

Cryptography theory

Harsh Gupta

Cse-ccvt 2020

500053088 || R110216070



## 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

```

1  import java.util.Scanner;
2
3  public class playfair
4  {
5      private String KeyWord      = new String();
6      private String Key          = new String();
7      private char  matrix_arr[][] = new char[5][5];
8
9      public void setKey(String k)
10     {
11         String K_adjust = new String();
12         boolean flag = false;
13         K_adjust = K_adjust + k.charAt(0);
14         for (int i = 1; i < k.length(); i++)
15         {
16             for (int j = 0; j < K_adjust.length(); j++)
17             {
18                 if (k.charAt(i) == K_adjust.charAt(j))
19                 {
20                     flag = true;
21                 }
22             }
23             if (flag == false)
24                 K_adjust = K_adjust + k.charAt(i);
25             flag = false;
26         }
27         KeyWord = K_adjust;
28     }
29
30     public void KeyGen()
31     {
32         boolean flag = true;

```

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 X source-new.txt source.txt cipher.txt

```

playfair.java > playfair
27     Keyword = K_adjust;
28 }
29
30 public void KeyGen()
31 {
32     boolean flag = true;
33     char current;
34     Key = Keyword;
35     for (int i = 0; i < 26; i++)
36     {
37         current = (char) (i + 97);
38         if (current == 'j')
39             continue;
40         for (int j = 0; j < Keyword.length(); j++)
41         {
42             if (current == Keyword.charAt(j))
43             {
44                 flag = false;
45                 break;
46             }
47         }
48         if (flag)
49             Key = Key + current;
50         flag = true;
51     }
52     System.out.println(Key);
53     matrix();
54 }
55
56 private void matrix()
57 {
58     int counter = 0;
59     for (int i = 0; i < 26; i++)

```

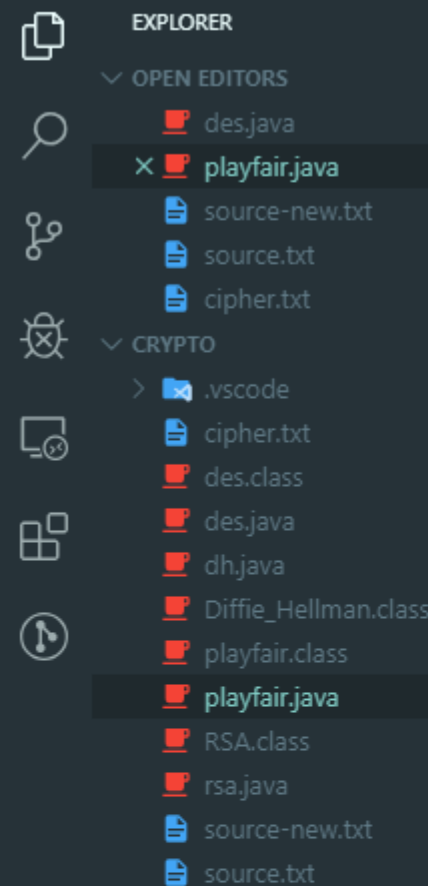
Visual Studio Code interface showing the playfair.java file being edited. The Explorer sidebar on the left lists files under OPEN EDITORS and CRYPTO. The main editor displays the code for playfair.java, including the matrix() method and the format() method.

**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

**playfair.java**

```
51  }
52  System.out.println(Key);
53  matrix();
54  }
55
56  private void matrix()
57  {
58      int counter = 0;
59      for (int i = 0; i < 5; i++)
60      {
61          for (int j = 0; j < 5; j++)
62          {
63              matrix_arr[i][j] = Key.charAt(counter);
64              System.out.print(matrix_arr[i][j] + " ");
65              counter++;
66          }
67          System.out.println();
68      }
69  }
70
71  private String format(String old_text)
72  {
73      int i = 0;
74      int len = 0;
75      String text = new String();
76      len = old_text.length();
77      for (int tmp = 0; tmp < len; tmp++)
78      {
79          if (old_text.charAt(tmp) == 'j')
80          {
81              text = text + 'i';
82          }
83          else
```



```

des.java
playfair.java > playfair
71
72 private String format(String old_text)
73 {
74     int i = 0;
75     int len = 0;
76     String text = new String();
77     len = old_text.length();
78     for (int tmp = 0; tmp < len; tmp++)
79     {
80         if (old_text.charAt(tmp) == 'j')
81         {
82             text = text + 'i';
83         }
84         else
85             text = text + old_text.charAt(tmp);
86     }
87     len = text.length();
88     for (i = 0; i < len; i = i + 2)
89     {
90         if (text.charAt(i + 1) == text.charAt(i))
91         {
92             text = text.substring(0, i + 1) + 'x' + text.substring(i + 1);
93         }
94     }
95     return text;
96 }
97
98 private String[] Divid2Pairs(String new_string)
99 {
100     String Original = format(new_string);
101     int size = Original.length();
102     if (size % 2 != 0)
103     {

