T.Y. B.Sc. C.S. Sem-V	Roll No: <b>713</b>

Date:11/09/2020

### Practical no 4

**AIM:** Write program to encrypt and decrypt strings using 1) DES Algorithm 2) AES Algorithm

## CODE

# 1) DES Algorithm

```
import java.util.logging.Level;
import java.util.logging.Logger;
import java.util.Base64;
import javax.crypto.Cipher;
import javax.crypto.KeyGenerator;
import javax.crypto.SecretKey;
public class DES {
  public static SecretKey getSecretEncryptionKey() throws Exception{
    KeyGenerator generator=KeyGenerator.getInstance("DES");
     SecretKey secKey=generator.generateKey();
    return secKey;
  }
  public String encrypt(SecretKey key,String Plaintext) throws Exception{
    byte[] utf8=Plaintext.getBytes();
     Cipher ecipher=Cipher.getInstance("DES");
     ecipher.init(Cipher.ENCRYPT MODE, key);
    byte[] enc=ecipher.doFinal(utf8);
     Base64.Encoder encoder=Base64.getEncoder();
     String et=encoder.encodeToString(enc);
```

```
return et:
}
public String decrypt(SecretKey key,String Ciphertext) throws Exception{
  Base64.Decoder decoder = Base64.getDecoder();
  byte[] dec=decoder.decode(Ciphertext);
  Cipher dcipher=Cipher.getInstance("DES");
  dcipher.init(Cipher.DECRYPT_MODE, key);
  byte[] utf8=dcipher.doFinal(dec);
  return new String(utf8,"UTF8");
}
public static void main(String[] args){
  try{
     System.out.println("INS Practical PERFORMED BY: krunal 713.");
     System.out.println("----'--Encrypting string using DES--'----");
     System.out.println();
     String message ="NETWORKSECURITY";
     DES d=new DES();
     SecretKey key=getSecretEncryptionKey();
     String Encrypted=d.encrypt(key, message);
     String Decrypted=d.decrypt(key, Encrypted);
     System.out.println("Original String is: "+ message);
     System.out.println("Encrypted String is: "+ Encrypted);
     System.out.println("Decrypted String is: "+ Decrypted);
  }catch (Exception ex){
     Logger.getLogger(DES.class.getName()).log(Level.SEVERE,null,ex);
```

# T.Y. B.Sc. C.S. Sem-V

```
}
}
}
```

### Output - DES (run) ×



run:



INS\_Practical PERFORMED BY : krunal 713.

Encryption Process :



Original string is : NETWORKSECURITY

Encrypted string is :wtopAnmYBNV9gl+TBVWOGg==

Decrypted string is :NETWORKSECURITY
BUILD SUCCESSFUL (total time: 1 second)

T.Y. B.Sc. C.S. Sem-V Roll No: 713

### b) AES CODE

```
package aes;
import java.util.logging.Logger;
import java.util.logging.Level;
import javax.crypto.Cipher;
import javax.crypto.KeyGenerator;
import javax.crypto.SecretKey;
public class AES {
  public static SecretKey getSecretEncryptionKey() throws Exception{
    KeyGenerator generator = KeyGenerator.getInstance("AES");
    generator.init(128);
    SecretKey secKey= generator.generateKey();
    return secKey;
  }
  public String encrypt(SecretKey key,String Plaintext)throws Exception{
    byte[] utf8= Plaintext.getBytes("UTF8");
    Cipher ecipher= Cipher.getInstance("AES");
    ecipher.init(Cipher.ENCRYPT MODE,key);
    byte[] enc= ecipher.doFinal(utf8);
    return new sun.misc.BASE64Encoder().encode(enc);
  }
  public String decrypt(SecretKey key,String Ciphertext) throws Exception{
    byte[] dec= new sun.misc.BASE64Decoder().decodeBuffer(Ciphertext);
    Cipher dcipher= Cipher.getInstance("AES");
    dcipher.init(Cipher.DECRYPT MODE,key);
    byte[] utf8= dcipher.doFinal(dec);
    return new String(utf8, "UTF8");
  }
  public static void main (String[]args) throws Exception
    try{
       System.out.println("Performed by : krunal ,713");
       System.out.println("Encryption using AES");
       String message="NETWORK SECURITY";
       AES d= new AES():
       SecretKey key= getSecretEncryptionKey();
       String Encrypted= d.encrypt(key, message);
```

### T.Y. B.Sc. C.S. Sem-V

Roll No: 713

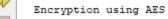
```
String decrypted = d.decrypt(key,Encrypted);
    System.out.println("Original string is:" +message);
    System.out.println("Encrypted string is:" + Encrypted);
    System.out.println("Decrypted string is:" +decrypted);
}
catch(Exception ex){
    Logger.getLogger(AES.class.getName()).log(Level.SEVERE,null,ex);
}
}
```

### Output - AES (run) X



```
run:
```

Performed by : krunal ,713



Original string is:NETWORK SECURITY



Encrypted string is:dsAYDHQI+U7gsRQlCJKKXNlYSu/gGkKJ/E00TAVy5xE=

Decrypted string is:NETWORK SECURITY

BUILD SUCCESSFUL (total time: 0 seconds)