National University
of computer and emerging sciences

ASSIGNMENT 1

INFORMATION SECURITY

Muhammad Ayaz Hasan [20k-1044]

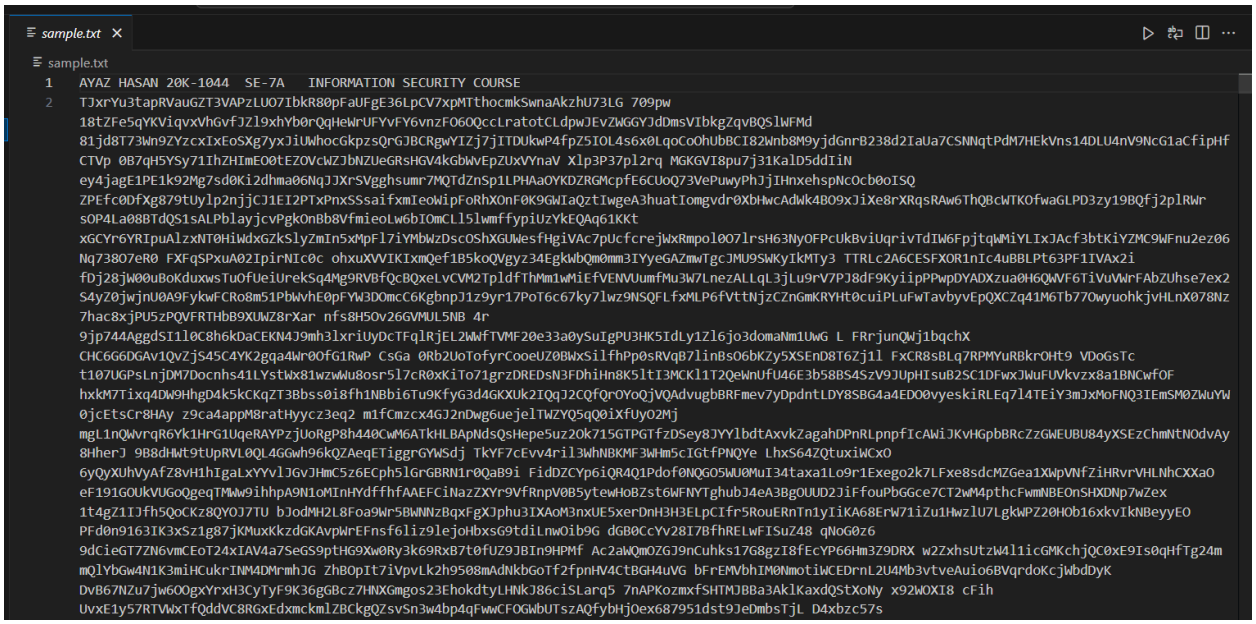
SE-7A

Submitted to:
Dr.Abdul Aziz

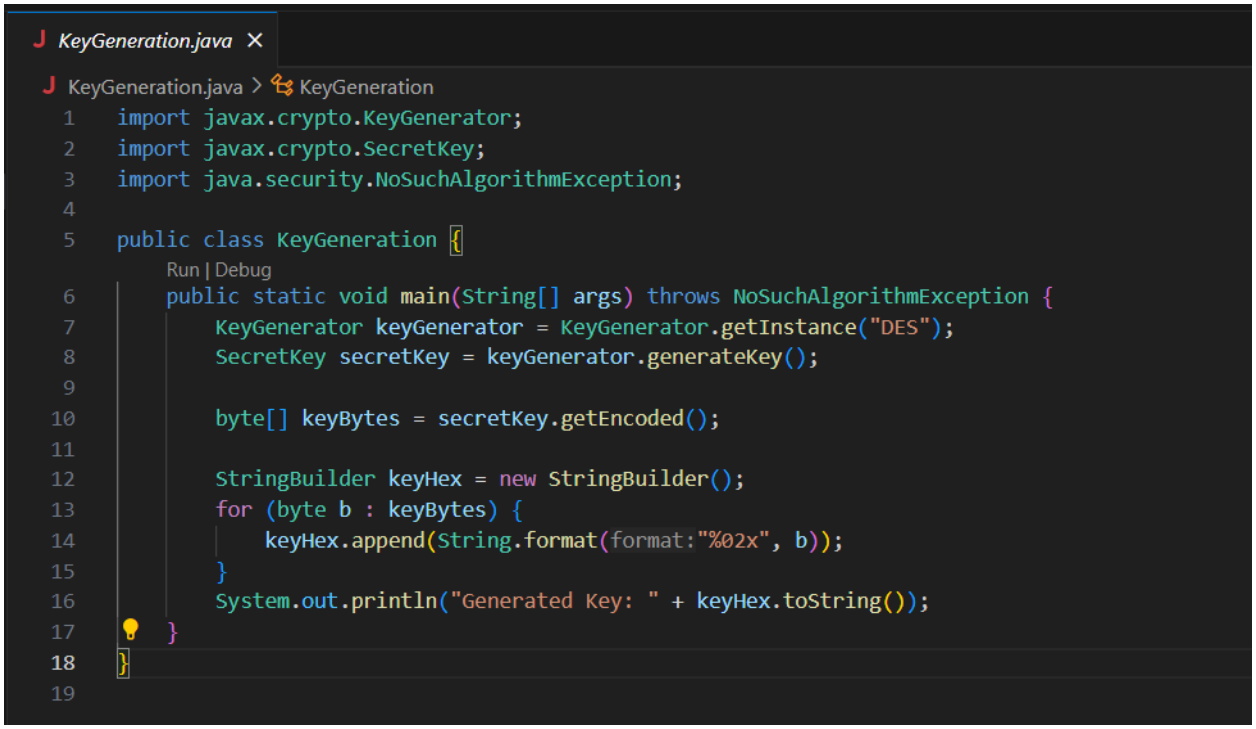
FAST-NUCES Karachi

DES ENCRYPTION/DECRYPTION(TXT FILE)

We have a Text file (sample.txt) with dummy data of upto size 10 mb.



First we generate the secret key:



```
gram Files\Java\jdk-19\bin\java.exe' '-XX:+ShowCodeDetailsInExceptionMessag
ca0830329e7734870d4b9fb7018fc4\redhat.java\jdt_ws\ASSIGNMENT 1_ea12118d\bin
Generated Key: f4196e85cbbcd99d
```