```

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

```

96
97 private String[] Divid2Pairs(String new_string)
98 {
99     String Original = format(new_string);
100     int size = Original.length();
101     if (size % 2 != 0)
102     {
103         size++;
104         Original = Original + 'x';
105     }
106     String x[] = new String[size / 2];
107     int counter = 0;
108     for (int i = 0; i < size / 2; i++)
109     {
110         x[i] = Original.substring(counter, counter + 2);
111         counter = counter + 2;
112     }
113     return x;
114 }
115
116 public int[] GetDiminsions(char letter)
117 {
118     int[] key = new int[2];
119     if (letter == 'j')
120         letter = 'i';
121     for (int i = 0; i < 5; i++)
122     {
123         for (int j = 0; j < 5; j++)
124         {
125             if (matrix_arr[i][j] == letter)
126             {
127                 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

```
119 playfair
120 if (letter == 'j')
121     letter = 'i';
122 for (int i = 0; i < 5; i++)
123 {
124     for (int j = 0; j < 5; j++)
125     {
126         if (matrix_arr[i][j] == letter)
127         {
128             key[0] = i;
129             key[1] = j;
130             break;
131         }
132     }
133 }
134 return key;
135 }
136
137 public String encryptMessage(String Source)
138 {
139     String src_arr[] = Divid2Pairs(Source);
140     String Code = new String();
141     char one;
142     char two;
143     int part1[] = new int[2];
144     int part2[] = new int[2];
145     for (int i = 0; i < src_arr.length; i++)
146     {
147         one = src_arr[i].charAt(0);
148         two = src_arr[i].charAt(1);
149         part1 = GetDiminsions(one);
150         part2 = GetDiminsions(two);
151         if (part1[0] == part2[0])
152         {
```

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

```
119 playfair
120 if (letter == 'j')
121     letter = 'i';
122 for (int i = 0; i < 5; i++)
123 {
124     for (int j = 0; j < 5; j++)
125     {
126         if (matrix_arr[i][j] == letter)
127         {
128             key[0] = i;
129             key[1] = j;
130             break;
131         }
132     }
133     return key;
134 }
135
136 public String encryptMessage(String Source)
137 {
138     String src_arr[] = Divid2Pairs(Source);
139     String Code = new String();
140     char one;
141     char two;
142     int part1[] = new int[2];
143     int part2[] = new int[2];
144     for (int i = 0; i < src_arr.length; i++)
145     {
146         one = src_arr[i].charAt(0);
147         two = src_arr[i].charAt(1);
148         part1 = GetDiminsions(one);
149         part2 = GetDiminsions(two);
150         if (part1[0] == part2[0])
151         {
```



Visual Studio Code interface showing the Explorer, Search, and Run and Debug views. The Explorer view displays the file structure of the project, including the 'CRYPTO' folder. The Search view shows the results of a search for 'playfair.java'. The Run and Debug view shows the execution of the 'playfair' program.

**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

**Search**

- playfair.java

**Run and Debug**

- 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;
        }
    }
}
```



