Introduction to Cryptography Techniques

Assignment-1

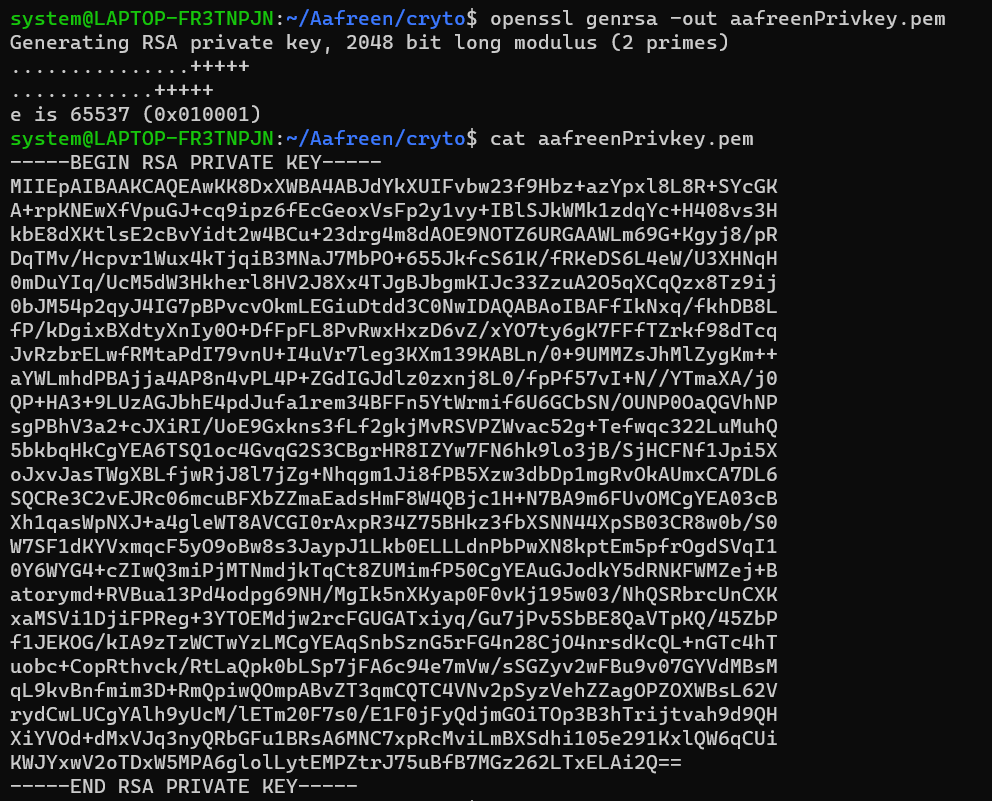
**Name:** AAFREEN.M

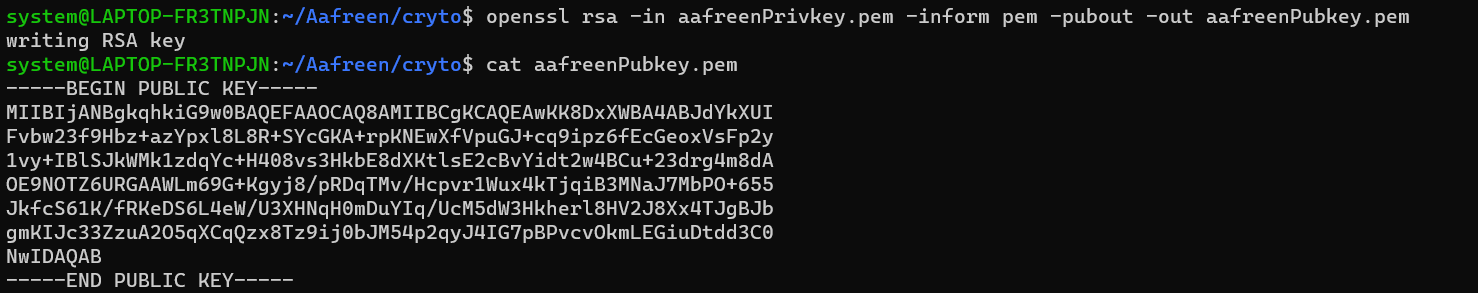
**Reg.No:**205001301

**Question No: I**

**a. Implement one Key Generation algorithm and generate the key pairs and evaluate their performance in terms of Computational Time, Computational complexity. Identity the limitations of each algorithm**

