

Cryptography and Network Security

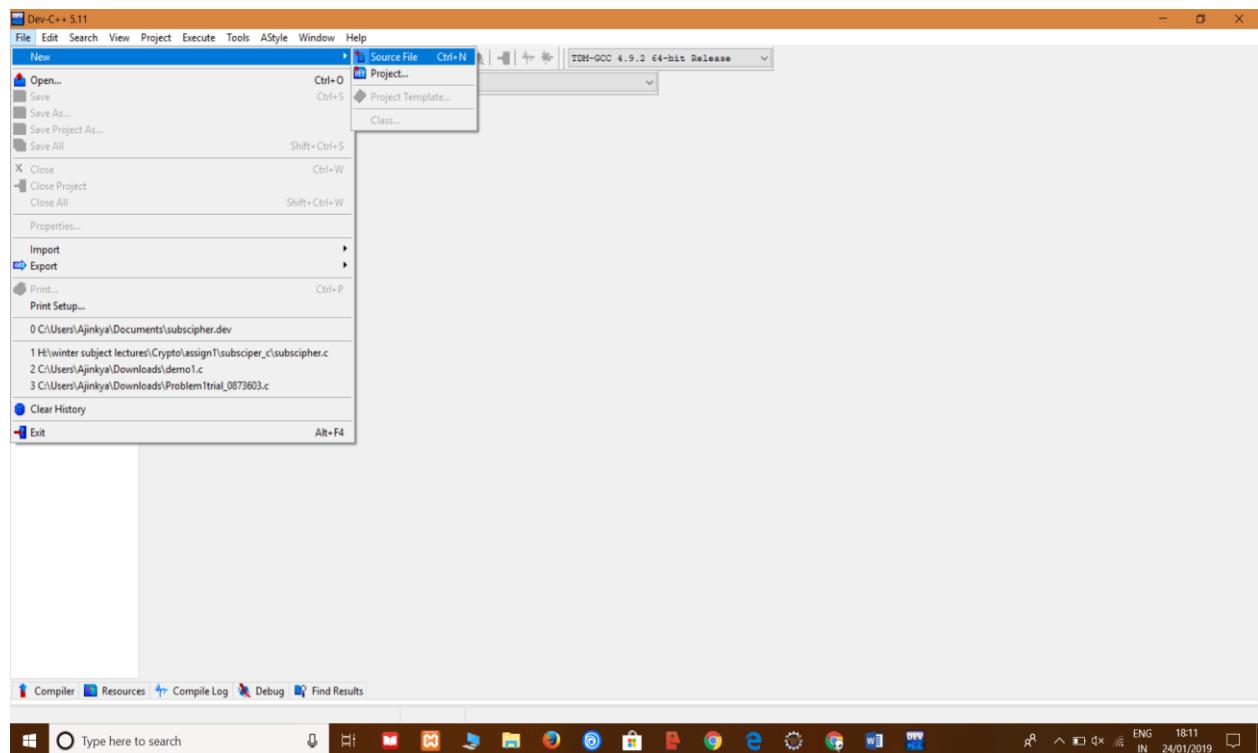
Documentation & Readme file for Assignment 1

Problem 1

1. Write computer programs for the Substitution Cipher based on Z29 which is corresponding to 26 alphabetic characters (0 - 25), space (26), and “,” (27) “.”(28). The key is a random permutation π on Z29. Write down encryption and decryption programs. Select a paragraph of text (I don't think any two people will choose a same paragraph if they choose independently) and encrypt it using your encryption algorithm. Then use your decryption program to check the correctness. You can use Java, C or other computer languages. Record your plaintext, cipher text and the key π in your answer sheet

Solution: (Folder name: subsciper, file name: subsciper.c)

- Language of choice: C language
 - Software/IDE used: Dev-C++
 - You can download the software from - <https://sourceforge.net/projects/orwelldevcpp/>
 - Name of the folder/file – subsciper/subscipher.c
 1. Download the software from above link and and create a new file as shown in below figure
 2. Copy paste the contents of ‘subscipher.c’ into the new file created



