MALLA REDDY UNIVERSITY

III Year B.Tech– II Semester

CRYPTOGRAPHY & NETWORK SECURITY LAB

WEEK-5

5. User A want to communicate with user B but it should be confidential by using Blowfish Algorithms send encrypt message.

AIM: To implement a java program using Blowfish algorithm logic

OBJECTIVE: To understand the encryption and decryption by using Blowfish algorithm.

THEORY:

Blowfish is a symmetric key block cipher. Blowfish provides a good encryption rate in software and no effective cryptanalysis of it has been found to date. Blowfish has a 64bit block size and a variable key length from 32 bits up to 448bits. It is a 16-round Feistel cipher and uses large key-dependent s-boxes.

ALGORITHM:

STEP-1: Blowfish has a 64-bit block size and a variable key length from 30 bits up to 448 bits.

STEP-2: It is a 16-round Feistel cipher and uses large key dependent s-boxes.

STEP-3: There are 5 sub key-arrays. One 18-entry p-array and four 256-entry s-boxes.

STEP-4: Every round r consists of 4 actions.

a) XOR the left half of the data with the ‘r’th p-array entry.

b) Use the XORed data as input for Blowfish algorithm.

c) F-function’s output with the right half (R) of the data.

d) Swap L and R.

STEP-5: The F-function splits the 32bits into four 8-bits quarters and uses the

quarters as input to the s-boxes.

STEP-6: The s-boxes accept 8-bit input and produce 32-bit output.The outputs are added modulo 2 power 32 and XORed to produce the final 32-bit output.

PROGRAM:

```
import java.io.UnsupportedEncodingException;
import java.nio.charset.Charset;
import java.security.InvalidKeyException;
import java.security.NoSuchAlgorithmException;
import java.util.Base64;
import javax.crypto.BadPaddingException;
import javax.crypto.Cipher;
import javax.crypto.IllegalBlockSizeException;
import javax.crypto.NoSuchPaddingException;
import javax.crypto.spec.SecretKeySpec;
public class BlowFish
{
 public String encrypt(String password, String key) throws
NoSuchAlgorithmException, NoSuchPaddingException,
InvalidKeyException, IllegalBlockSizeException,
BadPaddingException, UnsupportedEncodingException
{
    byte[] KeyData = key.getBytes();
SecretKeySpec KS = new SecretKeySpec(KeyData, "Blowfish");
Cipher cipher = Cipher.getInstance("Blowfish");
cipher.init(Cipher.ENCRYPT_MODE, KS);
String encryptedtext = Base64.getEncoder().
encodeToString(cipher.doFinal(password.getBytes("UTF-8")));
return encryptedtext;
}
public String decrypt(String encryptedtext, String key) throws
NoSuchAlgorithmException, NoSuchPaddingException,
InvalidKeyException, IllegalBlockSizeException,
BadPaddingException
{
    byte[] KeyData = key.getBytes();
SecretKeySpec KS = new SecretKeySpec(KeyData, "Blowfish");
```

```
byte[] ecryptedtexttobytes = Base64.getDecoder().decode(encryptedtext);
Cipher cipher = Cipher.getInstance("Blowfish");
cipher.init(Cipher.DECRYPT_MODE, KS);
byte[] decrypted = cipher.doFinal(ecryptedtexttobytes);
String decryptedString = new String(decrypted, Charset.forName("UTF-8"));
return decryptedString;
}
```

```
public static void main(String[] args) throws Exception
{
    final String password = "Malla Reddy University"; final String key =
"CSE";
System.out.println("Password: " + password);
BlowFish obj = new BlowFish();
String enc_output = obj.encrypt(password, key);
System.out.println("Encrypted text: " + enc_output);
String dec_output = obj.decrypt(enc_output, key);
System.out.println("Decrypted text: " + dec_output);
}
}
```

OUT PUT: