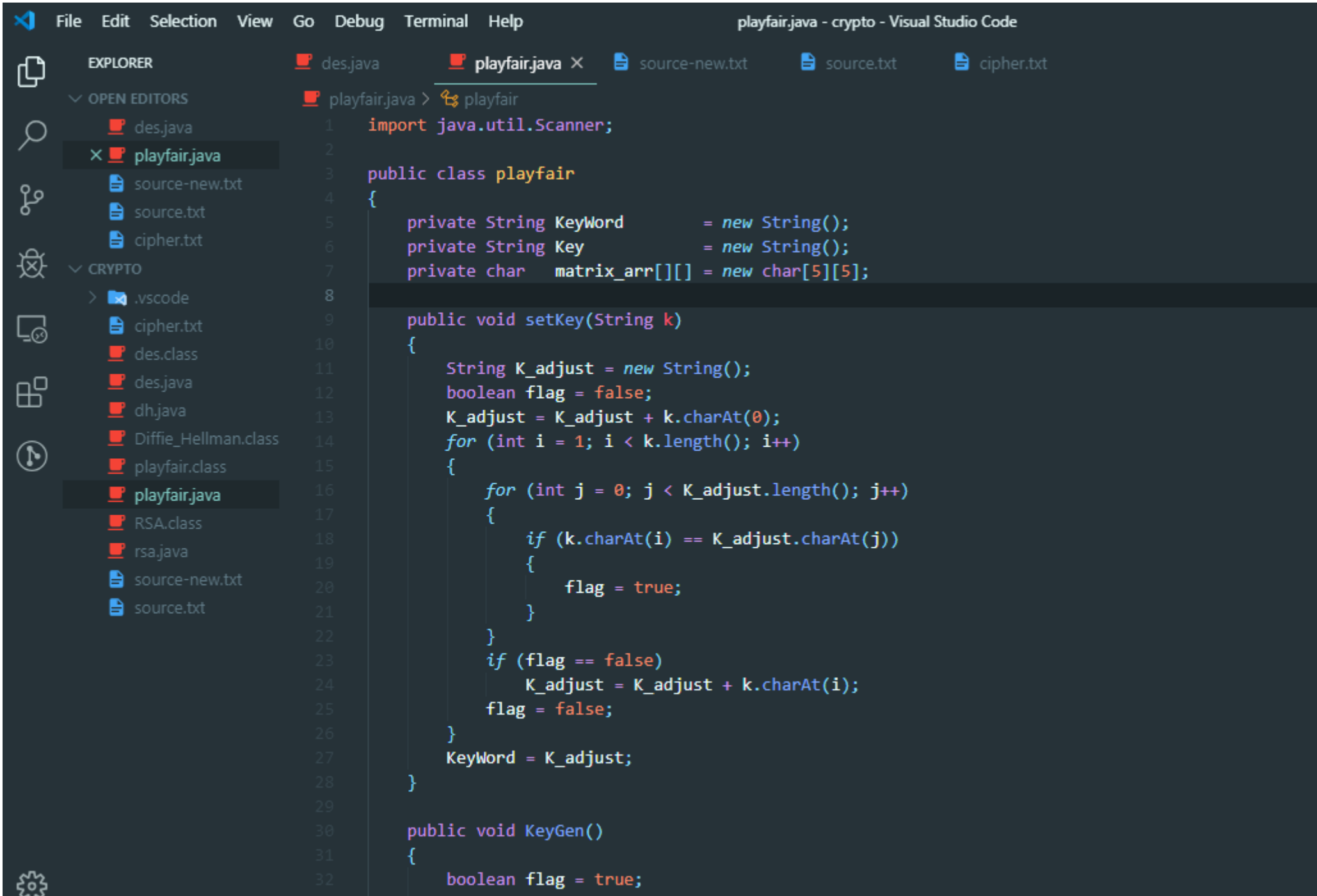
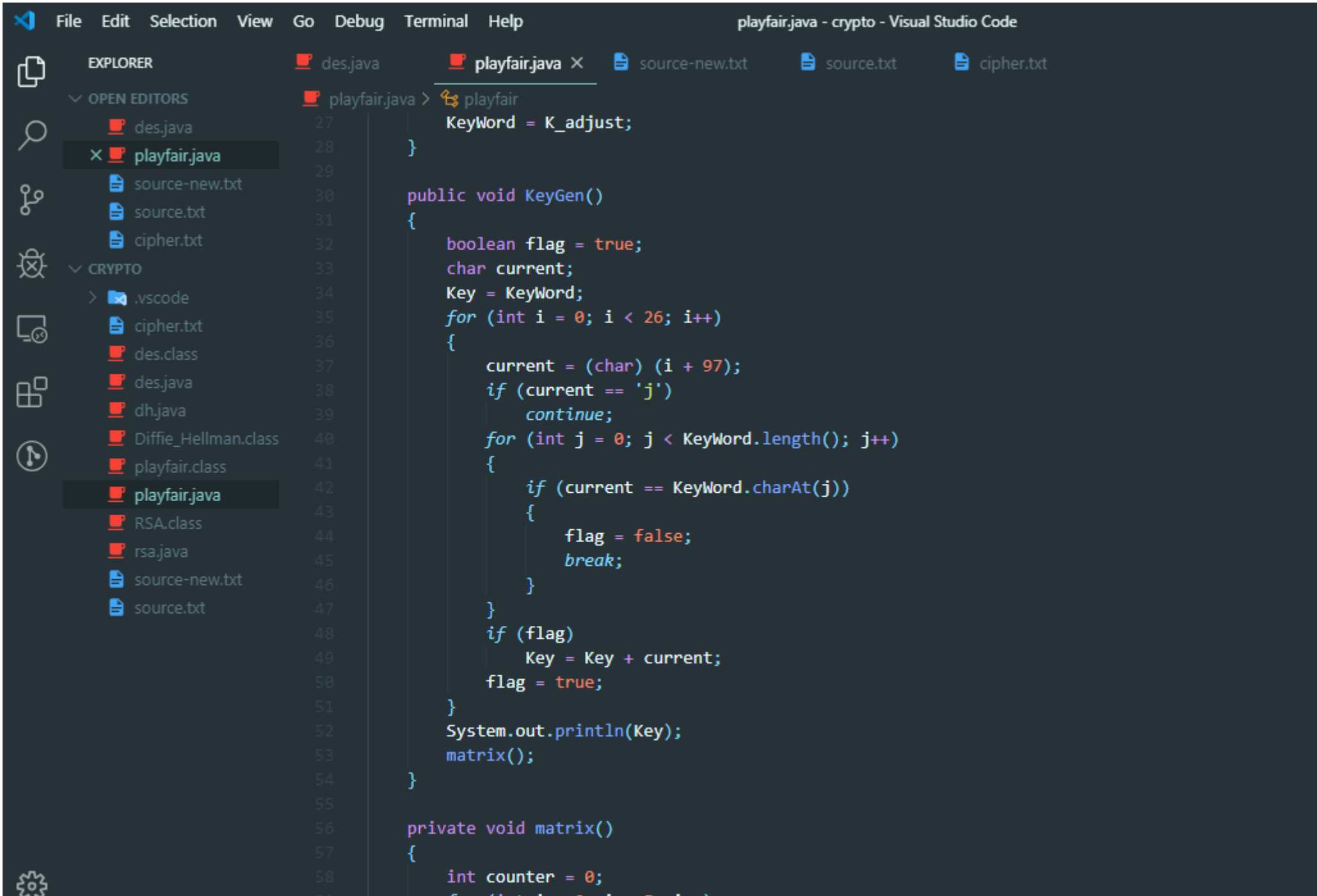
Cryptography theory