3. Copy paste the contents into the new ‘untitled’ c file

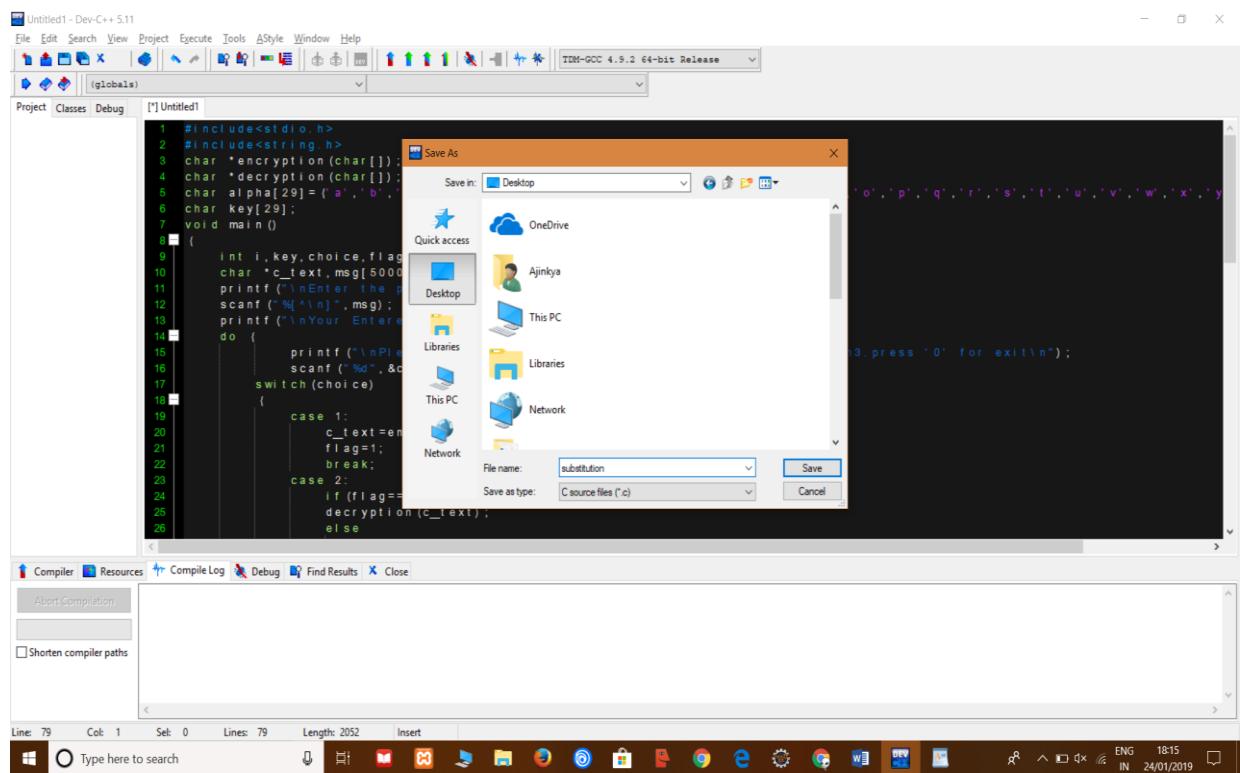
The screenshot shows the Dev-C++ IDE interface. The menu bar includes File, Edit, Search, View, Project, Execute, Tools, AStyle, Window, Help. The toolbar has icons for New, Open, Save, Run, Stop, and Build. The status bar at the bottom shows Line: 79, Col: 1, Sel: 0, Lines: 79, Length: 2052, Insert.

```
1 #include<stdio.h>
2 #include<string.h>
3 char *encryption(char[]);
4 char *decryption(char[]);
5 char alpha[29] = { 'a', 'b', 'c', 'd', 'e', 'f', 'g', 'h', 'i', 'j', 'k', 'l', 'm', 'n', 'o', 'p', 'q', 'r', 's', 't', 'u', 'v', 'w', 'x', 'y'
6 char key[29];
7 void main()
8 {
9     int i, key, choice, flag=0;
10    char *c_text, msg[5000];
11    printf ("\nEnter the plain text to be encrypted:\n");
12    scanf ("%[^n]", msg);
13    printf ("\nYour Entered Plain Text is:%s\n", msg);
14    do {
15        printf ("\nPlease enter your choice:\n1.Encryption\n2.Decryption\n3.press '0' for exit\n");
16        scanf ("%d", &choice);
17        switch (choice)
18        {
19            case 1:
20                c_text=encryption (msg);
21                flag=1;
22                break;
23            case 2:
24                if (flag==1)
25                    decryption (c_text);
26                else
27                    printf ("First do the encryption process");
28                break;
29            case 0:
30                break;
31            default:
32                printf ("\nPlease enter an appropriate option before proceeding.\n");
33                break;
34        }
35    } while (choice!=0);
```

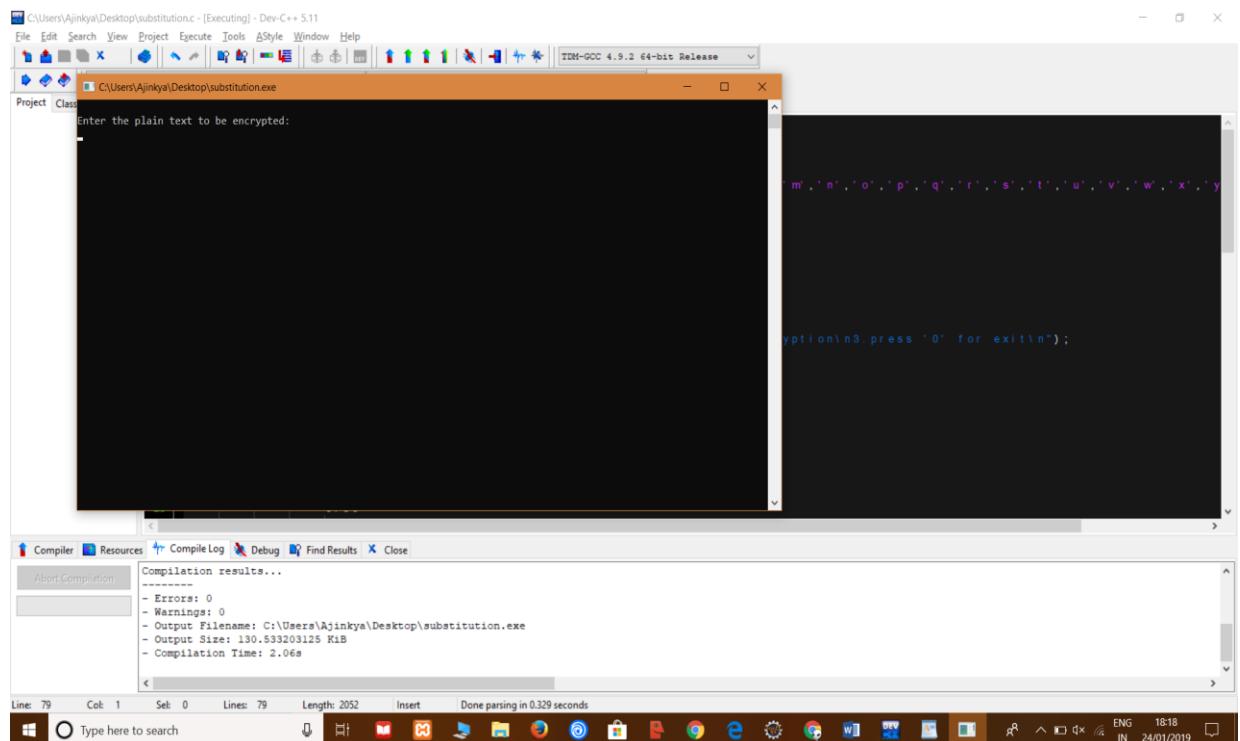
4. After pasting the content, go to Execute → Compile and run → save the file ‘filename.c’ to any location and let the code compile