We are using RSA algorithm to create a private key, public key pair





This is a public-key generation algorithm. Other examples are Elliptic Curve Digital Signature Algorithm, Edwards-curve Digital Signature Algorithm (EdDSA)

Compared to Elliptic Curve Digital Signature Algorithm, RSA is been for a long time and have been tested more than ECDSA. It is well studied and audited algorithm.

RSA is simpler compared to other algorithms. It is easy to implement in a public key infrastructure.

But ECDSA required shorter key length compared to RSA

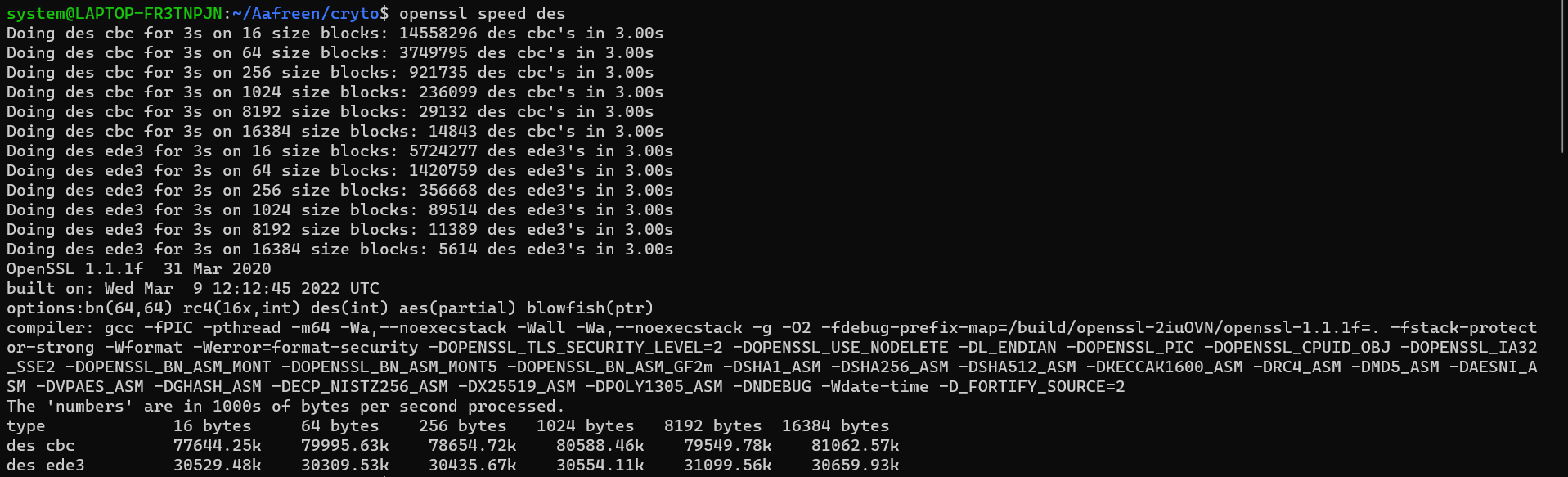
Private key algorithms is a single key infrastructure. A single key is used for communication.