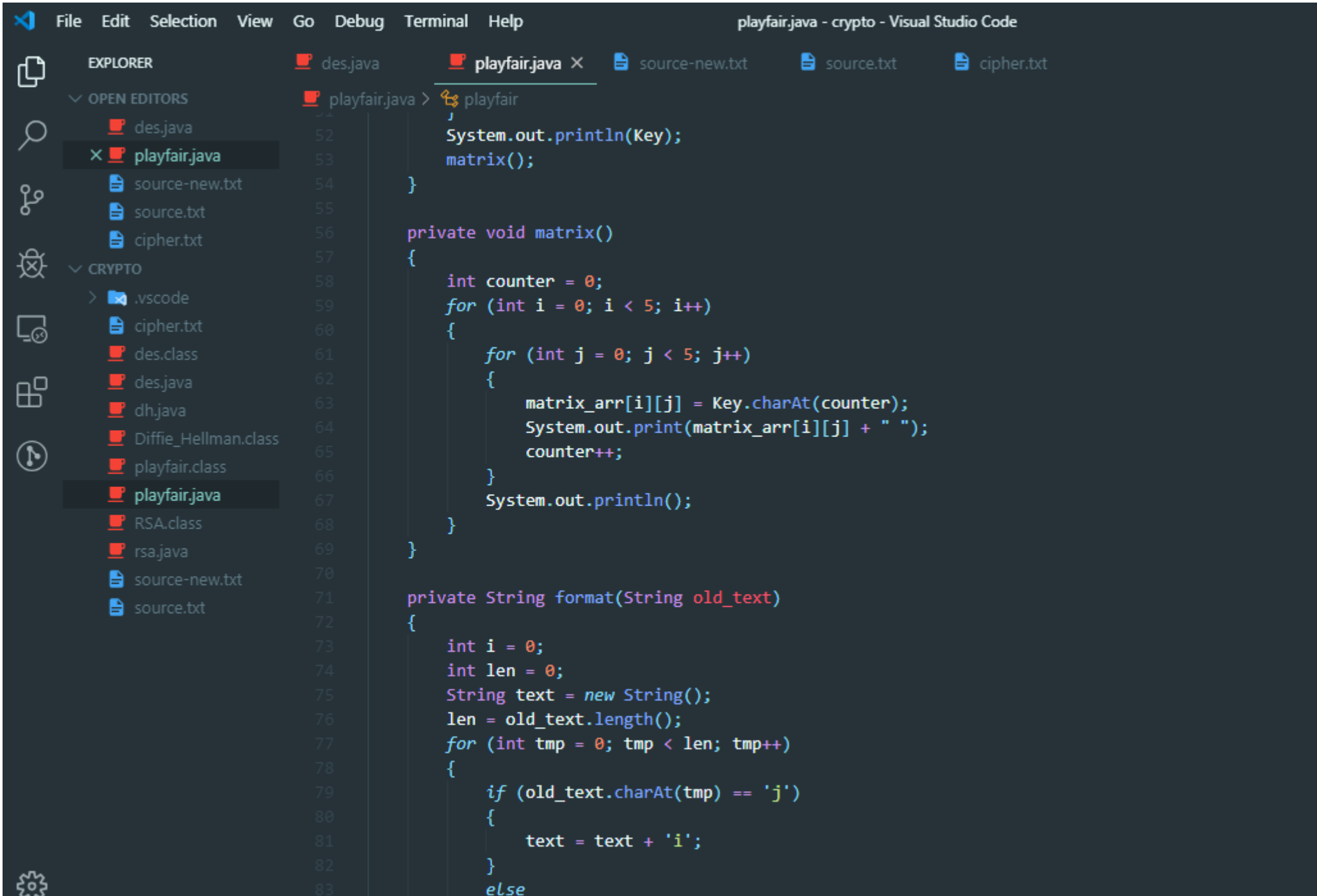
Harsh Gupta

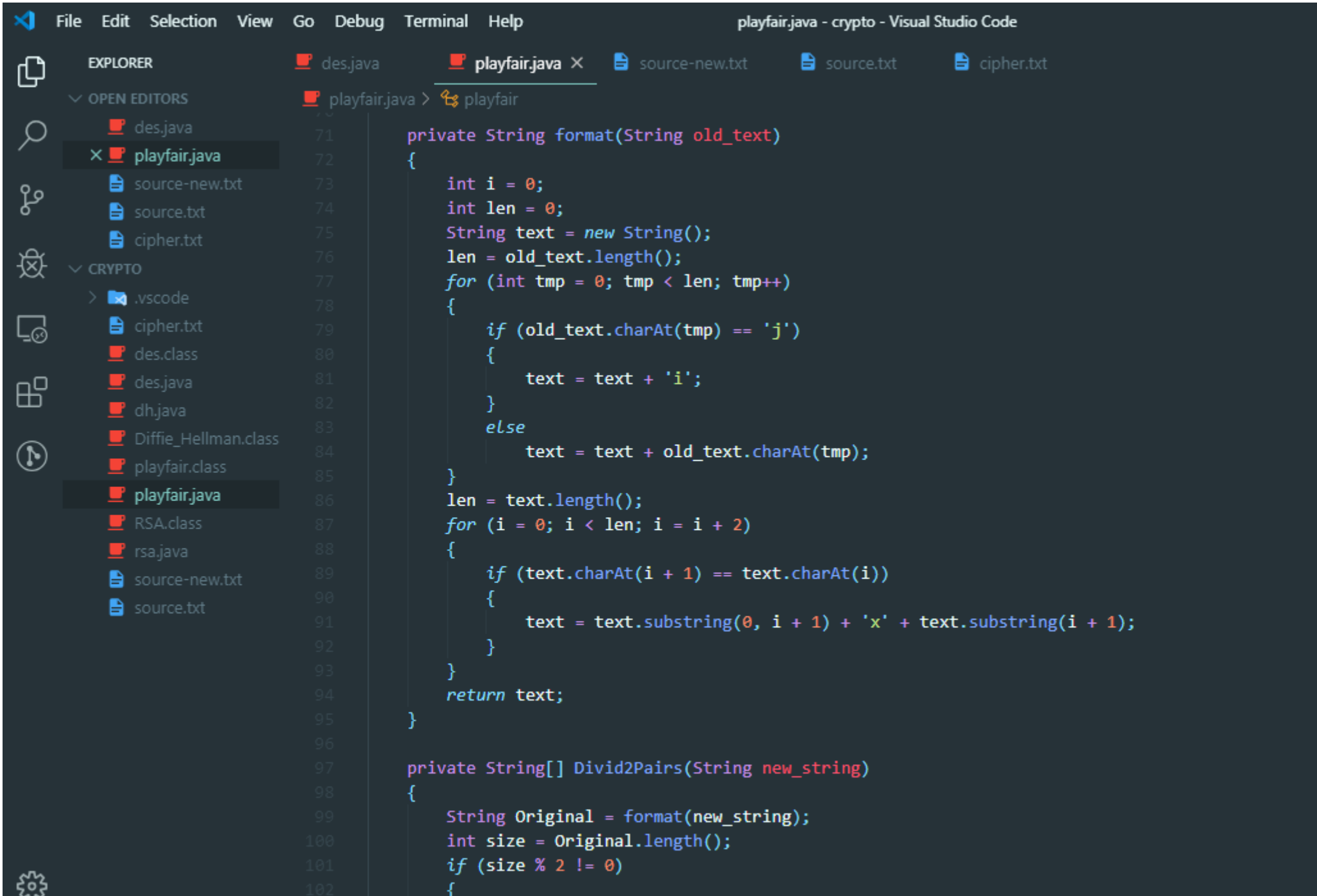
Cse-ccvt 2020

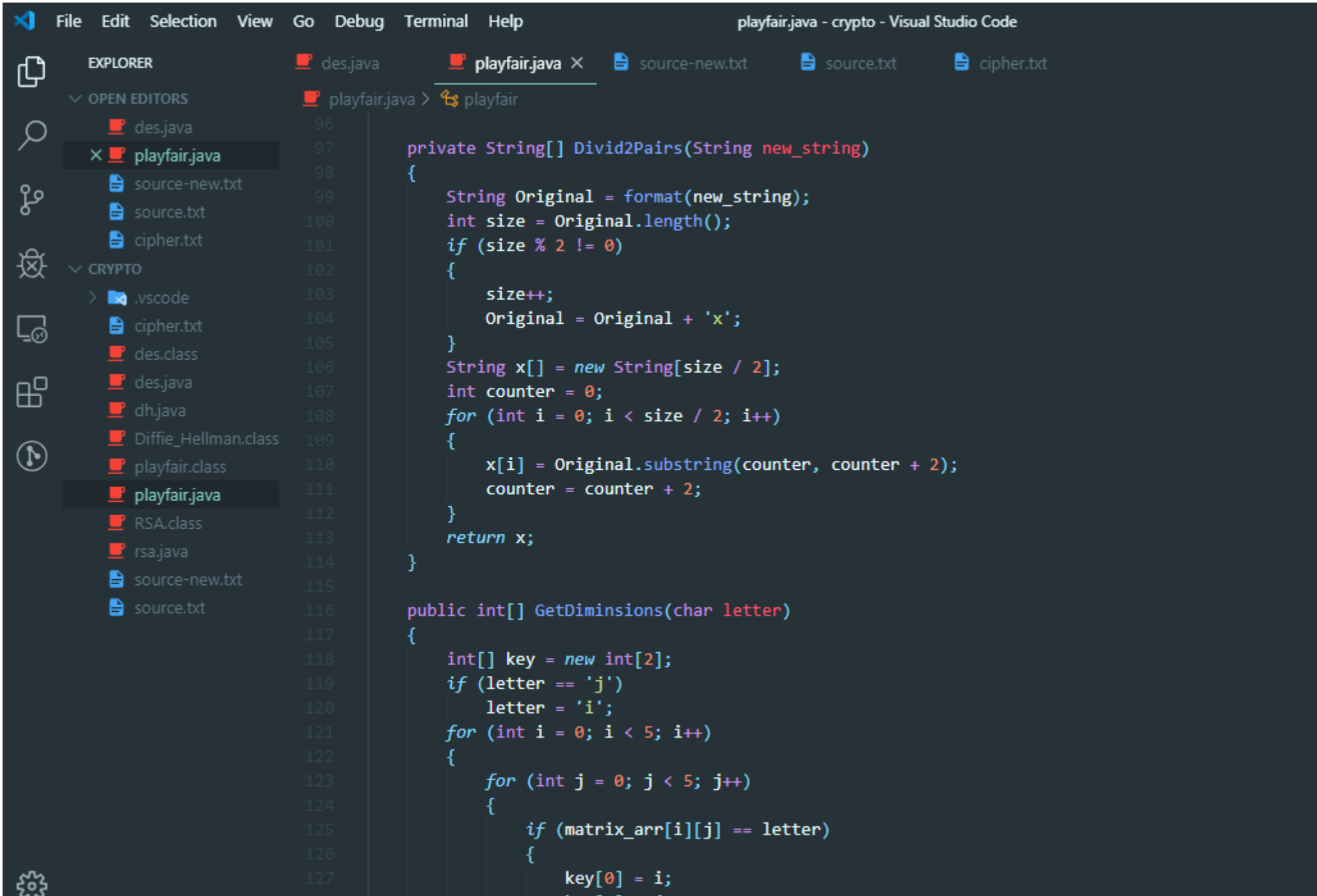
500053088 || R110216070

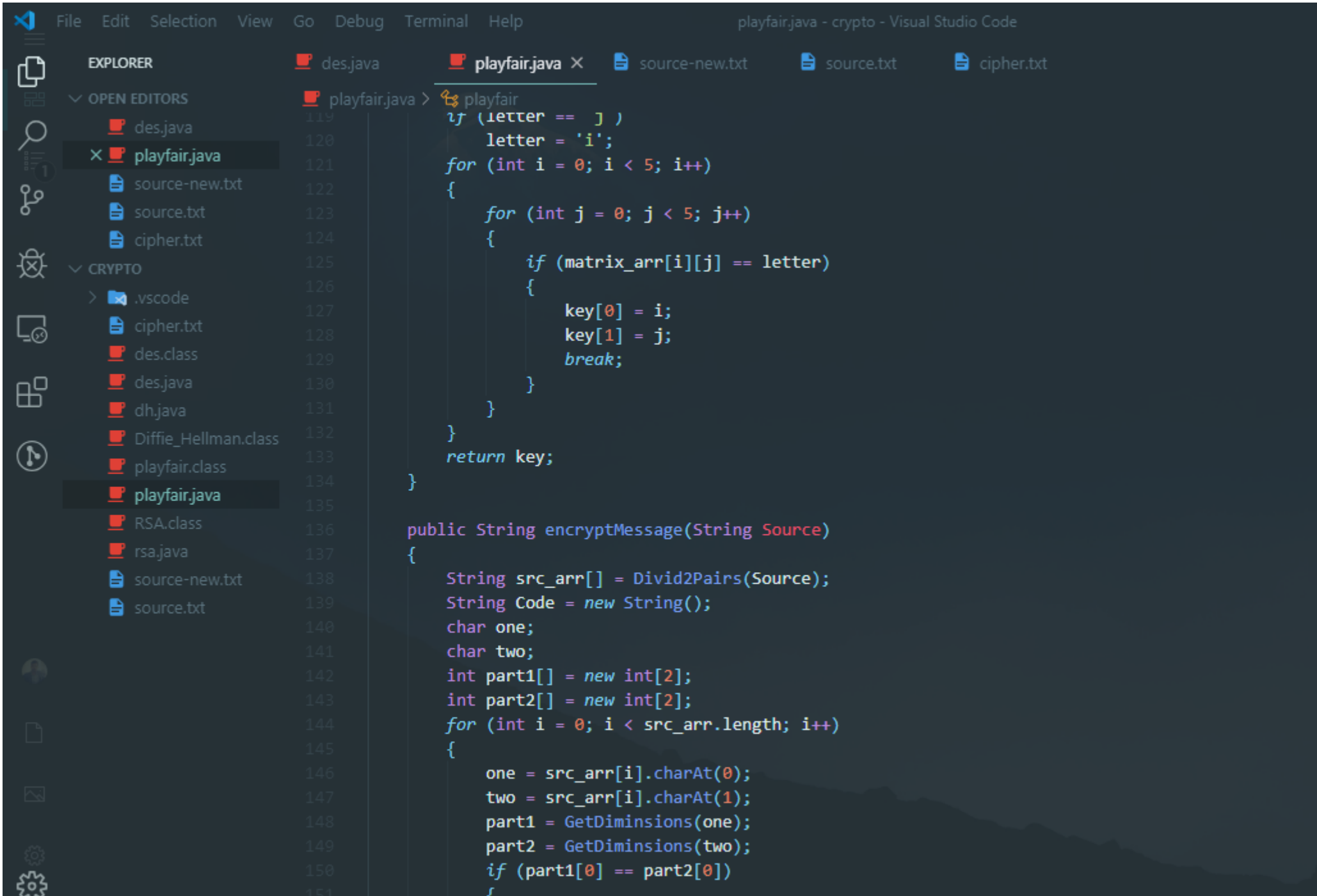

File Edit Selection View Go Debug Terminal Help
playfair.java - crypto - Visual Studio Code
EXPLORER
OPEN EDITORS
des.java
playfair.java
source-new.txt
source.txt
cipher.txt
CRYPTO
.vscode
cipher.txt
des.class
des.java
dh.java
Diffie_Hellman.class
playfair.class
playfair.java
RSA.class
rsa.java
source-new.txt
source.txt
des.java
playfair.java
source-new.txt
source.txt
cipher.txt
playfair.java > playfair
import java.util.Scanner;
public class playfair
{
private String KeyWord = new String();
private String Key = new String();
private char matrix_arr[][] = new char[5][5];
public void setKey(String k)
{
String K_adjust = new String();
boolean flag = false;
K_adjust = K_adjust + k.charAt(0);
for (int i = 1; i < k.length(); i++)
{
for (int j = 0; j < K_adjust.length(); j++)
{
if (k.charAt(i) == K_adjust.charAt(j))
{
flag = true;
}
}
if (flag == false)
K_adjust = K_adjust + k.charAt(i);
flag = false;
}
KeyWord = K_adjust;
}
public void KeyGen()
{
boolean flag = true;

