|  |  |  |  |
| --- | --- | --- | --- |
|  | 5/1/2015 |  | |
| |  |  | | --- | --- | |  |  | |  |  | |  |  | |  |  | | |  | |
| SSE 554 Project 4  *Encrypting the Bank* | | | |
|  |  | | |  |  |  | | --- | --- | --- | |  |  |  | |  |  |  | |  |  |  | |  |  |  | |  |  |  | |  |  |  | |
|  |  | | Daryl Ebanks & Josh Deremer |



SSE 554 Project 4

Encrypting the Bank

# Introduction

This project is the final installment of the banking concept initially created by Daryl in his first project. Since the inception of the program, multithreading, client-server interaction, and database storage have all been added to the original basic bank program. In this last portion, we will add encryption to the data being transmitted. The data will be encrypted before being sent from the client program to the server program and vice versa. Each direction will have its own encryption method, one created by Josh and the other created by Daryl. Once again, we will begin by discussing some key topics before presenting the integration of encryption into the basic bank program.

Table of Contents

[Introduction 1](#_Toc418279797)

[Encryption 2](#_Toc418279798)

[Symmetric Ciphers 2](#_Toc418279799)

[Public Key Ciphers 3](#_Toc418279800)

[Client to Server Encryption 4](#_Toc418279801)

# https://blog.spideroak.com/wp-uploads/encryption.jpgEncryption

Encryption is a very important aspect of security with digital information. In many situations, it is undesirable and even dangerous to have one’s transmitted data available for the world to read as it is traveling from its source to destination. When information is encrypted, it is not visible to anyone who might try to read it and requires a matching key in order to decrypt and make understandable.

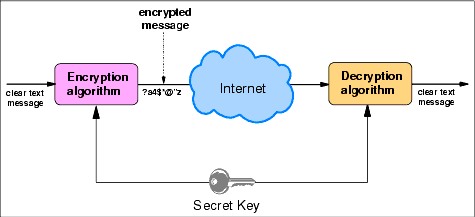
The encryption process involves using a cipher to encode and decode data. Ciphers can be personally created or randomly generated using the utilities available in the Java API. Throughout the years, more and more algorithms have been created to generate stronger and stronger ciphers in order to deter the continuing advancement of cyber thieving technology and computer processing capabilities. Because of this, there is a large number of cipher algorithms available, however, half or more are already outdated and can be easily cracked.

Most ciphers will generally require a cipher key to go along with them. This key can be used to ensure a particular behavior out of the cipher. Any changes in this key will result in changes from the output of the cipher. It is important when encrypting and decrypting data, the same key or matching keys are used, otherwise the data cannot be decrypted properly.

In this project, we make use of two different types of ciphers: symmetric ciphers and public key ciphers.

## Symmetric Ciphers

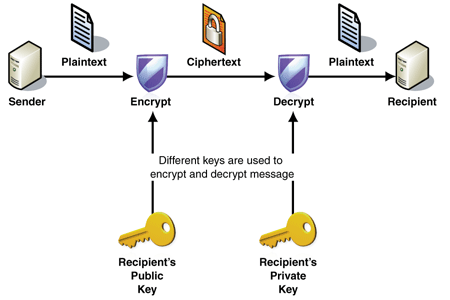
A symmetric cipher is a type of cipher that uses the exact same key for both encryption and decryption. This is a very common encryption method that has a wide variety of cipher algorithms created following this model. The process for a symmetric cipher involves first creating a secret key to be used with both encryption and decryption of data. Then, the user begins data transfer by accepting a plaintext message as the input and the encrypting the message by running it through the encryption algorithm which is governed by the secret key. The encrypted message then travels along the public path where the encryption is required to keep it secure, most often the internet. Once the message reaches its destination, it is run through the decryption algorithm, which is governed by the same secret key as before, and emerges as the original plaintext message. This process can be seen in the image below.



This encryption method is very economical in terms of processing resource usage, however, it requires that the secret key be known by both the sender and receiver of the message. This may be perfectly fine or could pose a serious problem depending on the application. Because of this, other ciphers were created, particularly the public key cipher.

## Public Key Ciphers

The issue mentioned earlier with the symmetric encryption cipher where both the sender and receiver need to know the secret key is known as key distribution. In order for one user to send a message to another user, the secondary user must have the same key the first user uses to encrypt the message. However, the first user cannot just send that new key through an unsecure channel, otherwise the purpose of encrypting the method in the first place is defeated.



