QUESTION 18

Program:

import javax.crypto.Cipher;

import javax.crypto.spec.IvParameterSpec;

import javax.crypto.spec.SecretKeySpec;

import java.nio.charset.StandardCharsets;

import java.security.MessageDigest;

import java.util.Arrays;

public class ThreeDESEncryptionExample {

private static final String ENCRYPTION\_ALGORITHM = "DESede/CBC/PKCS5Padding";

private static final String HASH\_ALGORITHM = "SHA-256";

public static void main(String[] args) throws Exception {

String plaintext = "Hello, World!";

byte[] key = "mysecretkey12345".getBytes(StandardCharsets.UTF\_8);

byte[] iv = "myiv1234".getBytes(StandardCharsets.UTF\_8); // 8-byte initialization vector

// Hash the key to make it the appropriate length for 3DES

MessageDigest digest = MessageDigest.getInstance(HASH\_ALGORITHM);

byte[] hashedKey = digest.digest(key);

byte[] tripleKey = Arrays.copyOf(hashedKey, 24);

// Create a 3DES CBC cipher object

SecretKeySpec keySpec = new SecretKeySpec(tripleKey, "DESede");

IvParameterSpec ivSpec = new IvParameterSpec(iv);

Cipher cipher = Cipher.getInstance(ENCRYPTION\_ALGORITHM);

cipher.init(Cipher.ENCRYPT\_MODE, keySpec, ivSpec);

// Encrypt the plaintext

byte[] ciphertext = cipher.doFinal(plaintext.getBytes(StandardCharsets.UTF\_8));

// Convert the ciphertext to Base64 for easy transmission/storage

String encodedCiphertext = Base64.getEncoder().encodeToString(ciphertext);

// Print the plaintext and ciphertext for demonstration purposes

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

System.out.println("Ciphertext: " + encodedCiphertext);

}

}

OUTPUT:

Plaintext: Hello, World!

Ciphertext: wgzFam/UTM9SGNH0CeaFRg==