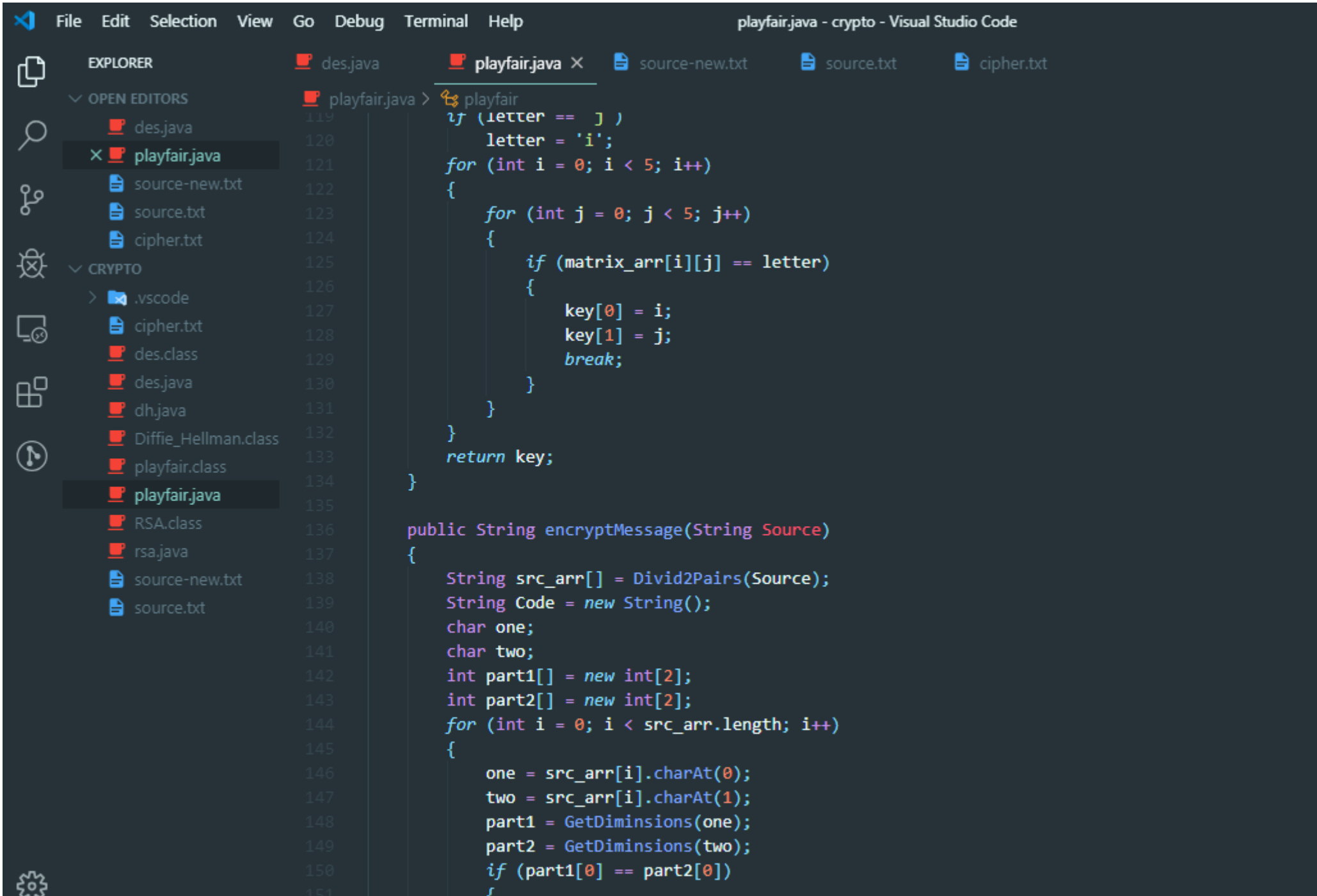

File Edit Selection View Go Debug Terminal Help
playfair.java - crypto - Visual Studio Code
EXPLORER
OPEN EDITORS
des.java
playfair.java
source-new.txt
source.txt
cipher.txt
CRYPTO
.vscode
cipher.txt
des.class
des.java
dh.java
Diffie_Hellman.class
playfair.class
playfair.java
RSA.class
rsa.java
source-new.txt
source.txt
des.java
playfair.java
source-new.txt
source.txt
cipher.txt
playfair.java > playfair
KeyWord = K_adjust;
}
public void KeyGen()
{
boolean flag = true;
char current;
Key = KeyWord;
for (int i = 0; i < 26; i++)
{
current = (char) (i + 97);
if (current == 'j')
continue;
for (int j = 0; j < KeyWord.length(); j++)
{
if (current == KeyWord.charAt(j))
{
flag = false;
break;
}
}
if (flag)
Key = Key + current;
flag = true;
}
System.out.println(Key);
matrix();
}
private void matrix()
{
int counter = 0;

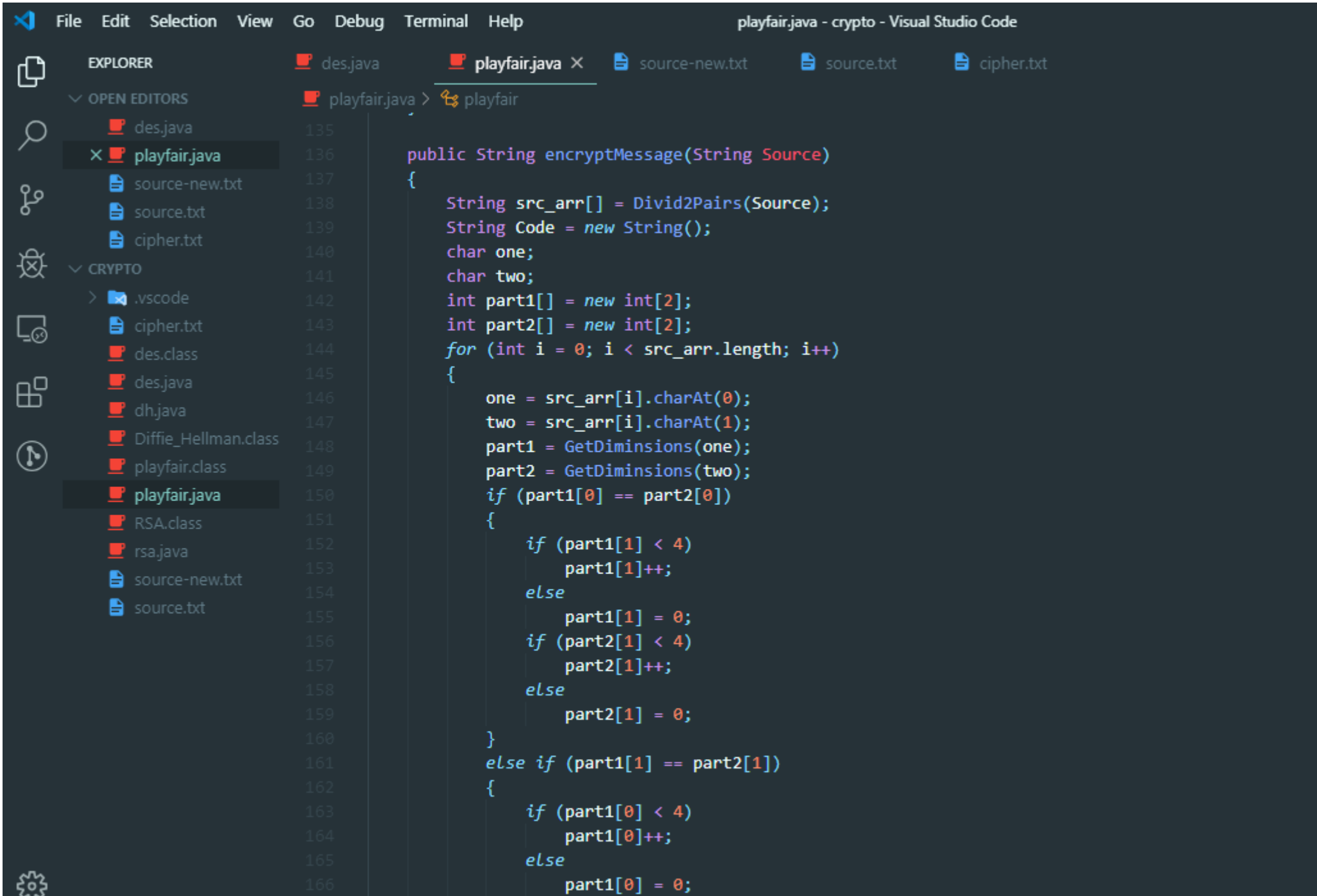

File Edit Selection View Go Debug Terminal Help
playfair.java - crypto - Visual Studio Code
EXPLORER
OPEN EDITORS
des.java
playfair.java
source-new.txt
source.txt
cipher.txt
CRYPTO
.vscode
cipher.txt
des.class
des.java
dh.java
Diffie_Hellman.class
playfair.class
playfair.java
RSA.class
rsa.java
source-new.txt
source.txt
des.java
playfair.java
source-new.txt
source.txt
cipher.txt
playfair.java > playfair
System.out.println(Key);
matrix();
}
private void matrix()
{
int counter = 0;
for (int i = 0; i < 5; i++)
{
for (int j = 0; j < 5; j++)
{
matrix_arr[i][j] = Key.charAt(counter);
System.out.print(matrix_arr[i][j] + " ");
counter++;
}
System.out.println();
}
}
private String format(String old_text)
{
int i = 0;
int len = 0;
String text = new String();
len = old_text.length();
for (int tmp = 0; tmp < len; tmp++)
{
if (old_text.charAt(tmp) == 'j')
{
text = text + 'i';
}
else