## 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 &gt; playfair

```
156         if (part2[1] < 4)
157             part2[1]++;
158         else
159             part2[1] = 0;
160     }
161     else if (part1[1] == part2[1])
162     {
163         if (part1[0] < 4)
164             part1[0]++;
165         else
166             part1[0] = 0;
167         if (part2[0] < 4)
168             part2[0]++;
169         else
170             part2[0] = 0;
171     }
172     else
173     {
174         int temp = part1[1];
175         part1[1] = part2[1];
176         part2[1] = temp;
177     }
178     Code = Code + matrix_arr[part1[0]][part1[1]]
179           + matrix_arr[part2[0]][part2[1]];
180 }
181 return Code;
182 }
183
184 public String decryptMessage(String Code)
185 {
186     String Original = new String();
187     String src_arr[] = Divid2Pairs(Code);
188     char one;
```



playfair.java - crypto - Visual Studio Code

File Edit Selection View Go Debug Terminal Help

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

```
215         if (part2[0] > 0)
216             part2[0]--;
217         else
218             part2[0] = 4;
219     }
220     else
221     {
222         int temp = part1[1];
223         part1[1] = part2[1];
224         part2[1] = temp;
225     }
226     Original = Original + matrix_arr[part1[0]][part1[1]]
227         + matrix_arr[part2[0]][part2[1]];
228 }
229 return Original;
230 }
231
232 public static void main(String[] args)
233 {
234     playfair x = new playfair();
235     Scanner sc = new Scanner(System.in);
236     System.out.println("Enter a keyword:");
237     String keyword = sc.next();
238     x.setKey(keyword);
239     x.KeyGen();
240     System.out
241         .println("Enter word to encrypt: (Make sure length of message is even)");
242     String key_input = sc.next();
243     if (key_input.length() % 2 == 0)
244     {
245         System.out.println("Encryption: " + x.encryptMessage(key_input));
246         System.out.println("Decryption: "
```

Visual Studio Code interface showing a Java project named "playfair.java - crypto". The Explorer sidebar on the left displays the file structure:

- EXPLORER
  - OPEN EDITORS
    - des.java
    - playfair.java (selected)
    - source-new.txt
    - source.txt
    - cipher.txt
  - CRYPTO
    - .vscode
    - cipher.txt
    - des.class
    - des.java
    - dh.java
    - Diffie\_Hellman.class
    - playfair.class
    - playfair.java (selected)
    - RSA.class
    - rsa.java
    - source-new.txt
    - source.txt

The main editor displays the code for `playfair.java`:

```
230 }
231
232 public static void main(String[] args)
233 {
234     playfair x = new playfair();
235     Scanner sc = new Scanner(System.in);
236     System.out.println("Enter a keyword:");
237     String keyword = sc.next();
238     x.setKey(keyword);
239     x.KeyGen();
240     System.out
241         .println("Enter word to encrypt: (Make sure length of message is even)");
242     String key_input = sc.next();
243     if (key_input.length() % 2 == 0)
244     {
245         System.out.println("Encryption: " + x.encryptMessage(key_input));
246         System.out.println("Decryption: "
247             + x.decryptMessage(x.encryptMessage(key_input)));
248     }
249     else
250     {
251         key_input=key_input+"x";
252         System.out.println("Encryption: " + x.encryptMessage(key_input));
253         System.out.println("Decryption: "
254             + x.decryptMessage(x.encryptMessage(key_input)));
255     }
256     sc.close();
257 }
258 }
259 }
```

The status bar at the bottom indicates the current position: Ln 8, Col 2, Spaces: 4, UTF-8, CRLF, Java. The Windows taskbar is visible at the very bottom.