The above generated key will be use for encryption and decryption.after run the file we will have two file generated encrypt.txt (having encrypted data),decrypt.txt (having decrypt/plain text)

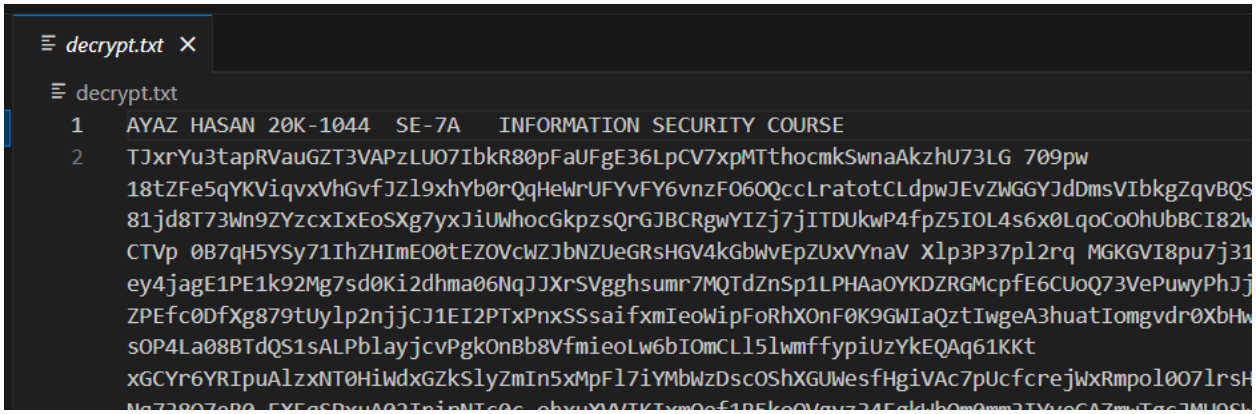
DesEncryption.java

```java
import javax.crypto.Cipher;
import javax.crypto.SecretKey;
import javax.crypto.SecretKeyFactory;
import javax.crypto.spec.DESKeySpec;
import java.io.*;
import java.security.spec.KeySpec;

public class DesEncryption {

    Run | Debug
    public static void main(String[] args) throws Exception {
        String inputFile = "sample.txt";
        String encryptedFile = "encrypt.txt";
        String decryptedFile = "decrypt.txt";
        String secretKey = "f4196e85cbbcd99d";
```

