compare the considered block chaining modes of DES (in terms of time for encryption on the same messages, versus the message block size on x-axis, try different block sizes. What are the advantages/drawbacks of each mode of them?

Important Notes

- **Copied projects from each other/from the internet will get zero!**
- You can use a cryptography library.
- You should work in group of size 2 students.

Deliverables:

- You should deliver all your code and a detailed report about your project, how you implemented it and the analysis results and your conclusions.

Project Due Date:

Tuesday, April 30th , 2019.