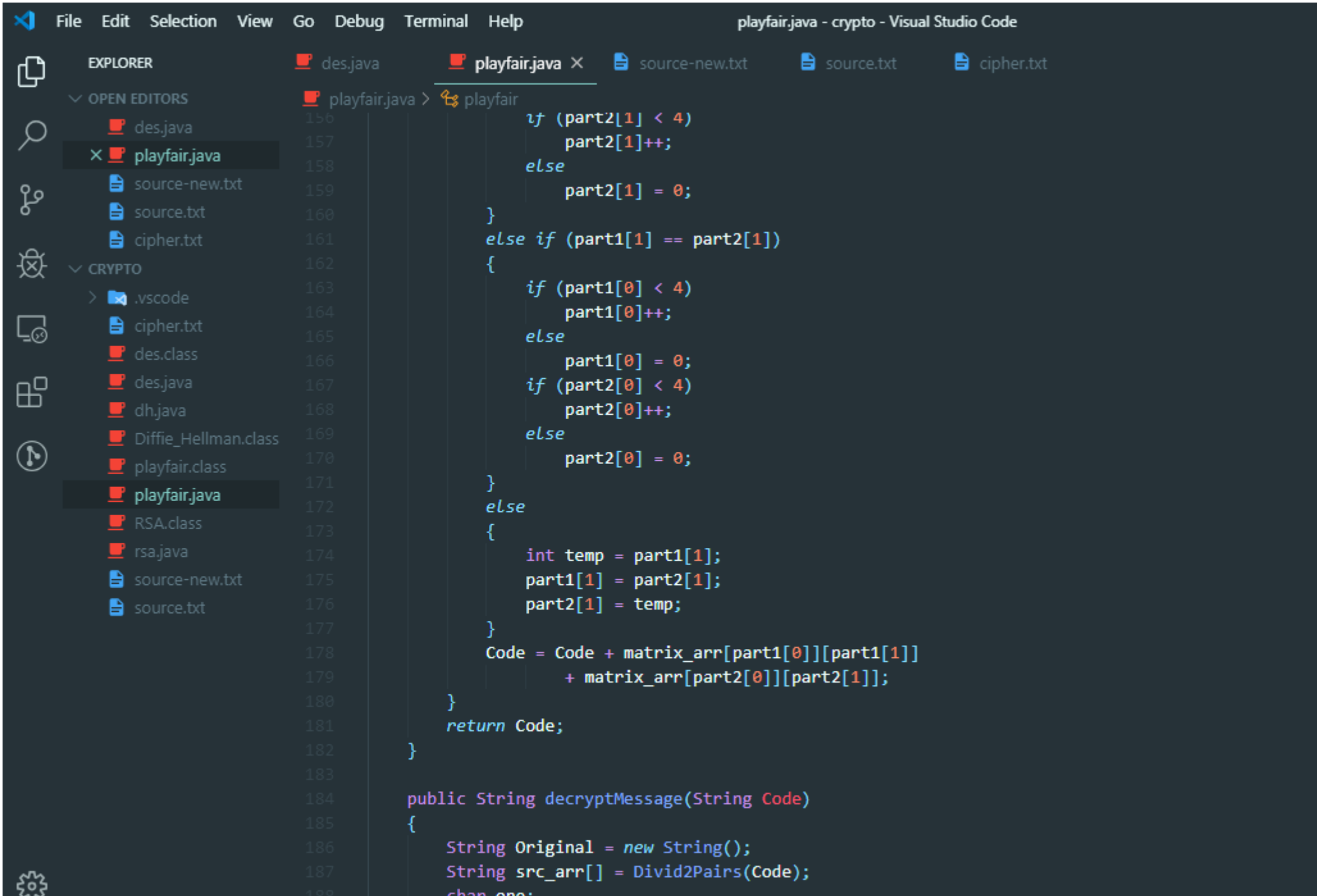

File Edit Selection View Go Debug Terminal Help
playfair.java - crypto - Visual Studio Code
EXPLORER
OPEN EDITORS
des.java
playfair.java
source-new.txt
source.txt
cipher.txt
CRYPTO
.vscode
cipher.txt
des.class
des.java
dh.java
Diffie_Hellman.class
playfair.class
playfair.java
RSA.class
rsa.java
source-new.txt
source.txt
des.java
playfair.java
source-new.txt
source.txt
cipher.txt
playfair.java > playfair
private String format(String old_text)
{
int i = 0;
int len = 0;
String text = new String();
len = old_text.length();
for (int tmp = 0; tmp < len; tmp++)
{
if (old_text.charAt(tmp) == 'j')
{
text = text + 'i';
}
else
text = text + old_text.charAt(tmp);
}
len = text.length();
for (i = 0; i < len; i = i + 2)
{
if (text.charAt(i + 1) == text.charAt(i))
{
text = text.substring(0, i + 1) + 'x' + text.substring(i + 1);
}
}
return text;
}
private String[] Divid2Pairs(String new_string)
{
String Original = format(new_string);
int size = Original.length();
if (size % 2 != 0)

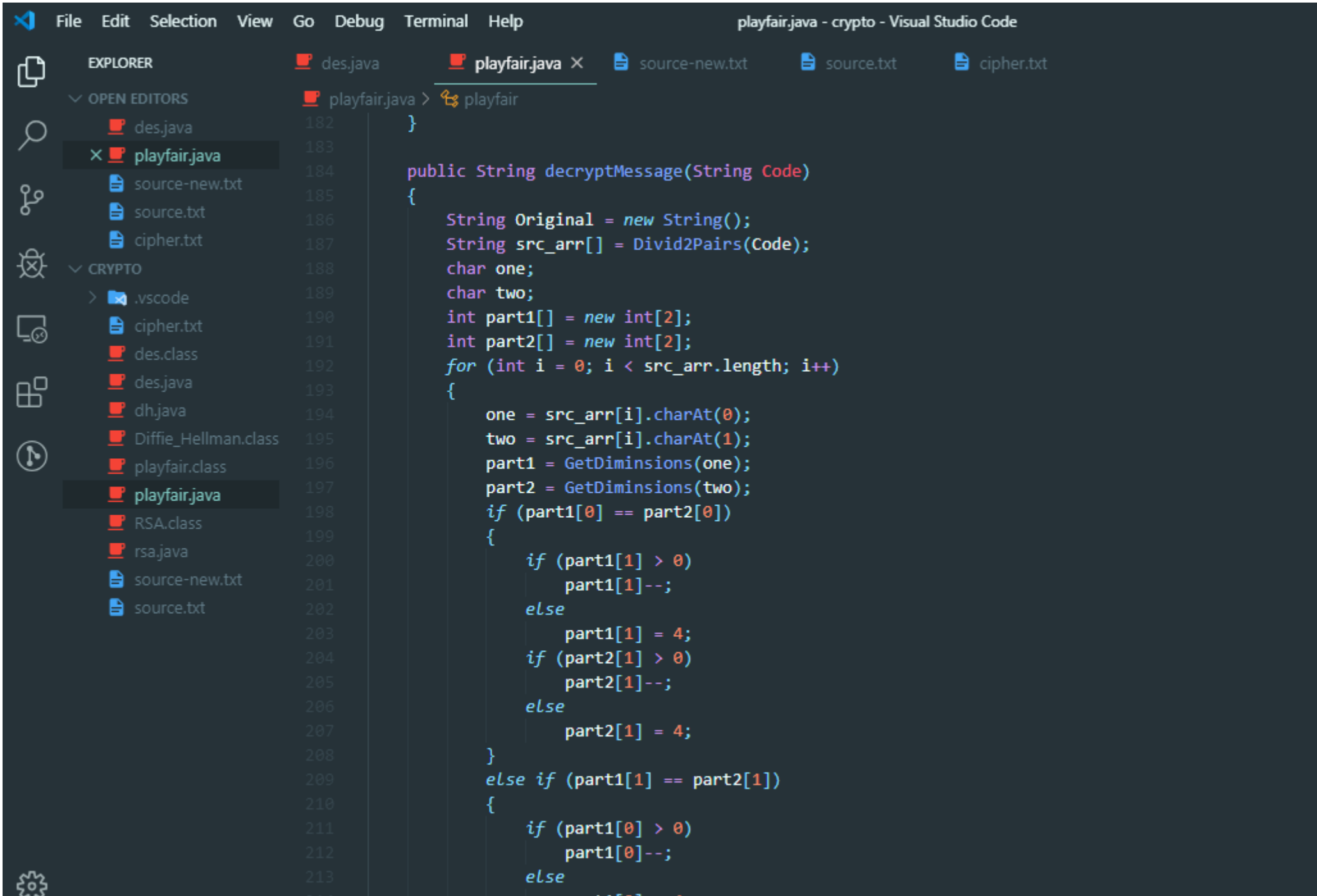

File Edit Selection View Go Debug Terminal Help
playfair.java - crypto - Visual Studio Code
EXPLORER
OPEN EDITORS
des.java
playfair.java
source-new.txt
source.txt
cipher.txt
CRYPTO
.vscode
cipher.txt
des.class
des.java
dh.java
Diffie_Hellman.class
playfair.class
playfair.java
RSA.class
rsa.java
source-new.txt
source.txt
des.java
playfair.java
source-new.txt
source.txt
cipher.txt
playfair.java > playfair
private String[] Divid2Pairs(String new_string)
{
String Original = format(new_string);
int size = Original.length();
if (size % 2 != 0)
{
size++;
Original = Original + 'x';
}
String x[] = new String[size / 2];
int counter = 0;
for (int i = 0; i < size / 2; i++)
{
x[i] = Original.substring(counter, counter + 2);
counter = counter + 2;
}
return x;
}
public int[] GetDiminsions(char letter)
{
int[] key = new int[2];
if (letter == 'j')
letter = 'i';
for (int i = 0; i < 5; i++)
{
for (int j = 0; j < 5; j++)
{
if (matrix_arr[i][j] == letter)
{
key[0] = i;

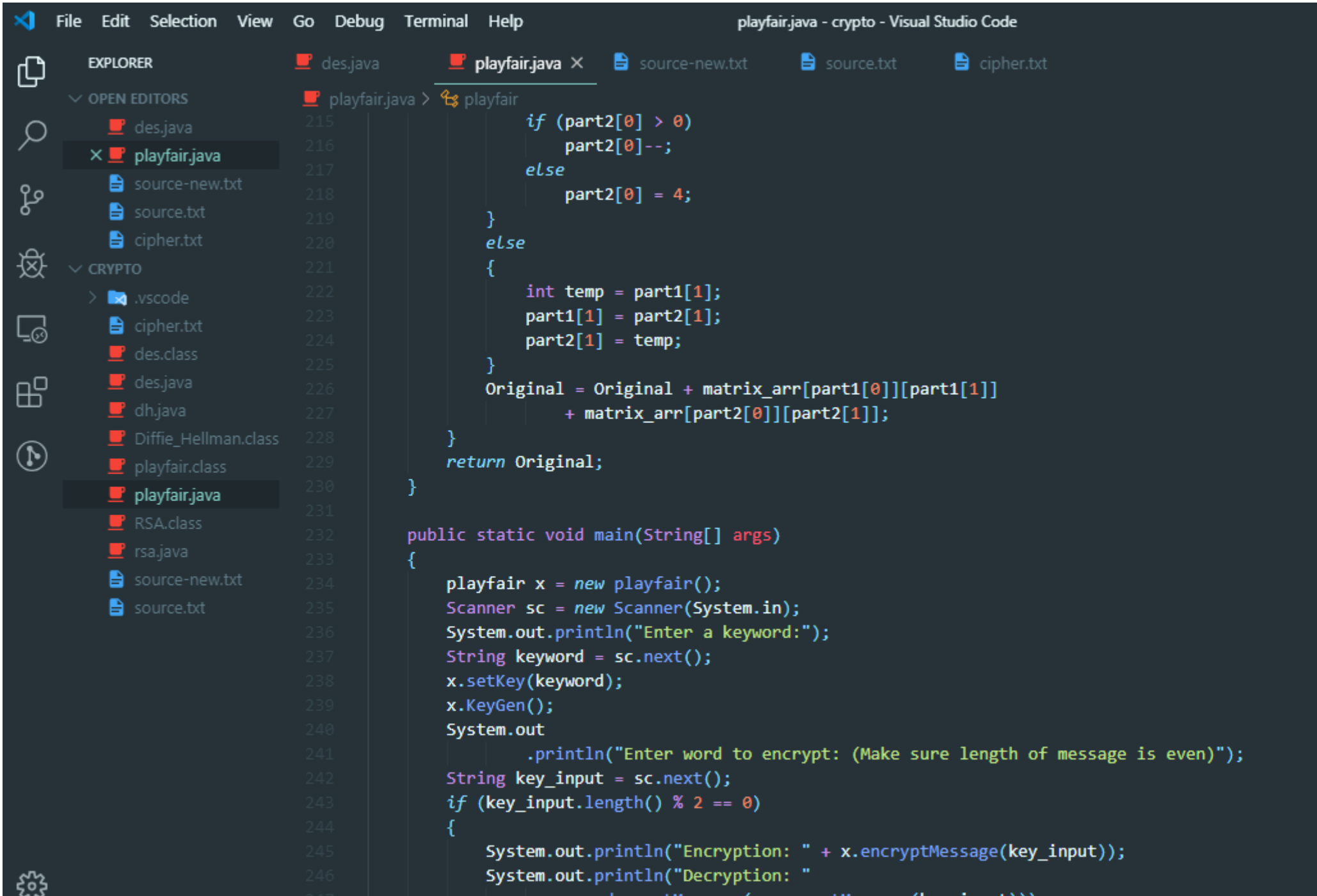

File Edit Selection View Go Debug Terminal Help
playfair.java - crypto - Visual Studio Code
EXPLORER
OPEN EDITORS
des.java
playfair.java
source-new.txt
source.txt
cipher.txt
CRYPTO
.vscode
cipher.txt
des.class
des.java
dh.java
Diffie_Hellman.class
playfair.class
playfair.java
RSA.class
rsa.java
source-new.txt
source.txt
des.java
playfair.java
source-new.txt
source.txt
cipher.txt
playfair.java > playfair
if (letter ==])
letter = 'i';
for (int i = 0; i < 5; i++)
{
for (int j = 0; j < 5; j++)
{
if (matrix_arr[i][j] == letter)
{
key[0] = i;
key[1] = j;
break;
}
}
}
return key;
}
public String encryptMessage(String Source)
{
String src_arr[] = Divid2Pairs(Source);
String Code = new String();
char one;
char two;
int part1[] = new int[2];
int part2[] = new int[2];
for (int i = 0; i < src_arr.length; i++)
{
one = src_arr[i].charAt(0);
two = src_arr[i].charAt(1);
part1 = GetDiminsions(one);
part2 = GetDiminsions(two);
if (part1[0] == part2[0])

