



# JAVA MINI PROJECT

By Rahul Alshi [2019110001]

Sneha Ghuge [2019110015]

**Problem Statement :** Write a program to Encrypt and Decrypt a Image file and data Text using JAVA.

**Encryption :** Design a class Encryption.

Convert the image into byte array, create the array of same size as the image. Use a key (that will act as a password) for encryption. Read the array and perform an XOR operation on each value of byte array due to which every value of image will change. Then write a new byte array value of image to Encrypt the image. Locate the array index out of bounds exception and catch it.

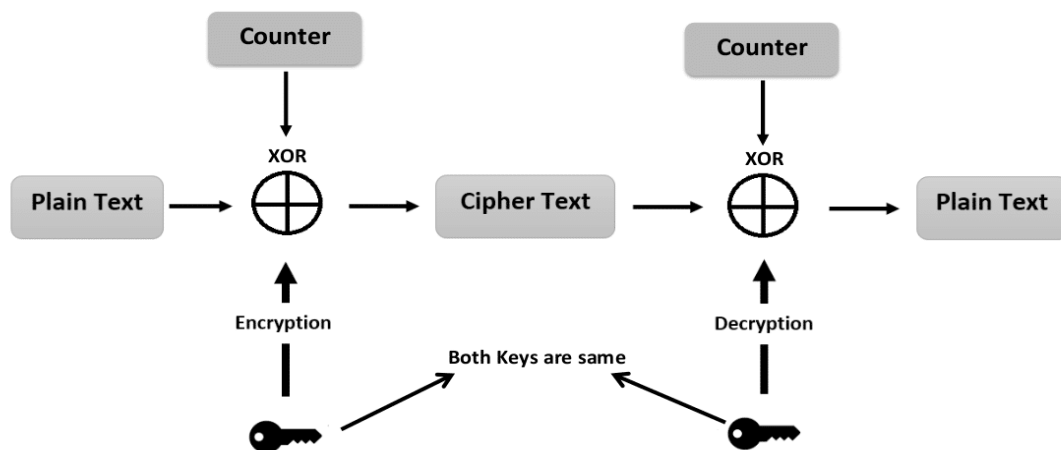
**Decryption :** Design a class Decryption. Convert the image into byte array, create the array of same size as the image. Use a key (that will act as a password) for decryption. Read the array and perform an XOR operation on each value of byte array to decrypt it. Then write decrypted data on the image. Locate the array index out of bounds exception and catch it.

We have developed a code on java which gives a dialog box to choose image or pdf file to encrypt and decrypt. Through this code we can also see the bits of the image being converted with the Xor operation with the key and the same for decryption.

### Text Encryption and Decryption :

Advanced Encryption Standard (AES) algorithm in Galois Counter Mode (GCM), known as AES-GCM. AES-GCM is a block cipher mode of operation that provides high speed of authenticated encryption and data integrity. In GCM mode, the block encryption is transformed into stream encryption, and therefore no padding is needed. The Additional Authenticated Data (AAD) will not be encrypted but used in the computation of Authentication Tag. The authenticated encryption operation takes Initialization Vector (IV), Additional Authenticated Data (AAD), Secret Key and 128-bit plaintext and gives a 128-bit ciphertext and authentication tag.

### Block Diagram :



Classes Used : 1. FileInputStream

2. FileOutputStream
3. Scanner
4. Secure Random
5. Key Generator
6. Base 64
7. Cipher
8. Secret key
9. GCMParameter Spec
10. SecretKeySpec
11. JButton
12. JTextField
13. Font Class
14. Flow Layout

Exceptions : 1. I/O Exception  
2. FileNotFoundException

Code 1 ; Encryption

```
import java.io.FileInputStream;
import java.io.FileNotFoundException;
import java.io.FileOutputStream;
import java.io.IOException;
import java.util.Scanner;

public class Encyption {
    public static void main(String[] args)
        throws FileNotFoundException, IOException
    {
        Scanner sc = new Scanner(System.in);
        System.out.println("Note : Encryption Key act as Password to Decrypt
the same Image,otherwise it will corrupt the Image.");

        // Here key is act as password to Encrypt and
```

```

// Decrypt the Image
System.out.print("Enter key for Encryption : ");
int key = sc.nextInt();

// Selecting a Image for operation
FileInputStream fis = new FileInputStream(
    "C:\\Users\\Student\\Desktop\\exampleimg.jpg");

// Converting Image into byte array, create a
// array of same size as Image size

byte data[] = new byte[fis.available()];

// Read the array
fis.read(data);
int i = 0;

// Performing an XOR operation on each value of
// byte array due to which every value of Image
// will change.
for (byte b : data) {
    data[i] = (byte)(b ^ key);
    i++;
}

// Opening a file for writing purpose
FileOutputStream fos = new
FileOutputStream("C:\\Users\\Student\\Desktop\\exampleimg.jpg");

// Writing new byte array value to image which
// will Encrypt it.

fos.write(data);

// Closing file
fos.close();
fis.close();
System.out.println("Encryption Done...");
}
}

```

Output :

exampleimg.jpg  
It appears that we don't support this file format.

