CS 131 Project Report

An Introduction to Classical Cryptography

Erick Barron

10.05.2023
CS 131 Professor Yuen

INTRODUCTION

My topic for this presentation is from chapter 4 in the book on the topic of Cryptography. Specifically I am focusing on 4.6.2 which is titled Classical Cryptography. I chose this topic since it seemed very interesting to me. The book defines classical cryptography as “cryptography, the subject of transforming information so that it cannot be easily recovered without special knowledge.” This chapter and specific section really caught my attention, because puzzles and decrypting secrets has always been something that interested me. My goal for this project is to help you understand this topic as in depth as I can and hopefully teach you as much as I have learned.

Process

My process for this project was simple. I first read all assignments and made sure I understood what was being asked of me. Next I chose my topic, for me it was an easy decision due to the topic really standing out. I actually did the code first and then started on the presentation. The code took me a bit to figure out, but was at a level that I could finish in a day. Next I outlined my presentation . I thought a good way to order it was an intro section for basic information. Then we get to the background section where I explain the history of cryptography and then the next slide explains the relevance in Discrete Mathematics. The next slides contain details on the formulas of the ciphers and also the examples that I go through to better explain and show to the viewer. Lastly I give some use case information and finally the conclusion.

Structure

1. Introduction
2. Background
3. Relevance in Discrete Mathematics
4. Formula and Process
5. Examples

6. Use Cases
7. Conclusion

Research

My research took me to my book where upon re-reading the section I developed a deeper understanding than my first read. I find it fascinating how much a re-read can really add to your knowledge. Since I wanted to provide background knowledge and use cases I felt the need to research from outside sources since the book was not focused on those topics. This led me to many articles and websites with very useful information which are attached here in the references section. This background knowledge helped me understand better due to the history and uses. I was able to connect and think about the topic in much more detail. I found the history fascinating since it actually did not start with Caesar, however I was not really able to add this part since it was not relevant. Part of my research was going over problems as well which was new to me since I was used to researching papers with no math or science problems. I feel very comfortable with this topic and I feel I have mastered the problems. My findings include the history and what discrete mathematics is as well as examples to my problems.

Code and user manual

For my code I used Java since it is what I am most comfortable with. For my process I knew that I had to be able to use the caesar's cipher so I made methods that would receive the letter and shift it 3 spaces and for decryption 23 so as to not get a negative integer. Next I made the method that would allow the processing of the message. Lastly the main method will run all of this and ask for input from the user. This will run the program. You can view the code in the link below:

https://github.com/S23-CS131-YUEN-16122/DS_Project_ErickBarron/blob/main/src/Barron_DS_Code.java

#Instructions for code

To run program you can use any IDE with java jdk compatibility

I do recommend using this site from browser at it will run my code
https://www.onlinegdb.com/

once there simply rename the program Barron_DS_Code.java and paste my code

From there run the code and enter a message must be letters

Then enter and choose either encrypt or decrypt and your message should encrypt or decrypt

Thanks!!!

Conclusion

This project really helped me understand what my topic was about on a greater level. It really does show you what it means to really understand a topic. The research and effort put into this has made me understand my topic on a deeper level. It also incorporated many aspects of the software cycle and has helped me program better. The Github portion is really good for students to learn such a valuable skill. The research put into might not be on the level of a high level class, but was enough that you really had to take time to find info you may need.

REFERENCES

"Cryptography and Its Types." *GeeksforGeeks*, 8 July 2019, www.geeksforgeeks.org/cryptography-and-its-types/#.

Rosen, Kenneth H. *Discrete Mathematics and Its Applications*. 8th ed., New York, Ny, Mcgraw-Hill, 2019.

Sidhpurwala, Huzaifa. "A Brief History of Cryptography." *Www.redhat.com*, 14 Aug. 2013, www.redhat.com/en/blog/brief-history-cryptography.

Štrobl, Roman. "Classical Cryptography in a Post-Quantum World." *Wultra Blog*, 3 June 2020, medium.com/wultra-blog/the-classical-cryptography-in-a-post-quantum-world-b3ec215ee915. Accessed 11 Dec. 2023.