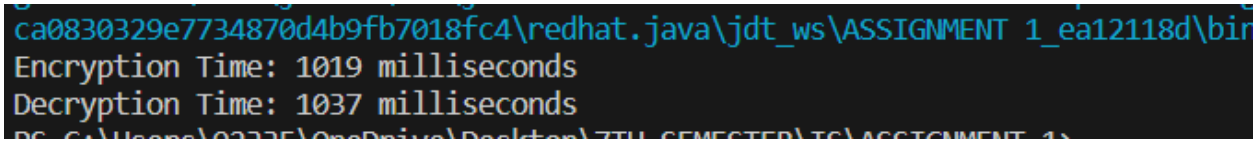
encrypt.txt

This document contains many invisible unicode characters Disable Invisible Highlight

```
GS␂B␂␂5␂'EMd"k␂␂␂␂␂q␂%␂␂␂␂␂?␂SUB␂␂␂c␂h␂WSYN␂]NUL␂FS␂
0␂d␂␂␂DC1␂]iψS␂␂␂FF␂Lp␂␂\␂GS␂
0␂29z␂␂␂S*␂␂␂u␂␂f$␂␂␂␂␂␂␂␂e]{.US␂,STX␂
M52␂P␂␂e>5~x␂␂4g␂@␂DEL␂ dRS␂{␂z%␂␂␂8l_ENQ␂$SUBSTX␂T␂(#␂VVnË2
␂DUE␂␂␂P1␂␂7␂ETBH%eDGSENQVTpA"9␂|FS␂]o
␂%SI1␂!␂␂␂U␂␂␂3␂␂␂9␂9rô␂␂␂?STXSTX␂␂&-k,␂ETBM␂␂␂␂␂`␂A␂C␂o␂␂UÃ␂␂␂␂SP␂)␂␂<␂3hRS␂ESCB␂Ni␂|␂G
sSIDC2␂4CAN␂I␂>␂R␂8␂L␂EM␂/␂SGSIx
3NAKlFFSv␂VENQ␂GS␂ESCt␂␂*␂SI␂x␂␂^␂NUL␂NAKDC3SDC1␂ßRS.␂uB␂)␂U␂␂ſ␂ZNAKWnc
,␂PØ␂␂ETB␂␂␂␂T␂n␂NUL␂␂ESCßNAKL!␂)e␂BSk␂␂\␂d2␂␂ţ␂;␂(␂␂␂SI␂␂Ж[␂z␂␂␂;␂␂
␂␂␂G(SO¾␂k␂_~␂#SOoY␂␂SOH␂␂␂u␂O␂␂␂C\n5␂ff_>␂%@+FSO␂␂$Uc_␂␂␂ˆ␂EOTüH␂␂oy␂␂π_V␂␂kW␂;SI␂␂S
EMSYN␂GSk␂␂p␂␂␂␂C␂BEL␂_␂␂9␂␂Y␂␂LBSM14ACK␂43␂rs␂␂SOH␂G]DC1␂T␂␂!EOT␂q␂FFtg␂␂:y&␂N0¼␂SSUB␂␂␂␂
K␂USCSUBN;DC1␂>␂␂ o‹S3lp␂␂ ␂DC4␂ETBGS␂;_␂␂&␂<␂NUL␂β␂␂0KMJ␂BSg␂PS5␂␂[␂i␂␂␂w8ZEM\␂␂␂G_␂$ˆ
␂␂␂␂dHY␂␂z␂RSa7␂fa␂ESC␂p?␂=X␂L␂%$È␂T␂aFFC>US␂␂y␂␂␂␂␂RS␂ ␂␂␂␂CwVT␂ETB␂␂ d␂␂␂SEOT␂US␂
␂l␂␂␂␂J␂ETXV␂␂␂/␂c␂a&␂␂␂␂{0DC3␂␂␂␂␂␂\b[␂␂␂L␂␂BQOY|@B)␂␂'VT␂K␂␂VTDC4aFS␂␂1␂␂DC3CTSzDC4␂
b␂␂h,␂0J␂␂␂V␂
j␂!␂9␂\FFESCDSIv␂";␂祠␂i"␂5␂&&0␂␂␂␂RSk␂␂␂␂␂␂]␂␂␂␂BSENQ␂SUB␂␂^␂␂␂␂␂W;V~␂␂lACK␂STX␂␂␂X"␂
i7␂NUL47n␂␂SYNA`␂;␂␂u␂*␂␂EOT␂[j"O␂␂␂␂␂R␂GSCY␂q␂_BSəf␂H␂S␂␂f(5C␂=␂␂␂EM␂j%K␂US␂dDC4@QSl␂␂#[
␂~
```