## Code 2 : For Decryption

```
import java.io.FileInputStream;
import java.io.FileNotFoundException;
import java.io.FileOutputStream;
import java.io.IOException;
import java.util.Scanner;

public class Decryption {

    public static void main(String[] args)
        throws FileNotFoundException, IOException
    {
        Scanner sc = new Scanner(System.in);
        System.out.println(
            "Note : Encryption Key act as Password to Decrypt the same Image
otherwise it will corrupt the Image.");

        System.out.print("Enter a key for Decryption : ");
        int key = sc.nextInt();

        // Selecting a Image for Decryption.

        FileInputStream fis = new FileInputStream(
            "C:\\Users\\Student\\Desktop\\exampleimg.jpg");
        // Converting image into byte array,it will
        // Create a array of same size as image.
        byte data[] = new byte[fis.available()];

        // Read the array

        fis.read(data);
        int i = 0;
```

```

// Performing an XOR operation
// on each value of
// byte array to Decrypt it.
for (byte b : data) {
    data[i] = (byte)(b ^ key);
    i++;
}

// Opening file for writting purpose
FileOutputStream fos = new FileOutputStream(
    "C:\\Users\\Student\\Desktop\\exampleimg.jpg");

// Writing Decrypted data on Image
fos.write(data);
fos.close();
fis.close();
System.out.println("Decryption Done...");
}
}

```

Output :



Code 3 :

```

import java.security.SecureRandom;
import java.util.Base64;

```

```

import javax.crypto.Cipher;
import javax.crypto.KeyGenerator;
import javax.crypto.SecretKey;
import javax.crypto.spec.GCMParameterSpec;
import javax.crypto.spec.SecretKeySpec;

public class project
{
    static String plainText = "Though it is one of the faded memories of my
life today, there are times when I remember his face clearly, especially his
eyes. As he had yellow spots on his eyes we called him spotty. He would have
been a stray dog, until, he came to me.I was seven years old. My dad had just
got transferred to Nasik. We had shifted into a rented house. The house was
surrounded by lots of bushes and vines. It was raining very heavily on the day
we shifted.I went out and felt those refreshing raindrops with a cool breeze
on my face. It was a cold dark night. We had our meal and went to
sleep.Somewhat in the midnight I heard a loud thud outside the main door. I
mustered courage and peeped out through the window adjoining the door and I
was really amused with what I saw outside.";
    public static final int AES_KEY_SIZE = 256;
    public static final int GCM_IV_LENGTH = 12;
    public static final int GCM_TAG_LENGTH = 16;

    public static void main(String[] args) throws Exception
    {
        KeyGenerator keyGenerator = KeyGenerator.getInstance("AES");
        keyGenerator.init(AES_KEY_SIZE);

        // Generate Key
        SecretKey key = keyGenerator.generateKey();
        byte[] IV = new byte[GCM_IV_LENGTH];
        SecureRandom random = new SecureRandom();
        random.nextBytes(IV);

        System.out.println("ORIGINAL TEXT : " + plainText);
        System.out.println(" ");
        System.out.println(" ");

        byte[] cipherText = encrypt(plainText.getBytes(), key, IV);
        System.out.println("ENCRYPTED TEXT : " +
Base64.getEncoder().encodeToString(cipherText));
        System.out.println(" ");
        System.out.println(" ");

        String decryptedText = decrypt(cipherText, key, IV);
        System.out.println("DECRYPTED TEXT : " + decryptedText);
    }
}