The screenshot shows the Dev-C++ IDE interface with the 'Execute' menu open. The 'Compile' option is selected. The status bar at the bottom shows Line: 79, Col: 1, Sel: 0, Lines: 79, Length: 2052, Insert.

```
1 // Encryption and Decryption program in C
2 // Author: [REDACTED]
3 // Date: [REDACTED]
4 // Description: This program performs encryption and decryption of text using a substitution cipher based on the Caesar cipher principle.
5 // The program reads plain text from the user and encrypts it using a key provided by the user.
6 // The encrypted text is then decrypted back to its original form using the same key.
7 // The program continues to loop until the user chooses to exit.
8
9 // Function prototypes
10
11 // Function to encrypt text
12 char *encryption(char[]);
13 // Function to decrypt text
14 char *decryption(char[]);
15
16 // Main function
17
18 int main()
19 {
20     // Initialize arrays for alpha and key
21     char alpha[29] = { 'a', 'b', 'c', 'd', 'e', 'f', 'g', 'h', 'i', 'j', 'k', 'l', 'm', 'n', 'o', 'p', 'q', 'r', 's', 't', 'u', 'v', 'w', 'x', 'y'
22     char key[29];
23
24     // Initialize flag variable
25     int flag=0;
26
27     // Initialize message buffer
28     char msg[5000];
29
30     // Print message to user
31     printf ("\nEnter the plain text to be encrypted:\n");
32
33     // Read message from user
34     scanf ("%[^n]", msg);
35
36     // Print message to user
37     printf ("\nYour Entered Plain Text is:%s\n", msg);
38
39     // Loop until user exits
40     do {
41         // Print message to user
42         printf ("\nPlease enter your choice:\n1.Encryption\n2.Decryption\n3.press '0' for exit\n");
43
44         // Read choice from user
45         scanf ("%d", &choice);
46
47         // Switch statement to handle user choice
48         switch (choice)
49         {
50             case 1:
51                 c_text=encryption (msg);
52                 flag=1;
53                 break;
54             case 2:
55                 if (flag==1)
56                     decryption (c_text);
57                 else
58                     printf ("First do the encryption process");
59                 break;
60             case 0:
61                 break;
62             default:
63                 printf ("\nPlease enter an appropriate option before proceeding.\n");
64                 break;
65         }
66     } while (choice!=0);
```



5. Watch the compilation process occurring in the bottom half ‘compile log’ and programs runs in a terminal



6. Output of the program

The screenshot shows a Dev-C++ interface with a terminal window displaying the output of a C program. The terminal window title is "C:\Users\Ajinkya\Desktop\substitution.c - [Executing] - Dev-C++ 5.11". The output text is as follows:

```
C:\Users\Ajinkya\Desktop\substitution.c - [Executing] - Dev-C++ 5.11
File  C:\Users\Ajinkya\Desktop\substitution.exe

Enter the plain text to be encrypted:
hello my name is ajinkya kunjir. I am pursuing masters in computer science at lakehead University, Thunderbay. My research interests are data science, machine learning and neural networks.

Your Entered Plain Text is:hello my name is ajinkya kunjir. I am pursuing masters in computer science at lakehead University, Thunderbay. My research interests are data science, machine learning and neural networks.

Please enter your choice
1.Encryption
2.Decryption
3.press '0' for exit
1
enter the Z29 unique characters for encryption(All 26 alphabets including [.,/]):qwertyuiopasdfghjklzxcvbnm,./

Graphical Representation of Characters Replaced

abcdefghijklmnopqrstuvwxyz,./
||||||||||||||||||||||| |
qwertyuiopasdfghjklzxcvbnm,./

Your encrypted message is:itddh fm gqft pz qapgsmq scgapl/ I qf jclzcpu fqzxtlz pg ehfjcctl zeptget qx dqstitqr Ugpvzlzpxm. Ticgrtlwqm/ Mm ltztqlei pgxtltzxz qlt rqxq zeptget. fqeipgt dtqlgpgu qgr gtclqd gtxbhlsz/
Please enter your choice
1.Encryption
2.Decryption
3.press '0' for exit
2
24          if (flag==1)
25              decryption(c_text);
26          else
```

Below the terminal window, the Dev-C++ toolbar includes Compiler, Resources, Compile Log, Debug, Find Results, and Close buttons. The Compile Log tab is active, showing compilation results:

```
Compilation results...
-----
- Errors: 0
- Warnings: 0
- Output Filename: C:\Users\Ajinkya\Desktop\substitution.exe
- Output Size: 130.533203125 KiB
- Compilation Time: 0.80s
```

