


National University of Computer and Emerging Sciences, Lahore Campus

| | | | | |
|-----------------------------------------------------------------------------------|--------------|----------------------|--------------|-----------|
|  | Course Name: | Information Security | Course Code: | CS3002 |
| | Program: | BS-CS | Semester: | Fall 2024 |
| | Section | C, D, E | Total Marks: | 10 |
| | Due Date: | 15-09-2024 | Weight | ~3.3% |
| | Exam Type: | Assignment 1 | Page(s): | 2 |

Task

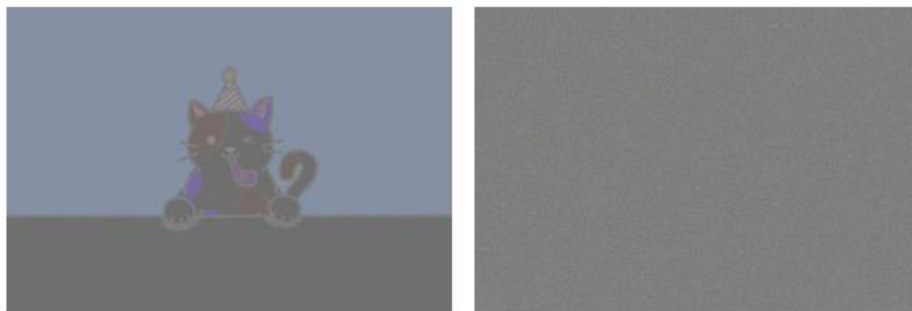
Create a CLI program for photo encryption. Prompt the user for an image file (jpg/png) and a password. Encrypt the image using DES algorithm, and render the ciphertext as an image.

Before you can encrypt the data, there are two prerequisite steps

- Derive a 56-bit DES key from the user-supplied password. Use **scrypt** algorithm for this purpose.
- Read the image data (RGB pixels) and flatten them to an array of bytes.

Once plaintext is available, encrypt it with DES cipher, operating in two block cipher modes: ECB (electronic codebook) and OFB (output feedback).

Both ciphertexts should be transformed back into an RGB image and displayed on screen as below.



You can implement the program in **C++, Java or Python**. Each language comes with well-known libraries for cryptographic functions. We recommend Crypto++, bouncy castle and pycryptodome respectively.

Deliverables

- 1) Submit a copy of your code and screenshot of output.
- 2) A document containing answers to following questions
 - A. You will notice that ECB mode requires a padding for data, but, OFB does not. Why?
 - B. Why does the output of ECB reveal so much about plaintext, but not OFB?
 - C. Explain the parameters that were required by scrypt key generation.

5 + 2 + 1 + 2 marks

Evaluation

You will have a viva about your code. Additionally, you should have a good understanding of ECB and OFB modes, as well as some idea of inner-workings of key derivation functions (like scrypt).