18/20

Will Wainscott

Software Development I

4/6/18

Project 2 Milestone

Title?

My project is based around encryption and decryption. Specifically, I am using the public and private key pair encryption method. This means creating two related keys, giving one to the public so they can encrypt their message, and then keeping the private key private, and using the it to decrypt the messages. To do this I am having the user create a text file, and then run my application that produces another text file with the encrypted method. Once the file is encrypted, it can be run through the same application and another text file will be created with the decrypted message inside.

With security and more specially cybersecurity becoming more and more needed in the digital technology field, I have been interested in all the ways companies protect our data. I think that the ability (or lack of) to protect both personal and corporate data will become the most prevalent issue in the computer science field. Because of this I wanted to learn more about how data can be protected using simple encryption and decryption methods. I think that the knowledge that I am gaining from this project is something that I can apply to my future work on both computer applications and security applications.

The system is very straightforward and is not very complicated to use. The first thing the user must do is create a text file with some sort of message in it. Once the user has a file with the message they want to encrypt, they run the program and specify the name of their file. The program creates both the public and private keys and encrypt the message using the RSA

encryption method. RSA stands for Ron Rivest, Adi Shamir and Leonard Adleman, who created the algorithm that encrypts the messages Once the program is done running, a sperate text file will be created with the title 'Encrypted Message.' Inside of the text file will be the text equivalent to the encrypted message, which is unreadable to a person. This text file can now be moved and sent to other computers, as well as both the public and private keys. Once a user wants to decrypt the message, all they need is the text file of the encrypted message, and the private key. Running the program with these will create another text file that will display the decrypted message.

GenerateKeys
-pairGen: KeyPairGenerator -pair: KeyPair -publicKey: PublicKey -privateKey: PrivateKey
+GenerateKeys() +createKeys(): void +getPublicKey(): PublicKey +getPrivateKey(): PrivateKey +createTextFile(key: byte[], name: String): void

Encrypt
-publicKey: PublicKey
+getPublicKey(): PublicKey +encryptFile(fileName: String) : void +main(): void

Decrypt
-privateKey: PriavteKey
+getPrivateKey(): PublicKey +decryptFile(fileName: String): void +main(): void

This system is addressing the increasing need for the safe transfer of data and information. With there being increasingly more incidents of cyber attacks and stolen data, we cannot be too safe when sending private information to other people over the web. While my system is a very basic example of what public and private key encryption is used for, the basic principles that I am using can and will apply to much bigger cybersecurity problems in the future.

There are many ways that data can be encrypted, and many of them have become incredibly fast and secure. I am using the RSA algorithm which is the most commonly used public-private key method of encryption. An example of another encryption method used by both the public and the U.S. government is the AES or the Advanced Encryption Standard. This algorithm is used by many large organizations and is mostly assumed to be impossible to break. This encryption method is thought to become the new standard of encryption in the coming years. There are endless ways that companies protect data, but the most common ones are often available in the public domain, making them even more refined and well attended.

The application should be used to send encrypted messages to other people via text files. A person can use the program to create their own encrypted messages, and then send the message, key, and the program to someone else so that they can decrypt the message. The public key can also be given to the person who is making the message, so the person who made the keys can use their private key to read what the message is.

In conclusion this application is something that is not only useful itself, but it can be applied to many different situations. Using a similar type of encryption can help encrypt more than just text files. While I think that there is a lot you can do with my system, the potential for expansion is what makes this project special.

Use the sections specified in the description of the project.

- Are you implementing the algorithms or just using existing libraries?