- Run → enter the plaintext → You are given a choice of Encryption, Decryption and exit → put either '1' or '2' (DO NOT PUT FULL STOP AFTER I.E '1.' Or '2.')
- For providing Z29 values, enter a random combination of all 26 alphabets on keyboard with comma(,), fullstop(.) and hash(/). That makes 29 in total.
- Graphical representation of alphabetic mapping is shown on the terminal.
- **Plaintext paragraph provided:** hello my name is ajinkya kunjir. I am pursuing masters in computer science at lakehead University, Thunderbay. My research interests are data science, machine learning and neural networks.
- **Encryption Obtained by substitution cipher:** itddh fm gqft pz qapgsmq scgapl/ I qf jclzcpu fqzxtlz pg ehfjcctl zeptget qx dqstitqr Ugpvzlzpxm. Ticgrtlwqm/ Mm ltztqlei pgxtltzxz qlt rqxq zeptget. fqeipgt dtqlgpgu qgr gtclqd gtxbhlsz/
- **Key Provided (Z29):** qwertyuiopasdfghjklzxcvbnm,./
- **Decryption Obtained by Cipher:** hello my name is ajinkya kunjir. I am pursuing masters in computer science at lakehead University,

Thunderbay. My research interests are data science, machine learning and neural networks.

- Screenshot of decryption is given below:

```
File C:\Users\Ajinkya\Desktop\substitution.exe
Project
abcdefgijklmnopqrstuvwxyz,./
|||||||||||||||||||||||
qwertyuiopasdfghjklzxcvbnm,./
Your encrypted message is:itddh fm gqft pz qapgsmq scgapl/ I qf jclzcpgu fqzxtlz pg ehfjctxl zeptget qx dqstitqr Ugpvtlz
pxm. Ticgrtlwqm/ Mm ltztqlei pxgxtlxz qlt rqxq zeptget. fqeipgt dtqlgpgu qgr gtclqd gtxbhlsz/
Please enter your choice
1.Encryption
2.Decryption
3.press '0' for exit
2

decryption

Graphical Representation of Characters Replaced
qwertyuiopasdfghjklzxcvbnm,./
|||||||||||||||||||||||
abcdefgijklmnopqrstuvwxyz,./
Your decrypted message is hello my name is ajinkya kunjir. I am pursuing masters in computer science at lakehead Univers
ity, Thunderbay. My research interests are data science, machine learning and neural networks.
Please enter your choice
1.Encryption
2.Decryption
3.press '0' for exit
77     printf (" Your decrypted message is: %s", cipher);
78     public int __cdecl printf ( const char * __restrict__ Format, ... )
79

Compiler Resources Compile Log Debug Find Results Close
Compilation results...
-----
- Errors: 0
- Warnings: 0
- Output Filename: C:\Users\Ajinkya\Desktop\substitution.exe
- Output Size: 130.533203125 KiB
- Compilation Time: 0.80s
```

- Finally , choose ‘3’ and exit the program

```
Document1 - Word (Product Activation Failed)
File C:\Users\Ajinkya\Desktop\substitution.exe
2
Past decryption
Graphical Representation of Characters Replaced
qwertyuiopasdfghjklzxcvbnm,./
|||||||||||||||||||||||
abcdefgijklmnopqrstuvwxyz,./
Your decrypted message is hello my name is ajinkya kunjir. I am pursuing masters in computer science at lakehead Univers
ity, Thunderbay. My research interests are data science, machine learning and neural networks.
Please enter your choice
1.Encryption
2.Decryption
3.press '0' for exit
0

-----
Process exited after 109.1 seconds with return value 0
Press any key to continue . . .

2.Decryption
3.press '0' for exit
77     printf (" Your decrypted message is: %s", cipher);
78     public int __cdecl printf ( const char * __restrict__ Format, ... )
79
```

Problem 2

2. Write computer programs for the Permutation Cipher based on Z29 as in Problem 1. In encryption program, the inputs are a value of m (the size of permutation), a permutation as the key and the plaintext, and the output is the ciphertext. Write the decryption program accordingly. Try your programs by some text. Note that since m and the length of plaintext is not fixed, paddings might be added to the end of plaintext by the program. You may think about what kind padding is better for the security and design your paddings.