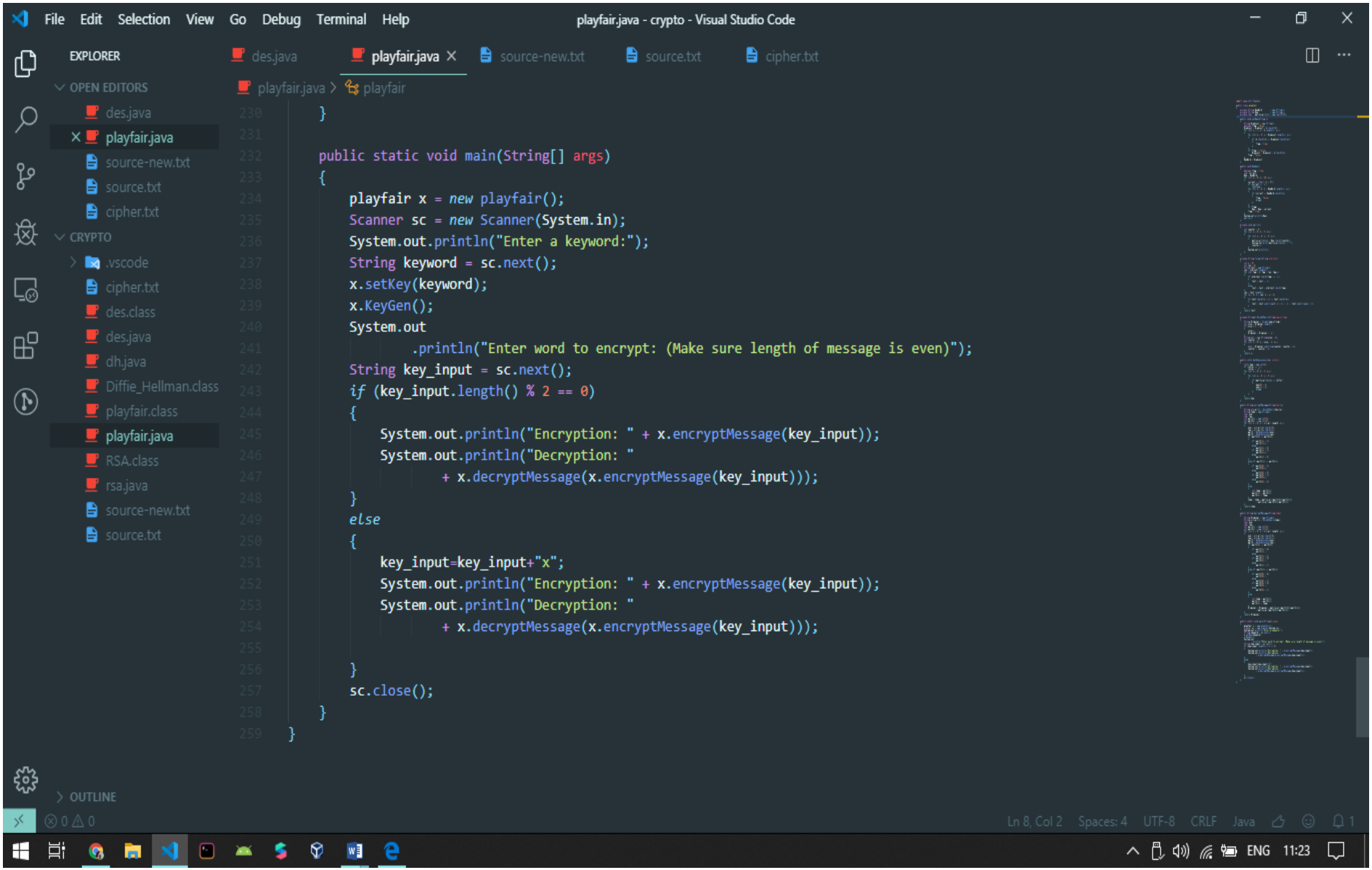

File Edit Selection View Go Debug Terminal Help
playfair.java - crypto - Visual Studio Code
EXPLORER
OPEN EDITORS
des.java
playfair.java
source-new.txt
source.txt
cipher.txt
CRYPTO
.vscode
cipher.txt
des.class
des.java
dh.java
Diffie_Hellman.class
playfair.class
playfair.java
RSA.class
rsa.java
source-new.txt
source.txt
des.java
playfair.java
source-new.txt
source.txt
cipher.txt
playfair.java > playfair
if (letter ==])
letter = 'i';
for (int i = 0; i < 5; i++)
{
for (int j = 0; j < 5; j++)
{
if (matrix_arr[i][j] == letter)
{
key[0] = i;
key[1] = j;
break;
}
}
}
return key;
}
public String encryptMessage(String Source)
{
String src_arr[] = Divid2Pairs(Source);
String Code = new String();
char one;
char two;
int part1[] = new int[2];
int part2[] = new int[2];
for (int i = 0; i < src_arr.length; i++)
{
one = src_arr[i].charAt(0);
two = src_arr[i].charAt(1);
part1 = GetDiminsions(one);
part2 = GetDiminsions(two);
if (part1[0] == part2[0])

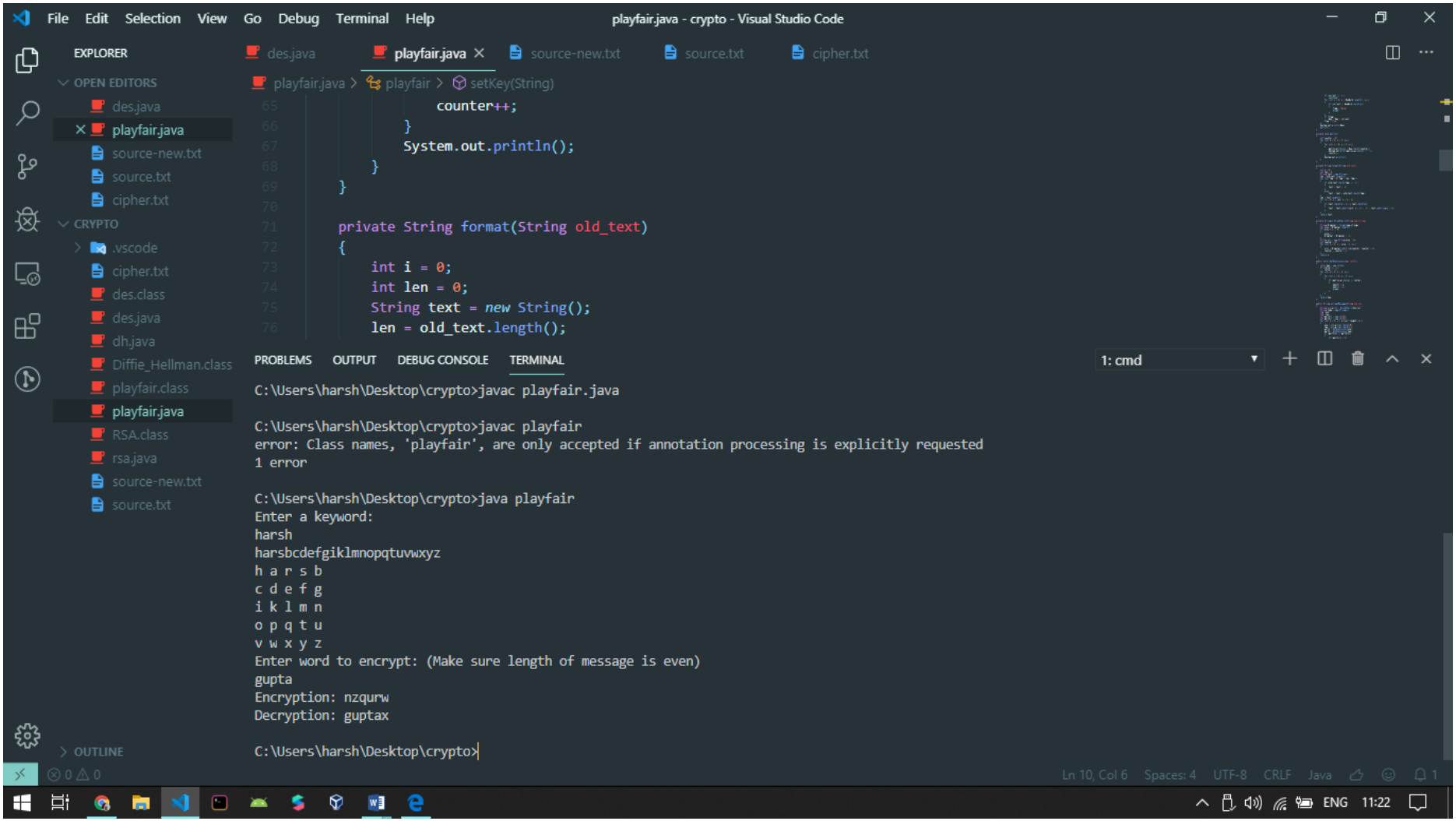

File Edit Selection View Go Debug Terminal Help
playfair.java - crypto - Visual Studio Code
EXPLORER
OPEN EDITORS
des.java
playfair.java
source-new.txt
source.txt
cipher.txt
CRYPTO
.vscode
cipher.txt
des.class
des.java
dh.java
Diffie_Hellman.class
playfair.class
playfair.java
RSA.class
rsa.java
source-new.txt
source.txt
des.java
playfair.java
source-new.txt
source.txt
cipher.txt
playfair.java > playfair
public String encryptMessage(String Source)
{
String src_arr[] = Divid2Pairs(Source);
String Code = new String();
char one;
char two;
int part1[] = new int[2];
int part2[] = new int[2];
for (int i = 0; i < src_arr.length; i++)
{
one = src_arr[i].charAt(0);
two = src_arr[i].charAt(1);
part1 = GetDiminsions(one);
part2 = GetDiminsions(two);
if (part1[0] == part2[0])
{
if (part1[1] < 4)
part1[1]++;
else
part1[1] = 0;
if (part2[1] < 4)
part2[1]++;
else
part2[1] = 0;
}
else if (part1[1] == part2[1])
{
if (part1[0] < 4)
part1[0]++;
else
part1[0] = 0;

