Ahimed

Pro. Forsyth

IT 4843

April 26, 2020

**Introduction**

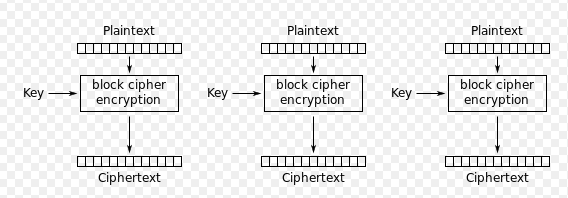
Information security affects the daily operations of individuals. It is crucial in protecting network resources from access by unauthorized people. The IT department of Organizations supervises and coordinates all servers and operating systems. The automated functionalities of Organizations depend on computing systems. For better service to the customer, Organizations should ensure that their operating systems and servers are up to date and always functional. Backup and recovery servers are recommended in the company to ensure that in case the direct server fails, the recovery database is used. IT infrastructure requires a secure place. Facilities are used in housing the IT infrastructure. Advancement of technology has resulted in the use of computers and mobile phones for personal and business purposes. Computers and mobile phones apply technology in offering security services. Password and Pin are used to protect computers and mobile phones from being accessed by unauthorized individuals. The project is made to identify the AES key used to encrypt the secret message, identify the secret message encrypted with that AES key, and finally determine the contents of that message.

**Environment**

The project was implemented using Java language. The IDE used was Eclipse. The project required a good understanding of programming languages. I am only familiar with Java as a scripting language and MySQL as a database and query language. It is hoped that MySQL will be integrated later to supplement the Java platform. Before the end of the term, the software stack required will be Eclipse, MySQL, and WordPad. Online sources were helpful in understanding what is to be done on the project. Stake overflow website was a friendly platform to help me understand how to create import in the Java file. It also helped in understanding the differences between a project and a class in Java language. How to use If Else in a statement in Java was made clear through the notes in Stake overflow website.

**Methodology**

I did the project alone though I mused about consulting from my classmates on what to do. I had tried to open my dataset without success, and my friend helped me understand what it contained. I did not have software to open the data set, so it was difficult to kick off the project. I used the prototype design approach so as to have a clear knowledge of what to be programmed. The main purpose of the project was to design a program that can be used to encrypt and decrypt public and private keys. The design was focused on implementing a program that can perform, as shown in the diagram below.



I did research on how to create a program that can be able to encrypt and decrypt the ciphertext. The knowledge obtained helped in understanding how the coding process will start. Password and Pin apply the knowledge of encryption and decryption—a user keys in the password that is encrypted to prevent its exposure to unauthorized users.

There is various execution path that will be required in the project. The first execution path will be to run the main code, while the other one will be to locate the database storage. The execution of the program will be prompted using the command $folder\_prompt. I will run the project from local disk D, which I have remained its coursework. The project is located in D:\ coursework\ethicalhacking\. The code will be accessed through the code File h = new File("..\ethicalhacking\file.xyz");

I encountered numerous challenges in the process of coming up with the project. I was not able to identify my assigned dataset; thus, I only wrote a code that can validate and identify the AES key used to encrypt the secret message and identify the secret message being decrypted. I also had a limited time to practice coding, and most of the time, my classmates were busy helping.

The project is still under development. I am still learning on how to incorporate database in the project to ensure it is able to record activities done. I am still trying to connect it to read the dataset provided.

**Metrics**

I could not succeed in identifying the number of messages, asymmetric keys, and symmetric keys found in the dataset. I will be in a position to report on them after a successful run of the project. I could not also validate the time taken of my solution to identify the contents of the secret message since I was able to identify the keys found in the dataset. At this moment, it is not possible to determine the execution time to be affected if the number of messages and keys was doubled. It is not possible to determine the contents of the secret message at the moment. I have to go back and ask my classmate to explain to me how to use the data so as to give a constructive report in the future.

Works Cited

Udebuana, Okpala Izunna, and Ikerionwu Charles. "Decision-Making Framework Using a Growth Hacking Model for Computerized Decision Support." *International Journal of Systems Science and Applied Mathematics* 4.2 (2019): 24.