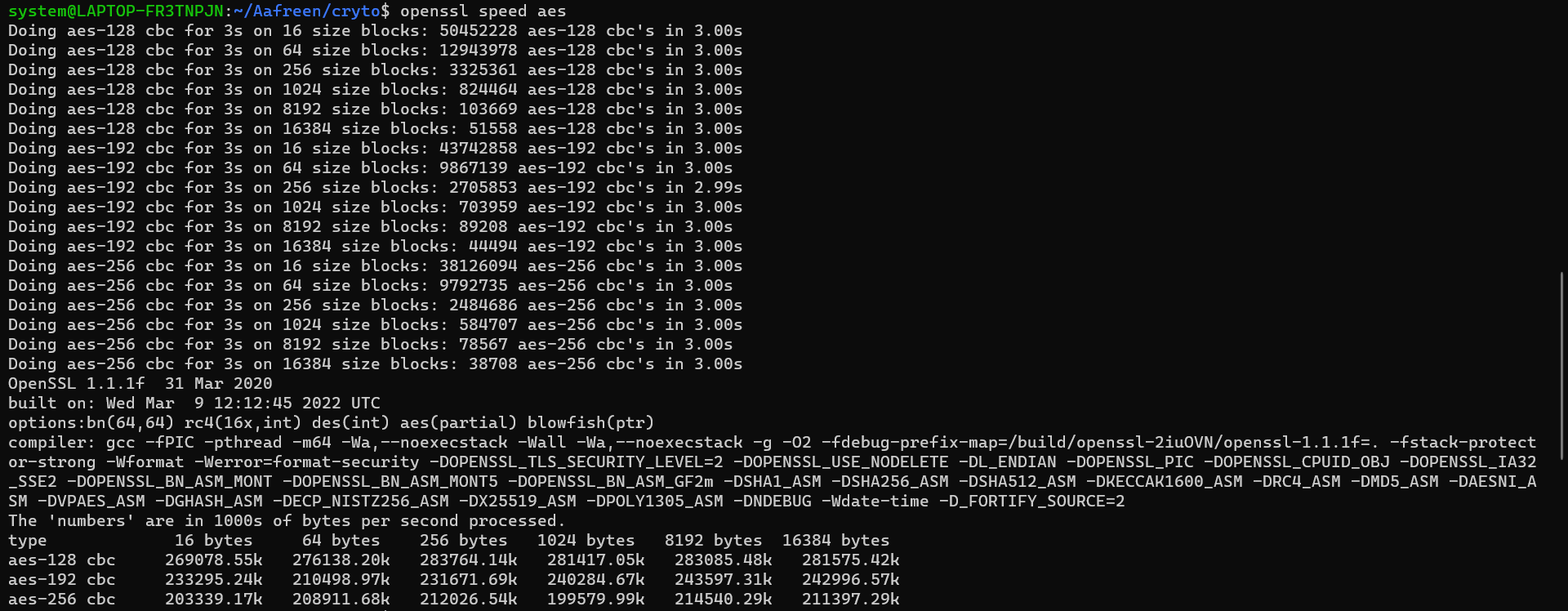
Same key is used to encrypt and decrypt the message. There are many private key algorithms such as AES , DES.

Public key cryptography is used to share the keys of private key cryptography.

Private key cryptography is faster than public key cryptography. Hence public key cryptography should be used to exchange keys and further communication should proceeded with private key cryptography.