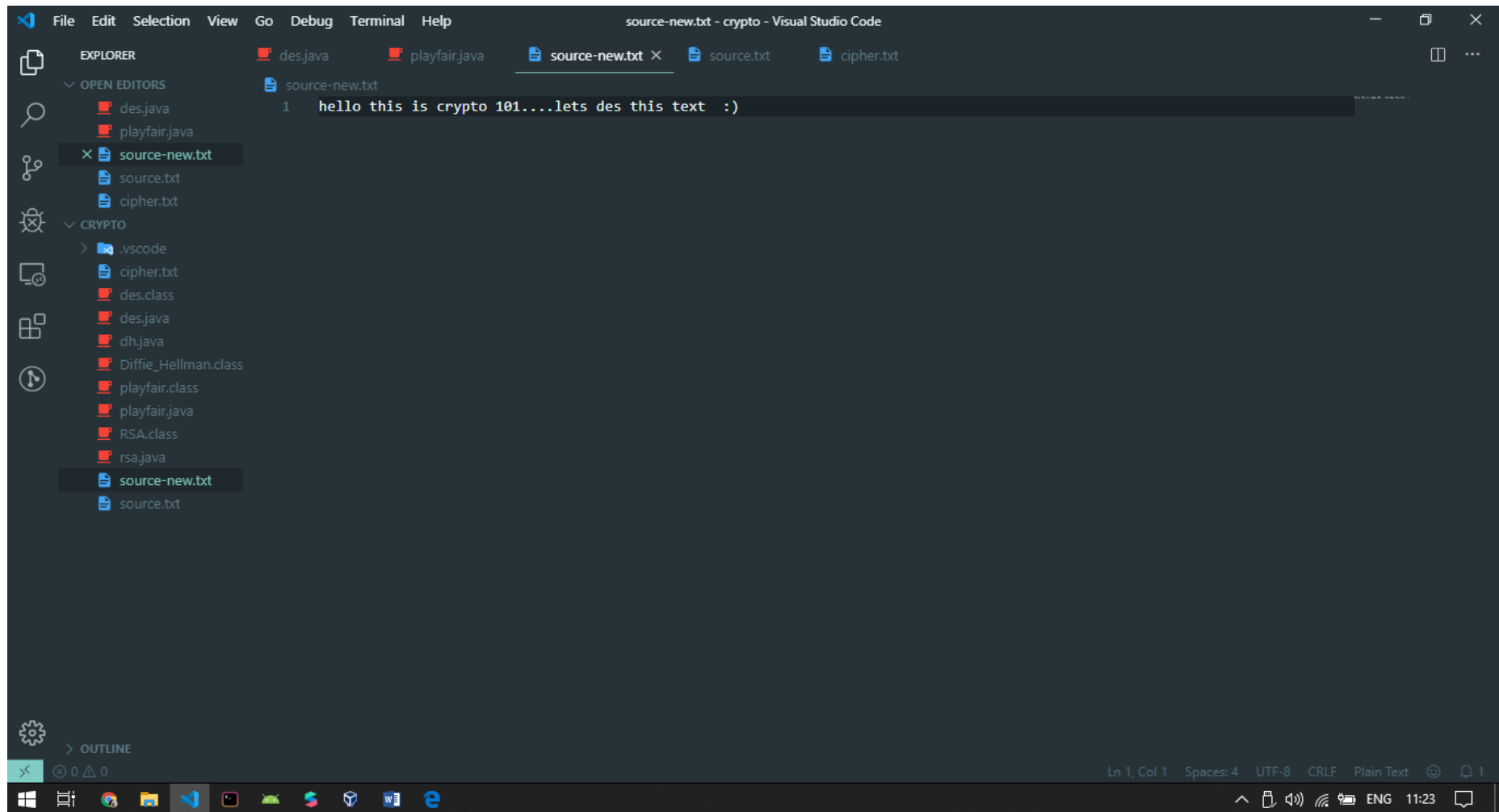
Visual Studio Code interface showing a Java project named "crypto" with a file named "playfair.java". The code in "playfair.java" includes a Playfair cipher implementation with methods for setting a key, formatting text, and performing encryption and decryption.