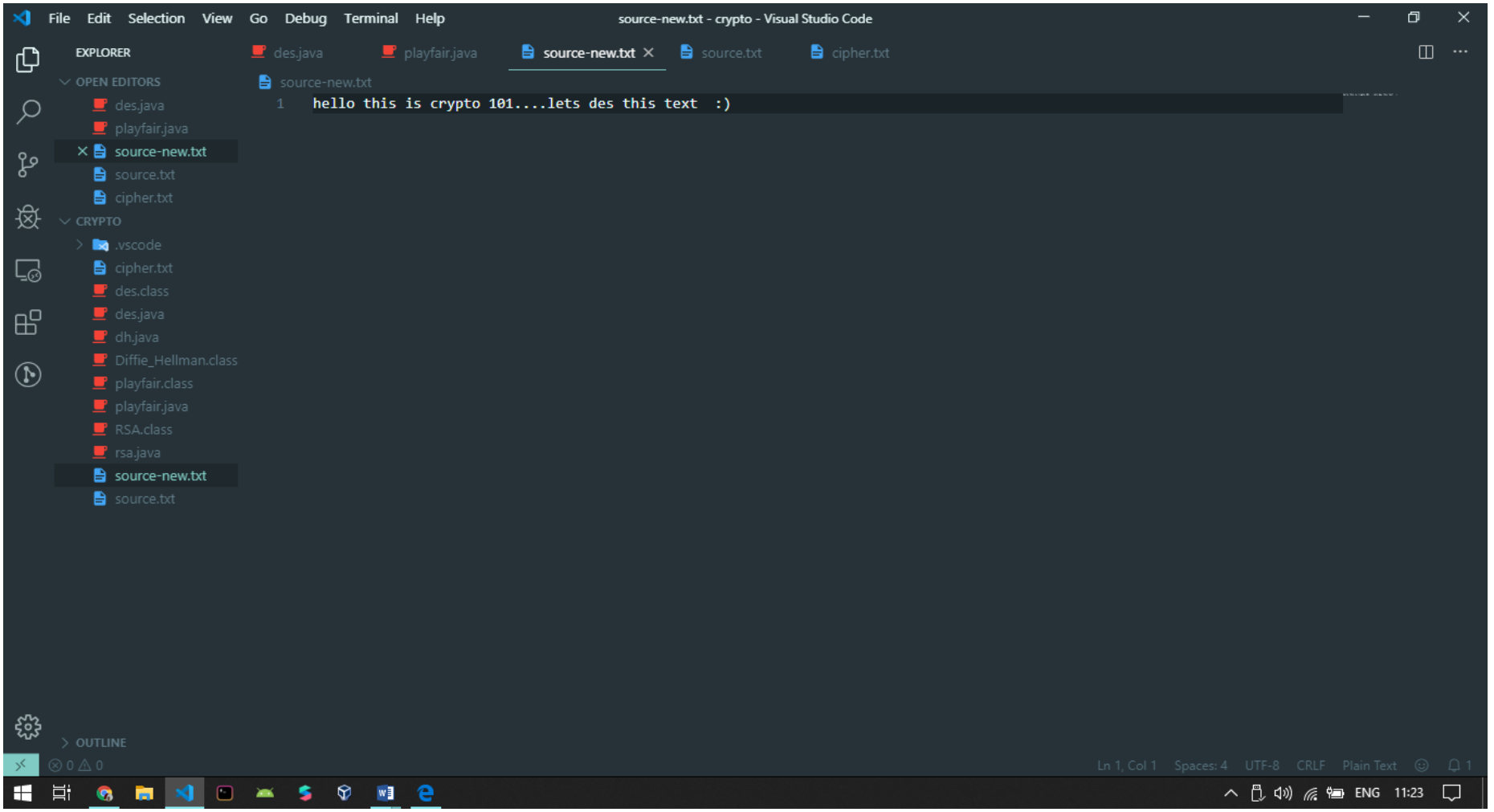

File Edit Selection View Go Debug Terminal Help
playfair.java - crypto - Visual Studio Code
EXPLORER
OPEN EDITORS
des.java
playfair.java
source-new.txt
source.txt
cipher.txt
CRYPTO
.vscode
cipher.txt
des.class
des.java
dh.java
Diffie_Hellman.class
playfair.class
playfair.java
RSA.class
rsa.java
source-new.txt
source.txt
des.java
playfair.java
source-new.txt
source.txt
cipher.txt
playfair.java > playfair
if (part2[1] < 4)
part2[1]++;
else
part2[1] = 0;
}
else if (part1[1] == part2[1])
{
if (part1[0] < 4)
part1[0]++;
else
part1[0] = 0;
if (part2[0] < 4)
part2[0]++;
else
part2[0] = 0;
}
else
{
int temp = part1[1];
part1[1] = part2[1];
part2[1] = temp;
}
Code = Code + matrix_arr[part1[0]][part1[1]]
+ matrix_arr[part2[0]][part2[1]];
}
return Code;
}
public String decryptMessage(String Code)
{
String Original = new String();
String src_arr[] = Divid2Pairs(Code);

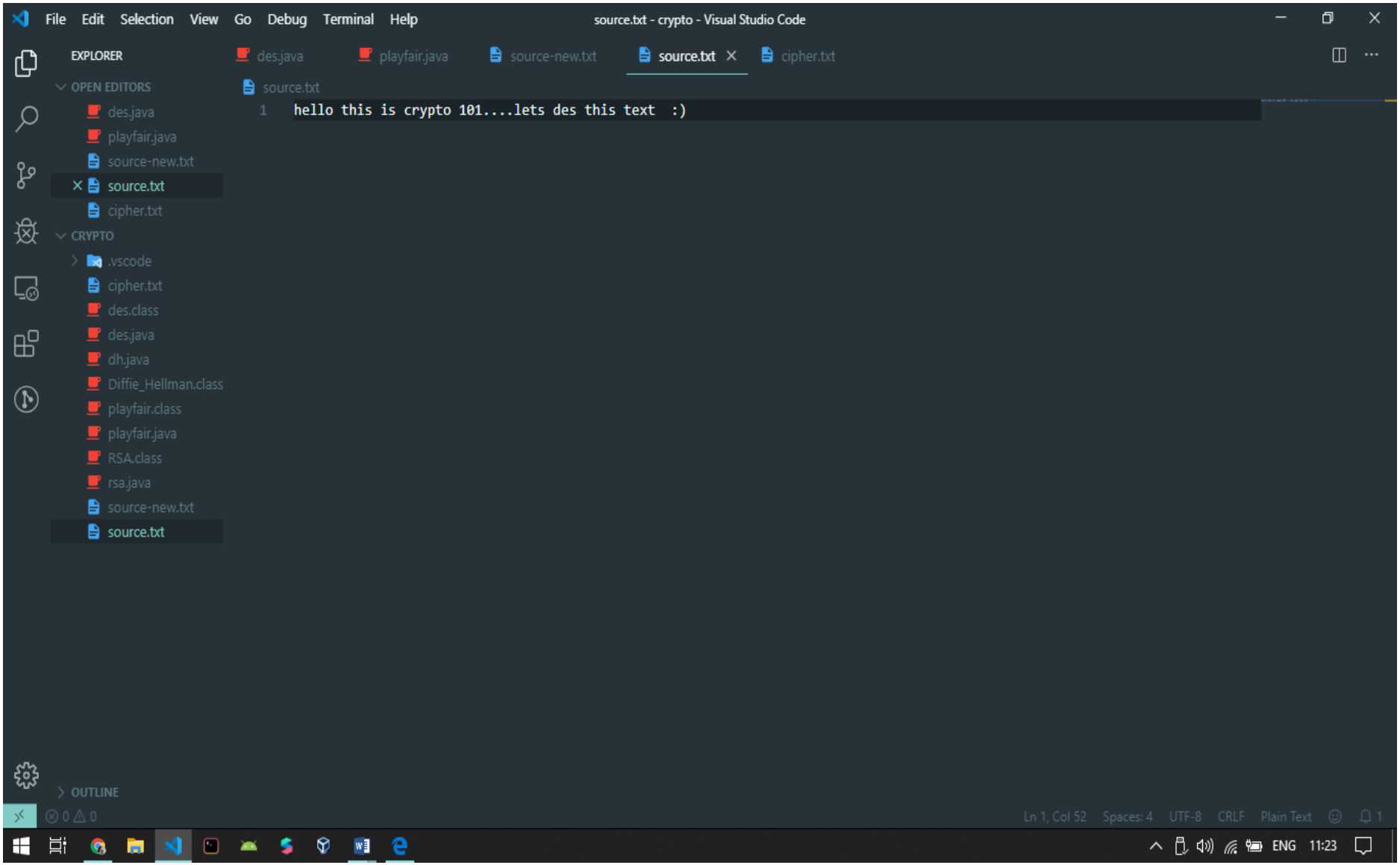

File Edit Selection View Go Debug Terminal Help
playfair.java - crypto - Visual Studio Code
EXPLORER
OPEN EDITORS
des.java
playfair.java
source-new.txt
source.txt
cipher.txt
CRYPTO
.vscode
cipher.txt
des.class
des.java
dh.java
Diffie_Hellman.class
playfair.class
playfair.java
RSA.class
rsa.java
source-new.txt
source.txt
des.java
playfair.java
source-new.txt
source.txt
cipher.txt
playfair.java > playfair
}
public String decryptMessage(String Code)
{
String Original = new String();
String src_arr[] = Divid2Pairs(Code);
char one;
char two;
int part1[] = new int[2];
int part2[] = new int[2];
for (int i = 0; i < src_arr.length; i++)
{
one = src_arr[i].charAt(0);
two = src_arr[i].charAt(1);
part1 = GetDiminsions(one);
part2 = GetDiminsions(two);
if (part1[0] == part2[0])
{
if (part1[1] > 0)
part1[1]--;
else
part1[1] = 4;
if (part2[1] > 0)
part2[1]--;
else
part2[1] = 4;
}
else if (part1[1] == part2[1])
{
if (part1[0] > 0)
part1[0]--;
else

