Ranjan Shettigar

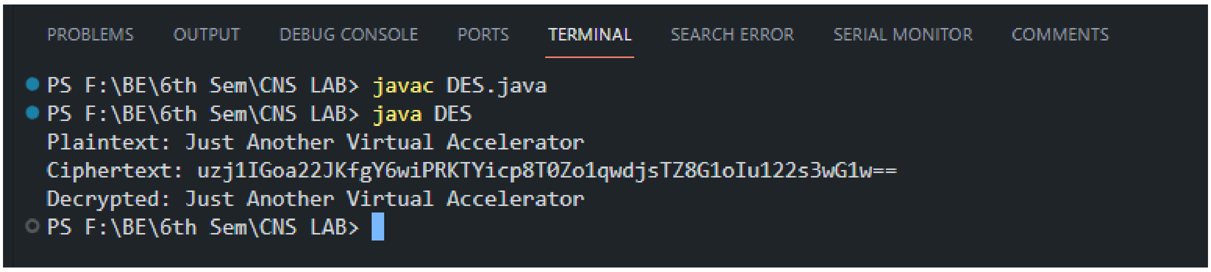
4NM22IS408

Date:18/03/2024

DES Using Java

```
import javax.crypto.Cipher;
import javax.crypto.SecretKey;
import javax.crypto.SecretKeyFactory;
import javax.crypto.spec.DESKeySpec;
import java.nio.charset.StandardCharsets;
import java.util.Base64;

public class DES {
    private SecretKey key;

    public DES(String keyString) throws Exception {
        // Initialize DES with key
        byte[] keyBytes = keyString.getBytes(StandardCharsets.UTF_8);
        DESKeySpec desKeySpec = new DESKeySpec(keyBytes);
        SecretKeyFactory keyFactory = SecretKeyFactory.getInstance("DES");
        key = keyFactory.generateSecret(desKeySpec);
    }

    public String encrypt(String plaintext) throws Exception {
        // Perform DES encryption on plaintext
        Cipher cipher = Cipher.getInstance("DES/ECB/PKCS5Padding");
        cipher.init(Cipher.ENCRYPT_MODE, key);
        byte[] encryptedBytes =
cipher.doFinal(plaintext.getBytes(StandardCharsets.UTF_8));
        // Return ciphertext as base64 encoded string
        return Base64.getEncoder().encodeToString(encryptedBytes);
    }

    public String decrypt(String ciphertext) throws Exception {
        // Parse base64 encoded ciphertext
        byte[] ciphertextBytes = Base64.getDecoder().decode(ciphertext);
        // Perform DES decryption on ciphertext
        Cipher cipher = Cipher.getInstance("DES/ECB/PKCS5Padding");
        cipher.init(Cipher.DECRYPT_MODE, key);
        byte[] decryptedBytes = cipher.doFinal(ciphertextBytes);
        // Return decrypted plaintext as UTF-8 string
        return new String(decryptedBytes, StandardCharsets.UTF_8);
    }
    public static void main(String[] args) {
        try {
            String key = "0123456789abcdef";
            String plaintext = "Just Another Virtual Accelerator";

            // Perform DES encryption
            DES des = new DES(key);
            String ciphertext = des.encrypt(plaintext);

            // Perform DES decryption
            String decrypted = des.decrypt(ciphertext);

            // Print results
            System.out.println("Plaintext: " + plaintext);
            System.out.println("Ciphertext: " + ciphertext);
            System.out.println("Decrypted: " + decrypted);
        } catch (Exception e) {
            e.printStackTrace();
        }
    }
}
```

Output:



```
PS F:\BE\6th Sem\CNS LAB> javac DES.java
PS F:\BE\6th Sem\CNS LAB> java DES
Plaintext: Just Another Virtual Accelerator
Ciphertext: uzj1IGoa22JKfgY6wiPRKTYicp8T0Zo1qwdjsTZ8G1oIu122s3wG1w==
Decrypted: Just Another Virtual Accelerator
PS F:\BE\6th Sem\CNS LAB>
```