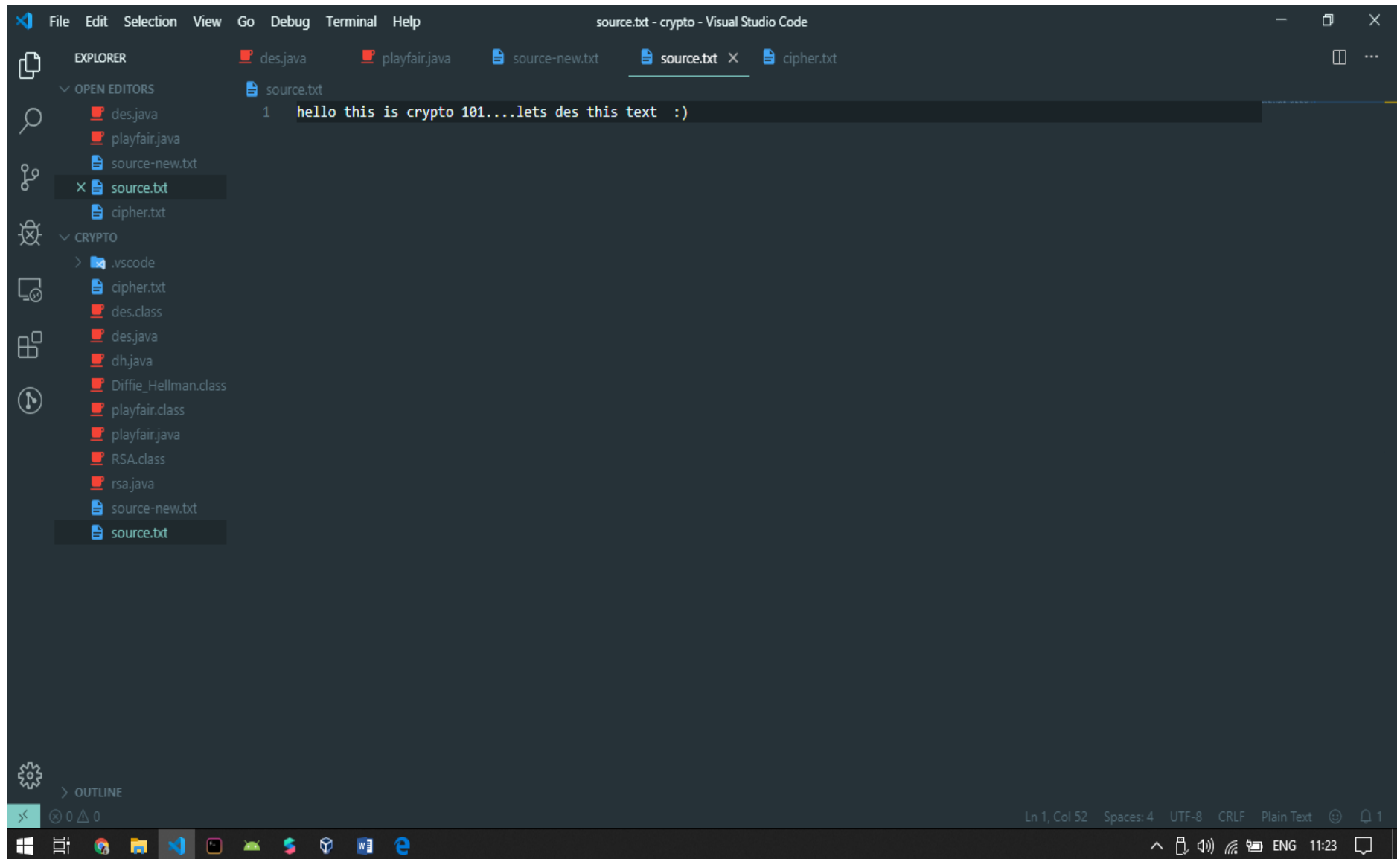
```
65  
66  
67  
68  
69  
70  
71  
72  
73  
74  
75  
76  
77  
78  
79  
80  
81  
82  
83  
84  
85  
86  
87  
88  
89  
90  
91  
92  
93  
94  
95  
96  
97  
98  
99  
100  
101  
102  
103  
104  
105  
106  
107  
108  
109  
110  
111  
112  
113  
114  
115  
116  
117  
118  
119  
120  
121  
122  
123  
124  
125  
126  
127  
128  
129  
130  
131  
132  
133  
134  
135  
136  
137  
138  
139  
140  
141  
142  
143  
144  
145  
146  
147  
148  
149  
150  
151  
152  
153  
154  
155  
156  
157  
158  
159  
160  
161  
162  
163  
164  
165  
166  
167  
168  
169  
170  
171  
172  
173  
174  
175  
176  
177  
178  
179  
180  
181  
182  
183  
184  
185  
186  
187  
188  
189  
190  
191  
192  
193  
194  
195  
196  
197  
198  
199  
200  
201  
202  
203  
204  
205  
206  
207  
208  
209  
210  
211  
212  
213  
214  
215  
216  
217  
218  
219  
220  
221  
222  
223  
224  
225  
226  
227  
228  
229  
230  
231  
232  
233  
234  
235  
236  
237  
238  
239  
240  
241  
242  
243  
244  
245  
246  
247  
248  
249  
250  
251  
252  
253  
254  
255  
256  
257  
258  
259  
260  
261  
262  
263  
264  
265  
266  
267  
268  
269  
270  
271  
272  
273  
274  
275  
276  
277  
278  
279  
280  
281  
282  
283  
284  
285  
286  
287  
288  
289  
290  
291  
292  
293  
294  
295  
296  
297  
298  
299  
300  
301  
302  
303  
304  
305  
306  
307  
308  
309  
310  
311  
312  
313  
314  
315  
316  
317  
318  
319  
320  
321  
322  
323  
324  
325  
326  
327  
328  
329  
330  
331  
332  
333  
334  
335  
336  
337  
338  
339  
340  
341  
342  
343  
344  
345  
346  
347  
348  
349  
350  
351  
352  
353  
354  
355  
356  
357  
358  
359  
360  
361  
362  
363  
364  
365  
366  
367  
368  
369  
370  
371  
372  
373  
374  
375  
376  
377  
378  
379  
380  
381  
382  
383  
384  
385  
386  
387  
388  
389  
390  
391  
392  
393  
394  
395  
396  
397  
398  
399  
400  
401  
402  
403  
404  
405  
406  
407  
408  
409  
410  
411  
412  
413  
414  
415  
416  
417  
418  
419  
420  
421  
422  
423  
424  
425  
426  
427  
428  
429  
430  
431  
432  
433  
434  
435  
436  
437  
438  
439  
440  
441  
442  
443  
444  
445  
446  
447  
448  
449  
450  
451  
452  
453  
454  
455  
456  
457  
458  
459  
460  
461  
462  
463  
464  
465  
466  
467  
468  
469  
470  
471  
472  
473  
474  
475  
476  
477  
478  
479  
480  
481  
482  
483  
484  
485  
486  
487  
488  
489  
490  
491  
492  
493  
494  
495  
496  
497  
498  
499  
500  
501  
502  
503  
504  
505  
506  
507  
508  
509  
510  
511  
512  
513  
514  
515  
516  
517  
518  
519  
520  
521  
522  
523  
524  
525  
526  
527  
528  
529  
530  
531  
