PRACTICAL 3

Aim: Write a program to implement DES algorithm.

Code:

```java
import java.util.Scanner;
import javax.crypto.*;
public class DES {
    Cipher encipher, dcipher;
    public static void main(String args[]) {
        System.out.println("Enter any String:");
        Scanner sc = new Scanner(System.in);
        String input = sc.nextLine();
        try {
            KeyGenerator k = KeyGenerator.getInstance("DES");
            SecretKey key = k.generateKey();
            DES en = new DES(key);
            String ct = en.encrypt(input);
            String decrypted = en.decrypt(ct);
            System.out.println("Original string is:" + input);
            System.out.println("Encrypted string is:" + ct);
            System.out.println("Decrypted string is:" + decrypted);
        } catch (Exception e) {
            System.out.println(e);
        }
    }
    public DES(SecretKey key) {
        try {
            encipher = Cipher.getInstance("DES");
            encipher.init(Cipher.ENCRYPT_MODE, key);
            dcipher = Cipher.getInstance("DES");
            dcipher.init(Cipher.DECRYPT_MODE, key);
        } catch (Exception e) {
            System.out.println(e);
        }
    }
    public String encrypt(String str) {
        try {
            byte[] b = str.getBytes();
            byte[] enc = encipher.doFinal(b);
            return new String(enc);
        } catch (Exception e) {
            System.out.println(e);
            // TODO: handle exception
```

```
        }
        return null;
    }
    public String decrypt(String str) {
        try {
            byte[] b = str.getBytes();
            byte[] dec = dcipher.doFinal(b);
            return new String(dec);
        } catch (Exception e) {
            System.out.println(e);
        }
        return null;
    }
}
```

Output:

AES algorithm

Code:

```java
import java.util.Scanner;
import javax.crypto.*;
public class AES {
    Cipher encipher, dcipher;
    public static void main(String args[]) {
        System.out.println("Enter any String:");
        Scanner sc = new Scanner(System.in);
        String input = sc.nextLine();
        try {
            KeyGenerator k = KeyGenerator.getInstance("AES");
            SecretKey key = k.generateKey();
            AES en = new AES(key);
            String ct = en.encrypt(input);
            String decrypted = en.decrypt(ct);
            System.out.println("Original string is:" + input);
            System.out.println("Encrypted string is:" + ct);
            System.out.println("Decrypted string is:" + decrypted);
```

```java
        } catch (Exception e) {
            System.out.println(e);
        }
    }
    public AES(SecretKey key) {
        try {
            encipher = Cipher.getInstance("AES");
            encipher.init(Cipher.ENCRYPT_MODE, key);
            dcipher = Cipher.getInstance("AES");
            dcipher.init(Cipher.DECRYPT_MODE, key);
        } catch (Exception e) {
            System.out.println(e);
        }
    }
    public String encrypt(String str) {
        try {
            byte[] b = str.getBytes();
            byte[] enc = encipher.doFinal(b);
            return new String(enc);
        } catch (Exception e) {
            System.out.println(e);
        }
        return null;
    }
    public String decrypt(String str) {
        try {
            byte[] b = str.getBytes();
            byte[] dec = dcipher.doFinal(b);
            return new String(dec);
        } catch (Exception e) {
            System.out.println(e);
        }
        return null;
    }
}
```

Output:

```
PS C:\Users\ADMIN\Downloads\INS Practical-20230814T033705Z-001\INS Practical\P3> javac AES.java
PS C:\Users\ADMIN\Downloads\INS Practical-20230814T033705Z-001\INS Practical\P3> java AES
Enter any String:
Atharva
Original string is:Atharva
Encrypted string is:%PR?0?a
mz?$n?N
Decrypted string is:Atharva
```