CSC 425 Wireless Security

Lab 1: Symmetric Key Cryptography Implementation and Study

Objectives

The objectives for this lab assignment are as follows:

- Implement Symmetric Key Cryptography algorithms (RC4, AES).
- Study the applications and limitations of Symmetric Key Cryptography algorithms.

Programming Language: Python

Requirements

Please read the requirements carefully, and finish the lab assignment accordingly:

Utilize symmetric key cryptography algorithms using Python. Please make use of built-in functions and cryptography libraries such as PyCrypto or PyCryptodome.

Task 1: Encryption and crack implementation

Using AES and RC4, encrypt the following plaintext, ***"this is the wireless security lab"***. For AES, the key is 128-bit 1s; for RC4, the key is 40-bit 1s.

Utilizing the resulting ciphertext (encrypted plaintext), try to crack them without knowing the key information except the key size and encryption algorithm.

Task Deliverable:

- Show all code used in this task (at end of document or via GitHub)
- Show the encrypted result of your plaintext as Bytes.
- Describe the method used to crack the ciphertext. State the vulnerabilities you are utilized of each algorithm to crack the ciphertext (and cite them where necessary). If you could not crack the ciphertext, please also state the reasons you were unable to do so.

(Hints: There are different modes you can choose to use for AES encryption. Make sure you explain the one you choose to use.)

Task 2: Observing Symmetric key Cryptography

Symmetric key cryptography has different modes of operation, including electronic codebook (ECB), cipher-block chaining (CBC), cipher feedback (CFB), output feedback (OFB), and counter mode (CTR). Two important properties of these encryption modes in this lab that we will explore are **pattern preservation** and **error propagation**.

Pattern preservation means that a block of plaintext is encrypted into a block of ciphertext the same way every time. The pattern preservation will enable attackers to find artifacts of the plaintext since a particular pattern exists in the ciphertext.

Error propagation means that a single bit error in transmission of a cipher text block can create errors not only in the decryption of the affected block but also propagate to the following blocks of the message.

Determine your own plaintext, and pick up the key to implement the different modes of operation and fill out the following table (Yes/No):

	ECB	CBC	CFB	OPB	CTR
Pattern preservation					
Error propagation					

Task Deliverable:

- Show all code used in this task (at end of document or via GitHub)
- Fill out the table based on your observed results (Yes/No)
- Any necessary explanation regarding the process used to find your results.

(Hints: For observing pattern preservation, you should have repeated blocks in your plaintext; For observing error propagation, you can encrypt plaintext first and change one bit in the ciphertext to check the decryption results.)

Questions

1. What are the advantages and disadvantages of AES and RC4?
2. Which one should you for file encryption? Why?
3. Discuss your experience during the crack implementations.
4. Discuss the features of different mode of operations and their applications.

Submission

You need to submit a detailed lab report to describe what you have done and what you have observed, including your code. Please also provide explanation to the observations that are interesting or surprising. You are encouraged to pursue further investigation, beyond what is required by the lab description to earn bonus points for extra efforts. (Please talk to your instructor for the further investigation)