```

```

    public static byte[] encrypt(byte[] plaintext, SecretKey key, byte[] IV)
throws Exception
    {
        // Get Cipher Instance
        Cipher cipher = Cipher.getInstance("AES/GCM/NoPadding");

        // Create SecretKeySpec
        SecretKeySpec keySpec = new SecretKeySpec(key.getEncoded(), "AES");

        // Create GCMParameterSpec
        GCMParameterSpec gcmParameterSpec = new
GCMParameterSpec(GCM_TAG_LENGTH * 8, IV);

        // Initialize Cipher for ENCRYPT_MODE
        cipher.init(Cipher.ENCRYPT_MODE, keySpec, gcmParameterSpec);

        // Perform Encryption
        byte[] cipherText = cipher.doFinal(plaintext);

        return cipherText;
    }

    public static String decrypt(byte[] cipherText, SecretKey key, byte[] IV)
throws Exception
    {
        // Get Cipher Instance
        Cipher cipher = Cipher.getInstance("AES/GCM/NoPadding");

        // Create SecretKeySpec
        SecretKeySpec keySpec = new SecretKeySpec(key.getEncoded(), "AES");

        // Create GCMParameterSpec
        GCMParameterSpec gcmParameterSpec = new
GCMParameterSpec(GCM_TAG_LENGTH * 8, IV);

        // Initialize Cipher for DECRYPT_MODE
        cipher.init(Cipher.DECRYPT_MODE, keySpec, gcmParameterSpec);

        // Perform Decryption
        byte[] decryptedText = cipher.doFinal(cipherText);

        return new String(decryptedText);
    }
}

```

Output :



ORIGINAL TEXT : Though it is one of the faded memories of my life today, there are times when I remember his face clearly, especially his eyes. As he had yellow spots on his eyes we called him spotty. He would have been a stray dog, until, he came to me. I was seven years old. My dad had just got transferred to Nasik. We had shifted to a rented house. The house was surrounded by lots of bushes and vines. It was raining very heavily on the day we shifted. I went out and felt those refreshing raindrops with a cool breeze on my face. It was a cold dark night. We had our meal and went to sleep. Somehow in the midnight I heard a loud thud outside the main door. I mustered courage and peeped out through the window adjoining the door and I was really amused with what I saw outside.

ENCRYPTED TEXT : rPNwTd26Es05GFLQhF9MUyQjib3LWl0zQ9Rc0b/Wgog1MghqfVvBtjftBY5wGGTH66/JJoR+dS/1Ph2CY9HcvuoqTV6TbuejWlzSU2THzOehOXvxxURDJ8WrcLoD4zgJp8x2Vq3CLX8cTQSHVxh04LravvnraU7MqVUiW7g9PpNC7/PxTbPQp9jBpdd3Prcg3/2Nlpb3zi8VdMLHotcJev4IpdMonVeToZROABHUH6XJSPFqLm0jMTR+m9obE/+23WUDNN4plbjMa+s2hOX5HoxssXjMgMUAd3Ks536LDiuhCnz19UN8xW4OGypXeTlxqzJGw39U/0TNUWjm4aUan3d3pTtrk0bx2E2e3VC2jZjh0fKaysVcaYHG/VMLQ3chbcjFam8aJnyWP4dy03V9WfU/Z15gh6iCaiRDj1jAMj/010giP8dcdZzUF7hZ7qVD4HPuc2D2yA119kn6rA11vN38ycX0br4Iqwazqe1xXzJpIv1CwOKxtZujkkuyumznDmEeE+4mh9IT2WRNq1Kgysixc5Pu1zn24vTGmsvPN0Nmnrk8Qo9jhrPUxDQugeXvhSiEu51xL8g5BfrhJCYZwh9eA14ISVjf2eatsSFY+VANqEQQLriSQ6D8j8XAtHKNP94sUWca7wKXlq3790FBttNj+1n2wsEasgZmXwOlmae0FWLcmeFBrLptR9P1Mn7cpnf9ij7NUTIoemPm3fCVIXV1ApaVB6dcjehhLiHKuLG/YkgI7LG2yE6uLZH5K6DmHYfaAGuqh7GNMfdiayeHwvyjXi/vS5FipSftdvpSUZJ5sr4j1K91KV29GKPyMsn28xw0X+YHbgUmbp6iVSP2NUpa23x0RZXnpjFDsUgOj1k4GA36i3ne0fKe50Ioz7rmOggtfdyj3KMMyJWY1uEnHtnSHXUHWdq8YiUzKN50E6mBc5XwcZ9j1Dfp9c53+EX8eZ6v+zH/CZCK4y55KeG576cctJglgJpfd42xKIqcbBE5Wdzc1W0Hqgbxdu8r9W0uzNy1qyf0pg==

DECRYPTED TEXT : Though it is one of the faded memories of my life today, there are times when I remember his face clearly, especially his eyes. As he had yellow spots on his eyes we called him spotty. He would have been a stray dog, until, he came to me. I was seven years old. My dad had just got transferred to Nasik. We had shifted into a rented house. The house was surrounded by lots of bushes and vines. It was raining very heavily on the day we shifted. I went out and felt those refreshing raindrops with a cool breeze on my face. It was a cold dark night. We had our meal and went to sleep. Somehow in the midnight I heard a loud thud outside the main door. I mustered courage and peeped out through the window adjoining the door and I was really amused with what I saw outside.