This is where public key cryptography comes in. With a public key cipher, the users can have a key pair consisting of a public key and a matching private key. The public key can be access and used by anyone to encrypt a message and send it to the user with the private key. Only the private key can then decrypt the message. Therefore, one user can simply publish their public key anywhere. The second user can grab the public key and use it to encrypt their message. Then, the second user sends the encrypted message to the first user who decrypts the message using the matching private key.

However, as fantastic as that may sound, there are still drawbacks to using public key ciphers. First and foremost is that public key algorithms are much slower than symmetric key algorithms. Because of this, the transfer of large quantities of data is not conceivable for public key ciphers. In order to find a feasible use for ciphers, we combine the two.

# Testing

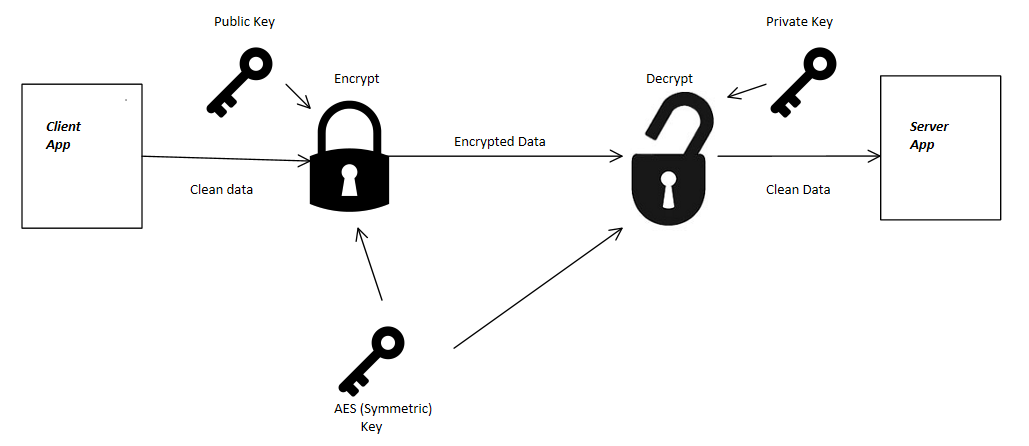
The testing for this project was very simple. The objective was to create an encryption scheme that could encrypt and decrypt text. The resulting unit test simply creates a string, encrypts it, compares it to the original, decrypts it and compares it again. A lot of time was spent attempting to devise a method of generating a symmetric key on separate machines without explicit communication. When these methods failed, or were too obvious to provide adequate security, they were abandoned for the method described in the book.



# 

# Client to Server Encryption

The client to server encryption method makes use of both the symmetric cipher and the public key cipher. By using the public key cipher first, the server can create a key pair and send the pubic key out to the client. The client then creates a symmetric key and uses the public key to encrypt the symmetric key and send the encrypted key back to the server. Next, the server unencrypts the symmetric key. Now, both the server and the client have a matching symmetric key and can send and receive data using the symmetric cipher method. Using this method, the expensive public key encryption is only applied to a small amount of data.



The symmetric cipher was encrypted using the Advanced Encryption Standard (AES) algorithm. A key for the cipher was generated using the SecureRandom generator from the Java API. The public key cipher made use of the RSA algorithm which was invented by Rivest, Shamir and Adleman. This cipher also generated a random key pair using the SecureRandom generator.

Two classes were created to perform the cryptography. The server side class, ServerDecryptor, keeps the private key for the public key cipher and only decrypts messages from the client side application. The client side class, ClientEncryptor, gets the public key for the public key cipher and only encrypts messages to send to the server application. The encryption and decryption methods convert the byte arrays to strings and vice versa to send and receive the information.

The ClientEncryptor was initiated in the client application and encrypts every message before sending it out to the server. Meanwhile, the ServerDecryptor is initiated in the server application and is used to decrypt every message coming from the client.

# Server to Client Encryption

The server to client encryption method also uses the same method of encryption; a symmetric encryption key wrapped by a public key. The main difference is the implementation. The server to client encryption code is implemented as a single class that handles both encryption and decryption.

This Encryption Utility class requires the same steps be taken, but some of the steps are bound together for simplicity of use.

The two constructors initialize the utility for either encryption or decryption. The encryption functionality requires a public key to be passed into the constructor. The constructors call the createKeyPair or generateSymmetricKey depending on how the constructor is called.

The wrapSymmetric method uses the public key provided in the