import javax.crypto.Cipher;

import javax.crypto.SecretKey;

import javax.crypto.spec.SecretKeySpec;

import java.util.Base64;

import java.util.Scanner;

public class AESExample {

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

// Create a Scanner object to read user input

Scanner scanner = new Scanner(System.in);

// Prompt the user to enter the data to be encrypted

System.out.println("Enter the data to be encrypted:");

String inputData = scanner.nextLine();

// Prompt the user to enter the encryption key

System.out.println("Enter the encryption key (16 characters):");

String keyString = scanner.nextLine();

// Convert the key string to bytes

byte[] keyBytes = keyString.getBytes();

// Ensure the key is exactly 16 characters long (128 bits)

if (keyBytes.length != 16) {

System.out.println("Invalid key length. The key must be 16 characters long.");

return;

}

// Create a SecretKey object from the key bytes

SecretKey secretKey = new SecretKeySpec(keyBytes, "AES");

// Create an AES cipher instance

Cipher cipher = Cipher.getInstance("AES");

// Initialize the cipher for encryption

cipher.init(Cipher.ENCRYPT\_MODE, secretKey);

// Convert the input data to bytes

byte[] data = inputData.getBytes();

// Perform encryption

byte[] encryptedData = cipher.doFinal(data);

// Convert encrypted data to Base64 for easier printing

String encryptedDataString = Base64.getEncoder().encodeToString(encryptedData);

System.out.println("Encrypted data: " + encryptedDataString);

// Initialize the cipher for decryption

cipher.init(Cipher.DECRYPT\_MODE, secretKey);

// Perform decryption

byte[] decryptedData = cipher.doFinal(encryptedData);

System.out.println("Decrypted data: " + new String(decryptedData));

// Close the Scanner

scanner.close();

}

}