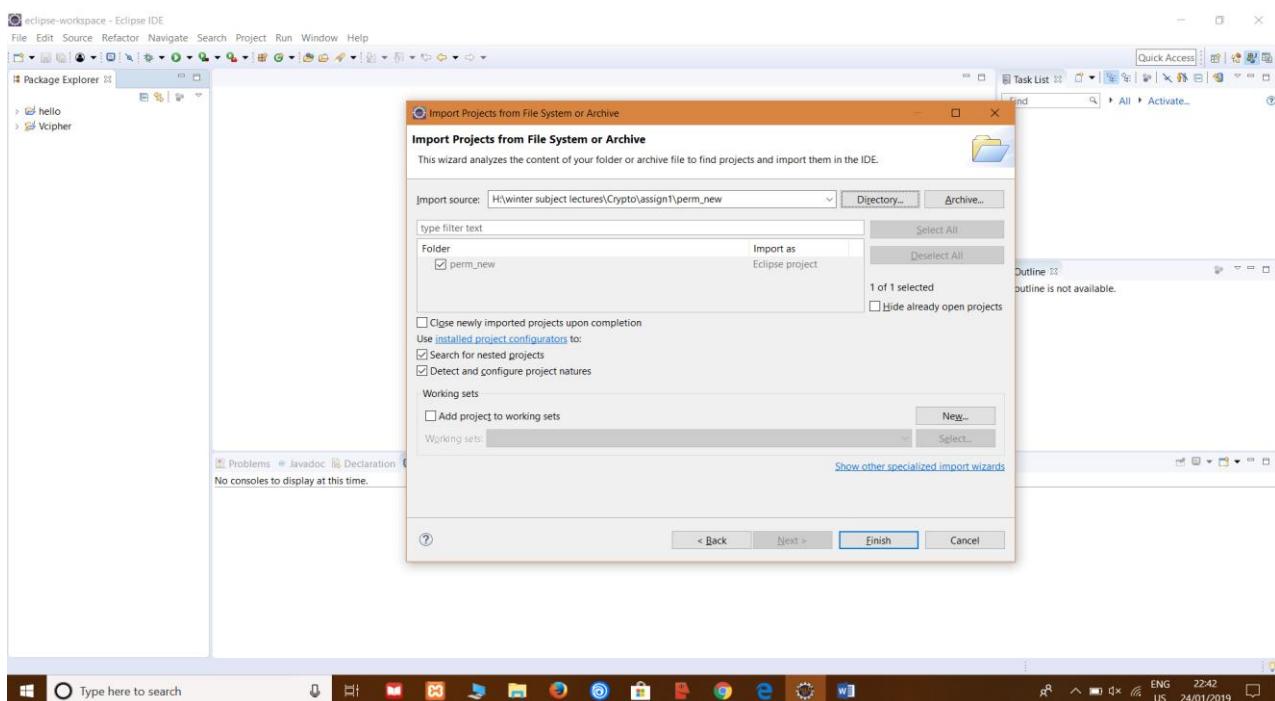
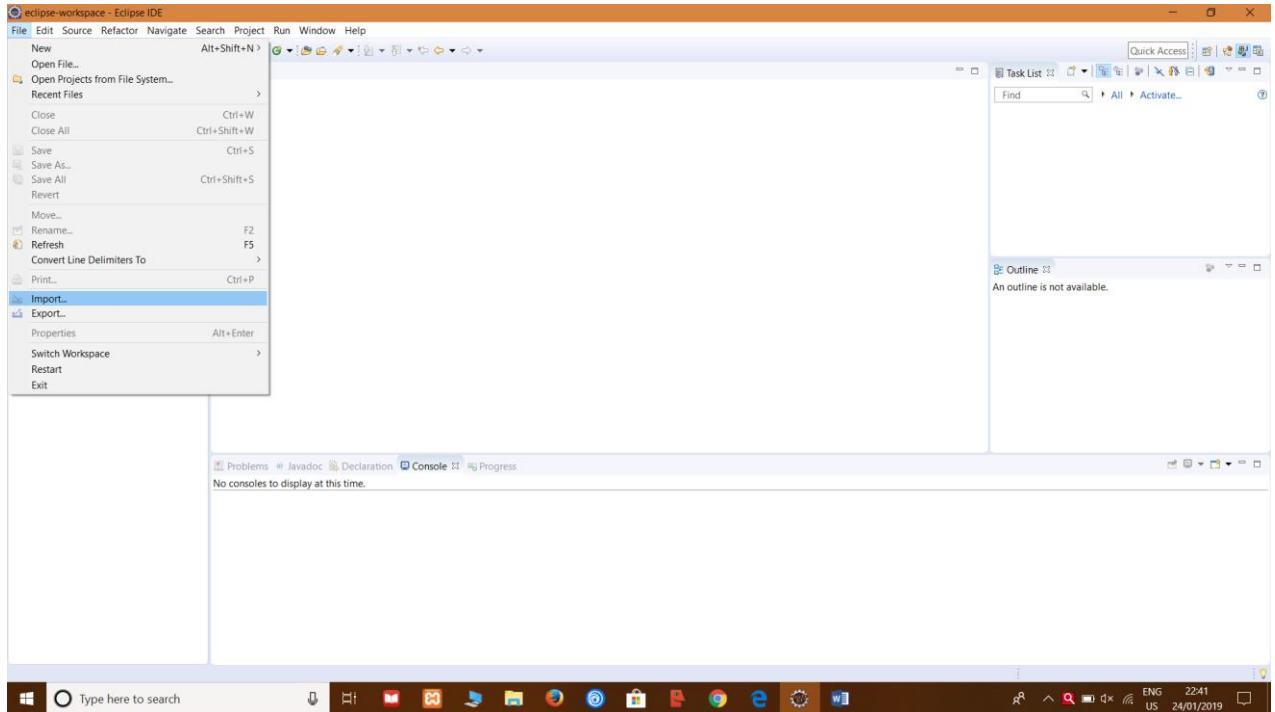
Solution: (folder – perm_new)

- Language of choice: Java language
- Software/IDE used: Eclipse IDE for Java
- You can download the Eclipse software from - <https://www.eclipse.org/downloads/>
- Download the JDK for windows from <https://www.oracle.com/technetwork/java/javase/downloads/jdk8-downloads-2133151.html>
- Name of the folder : perm_new

➤ *Steps to follow:*

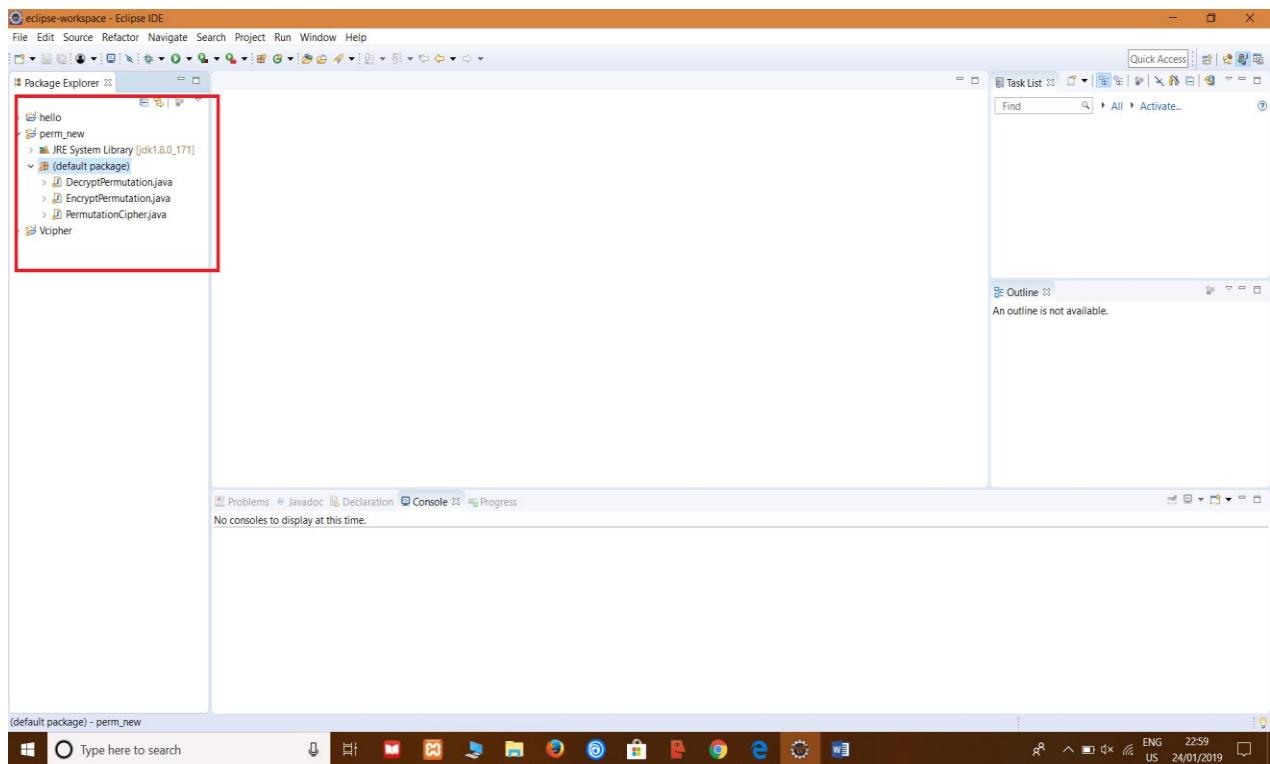
1. Download Eclipse IDE and JDK from the websites mentioned above and set the environment of Eclipse IDE to open perspective – Java.
2. Follow the screenshots given below for importing and running the project

1. Open eclipse IDE → Import, click on Import and import the folder by selecting ‘projects from archive’



2. After selecting the directory, you will see the contents in the package explorer window. Refer the image given below

3. The program saves the ‘m’ sized key in the ‘output_key.txt’ file after generation, hence delete the txt. File if present while importing in the folder.



4. Now , left click on the folder in package explorer and select ‘Run as’ → Java application
5. Keep your eyes on the console window at the bottom
6. Follow the instructions and enter the plaintext

Plaintext Entered: There is a tide in the affairs of men, which taken at the flood, leads on to fortune. Omitted, all the voyage of their life is bound in shallows and in miseries. On such a full sea are we now afloat. And we must take the current when it serves, or lose our ventures.

7. Put the plaintext, enter the size of key ‘m’ (size can be any 5,6,7,8....so on)

‘m’ = 5

‘m’ = 6

‘m’ = 7.....Any key number

The screenshot shows the Eclipse IDE interface with the following details:

- Project Explorer:** Shows a package named "perm_new" containing classes: EncryptPermutation.java, PermutationCipher.java, and DecryptPermutation.java.
- Code Editor:** Displays the content of `DecryptPermutation.java`. The code implements a class `DecryptPermutation` that uses a `TreeMap` to map characters from the key to the corresponding characters in the ciphertext. It includes methods for generating mappings based on a key and value string, and for decrypting a given string.
- Outline View:** Shows the class structure with methods `Generator`, `Decryptor`, and `Padding`.
- Terminal Window:** A red box highlights the terminal output area. It shows the command `java PermutationCipher` being run, followed by user input for plaintext ("There is a tide in the affairs of men, which taken at the flood, leads on to fortune. Omitted, all the voyage of their life is bound in shallows and in miseries. On such a full") and key size ("6"). The terminal then prompts the user to type "encrypt" or "decrypt".

8. Type ‘encrypt’ or ‘decrypt’ based on the preference. If you type ‘decrypt’ then the program will ask you to encrypt the data first.

The screenshot shows the Eclipse IDE interface with the following details:

- Project Explorer:** Shows a package named "perm_new" containing classes: EncryptPermutation.java, PermutationCipher.java, and DecryptPermutation.java.
- Code Editor:** Displays the content of `DecryptPermutation.java`. The code is identical to the one in the previous screenshot.
- Outline View:** Shows the class structure with methods `Generator`, `Decryptor`, and `Padding`.
- Terminal Window:** A red box highlights the terminal output area. It shows the command `java PermutationCipher` being run, followed by user input for plaintext ("There is a tide in the affairs of men, which taken at the flood, leads on to fortune. Omitted, all the voyage of their life is bound in shallows and in miseries. On such a full") and key size ("6"). The terminal then prompts the user to type "encrypt" or "decrypt". The user has typed "decrypt", and the terminal responds with "The encrypted plaintext is: hre eTsa t id eniiteha fiasrfo fem ,w ihnht kacna teh elfto,d1 oasd0 e oft nruteno m0ti.e,da tlt ehlyoga fot eeril hf esibuodn i nhs lolswaadni imesnise .rms cu0 aufhl".