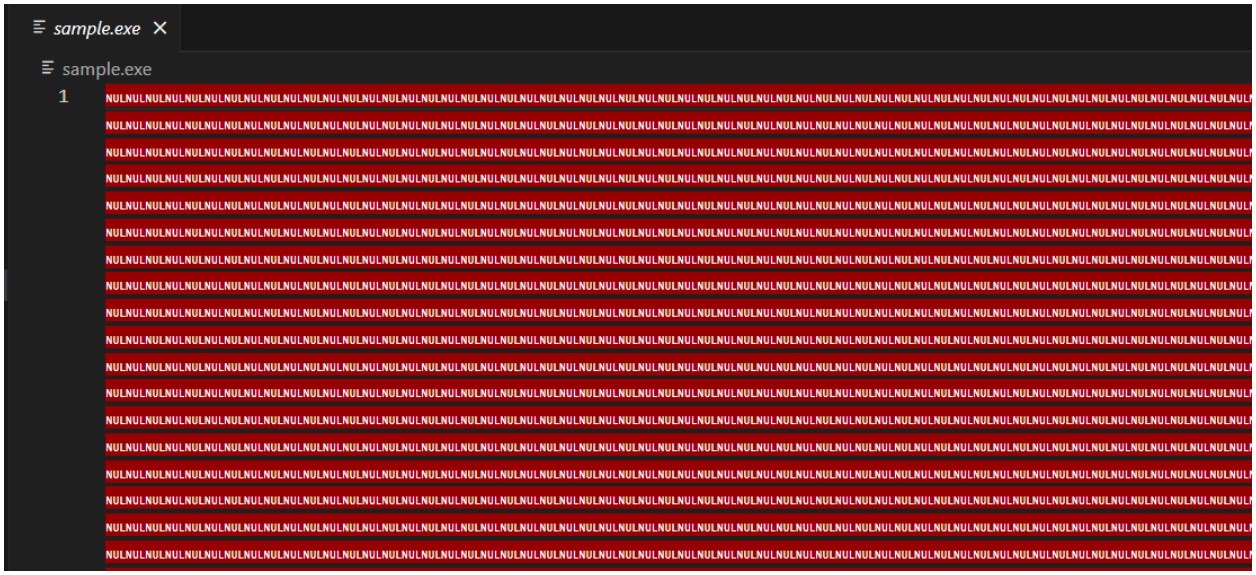
Also we will get the total encryption and decryption time



