CSCI 6708 Assignment-5

Manan Amin (B00897712)
mn959427@dal.ca

Exercise 1: AES (Advanced Encryption Standard)

Overview :

- It’s a standard Symmetric Encryption technique to protect digital data standardized by NIST.
- It is a block encryption technique that encrypts plaintext by dividing it into 128 bits of block and uses the key of variable length depending upon requirements.

Features:

- It has been implemented in both hardware and software, it makes AES very fast because of hardware-level instructions available in the CPU.
- There aren’t any practical attacks found for AES which makes it robust.
- Basically, AES performs some mathematical operations on the Galois field(Finite Field).

Algorithms:

1. SubBytes: In this operation, Bytes would be shuffled accordingly substitution table. The lookup table is designed in such a way that it does not have a linear relationship between input and output.
2. Shift rows: In this operation, Rows would be shifted. All rows shifted in different numbers thus, it will create some random shuffle.
3. MixColumns: This operation will map each column bytes using a non-linear function. Operation look similar to matrix multiplication using XOR and modulo operation to avoid overflow.
4. Addroundkey: XOR operation with the encryption key.

AES security :

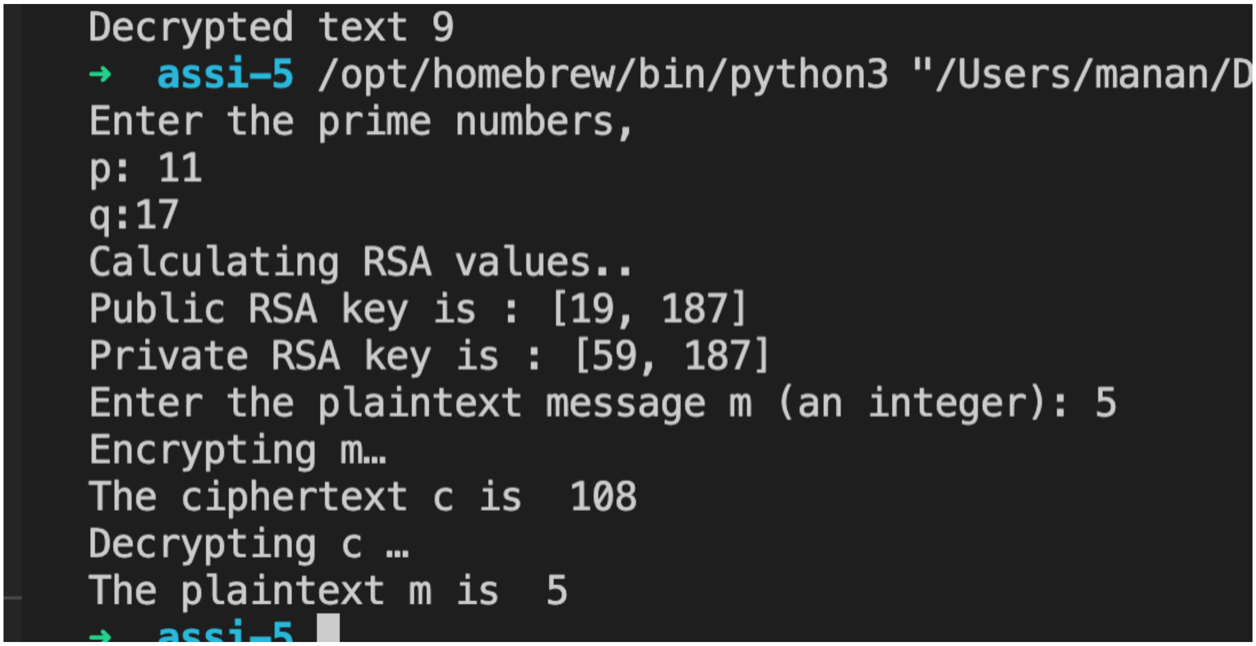
Advantages

- It uses key size >=128 bits which makes it really hard to brute force with any machine.
- There have not been any practical cryptanalytic attacks against AES.
- It supports a larger size of keys for more security.
- It is fast as most modern CPUs support AES-related instructions.

Drawbacks

- It uses simple algebraic functions to encrypt.
- All blocks and each round are encrypted in the same way.
- It is a symmetric encryption algorithm thus, System needs an additional method or channel to exchange keys.

Exercise 2 (RSA):



```
Decrypted text 9
→  assi-5 /opt/homebrew/bin/python3 "/Users/manan/D
Enter the prime numbers,
p: 11
q:17
Calculating RSA values..
Public RSA key is : [19, 187]
Private RSA key is : [59, 187]
Enter the plaintext message m (an integer): 5
Encrypting m…
The ciphertext c is  108
Decrypting c …
The plaintext m is  5
→  assi-5
```

References:

[1] “Advanced encryption standard,” Wikipedia, 30-Mar-2022. [Online]. Available: https://en.wikipedia.org/wiki/Advanced_Encryption_Standard. [Accessed: 04-Apr-2022].

[2] M. Pound, “AES Explained (Advanced Encryption Standard) - Computerphile.” [Online]. Available: https://youtu.be/xy6ooR9urFE. [Accessed: 04-Apr-2022].

[3] “RSA explained in python,” Gist. [Online]. Available: https://gist.github.com/tylerl/1239116/8d9d75de90a37112be665a2aa1478eabfbdd6087. [Accessed: 04-Apr-2022].