CSE439 COMPUTER SECURITY

A BASIC HOST BASED IDS TERM PROJECT

HÜRKAN UĞUR 20160702051

DATA STRUCTURES

```
public class HostBasedIDS

private static ArrayList<String> originalFileLocations = new ArrayList<String>(); //[Directory\hurkanugur.txt]

private static HashMap<String,byte[]> originalFileContents = new HashMap<String,byte[]>(); //[KEY: Directory\hurkanugur.txt]

private static HashMap<String,String> backupFileLocations = new HashMap<String,String>(); //[KEY: Directory\hurkanugur.txt]

private static HashMap<String,String> backupFileLocations = new HashMap<String,String>(); //[KEY: Directory\hurkanugur.txt]

private static HashMap<String,byte[]> backupFileContents = new HashMap<String,byte[]>(); //[KEY: Directory\$Directory\substruction;
```

String originalDirectoryLocation [HUKO]

Contains the path of the directory that contains original files.

String backupDirectoryLocation [HUKO\\$HUKO]

Contains the path of the backup directory that contains encrypted files.

ArrayList<String> originalFileLocations [HUKO\cse.mp3]

Contains the location of the original files.

<u>HashMap<String, byte[]> originalFileContents</u> [K= HUKO\cse.mp3][V= BINARY DATA]

Contains the data of original files.

<u>ArrayList<String</u>, <u>String> backupFileLocations</u> [K= HUKO\cse.mp3][V= HUKO\\$HUKO\\$cse.mp3]

Contains the location of the encrypted backup files.

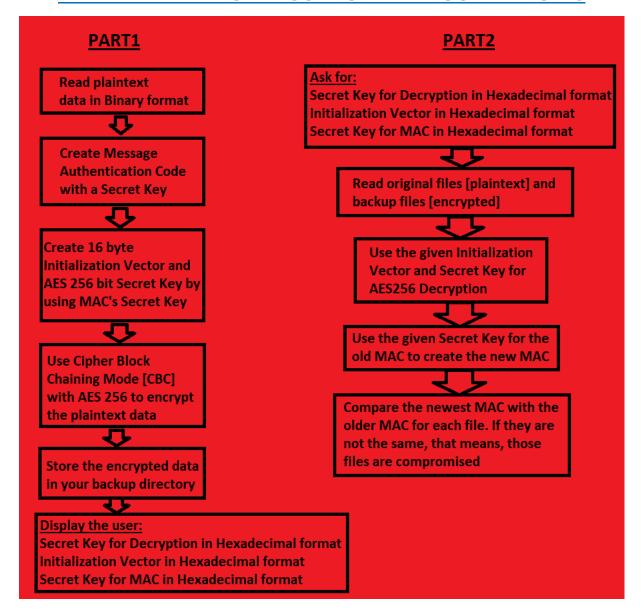
HashMap<String, byte[]> backupFileContents [K = \$HUKO\\$cse.mp3][V = BINARY DATA]
Contains the data of the encrypted backup files.

CLASSES AND METHODS

```
public class HostBasedIDS
                                                     MY OWN AES-256 BIT ENCRYPTION CLASS
    public static class HukoAES256□
    public static boolean ReadOriginals()[
   public static boolean StoreBackup()[
    public static boolean ReadBackup()
    public static String ConvertByteArrayToHexadecimalString(byte[] byteArray) []
   //CONVERT HEX VALUE STRING -> BYTE[]
public static byte[] ConvertHexadecimalStringToByteArray(String hexadecimalString) []
   public static SecretKey SecretKeyGenerator()[
    public static boolean CreateMessageAuthenticationCode()
    public static void ControlMessageAuthenticationCode()[]
public static void main(String[] args) []
 //AES256 ENCRYPTION & DECRYPTION CLASS
      private static SecretKey secretKey = null;
     private static IvParameterSpec initializationVector = null;
     private static String hexadecimalStringSecretKey = null;
      private static String hexadecimalStringInitializationVector = null;
```

```
public static SecretKey GetSecretKeyOfAES256()[]
public static void SetSecretKeyOfAES256(SecretKey secretKey)[]
public static String GetHexSecretKeyAES256()[
public static void SetHexSecretKeyAES256(String secretKey) throws Exception.
private static IvParameterSpec InitializationVectorGenerator() throws Exception[]
public static String GetHexInitializationVector()[
private static void SetHexInitializationVector(String initializationVector) throws Exception
public static void GenerateAES256SecretKeyFromMACSecretKey(String MAC_SECRET_KEY)[]
public static byte[] EncryptionWithAES256(byte[] Data)[]
public static byte[] DecryptionWithAES256(String Data) throws Exception.
```

A BRIEF EXPLANATION ABOUT HOW MY PROGRAM WORKS



PART1: CREATING BACKUP OF THE ALL FILES IN THE DIRECTORY

Dosya Düzen Biçim Görünüm Yardım

Harry Potter is a series of seven fantasy novels written by British author J. K. Rowling. The novels chronicle the lives of a young wizard, Harry Potter, and his friends Hermione Granger and Ron Weasley, all of whom are students at Hogwarts School of Witchcraft and Wizardry. The main story arc concerns Harry's struggle against Lord Voldemort, a dark wizard who intends to

become immortal, overthrow the wizard governing body

known as the Ministry of Magic and subjugate all

wizards and Muggles (non-magical people).