532  
533  
534  
535  
536  
537  
538  
539  
540  
541  
542  
543  
544  
545  
546  
547  
548  
549  
550  
551  
552  
553  
554  
555  
556  
557  
558  
559  
560  
561  
562  
563  
564  
565  
566  
567  
568  
569  
570  
571  
572  
573  
574  
575  
576  
577  
578  
579  
580  
581  
582  
583  
584  
585  
586  
587  
588  
589  
590  
591  
592  
593  
594  
595  
596  
597  
598  
599  
600  
601  
602  
603  
604  
605  
606  
607  
608  
609  
610  
611  
612  
613  
614  
615  
616  
617  
618  
619  
620  
621  
622  
623  
624  
625  
626  
627  
628  
629  
630  
631  
632  
633  
634  
635  
636  
637  
638  
639  
640  
641  
642  
643  
644  
645  
646  
647  
648  
649  
650  
651  
652  
653  
654  
655  
656  
657  
658  
659  
660  
661  
662  
663  
664  
665  
666  
667  
668  
669  
670  
671  
672  
673  
674  
675  
676  
677  
678  
679  
680  
681  
682  
683  
684  
685  
686  
687  
688  
689  
690  
691  
692  
693  
694  
695  
696  
697  
698  
699  
700  
701  
702  
703  
704  
705  
706  
707  
708  
709  
710  
711  
712  
713  
714  
715  
716  
717  
718  
719  
720  
721  
722  
723  
724  
725  
726  
727  
728  
729  
730  
731  
732  
733  
734  
735  
736  
737  
738  
739  
740  
741  
742  
743  
744  
745  
746  
747  
748  
749  
750  
751  
752  
753  
754  
755  
756  
757  
758  
759  
760  
761  
762  
763  
764  
765  
766  
767  
768  
769  
770  
771  
772  
773  
774  
775  
776  
777  
778  
779  
780  
781  
782  
783  
784  
785  
786  
787  
788  
789  
790  
791  
792  
793  
794  
795  
796  
797  
798  
799  
800  
801  
802  
803  
804  
805  
806  
807  
808  
809  
810  
811  
812  
813  
814  
815  
816  
817  
818  
819  
820  
821  
822  
823  
824  
825  
826  
827  
828  
829  
830  
831  
832  
833  
834  
835  
836  
837  
838  
839  
840  
841  
842  
843  
844  
845  
846  
847  
848  
849  
850  
851  
852  
853  
854  
855  
856  
857  
858  
859  
860  
861  
862  
863  
864  
865  
866  
867  
868  
869  
870  
871  
872  
873  
874  
875  
876  
877  
878  
879  
880  
881  
882  
883  
884  
885  
886  
887  
888  
889  
890  
891  
892  
893  
894  
895  
896  
897  
898  
899  
900  
901  
902  
903  
904  
905  
906  
907  
908  
909  
910  
911  
912  
913  
914  
915  
916  
917  
918  
919  
920  
921  
922  
923  
924  
925  
926  
927  
928  
929  
930  
931  
932  
933  
934  
935  
936  
937  
938  
939  
940  
941  
942  
943  
944  
945  
946  
947  
948  
949  
950  
951  
952  
953  
954  
955  
956  
957  
958  
959  
960  
961  
962  
963  
964  
965  
966  
967  
968  
969  
970  
971  
972  
973  
974  
975  
976  
977  
978  
979  
980  
981  
982  
983  
984  
985  
986  
987  
988  
989  
990  
991  
992  
993  
994  
995  
996  
997  
998  
999  
1000
```