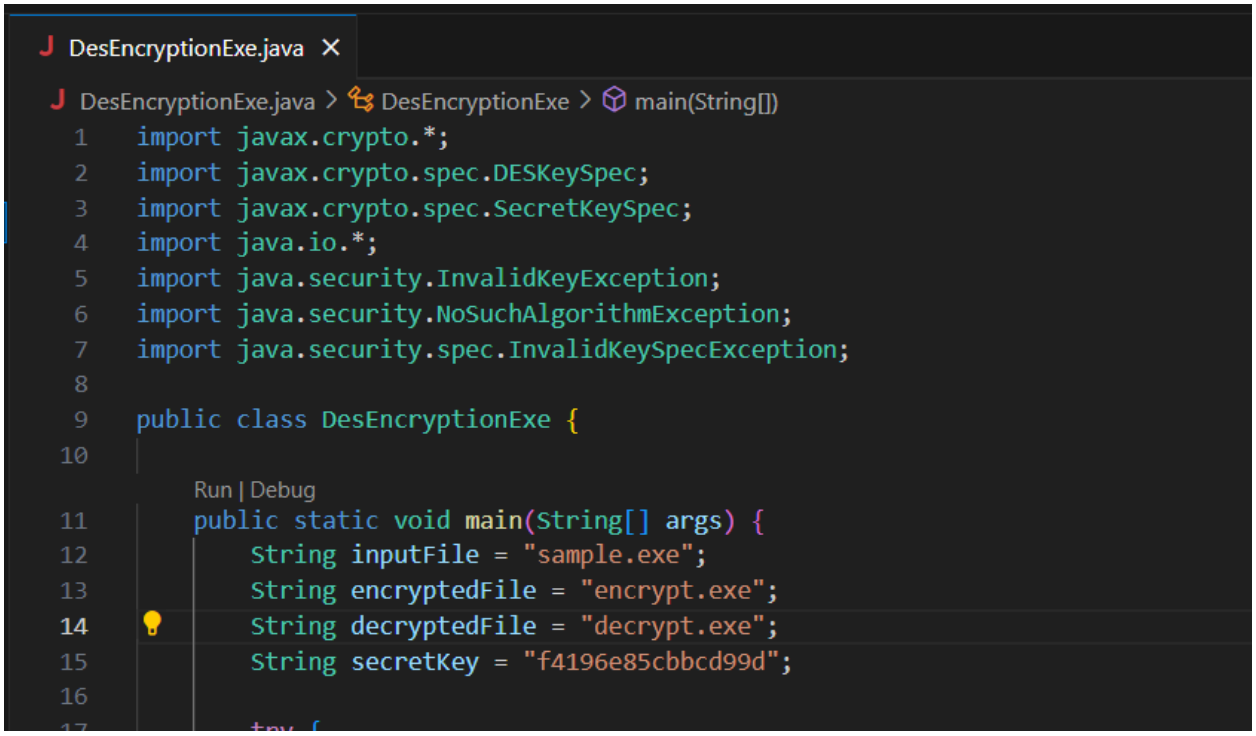
DES ENCRYPTION/DECRYPTION(EXE FILE)

First we generate the exe file(sample.exe) as it is complex to get it from online resources due to its unsecure