Since the release of the first novel, Harry Potter and the Philosopher's Stone, on 26 June 1997, the books have found immense popularity, positive reviews, and commercial success worldwide. They have attracted a wide adult audience as well as younger readers and are often considered cornerstones of modern young adult literature.[2] As of February 2018, the books have sold more than 500 million copies worldwide, making them the best-selling book series in history, and have been translated into eighty languages.[3] The last four books consecutively set records as the fastest-selling books in history, with the final instalment selling roughly eleven million copies in the United States within twenty-four hours of its release.

The series was originally published in English by two major publishers, Bloomsbury in the United Kingdom and Scholastic Press in the United States. A play, Harry Dosya Düzen Biçim Görünüm Yardım
6Hf395BG239Y1YLPoZz9eS89fVZus7exDTWVI4jVxfKbky

\$hurkanugur.txt - Not Defteri

П

- +SAvXwowdD30lfL9nYsirkcZklXJY7K055NwBLc/4tbDn1 riDSV4c3N
- +G9XWJM2EG80kKkDUI2enEo5mbHQNoeLV6KIYD6qTp XY+CURdooYVd8GtbhybWDja9cStlbqJqX+uOkVhd2M
- +ObEUcrDRrC4clJFKOvoDIFUYtim/PlbHrPrNb4lngYxUQf v9FdluBsVV3ZuaNbm761jd/za8XTJkg9yxkQTpsoeRY6dt
- KGuOH5ZEuNBq2ECr2i2R+404H90FHWhvY9rdoQr +X/G2PkdUIYwMEX06BTIFiuqIbOF2vC4BIHIYtbcrhnSwp p0HVjQCiNOpIUMBc5hSx2hUtDSej/Bdi3fU1E9Ohymz13A pclpNWt72VyC6zEXvuN4ANiVstbkPgVihxXwikFNvkj
- +bTK4kpiCuyaBohylJyCR+YMF/jKkxCUXD1tep
- +Pi2XP/SG/P6Pp7FQ7C0XzI/A5X7XSN0nam4AdsExmVkq VEyw5OHWyRE9odUKkX245ZPV6ThX9ico4U5p
- +eDyqAeDDh2W4TQGuZUKHIDz+
- +YDIOi7NWtdhADSqpdTy99KZ/U54gwyVKbNHOlijwgdO UFYfQufUhnsOYzPzMLSR3q++RIRx
- +wdwYD4v8fe2RAQIY8eIOdDLgzt5fmDUBMErI
- +TyVYRt0NcBjmVGV7G43KyMnOskl/mXgFQCS65ZHVXb +rPfrqKoCEEecRUTIOhJxamDGGrs2oIPzp814hHBTNjp0z NMAmuHsQ4gJ3+XO9HIM9ztPGPXPF0JN2MoWBOv6d1H PBOPYHODoqTZS6wvxrbQ44csLKGo0sCNUinWMgKN0N XAbkAoQuv7buiSHH0lb7Ba4cDztl/l4vlqz2mveD2w7J0SFi
- +Ylelg3pbBo0flVUlbSIEuTYtLOqL5S8vA5JoEuCuTQ1Bxl cnDpl6hufij
- +WVF1PeT12K6F6bOLfmNIZ3/wKyWZplmKLoPPQGtAgui

PART2: IF THERE IS NO INTRUSION

```
HostBasedIDS [Java Application] C.\Program Files\Java\jdk1.8.0_144\bin\javaw.exe (8 May 2021 00:34:52)

[0]: Create backup of a Directory
[1]: Check if there is an Intrusion
[2]: Exit

[Your Choice]: 1

Enter the Directory name to be scanned: HUKO
Enter Decryption Secret Key: 4D69646F6E46665A6B4377514D337566644A4D764D7334436474395341712B2B474254362B2B6679792F773D
Enter Initialization Vector: 76CEBDA71EC8E718AE18FBF4DC9BFFFC
Enter MAC Secret Key: 752F79594A5564717A6A6D3555596C64556C714C586B54676A477133506647563358496243455856584A733D
[Original File Reading]: 6 file(s) are read successfully from [HUKO]
[Backup File Reading]: 6 file(s) are read successfully from [HUKO]
[Scanning Result]: Everything is OK !
```

PART2: IF THERE IS AN INTRUSION