The terminal output shows the execution of the Java program, which prompts for a keyword and a message to encrypt. The keyword "harsh" and message "gupta" are entered, resulting in the encrypted text "nzqurw" and decrypted text "guptax".

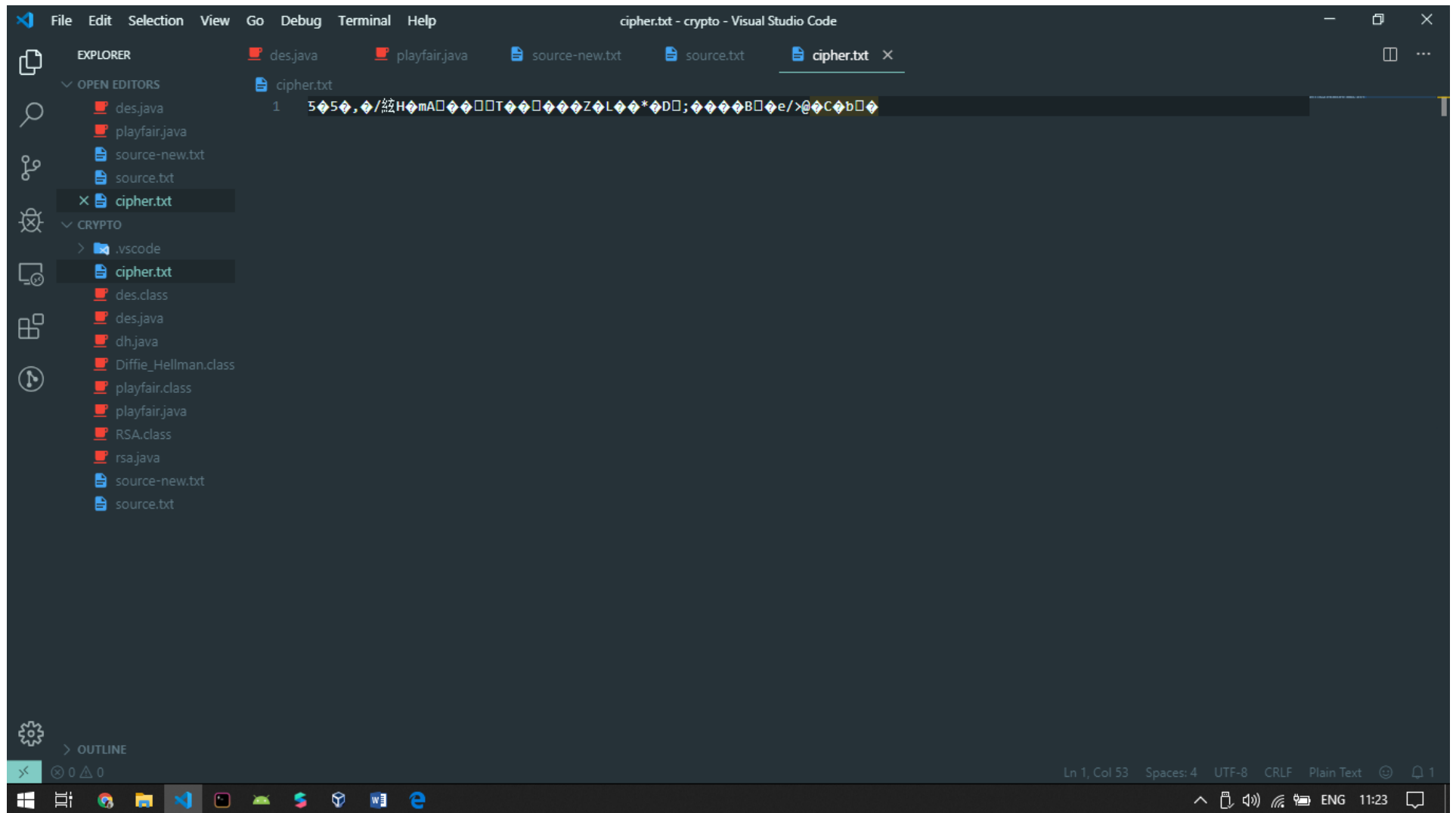
1: cmd

Ln 10, Col 6 Spaces: 4 UTF-8 CRLF Java ENG 11:22











## EXPLORER

## OPEN EDITORS

X des.java

playfair.java

source-new.txt

source.txt

cipher.txt



## CRYPTO

&gt; .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 &gt; ...

```
1  import java.io.FileInputStream;
2  import java.io.FileOutputStream;
3  import java.io.IOException;
4  import java.io.InputStream;
5  import java.io.OutputStream;
6  import java.security.InvalidAlgorithmParameterException;
7  import java.security.InvalidKeyException;
8  import java.security.NoSuchAlgorithmException;
9  import java.security.spec.AlgorithmParameterSpec;
10
11 import javax.crypto.Cipher;
12 import javax.crypto.CipherInputStream;
13 import javax.crypto.CipherOutputStream;
14 import javax.crypto.KeyGenerator;
15 import javax.crypto.NoSuchPaddingException;
16 import javax.crypto.SecretKey;
17 import javax.crypto.spec.IvParameterSpec;
18
19 public class des {
20     private static Cipher encryptCipher;
21     private static Cipher decryptCipher;
22     private static final byte[] iv = { 11, 22, 33, 44, 99, 88, 77, 66 };
23
24     public static void main(String[] args) {
25         String clearTextFile = "/Users/harsh/Desktop/crypto/source.txt";
26         String cipherTextFile = "/Users/harsh/Desktop/crypto/cipher.txt";
27         String clearTextNewFile = "/Users/harsh/Desktop/crypto/source-new.txt";