## Code 4 :

```
import javax.swing.JFrame;
import javax.swing.JOptionPane;
import javax.swing.JTextField;
import java.awt.FlowLayout;
import java.awt.Font;
import java.io.File;
import java.io.FileInputStream;
import java.io.FileOutputStream;
public class project2 {

    public static void operate(int key)
    {

        JFileChooser fileChooser=new JFileChooser();
        fileChooser.showOpenDialog(null);
        File file=fileChooser.getSelectedFile();
        //file FileInputStream
        try
        {

            FileInputStream fis=new FileInputStream(file);

            byte []data=new byte[fis.available()];
            fis.read(data);
            int i=0;
            for(byte b:data)
            {

                System.out.println(b);
                data[i]=(byte)(b^key);
                i++;
            }
        }
    }
}
```

```

        FileOutputStream fos=new FileOutputStream(file);
        fos.write(data);
        fos.close();
        fis.close();
        JOptionPane.showMessageDialog(null, "Done");

    }catch(Exception e)
    {
        e.printStackTrace();
    }
}

public static void main(String[] args) {

    System.out.println("this is testing");

    JFrame f=new JFrame();
    f.setTitle("Image Operation");
    f.setSize(400,400);
    f.setLocationRelativeTo(null);
    f.setDefaultCloseOperation(JFrame.EXIT_ON_CLOSE);

    Font font=new Font("Roboto",Font.BOLD,25);
    //creating button
    JButton button=new JButton();
    button.setText("Open Image");
    button.setFont(font);

    //creating text field

    JTextField textField=new JTextField(10);
    textField.setFont(font);

    button.addActionListener(e->{
        System.out.println("button clicked");
        String text=textField.getText();
        int temp=Integer.parseInt(text);
        operate(temp);
    });

    f.setLayout(new FlowLayout());

    f.add(button);
    f.add(textField);
    f.setVisible(true);
}

```

```
}  
}
```

Output :

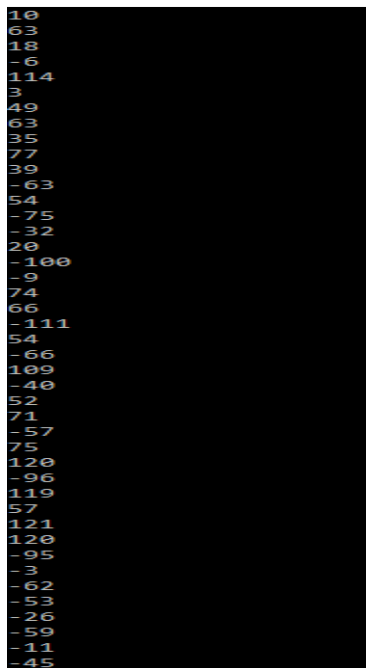
Encrypted bits :

```
0  
53  
24  
-16  
120  
9  
59  
53  
41  
71  
45  
-53  
60  
-65  
-22  
30  
-106  
-3  
64  
72  
-101  
60  
-76  
103  
-46  
62  
77  
-51  
65  
114  
-86  
125  
51  
115  
114  
-85  
-9  
-56  
-63  
-20  
-49  
-1  
-39
```

Encrypted image

exampleimg.jpg  
It appears that we don't support this file format.

Decrypted bits :



10  
63  
18  
-6  
114  
3  
49  
63  
35  
77  
39  
-63  
54  
-75  
-32  
20  
-100  
-9  
74  
66  
-111  
54  
-66  
109  
-40  
52  
71  
-57  
75  
120  
-96  
119  
57  
121  
120  
-95  
-3  
-62  
-53  
-26  
-59  
-11  
-45

Decrypted Image



### Conclusion :

1. In today's world almost all digital devices like internet communication , medical and military imaging systems, multimedia system needs a high security level in order to safely store and transmit digital images containing critical information. This is because of the faster growth in multimedia technology. Therefore there is need for image encryption techniques in order to hide images from such attacks
2. The size of the image which we have encrypted and decrypted is 48.9KB with dimensions of 500\*375.
3. Using the 4<sup>th</sup> code we can not only encrypt and decrypt the image but also pdfs and documents.
4. Encryption is a process of translating plain text data or a image that appears to be random , meaningless which is also called Cipher Text. Such Encryption techniques helps to avoid intrusion attacks.
5. Decryption is a process of converting Cipher Text into plain text.