Encrypted Plaintext: hre eTsa t id eniiteha fiasrfo fem ,w ihnht kacna teh elfto,dl oasd o e oft nruteno mOti.e,da tlt ehlvyoga fot eeril hf esii buodn i nhs lolswaadni imesnise .rns cuO aufhls aelaerw on wefoltaa nA d.em suw atektt ehc rertnuweh n ts reie,so v olesroruv nutere.

9. You have to copy the encrypted text from the console, re-run the program and choose to ‘decrypt’ now. Insert the encrypted text (output of encryption) as the input for decryption.
10. Note: Size of key ‘m’ doesn’t matter much, you can enter any number suitable to you. (I have used 6 in this example)

The screenshot shows the Eclipse IDE interface with the following details:

- Left Side (Package Explorer):** Shows the project structure with packages like 'Hello' and 'perm_new' containing classes like 'EncryptPermutation.java', 'DecryptPermutation.java', and 'PermutationCipher.java'.
- Middle (Code Editor):** Displays the 'DecryptPermutation.java' code. A red box highlights the line "Feed Encrypted text as a plaintext and decrypt it". A red arrow points from this box to the console window below.
- Bottom (Console):** Shows the Java application's output. It prompts for plaintext, displays the encrypted input, asks for key size, and then shows the decrypted output: "The decrypted ciphertext is: There is a tide in the affairs of men, which taken at the flood, leads on to fortune. Omitted, all the voyage of their life is bound in shallows and in miseries. On such a full...
- Annotations:**
 - A red box with a red arrow points to the 'Console' tab in the bottom-left corner.
 - A red box with a red arrow points to the first line of the console output: "Type 'decrypt' and obtain the original plaintext back after decryption".

11. You obtain the original plaintext back after decrypting the ciphertext as shown in the image above.

Problem 4. (For CS 5413 students only)

Read “2.5 The Vigenère Cipher” of the lecture notes posted in course web carefully and try to understand the materials in this subsection. Then solve the following problem: The following is a piece of ciphertext which is encrypted by Vigenère Cipher.

Plaintext - cjnpkgrlilqwawbnuptgkerwxuzviaiisxckwdntjawnhqcuttvp
tewtrpgvcwlkkgczafsihrimixukrwxrfmgfgkfxgukpjvvzmcjm
vawbnuptgcicvkvkgczkekgcqbchvnqrhhwiadfrcyxgvzqqtuvbd
guvttkccdpvvfphftamzxqwrtrgukcelqlrxgvycwtncbjkkeerecj
qihvrjzpkkfexqgjtpjfupemswwcjqxzpjtxkvlyaeaemwhovudk
mnfxegfrwxtdyiaecyhl gjfpogymbxyfpzxxvpngkxfitnkfdniyr
wxukssxpqabmvkgcqbciaagpadfrcyxgvyyimjvwpkgscwbpurwxq
kftkorrwvnrqhxurlslgvjxmccraceathhtpmeygczwgutttvt
katmcvgiltwcsmjmvghitzaxodkbf

Try to find the plaintext. You need to write programs for computing index of coincidence I_c and mutual index of coincidence M_i . Use the methods discussed in the lecture notes to find the key size m first, and then find out the key. Using the found key you are able to decrypt the ciphertext.

Solution: (folder – Vcipher, file- Vcipher.java)

- Language of choice: Java language
- Software/IDE used: Eclipse IDE for Java
- You can download the Eclipse software from - <https://www.eclipse.org/downloads/>
- Download the JDK for windows from <https://www.oracle.com/technetwork/java/javase/downloads/jdk8-downloads-2133151.html>
- Name of the folder-file: Vcipher/Vcipher.java

➤ Steps to follow:

