CYEN 406/CS 444
Sangam Mulmi

Assignment 3: File Encryption Tool

Total Points: 40

Due: May 3, 2017 (Wednesday) at 11:55 PM

Hey, Cryptographer! For this assignment, you are required to write a program in **Python 2.7** to develop a tool that can encipher any digital file using *Advanced Encryption Standard (AES)*. Additionally, this program must also be able to decipher any file that has been enciphered using it. **'aes.py' program file has been given** to help you get started.

Instructions:

- Take **three** arguments from the command-line:
  1. Action: 'enc' or 'dec' for enciphering or deciphering respectively.
  2. Key: Combination of letters, numbers, and symbols. Must be 16, 24, or 32 bytes long.
  3. Filename: A file to encipher or decipher.
- **Encrypt the file:**
  - Read the content of the file. Perform any bit/byte conversion, if needed.
  - Use the key to create an *AES* object from *Crypto.Cipher* library.
  - Encipher the content (pad, if necessary) of the file using this object to get the *ciphertext*.
  - Hash the key with *SHA-256*.
  - Concatenate the *key's hash value* and *ciphertext*, i.e. *user inputted key's hash value* + *ciphertext*.
  - Write the whole thing into a new file: *OriginalFileName_enc.OriginalExtension.*
- **Decrypt the file**:
  - Read the content (*key's hash value* + *ciphertext*) from the file. Perform any bit/byte conversion, if needed.
  - Hash the key received from command-line using *SHA-256*.
  - Extract the hashed key from the input file, which was saved at the beginning of the encrypted file.
  - Verify if hashed input key matches with the hashed key stored in the encrypted file.
  - If they match, use the input key to create an *AES* object; else, display an error message.
  - Use this object to decrypt the content of the encrypted file (only the *ciphertext* portion.)
  - Write the decrypted content into a new file: *OriginalFileName_dec.OriginalExtension*.

Sample Execution Commands:

Encryption

```
$  python  enc  WATERMELONISNICE  mysecretdocument.docx
       Output: mysecretdocument_enc.docx
```

Decryption

```
$  python  dec  WATERMELONISNICE  mysecretdocument_enc.docx
       Output: mysecretdocument_dec.docx
```

Please note that you will want to use *Python Cryptography Toolkit* (pycrypto) for this assignment. It can be downloaded from here: https://pypi.python.org/pypi/pycrypto.

Submission Guidelines:

1. Write comments on your source code file (*file_encrypter.py*). Include *author's name*, *date*, *description*, *list of resources used*, and so on.
2. Upload the source code file to **Moodle** by the deadline.