Lab 9

Name- Adarsh Nandanwar
BITS ID- 2018A7PS0396G

Public Private RSA Encryption and Decryption in C

Usage Instructions

1. Install OpenSSL library.
2. Open a terminal window in the directory containing `encrypt.c` and `decrypt.c` file.
3. Ensure the directory contains the required keys: `public.pem` and `private.pem`
4. Compile the c programs.

```
$ gcc encrypt.c -o encrypt -lcrypto -lssl
$ gcc decrypt.c -o decrypt -lcrypto -lssl
```

5. Encrypt the input file using the executable `encrypt`. Parameters: {public_key, input_file_name, encrypted_file_name}

```
$ ./encrypt public.pem input_file.txt encrypted_file.txt
```

6. Decrypt the encrypted file using the executable `decrypt`. Parameters: {private_key, encrypted_file_name, decrypted_file_name}

```
$ ./decrypt private.pem encrypted_file.txt decrypted_file.txt
```

Generating Keys

- The RSA key was geenrated using;

```
$ openssl genrsa -out private.pem 10000
$ openssl rsa -in private.pem -pubout -out public.pem
```

- `RSA_PKCS1_PADDING` padding was used in the program. Using this, maximum input file size that can be encrypted using RSA is:

```
max_input_size (in bytes)
    = (key_size/8)-11
    = (10000/8)-11
    = 1239
```