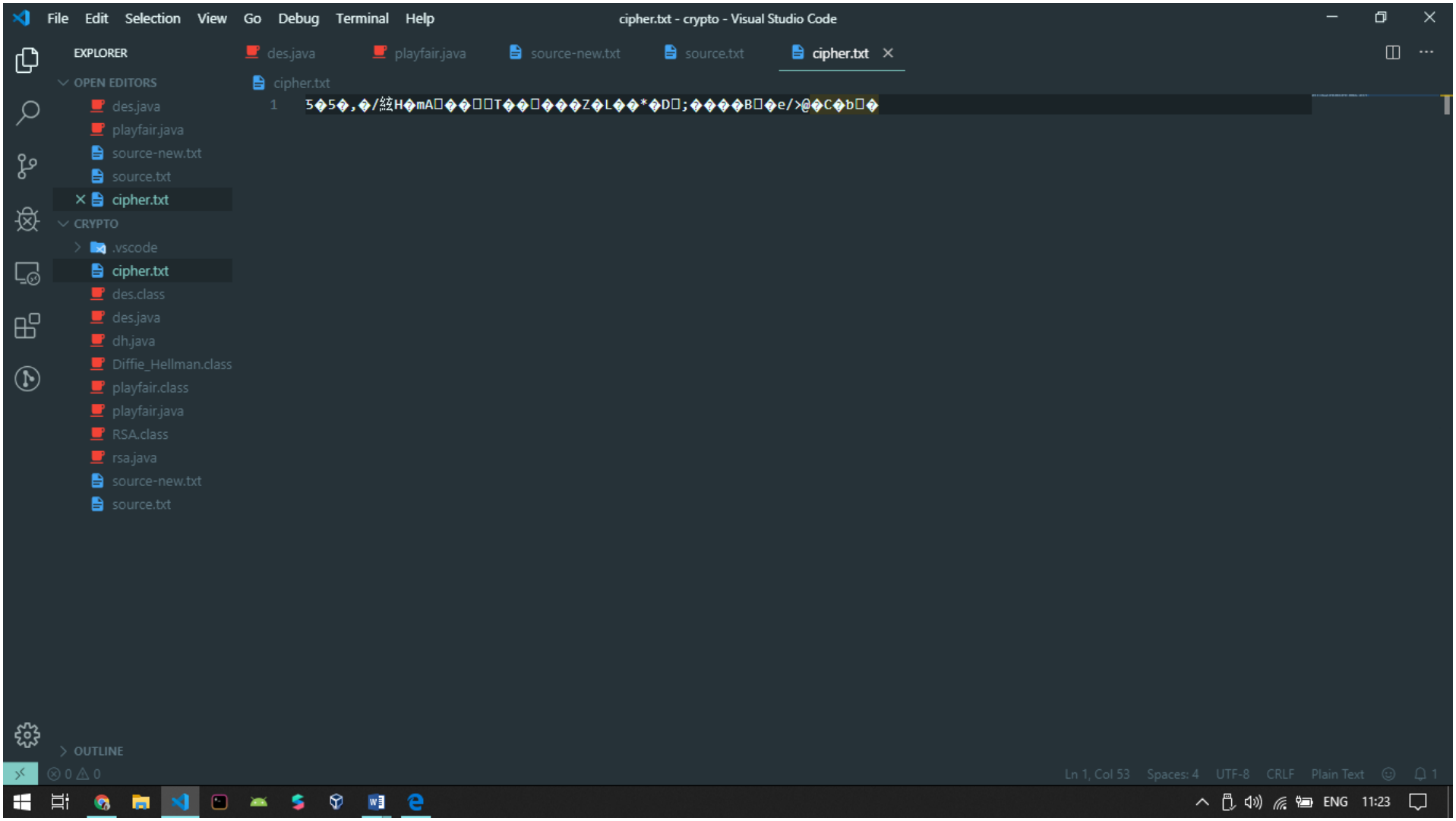

File Edit Selection View Go Debug Terminal Help
playfair.java - crypto - Visual Studio Code
EXPLORER
OPEN EDITORS
des.java
playfair.java
source-new.txt
source.txt
cipher.txt
CRYPTO
.vscode
cipher.txt
des.class
des.java
dh.java
Diffie_Hellman.class
playfair.class
playfair.java
RSA.class
rsa.java
source-new.txt
source.txt
des.java
playfair.java
source-new.txt
source.txt
cipher.txt
playfair.java > playfair
if (part2[0] > 0)
part2[0]--;
else
part2[0] = 4;
}
else
{
int temp = part1[1];
part1[1] = part2[1];
part2[1] = temp;
}
Original = Original + matrix_arr[part1[0]][part1[1]]
+ matrix_arr[part2[0]][part2[1]];
}
return Original;
}
public static void main(String[] args)
{
playfair x = new playfair();
Scanner sc = new Scanner(System.in);
System.out.println("Enter a keyword:");
String keyword = sc.next();
x.setKey(keyword);
x.KeyGen();
System.out
.println("Enter word to encrypt: (Make sure length of message is even)");
String key_input = sc.next();
if (key_input.length() % 2 == 0)
{
System.out.println("Encryption: " + x.encryptMessage(key_input));
System.out.println("Decryption: "

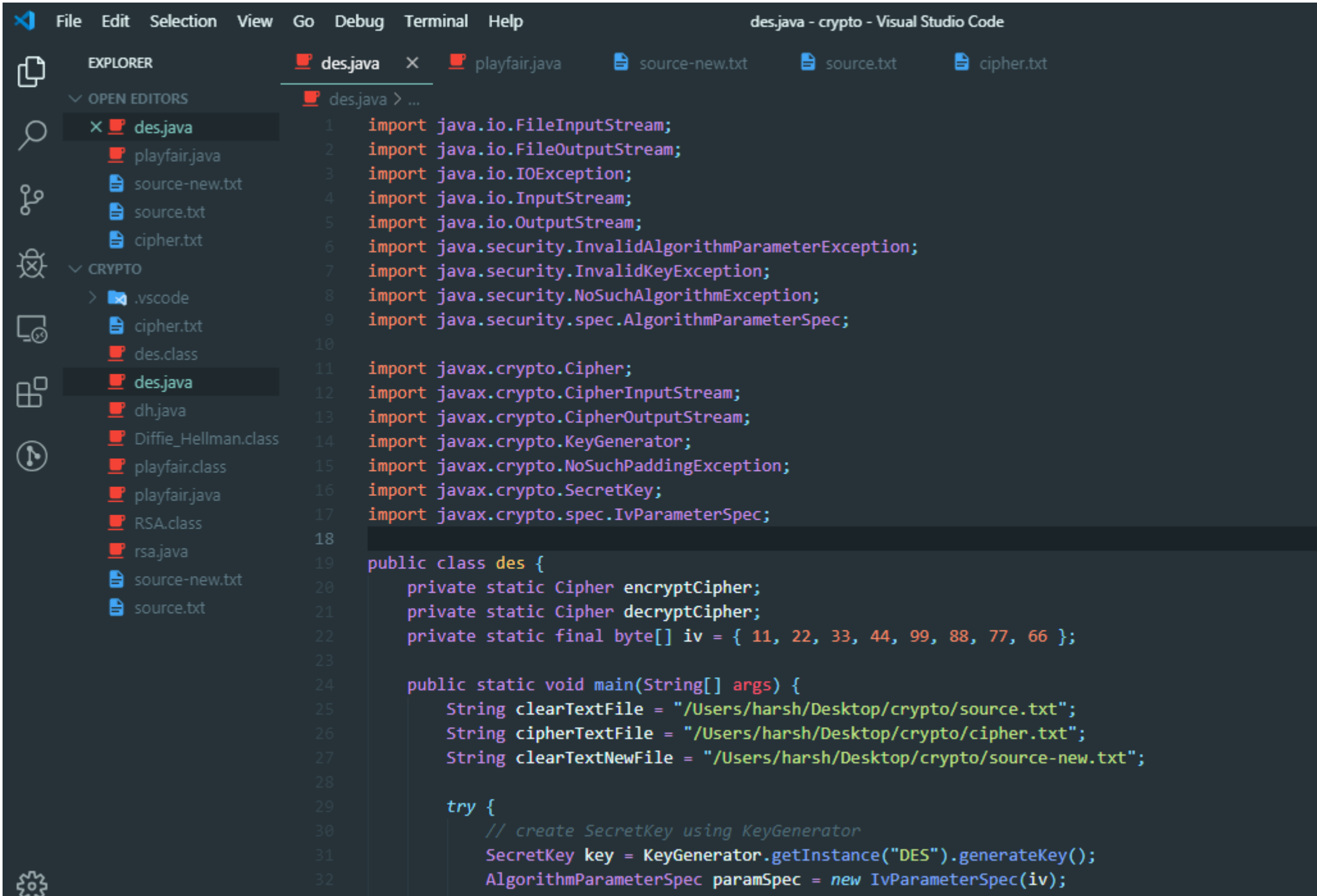

File Edit Selection View Go Debug Terminal Help
playfair.java - crypto - Visual Studio Code
EXPLORER
OPEN EDITORS
des.java
playfair.java
source-new.txt
source.txt
cipher.txt
CRYPTO
.vscode
cipher.txt
des.class
des.java
dh.java
Diffie_Hellman.class
playfair.class
playfair.java
RSA.class
rsa.java
source-new.txt
source.txt
OUTLINE
playfair.java > playfair
}
public static void main(String[] args)
{
playfair x = new playfair();
Scanner sc = new Scanner(System.in);
System.out.println("Enter a keyword:");
String keyword = sc.next();
x.setKey(keyword);
x.KeyGen();
System.out
.println("Enter word to encrypt: (Make sure length of message is even)");
String key_input = sc.next();
if (key_input.length() % 2 == 0)
{
System.out.println("Encryption: " + x.encryptMessage(key_input));
System.out.println("Decryption: "
+ x.decryptMessage(x.encryptMessage(key_input)));
}
else
{
key_input=key_input+"x";
System.out.println("Encryption: " + x.encryptMessage(key_input));
System.out.println("Decryption: "
+ x.decryptMessage(x.encryptMessage(key_input)));
}
sc.close();
}
}
Ln 8, Col 2 Spaces: 4 UTF-8 CRLF Java
ENG 11:23

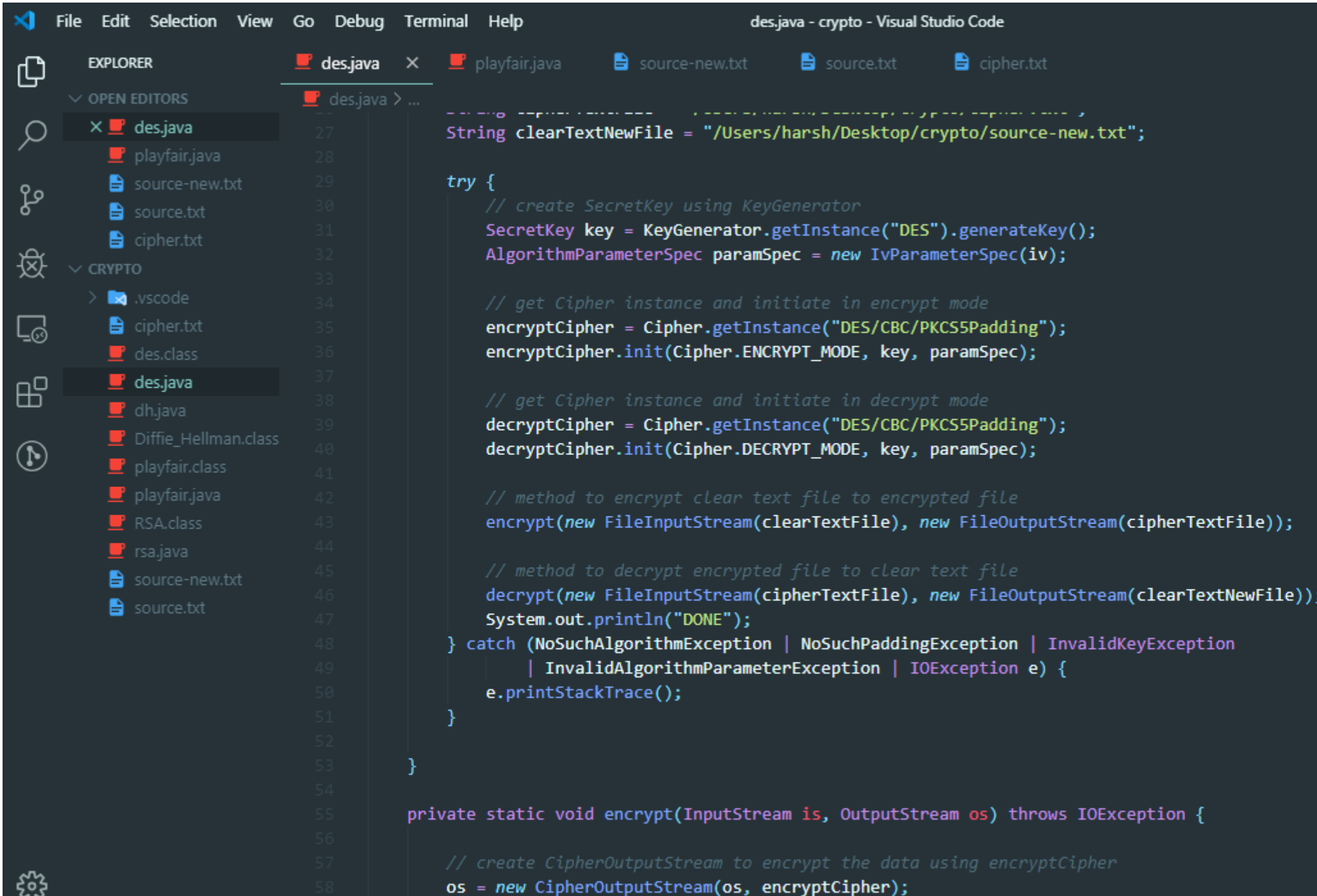

File Edit Selection View Go Debug Terminal Help
playfair.java - crypto - Visual Studio Code
EXPLORER
OPEN EDITORS
des.java
playfair.java
source-new.txt
source.txt
cipher.txt
CRYPTO
.vscode
cipher.txt
des.class
des.java
dh.java
Diffie_Hellman.class
playfair.class
playfair.java
RSA.class
rsa.java
source-new.txt
source.txt
OUTLINE
playfair.java > playfair > setKey(String)
counter++;
}
System.out.println();
}
}
private String format(String old_text)
{
int i = 0;
int len = 0;
String text = new String();
len = old_text.length();
PROBLEMS OUTPUT DEBUG CONSOLE TERMINAL
1: cmd
C:\Users\harsh\Desktop\crypto>javac playfair.java
C:\Users\harsh\Desktop\crypto>javac playfair
error: Class names, 'playfair', are only accepted if annotation processing is explicitly requested
1 error
C:\Users\harsh\Desktop\crypto>java playfair
Enter a keyword:
harsh
harsbcdefgiklmnopqtuvwxyz
h a r s b
c d e f g
i k l m n
o p q t u
v w x y z
Enter word to encrypt: (Make sure length of message is even)
gupta
Encryption: nzqurw
Decryption: guptax
C:\Users\harsh\Desktop\crypto>
Ln 10, Col 6 Spaces: 4 UTF-8 CRLF Java
ENG 11:22

