IZMIR INSTITUTE OF TECHNOLOGY
CENG471 – Cryptography
Homework #1

Deadline: 17.11.2022, 11:55 pm

In this homework, you will perform encryption and decryption of a text message using a symmetric cipher that is combined with a password-based key derivation function. You need to write your codes in the Python programming language. You are expected to use **pycryptodome** package. You will write one Python script **aes_cipher.py** that takes arguments from the command line.

Encryption:

Encrypts a text message (**m**) using the given password (**p**). It has the following steps:

- Derive a key from the password using Scrypt (N=2**14, r=16, p=1) with random salt (128 bits). The key length (**k**) is determined by the user. The key will be used for encryption and decryption.
- Pad the input message using the PKCS7 algorithm to a length, that is a multiple of 16 bytes (128 bits).
- Encrypt the padded message using the AES with CBC mode of operation using the derived encryption key. Use a randomly generated 128-bit initialization vector (IV).
- Create a json file (**f**) that holds the randomly generated salt used for Scrypt, the randomly generated iv used for AES, and the produced ciphertext from AES.

Decryption:

Decrypts an encrypted message using the given password (**p**).

- Read the json file (**f**) given as input.
- Derive a key from the password using Scrypt (N=2**14, r=16, p=1) with the salt (from json).
- Decrypt the ciphertext using AES using the derived key and IV (from json).

Execution examples for encryption and decryption are given below. Make sure that you clearly display each calculated value as in the examples. You need to apply Base64 encoding for bytes-like objects to represent them in the readable form.

python aes_cipher.py enc -m "A secret message" -p "My password" -k 32 -f enc_info.json
Encryption result:
{"salt": "PnWgsTjRip9cRIhSowGCvg==", "iv": "uuhTXi+F7JjiBIngaDboig==", "ciphertext": "MDE9d1/a1AERKSu28P1/z12WTtHfLbj0eU7IMxF6sBg="}

python aes_cipher.py dec -p "My password" -f enc_info.json
Plaintext:
A secret message

Note that you can run the above example by setting the salt and IV to the given values while checking whether you obtain the given result.

Report:

You need to prepare a report (1-2 pages) to answer the following questions.

1. The types of symmetric ciphers are stream ciphers and block ciphers. Write the general properties of them in 2-3 sentences. In which situations, which type is preferred? Give an example where each type is used.
2. In CBC mode of operation, is the IV public or secret? Discuss how the IV can be sent to the receiver?
3. Is CBC mode secure? Are there any new modes that can be worked with AES? What is the novelty of them in general?

Grading Policy

- Implementation of Encryption (40 points)
- Implementation of Decryption (40 points)
- Report (20 points, 10 + 5 + 5)

Rules:

- You can do this homework in pairs or individually.
- Submit your homework as a zip file that contains **aes_cipher.py** and **report.pdf**.
- If you did the homework in pairs, one of the team members must submit it and the file should be named as **ceng471_hw1_<studentno1>_<studentno2>.zip**.
- If you did it individually, the file should be named as **ceng471_hw1_<studentno>.zip**.
- Any cheating will be graded as 0 for both sides.
- Write your student number(s) at the beginning of each file rather than your name(s).
- For your questions, you can contact me via email or Teams (Leyla Tekin, leylatekin@iyte.edu.tr).