28
29         try {
30             // create SecretKey using KeyGenerator
31             SecretKey key = KeyGenerator.getInstance("DES").generateKey();
32             AlgorithmParameterSpec paramSpec = new IvParameterSpec(iv);
```

des.java - crypto - Visual Studio Code

File Edit Selection View Go Debug Terminal Help

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

27

28

29

30

31

32

33

34

35

36

37

38

39

40

41

42

43

44

45

46

47

48

49

50

51

52

53

54

55

56

57

58

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

des.java playfair.java source-new.txt source.txt cipher.txt

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

51 }  
52  
53 }  
54  
55 private static void encrypt(InputStream is, OutputStream os) throws IOException {  
56  
57 // create CipherOutputStream to encrypt the data using encryptCipher  
58 os = new CipherOutputStream(os, encryptCipher);  
59 writeData(is, os);  
60 }  
61  
62 private static void decrypt(InputStream is, OutputStream os) throws IOException {  
63  
64 // create CipherOutputStream to decrypt the data using decryptCipher  
65 is = new CipherInputStream(is, decryptCipher);  
66 writeData(is, os);  
67 }  
68  
69 // utility method to read data from input stream and write to output stream  
70 private static void writeData(InputStream is, OutputStream os) throws IOException {  
71 byte[] buf = new byte[1024];  
72 int numRead = 0;  
73 // read and write operation  
74 while ((numRead = is.read(buf)) >= 0) {  
75 os.write(buf, 0, numRead);  
76 }  
77 os.close();  
78 is.close();  
79 }  
80  
81 }