

## AES Algorithm

### Program:

```
import java.security.MessageDigest;

import java.util.Arrays;

import javax.crypto.KeyGenerator;

import javax.crypto.SecretKey;

import javax.crypto.spec.SecretKeySpec;

import javax.crypto.spec.IvParameterSpec;

import javax.crypto.Cipher;

import javax.crypto.spec.IvParameterSpec;

import javax.crypto.spec.SecretKeySpec;

public class AES {

    static String IV = "AAAAAAAAAAAAAAAA";

    static String plaintext = "comp uter has\u0000\u0000\u0000"; /*Note null padding*/

    static String encryptionKey = "0123456789abcdef";

    public static void main(String[] args) {

        try {

            System.out.println("==Java==");

            System.out.println("plain: " + plaintext);

            byte[] cipher = encrypt(plaintext, encryptionKey);

            System.out.print("cipher: ");

            for (int i = 0; i < cipher.length; i++)

                System.out.print(new Integer(cipher[i]) + " ");

            System.out.println("");

            String decrypted = decrypt(cipher, encryptionKey);

            System.out.println("decrypt: " + decrypted);

        } catch (Exception e) {

            e.printStackTrace();

        }

    }

}
```

```

    } catch (Exception e) {

        e.printStackTrace();

    }
}

public static byte[] encrypt(String plainText, String encryptionKey) throws Exception {

    Cipher cipher = Cipher.getInstance("AES/CBC/NoPadding", "SunJCE");

    SecretKeySpec key = new SecretKeySpec(encryptionKey.getBytes("UTF-8"), "AES");

    cipher.init(Cipher.ENCRYPT_MODE, key, new IvParameterSpec(IV.getBytes("UTF-8")));

    return cipher.doFinal(plainText.getBytes("UTF-8"));

}

public static String decrypt(byte[] cipherText, String encryptionKey) throws Exception {

    Cipher cipher = Cipher.getInstance("AES/CBC/NoPadding", "SunJCE");

    SecretKeySpec key = new SecretKeySpec(encryptionKey.getBytes("UTF-8"), "AES");

    cipher.init(Cipher.DECRYPT_MODE, key, new IvParameterSpec(IV.getBytes("UTF-8")));

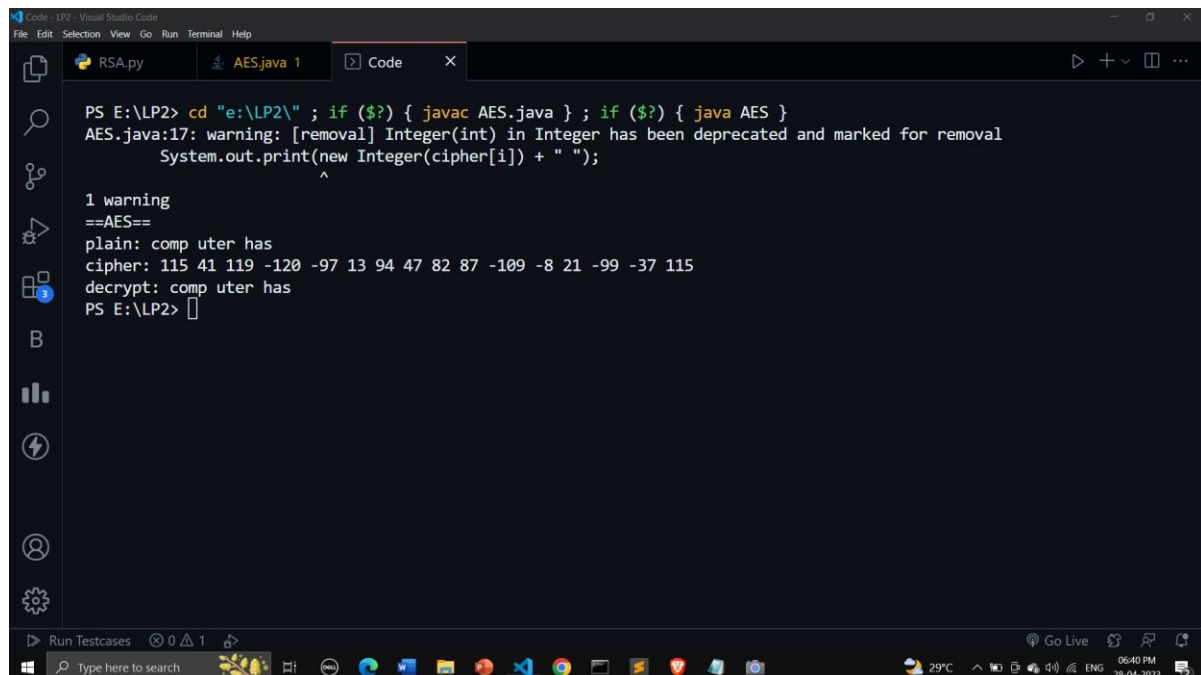
    return new String(cipher.doFinal(cipherText), "UTF-8");

}

}

```

## Output:



```

PS E:\LP2> cd "e:\LP2\" ; if ($?) { javac AES.java } ; if ($?) { java AES }
AES.java:17: warning: [removal] Integer(int) in Integer has been deprecated and marked for removal
    System.out.print(new Integer(cipher[i]) + " ");
                        ^
1 warning
==AES==
plain: comp uter has
cipher: 115 41 119 -120 -97 13 94 47 82 87 -109 -8 21 -99 -37 115
decrypt: comp uter has
PS E:\LP2>

```