

Emily Gorelik
Software Development Milestone
Professor Arias
4/6/18

Abstract

This program is an image encryptor and decryptor that uses a linear feedback shift register to generate a cypher that will create an encrypted image.

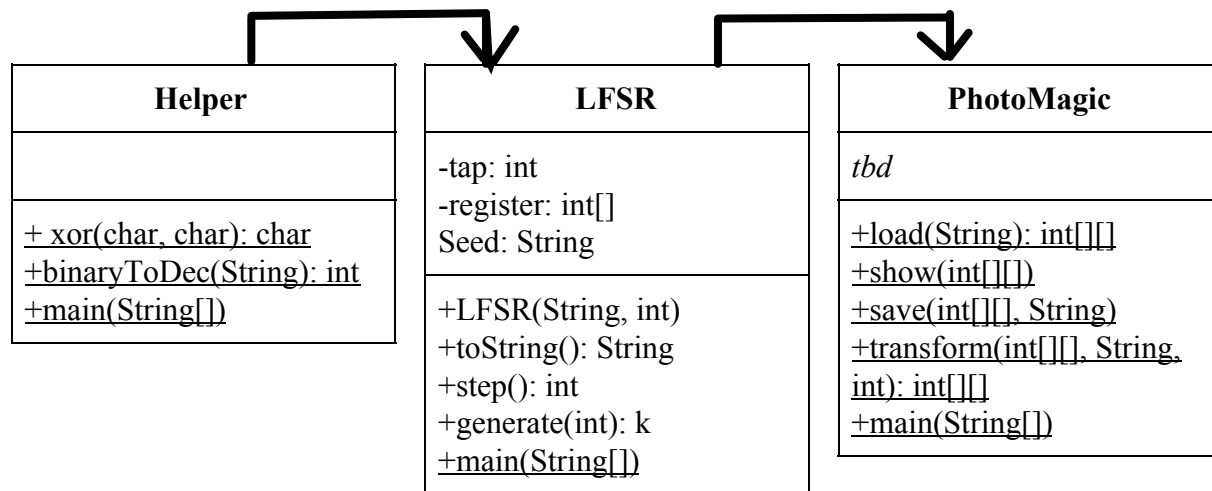
Introduction

Though Java includes many ways to work with images, they can be clunky and difficult to use. This program allows for an easy way to encrypt and decrypt an image by generating a password that is used to modify the image. This paper will include a description of how the program works, why it is necessary, similar systems, and how the program should be used.

System Description

This system develops a pseudo-random code that will later be used to encrypt and decrypt an image. The Helper class is made up three static methods. One applies the xor function on two chars that are either a one or zero. The other converts a binary number represented by a string into a decimal integer. The last one tests the two methods. The LFSR class uses the static methods in Helper to execute the linear shift on a binary number. The PhotoMagic class will use a randomly generated 32-bit integer (made by the LFSR class) to update each pixel of an image. It will also use methods from the Picture class, found in the Java Standard Libraries in order to modify the image file. A user would, through the command line, input the name of the image file, the initial LFSR seed, and the tap number. The encrypted image would then display and a

user could save it. Then, if they wish to decrypt the image, they can use the same seed and tap with the new file name and retrieve the original image.



Requirements

This system allows a user to easily encrypt an image without altering the original image file.

Literature Survey

There have been many systems made to encrypt images. They come in many different forms with various levels of security and complexity. There are a wide variety of cyphers used, such as Vigenere Ciphers, RC4, RC5, RC6, etc (Kumari, Gupta, Sardana).

User Manual

First, a user would need to come up with a binary password and an integer, as well as the image they would like to encrypt. Then, through the command line, they would type in “% java PhotoMagic [image file name] [binary password] [integer].” This will cause the encrypted image to display where a user could then save the image under another name. If a user wished to

decrypt the image, they would simply follow the same steps and input the encrypted image file with the same password and integer.

Conclusion

All in all, this program seeks to provide a simple method of encrypting and decrypting an image from one's computer.

References

Kumari, M., Gupta, S. & Sardana, P. 3D Res (2017) 8: 37.

<https://doi.org/10.1007/s13319-017-0148-5>

