MAIN. JAVA

```
import javax.crypto.Cipher;
import javax.crypto.spec.IvParameterSpec;
import javax.crypto.spec.SecretKeySpec;
import java.io.*;
import java.security.Key;
import java.security.MessageDigest;
import java.util.Base64;
public class Main {
private static final String ALGORITHM = "AES";
private static final String TRANSFORMATION = "AES";
private static final String KEY = "ZZHHYYTTUUHHGGRR";
private static final String IV = "AAACCCDDDYYUURRS";
public static void main(String[] args) {
try {
test_encrypt_decrypt();
} catch (Exception e) {
System.out.println("Error: " + e.getMessage());
System.exit(1);
}
}
public static void test_encrypt_decrypt() throws Exception {
// encrypt "in.txt" -> "out.txt"
String s = readFile("D:\\a.txt");
2
String res = encrypt("mykey", IV, s);
PrintWriter writer = new PrintWriter("out.txt", "UTF-8");
writer.print(res);
writer.close();
// decrypt "out.txt" -> "out2.txt"
s = readFile("D:\\a.txt");
res = decrypt("mykey", IV, s);
writer = new PrintWriter("out2.txt", "UTF-8");
writer.print(res);
writer.close();
}
public static String encrypt(String key, String iv, String msg) throws Exception
{
byte[] bytesOfKey = key.getBytes("UTF-8");
MessageDigest md = MessageDigest.getInstance("MD5");
byte[] keyBytes = md.digest(bytesOfKey);
final byte[] ivBytes = iv.getBytes();
SecretKeySpec secretKeySpec = new SecretKeySpec(keyBytes, "AES");
Cipher cipher = Cipher.getInstance("AES/CBC/PKCS5Padding");
cipher.init(Cipher.ENCRYPT_MODE, secretKeySpec, new
IvParameterSpec(ivBytes));
final byte[] resultBytes = cipher.doFinal(msg.getBytes());
```

```
return Base64.getMimeEncoder().encodeToString(resultBytes);
}
public static void test_decrypt() throws Exception {
String s = readFile("D:\\a.txt");
String res = decrypt(KEY, IV, s);
System.out.println("res:\n" + res);
3
}
public static String decrypt(String key, String iv, String encrypted) throws
Exception {
byte[] bytesOfKey = key.getBytes("UTF-8");
MessageDigest md = MessageDigest.getInstance("MD5");
byte[] keyBytes = md.digest(bytesOfKey);
final byte[] ivBytes = iv.getBytes();
final byte[] encryptedBytes = Base64.getMimeDecoder().decode(encrypted);
SecretKeySpec secretKeySpec = new SecretKeySpec(keyBytes, "AES");
Cipher cipher = Cipher.getInstance("AES/CBC/PKCS5Padding");
cipher.init(Cipher.DECRYPT_MODE, secretKeySpec, new
IvParameterSpec(ivBytes));
final byte[] resultBytes = cipher.doFinal(encryptedBytes);
return new String(resultBytes);
}
public static String readFile(String filename) throws Exception {
BufferedReader br = new BufferedReader(new FileReader(filename));
try {
StringBuilder sb = new StringBuilder();
String line = br.readLine();
while (line != null) {
sb.append(line);
sb.append(System.lineSeparator());
line = br.readLine();
}
String everything = sb.toString();
return everything;
4
} finally {
br.close();
}
}
public static void test_read_file() throws Exception {
String s = readFile("D:\\a.txt");
System.out.println("D:\\a.txt" + s);
}
public static void encrypt(String key, File inputFile, File outputFile) throws
Exception {
doCrypto(Cipher.ENCRYPT_MODE, key, inputFile, outputFile);
}
public static void decrypt(String key, File inputFile, File outputFile) throws
```

```
Exception {
doCrypto(Cipher.DECRYPT_MODE, key, inputFile, outputFile);
}
static void doCrypto(int cipherMode, String key, File inputFile,
File outputFile) throws Exception {
Key secretKey = new SecretKeySpec(key.getBytes(), ALGORITHM);
Cipher cipher = Cipher.getInstance(TRANSFORMATION);
cipher.init(cipherMode, secretKey);
FileInputStream inputStream = new FileInputStream(inputFile);
byte[] inputBytes = new byte[(int) inputFile.length()];
inputStream.read(inputBytes);
byte[] outputBytes = cipher.doFinal(inputBytes);
FileOutputStream outputStream = new FileOutputStream(outputFile);
outputStream.write(outputBytes);
inputStream.close();
5
outputStream.close();
}
public static void test_doCrypto(String filename) throws Exception {
String key = "Mary has one cat";
File inputFile = new File("document.txt");
File encryptedFile = new File("document.encrypted");
File decryptedFile = new File("document.decrypted");
encrypt(key, inputFile, encryptedFile);
decrypt(key, encryptedFile, decryptedFile);
}
public static void test_write_to_file(String filename) throws Exception {
PrintWriter writer = new PrintWriter(filename, "UTF-8");
writer.println("The first line");
writer.println("The second line");
writer.close();
}
```