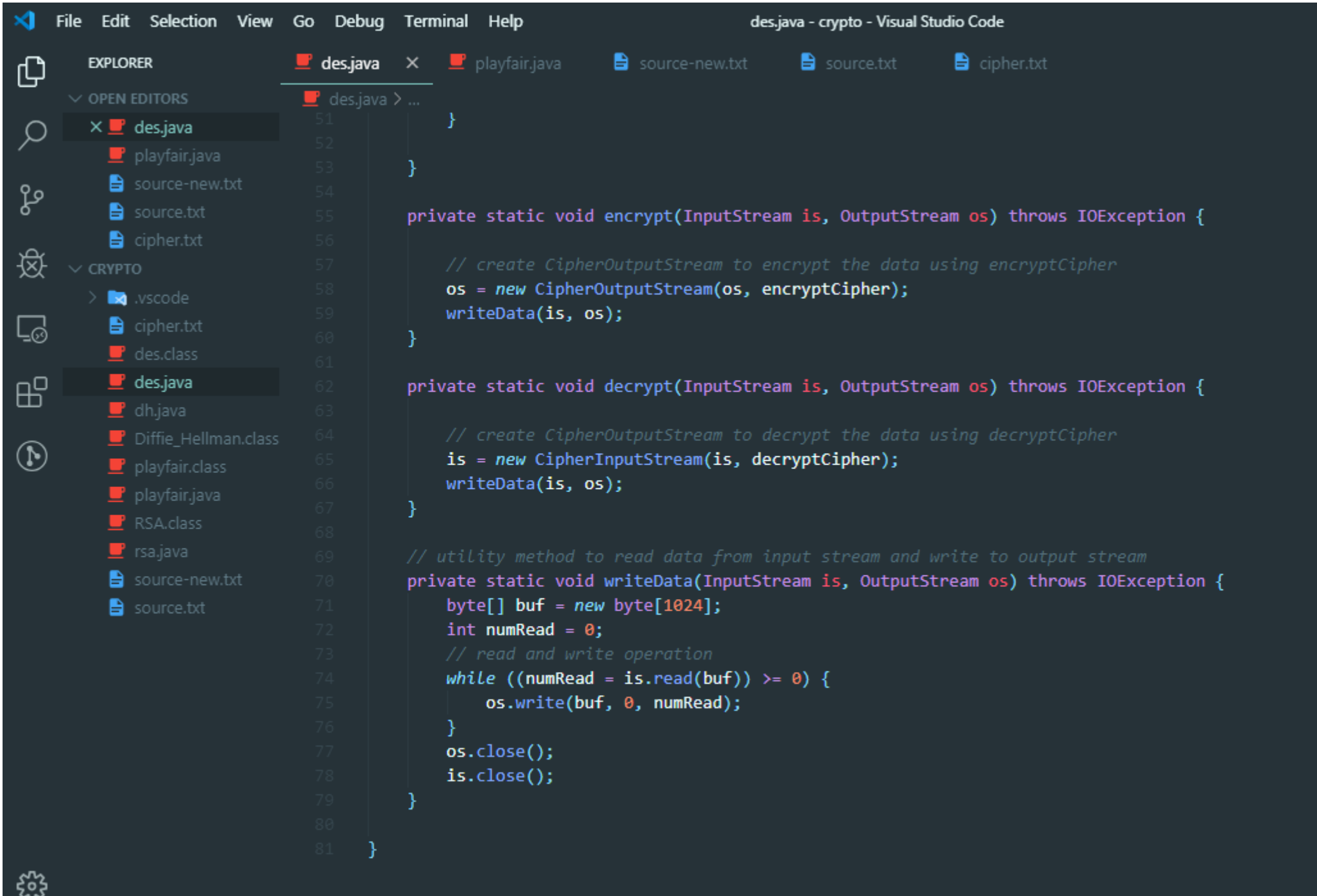

File Edit Selection View Go Debug Terminal Help
source-new.txt - crypto - Visual Studio Code
EXPLORER
des.java
playfair.java
source-new.txt
source.txt
cipher.txt
OPEN EDITORS
CRYPTO
.vscode
dh.java
Diffie_Hellman.class
playfair.class
RSA.class
rsa.java
OUTLINE
hello this is crypto 101....lets des this text :)
Ln 1, Col 1
Spaces: 4
UTF-8
CRLF
Plain Text
ENG
11:23


File Edit Selection View Go Debug Terminal Help
source.txt - crypto - Visual Studio Code
EXPLORER
des.java
playfair.java
source-new.txt
source.txt
cipher.txt
OPEN EDITORS
CRYPTO
.vscode
dh.java
Diffie_Hellman.class
RSA.class
rsa.java
1 hello this is crypto 101....lets des this text :)
OUTLINE
Ln 1, Col 52 Spaces: 4 UTF-8 CRLF Plain Text
ENG 11:23


File Edit Selection View Go Debug Terminal Help
cipher.txt - crypto - Visual Studio Code
EXPLORER
des.java
playfair.java
source-new.txt
source.txt
cipher.txt
OPEN EDITORS
CRYPTO
.vscode
des.class
dh.java
Diffie_Hellman.class
playfair.class
RSA.class
rsa.java
OUTLINE
Ln 1, Col 53
Spaces: 4
UTF-8
CRLF
Plain Text
ENG
11:23


File Edit Selection View Go Debug Terminal Help
des.java - crypto - Visual Studio Code
EXPLORER
OPEN EDITORS
des.java
playfair.java
source-new.txt
source.txt
cipher.txt
CRYPTO
.vscode
cipher.txt
des.class
des.java
dh.java
Diffie_Hellman.class
playfair.class
playfair.java
RSA.class
rsa.java
source-new.txt
source.txt
des.java
playfair.java
source-new.txt
source.txt
cipher.txt
des.java > ...
import java.io.FileInputStream;
import java.io.FileOutputStream;
import java.io.IOException;
import java.io.InputStream;
import java.io.OutputStream;
import java.security.InvalidAlgorithmParameterException;
import java.security.InvalidKeyException;
import java.security.NoSuchAlgorithmException;
import java.security.spec.AlgorithmParameterSpec;
import javax.crypto.Cipher;
import javax.crypto.CipherInputStream;
import javax.crypto.CipherOutputStream;
import javax.crypto.KeyGenerator;
import javax.crypto.NoSuchPaddingException;
import javax.crypto.SecretKey;
import javax.crypto.spec.IvParameterSpec;
public class des {
private static Cipher encryptCipher;
private static Cipher decryptCipher;
private static final byte[] iv = { 11, 22, 33, 44, 99, 88, 77, 66 };
public static void main(String[] args) {
String clearTextFile = "/Users/harsh/Desktop/crypto/source.txt";
String cipherTextFile = "/Users/harsh/Desktop/crypto/cipher.txt";
String clearTextNewFile = "/Users/harsh/Desktop/crypto/source-new.txt";
try {
// create SecretKey using KeyGenerator
SecretKey key = KeyGenerator.getInstance("DES").generateKey();
AlgorithmParameterSpec paramSpec = new IvParameterSpec(iv);


File Edit Selection View Go Debug Terminal Help
des.java - crypto - Visual Studio Code
EXPLORER
OPEN EDITORS
des.java
playfair.java
source-new.txt
source.txt
cipher.txt
CRYPTO
.vscode
cipher.txt
des.class
des.java
dh.java
Diffie_Hellman.class
playfair.class
playfair.java
RSA.class
rsa.java
source-new.txt
source.txt
des.java
playfair.java
source-new.txt
source.txt
cipher.txt
des.java > ...
String clearTextNewFile = "/Users/harsh/Desktop/crypto/source-new.txt";
try {
// create SecretKey using KeyGenerator
SecretKey key = KeyGenerator.getInstance("DES").generateKey();
AlgorithmParameterSpec paramSpec = new IvParameterSpec(iv);
// get Cipher instance and initiate in encrypt mode
encryptCipher = Cipher.getInstance("DES/CBC/PKCS5Padding");
encryptCipher.init(Cipher.ENCRYPT_MODE, key, paramSpec);
// get Cipher instance and initiate in decrypt mode
decryptCipher = Cipher.getInstance("DES/CBC/PKCS5Padding");
decryptCipher.init(Cipher.DECRYPT_MODE, key, paramSpec);
// method to encrypt clear text file to encrypted file
encrypt(new FileInputStream(clearTextFile), new FileOutputStream(cipherTextFile));
// method to decrypt encrypted file to clear text file
decrypt(new FileInputStream(cipherTextFile), new FileOutputStream(clearTextNewFile));
System.out.println("DONE");
} catch (NoSuchAlgorithmException | NoSuchPaddingException | InvalidKeyException
| InvalidAlgorithmParameterException | IOException e) {
e.printStackTrace();
}
}
private static void encrypt(InputStream is, OutputStream os) throws IOException {
// create CipherOutputStream to encrypt the data using encryptCipher
os = new CipherOutputStream(os, encryptCipher);


File Edit Selection View Go Debug Terminal Help
des.java - crypto - Visual Studio Code
EXPLORER
OPEN EDITORS
des.java
playfair.java
source-new.txt
source.txt
cipher.txt
CRYPTO
.vscode
cipher.txt
des.class
des.java
dh.java
Diffie_Hellman.class
playfair.class
playfair.java
RSA.class
rsa.java
source-new.txt
source.txt
des.java
playfair.java
source-new.txt
source.txt
cipher.txt
des.java > ...
}
}
private static void encrypt(InputStream is, OutputStream os) throws IOException {
// create CipherOutputStream to encrypt the data using encryptCipher
os = new CipherOutputStream(os, encryptCipher);
writeData(is, os);
}
private static void decrypt(InputStream is, OutputStream os) throws IOException {
// create CipherOutputStream to decrypt the data using decryptCipher
is = new CipherInputStream(is, decryptCipher);
writeData(is, os);
}
// utility method to read data from input stream and write to output stream
private static void writeData(InputStream is, OutputStream os) throws IOException {
byte[] buf = new byte[1024];
int numRead = 0;
// read and write operation
while ((numRead = is.read(buf)) >= 0) {
os.write(buf, 0, numRead);
}
os.close();
is.close();
}
}