SPEED

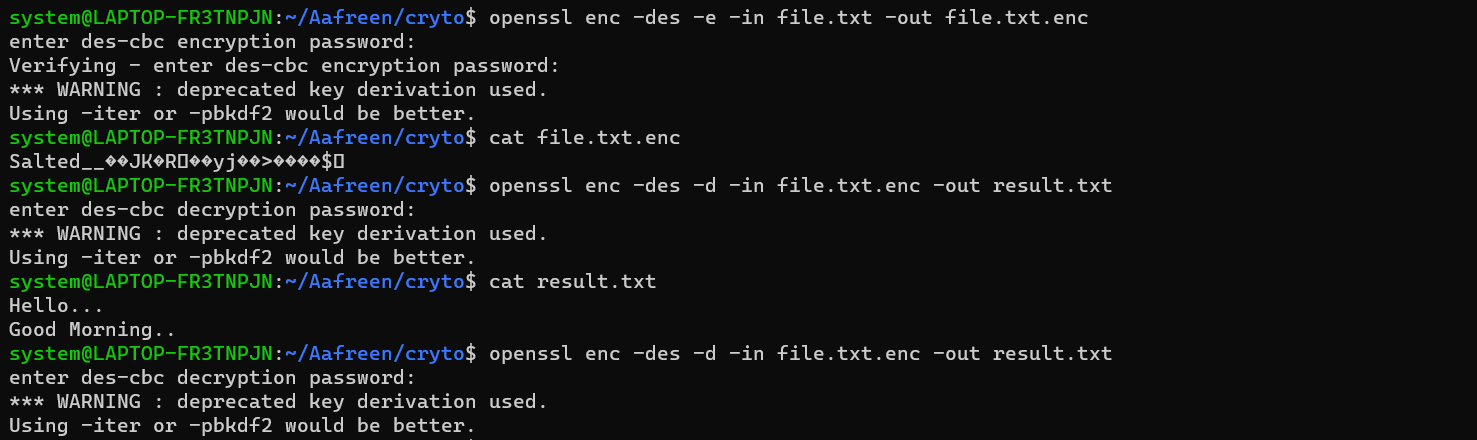






**b) Using the above keys, encrypt a given message and evaluate various techniques to ensure the integrity of the data. Identity the deficiency of each approach.**

Using DES to encrypt and decrypt



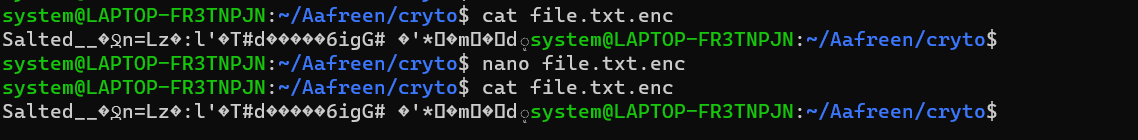
Using RSA encryption

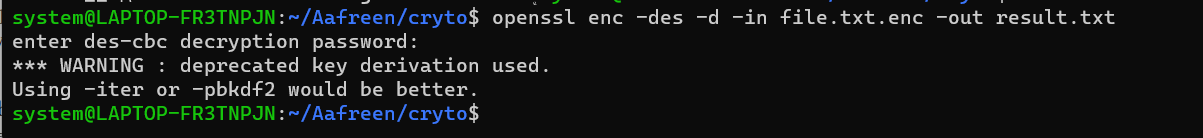


As we can see, by entering a wrong password or using wrong key, the contents of the cipher text is unavailable.

Hence the password(private key encryption) or private key should be known to decipher the text.

By changing the contents of cipher text, the content cannot be decipherd.





**c) Identify the need for each approach and comprehend its significance.**

**DES** -> Data encryption standard. It is a symmetric key block cipher.

Plaintext is divided into two halves in DES encryption, and then DES uses a 64-bit plaintext and a 56-bit key to generate a 64-bit ciphertext, which is an encrypted representation of the data.

The key length used for encryption in DES is 56 bits, although the block size is 64 bits .DES entails 16 rounds of identical procedures, regardless of key length.

Because the amount of operations in DES is fixed and no permutation combinations are permitted, it is easier to break the encryption, making it less secure than AES.

**AES** -> Advanced Encryption Standard developed after DES. AES is currently implemented world wide both in hardware and software.

AES uses a 128-bit plaintext and a 128-bit secret key to create a 128-bit block, which is then processed to produce 16 bytes (128-bit) ciphertext.

In the case of AES, the key length might be 128 bits, 192 bits, or 256 bits, with 10 rounds (128 bits), 12 rounds (192 bits), or 14 rounds (256 bits).

AES, on the other hand, is more secure than DES encryption and has become the de facto international standard.

**RSA** ->RSA is widely used for secure data transmission. 2 keys are generated. One is public known to all while other is private. Message to the owner is encrypted using public key and only the owner can decipher using private key.

The owner can use the private key as a digital signature which can be verified by the public using public key.

The security of RSA relies on the practical difficulty of factoring the product of two large prime numbers. It is a slow algorithm compared to others.

**Elliptic Curve Cryptography** -> It is a key-based technique for encrypting data. ECC focuses on pairs of public and private keys for decryption and encryption of web traffic.

Unlike RSA , it is more powerful. ECC has grown in popularity due to its smaller key size and ability to maintain security. ECC bases its approach to public key cryptographic systems on how elliptic curves are structured algebraically over finite fields. Therefore, ECC creates keys that are more difficult, mathematically, to crack.