INTRODUCTION TO CRYPTOGRAPHY – LAB 5

B.Tech. Computer Science and Engineering (Cybersecurity)

|  |  |
| --- | --- |
| Name: Anish Sudhan Nair | Roll No.: K041 |
| Batch: K2/A2 | Date of performance: 09/02/2022 |

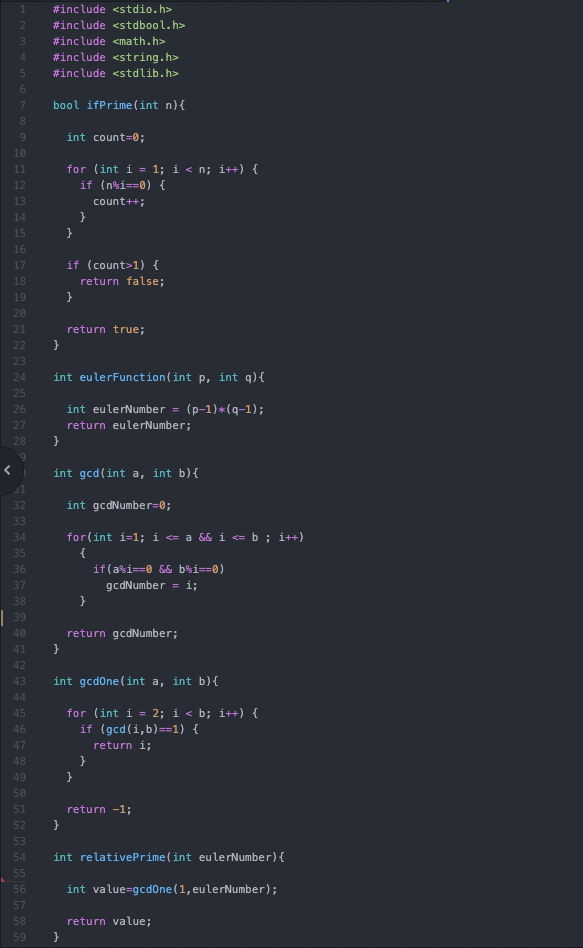
Aim: To code the RSA algorithm

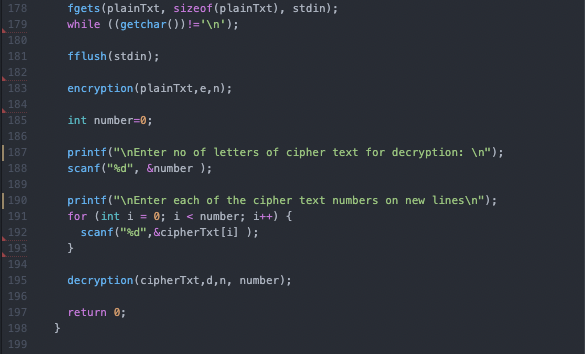
**Code:**

Language: C

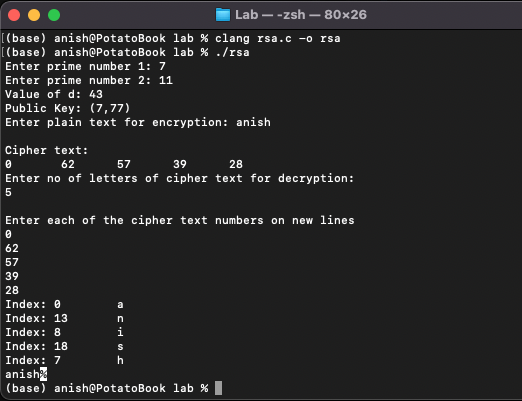
Editor: Atom

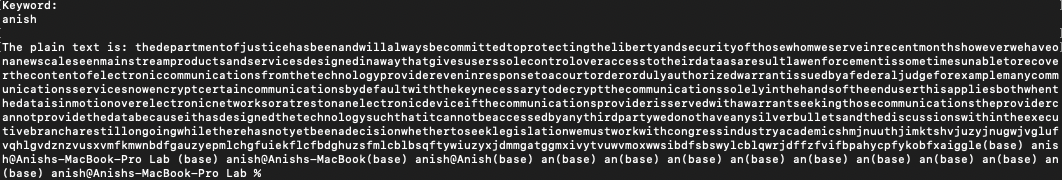
Compiler: clang/ZSH





**Complete Output:**





Questions:

1. Compare and contrast symmetric key encryption and asymmetric key encryption.

The Diffie-Hellman key exchange algorithm enables encrypted communication over an unsafe channel by using a public key.

Consider two user Anish and Hasin, who wish to communicate over a channel. In DH algorithm, each user would have a private key generated for them that is not disclosed to anyone. Using the private key and publicly informed prime numbers they each generate a key which they then share with each other. Using this shared key, their private key and the prime numbers, they generate the symmetric key which is used for encrypting and decrypting their messages.

2. Explain few of the applications of RSA.

- Secure Shell (SSH) [More secure than Telnet]

- Internet Protocol Security (IPSec)

- Transport Layer Security (TLS)

3. List advantages and limitations of RSA.

Advantages:

* It provides a symmetric key which enables communication in insecure channels
* Due to the symmetric key exchange the users need not necessarily know each other
* The keys are generated using large numbers and so manually cracking them is quite exhaustive

Disadvantages:

* It can only be used for symmetric key exchange
* It is very resource exhaustive (computational power)
* The algorithm itself does not perform the encryption
* There is no authentication process involved opening vulnerabilities for Man in the Middle Attacks

4. What are the most popular values of e in practice? Why?

5. Why does decryption using RSA take more time as compared to encryption?