Team:

Ajit Sunil Wadalkar
Ambika Koushik
Kranthi Rekha Rudraraju

Project Implementation:

Operating System: Windows 10, Elementary OS

Programming Language: Java 8

Crypto Libraries Used:
javax.crypto.*; javax.crypto.spec.IvParameterSpec; javax.crypto.spec.SecretKeySpec; javax.xml.bind.DatatypeConverter; java.security.InvalidKeyException; java.security.NoSuchAlgorithmException; java.security.SecureRandom

Generation of keys:

This function is called when choose option 1 to generate keys. It takes a lambda value as an input and generates 2 keys, one for PRF and one for AES and writes them to corresponding text files (skprf.txt and skaes.txt). The output when lambda is chosen as 128 is as below

```
Following are the functionalities in the code, choose anyone:
1.Generate Keys
2.Print Inverted Index
3.Generate Encrypted Inverted Index and Encrypt Files
4.Token Generation
5.Search token
6.Exit
Please choose the value in between 1,2,3,4,5 or 6
1

------------------------------------------------------------------------------------------------------------------------------------------------------------------------
Selected Function is Generate Keys.
 Please enter the value of lambda, suggested values:128,192,256
128
The function took 0.499088897 seconds to execute.
AES Key: 5ACD5D944DEF65E1814A180B7DA6FC1B
PRF Key: 69F3C413F1CEB1088E540406314AE2C3
------------------------------------------------------------------------------------------------------------------------------------------------------------------------

Do you want to re-run the program?
Please choose from the following.
1. Yes
2. No
```

Printing Inverted Index:

This function is called when option 2 for printing plain index is chosen. This prints the inverted index for the plain text.

```
Following are the functionalities in the code, choose anyone:
1.Generate Keys
2.Print Inverted Index
3.Generate Encrypted Inverted Index and Encrypt Files
4.Token Generation
5.Search token
6.Exit
Please choose the value in between 1,2,3,4,5 or 6
2

----------------------------------------------------------------------------------------------------------------------------------------------------------------
Invertedindex for plaintext:
bengals f1.txt f4.txt f6.txt
packers f1.txt f2.txt f3.txt f5.txt
steelers f1.txt f4.txt f5.txt
patriots f2.txt
----------------------------------------------------------------------------------------------------------------------------------------------------------------
```

Generating encrypted inverted index and encrypting files:

This function is called when option 3 is chosen. This function generates the encrypted by reading all the files and the keys generated. This function also encrypts the data files and writes the cipher texts to encrypted files. The encrypted index is written to index.txt file. The output of the function is as shown below

```
Following are the functionalities in the code, choose anyone:
1.Generate Keys
2.Print Inverted Index
3.Generate Encrypted Inverted Index and Encrypt Files
4.Token Generation
5.Search token
6.Exit
Please choose the value in between 1,2,3,4,5 or 6
3

----------------------------------------------------------------------------------------------------------------------------------------------------------------
Selected Function is Generate Encrypted Inverted Index and Encrypt Files
The function took 0.582561432 seconds to execute.
Generated Inverted Index is:
4D76F2FE2D5DFB84F8A99B49D066ACC8 c1.txt c4.txt c6.txt
1EBFC7DAF333CDFD68E80935C39677AB c1.txt c2.txt c3.txt c5.txt
085C6EF39D3ECCD75047EEF71171B097 c1.txt c4.txt c5.txt
821B48BAA5A798ED4A1B1BABB837A301 c2.txt
----------------------------------------------------------------------------------------------------------------------------------------------------------------
```

Time Taken: This function also logs the time taken for the generating encrypted index and also encrypting all the data files . The time logged is **0.582561432 seconds** as shown above.

Token Generation:

This function is called when option 4 in chosen from the console. We need to input a word that is to be searched. For the given word and the secret key from skprf.txt, a token is generated and written to the text file token.txt.

```
Following are the functionalities in the code, choose anyone:
1.Generate Keys
2.Print Inverted Index
3.Generate Encrypted Inverted Index and Encrypt Files
4.Token Generation
5.Search token
6.Exit
Please choose the value in between 1,2,3,4,5 or 6
4

---------------------------------------------------------------------------------------------------------------------------------------------------------
Selected Function is Token Generation Function.
Please enter word you want to search.
bengals
The token generated is 4D76F2FE2D5DFB84F8A99B49D066ACC8
The function took 0.390615986 seconds to execute.
---------------------------------------------------------------------------------------------------------------------------------------------------------
```

Search Function:

This function will be called when you choose option 5 to search token from the console. This function takes the encrypted index from index.txt and token that has been generated from token.txt. It finds all the files with the token over encrypted index, decrypts the encrypted files using AES-CBC-256 and prints them in terminal and writes the result to result.txt file.

```
Following are the functionalities in the code, choose anyone:
1.Generate Keys
2.Print Inverted Index
3.Generate Encrypted Inverted Index and Encrypt Files
4.Token Generation
5.Search token
6.Exit
Please choose the value in between 1,2,3,4,5 or 6
5

---------------------------------------------------------------------------------------------------------------------------------------------------------
Selected Function is Search Token
c1.txt c4.txt c6.txt
c1.txt bengals steelers packers
c4.txt steelers bengals
c6.txt bengals
The function took 0.413469061 seconds to execute.
---------------------------------------------------------------------------------------------------------------------------------------------------------
```

Search Time for keyword “packers”:

```
--------------------------------------------------------------------------------------------------------------------------------------------------------
Selected Function is Token Generation Function.
Please enter word you want to search.
packers
Saved token is: FCFFE05BF5D946D7E460FDEB01DD04E4
The function took 0.305434013 seconds to execute.
--------------------------------------------------------------------------------------------------------------------------------------------------------

Do you want to re-run the program?
Please choose from the following.
1. Yes
2. No
1

Following are the functionalities in the code, choose anyone:
1.Generate Keys
2.Print Inverted Index
3.Generate Encrypted Inverted Index and Encrypt Files
4.Token Generation
5.Search token
6.Exit
Please choose the value in between 1,2,3,4,5 or 6
5

--------------------------------------------------------------------------------------------------------------------------------------------------------
Selected Function is Search Token
c3.txt c2.txt c5.txt c1.txt
c3.txt packers
c2.txt packers patriots
c5.txt steelers packers
c1.txt bengals steelers packers
The function took 0.00747914 seconds to execute.
--------------------------------------------------------------------------------------------------------------------------------------------------------

Do you want to re-run the program?
Please choose from the following.
1. Yes
2. No
```

The search time for keyword packers which includes the time to find those encrypted files and the time to decrypt those files is **0.305434013 seconds**.