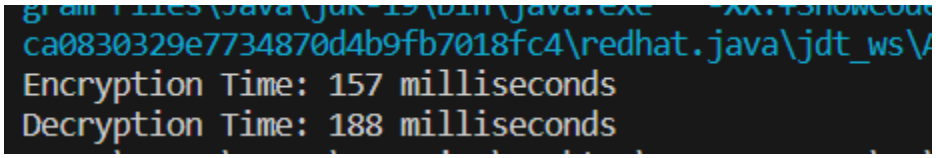
Here we have dummy exe file



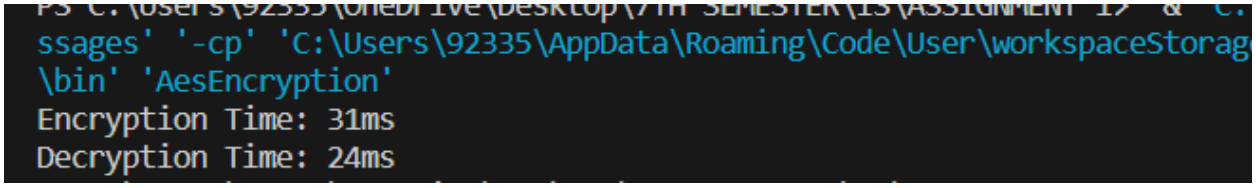
Now after run the DES .we got two file encrypt.exe(for encrypted data)and decrypt.exe(for decrypted data)



Here is the total time for running this algorithm



AES ENCRYPTION/DECRYPTION(TXT FILE)



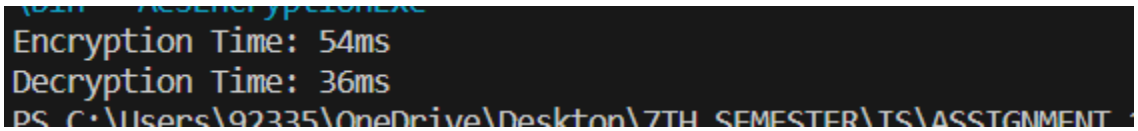
AesEncryption.java

```java
import javax.crypto.Cipher;
import javax.crypto.spec.SecretKeySpec;
import java.io.*;
import java.security.Key;

public class AesEncryption{
    Run | Debug
    public static void main(String[] args) {
        try {
            byte[] keyBytes = "f4196e85cbbcd99d".getBytes();
            Key secretKey = new SecretKeySpec(keyBytes, "AES");

            Cipher cipher = Cipher.getInstance("AES");

            File inputFile = new File(pathname:"sample.txt");
            FileInputStream inputStream = new FileInputStream(inputFile);
            byte[] inputBytes = new byte[(int) inputFile.length()];
            inputStream.read(inputBytes);
            inputStream.close();

            long startTime = System.currentTimeMillis();

```

AesEncryption.java | encrypt.txt

encrypt.txt

AES ENCRYPTION/DECRYPTION(EXE FILE)



AesEncryptionExe.java

```java
import javax.crypto.Cipher;
import javax.crypto.spec.SecretKeySpec;
import java.io.*;
import java.security.Key;

public class AesEncryptionExe {
    Run | Debug
    public static void main(String[] args) {
        try {
            byte[] keyBytes = "f4196e85cbbcd99d".getBytes();
            Key secretKey = new SecretKeySpec(keyBytes, "AES");

            Cipher cipher = Cipher.getInstance("AES");

            String inputFile = "sample.exe";
            String encryptedFile = "encrypt.exe";
            String decryptedFile = "decrypt.exe";

            long startTime = System.currentTimeMillis();

            cipher.init(Cipher.ENCRYPT_MODE, secretKey);

```

AesEncryptionExe.java | encrypt.exe

encrypt.exe

```
1   ?`gs!???#?   b
2   syn$c?`gs!???#?    b
3   syn$c?`gs!???#?    b
4   syn$c?`gs!???#?    b
5   syn$c?`gs!???#?    b
6   syn$c?`gs!???#?    b
7   syn$c?`gs!???#?    b
8   syn$c?`gs!???#?    b
9   syn$c?`gs!???#?    b
10  syn$c?`gs!???#?    b
11  syn$c?`gs!???#?    b
12  syn$c?`gs!???#?    b
13  syn$c?`gs!???#?    b
14  syn$c?`gs!???#?    b
15  syn$c?`gs!???#?    b
16  syn$c?`gs!???#?    b
17  syn$c?`gs!???#?    b
18  syn$c?`gs!???#?    b
19  syn$c?`gs!???#?    b
```