University of Jeddah
College of Computer Science and Engineering
Department of Cybersecurity
CCCY 312: Cryptography Project
Due date: Jun. 8

Groups

This project is to be done in groups of Three (Maximum). Please note "If you copy the code, share your code, and/or any form of cheating, your project will not be graded".

Project Title: Secure File Transfer using RSA Encryption

Project Description: In this project, students will create a program that can securely transfer files between two computers using RSA encryption. RSA is a widely used public key encryption algorithm that uses two keys, a public key for encryption and a private key for decryption.

Project Requirements:

1. The program should allow the user to select a file to transfer and the public key of the recipient.
2. Implement a key exchange protocol, such as Diffie-Hellman key exchange, to securely exchange the public keys between the sender and the recipient.
3. The program should then encrypt the file using RSA encryption with the recipient's public key or create your own encryption algorithm.
4. The program should transfer the encrypted file to the recipient's computer using a secure connection, such as SSH or HTTPS.
5. The recipient's computer should then use their private key to decrypt the file.

Project Implementation:

1. Start by importing the necessary libraries for RSA encryption, such as `openssl/rsa.h` and `openssl/pem.h`.
2. Define a function that takes two arguments: the file to be encrypted and the public key of the recipient.
3. Use the RSA algorithm to encrypt the file with the recipient's public key, using a block size of 128 bits and padding scheme such as PKCS#1 v1.5 or OAEP.
4. Use a secure connection protocol, such as SSH or HTTPS, to transfer the encrypted file to the recipient's computer.
5. On the recipient's computer, use their private key to decrypt the file, using the same RSA algorithm and padding scheme as before.
6. Test the function by transferring files between two computers and verifying that the files are correctly encrypted and decrypted.

Project Extension: (5 point bonus)

To extend the project, you can work on the following modifications:

1. Add a checksum to the encrypted file to ensure that it has not been tampered with during transfer.
2. Implement a secure file transfer protocol, such as SFTP or SCP, to transfer the encrypted file without relying on a separate secure connection.
3. Apply the encryption technique to a larger dataset, such as a database of sensitive information or a cloud storage service.

Good luck!