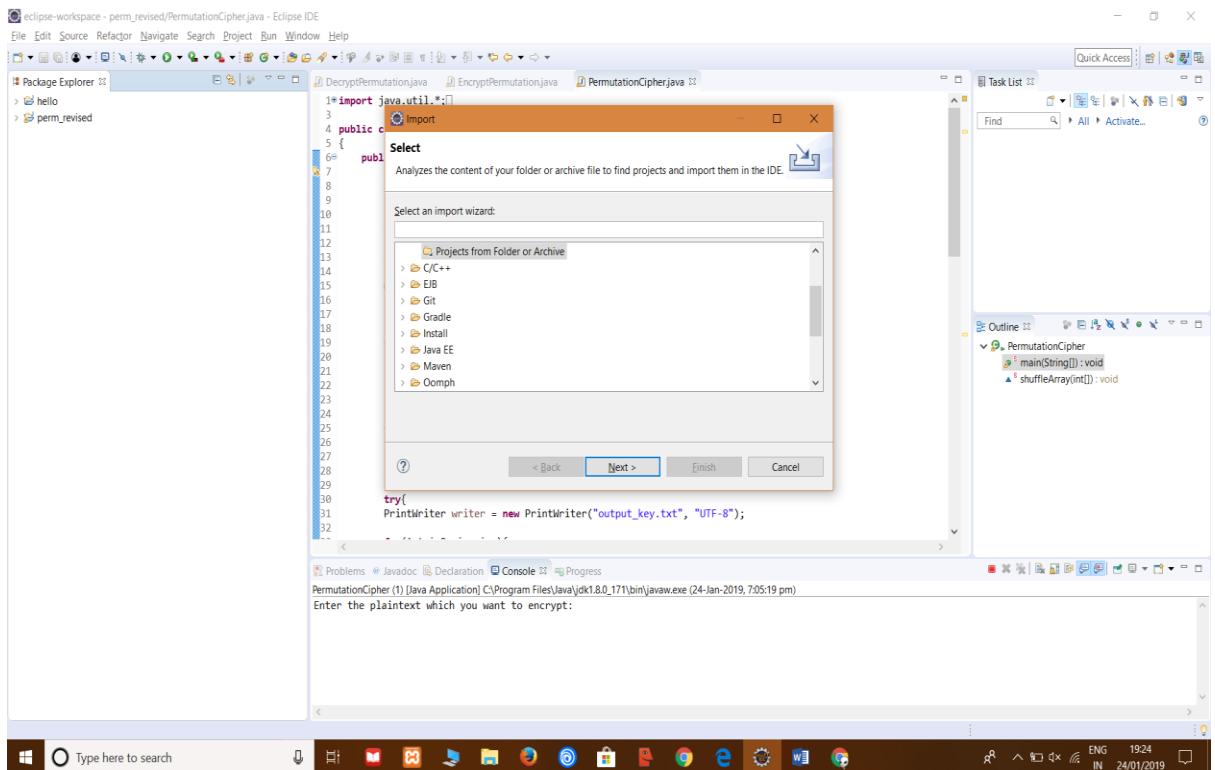
1. Download Eclipse IDE and JDK from the websites mentioned above and set the environment of Eclipse IDE to open perspective – Java.
2. Follow the screenshots given below for importing and running the project

```

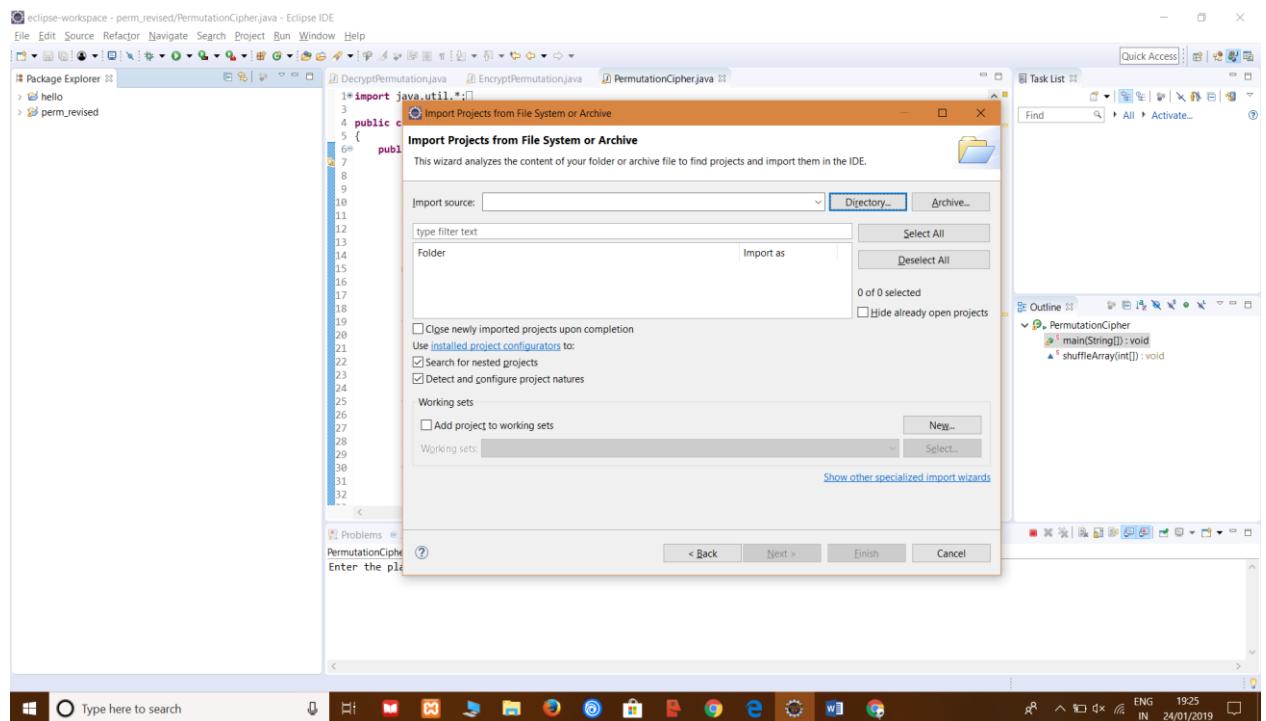
eclipse-workspace - perm_revised/PermutationCipher.java - Eclipse IDE
File Edit Source Refactor Navigate Search Project Run Window Help
New Alt+Shift+N >
Open File... Ctrl+S
Open Projects from File System...
Recent Files
Close Ctrl+W
Close All Ctrl+Shift+W
Save Ctrl+S
Save As... Ctrl+Shift+S
Revert
Move...
Rename... F2
Refresh F5
Convert Line Delimiters To >
Print... Ctrl+P
Import... >
Export... >
Properties Alt+Enter
Switch Workspace >
Restart
Exit
1*import java.util.*;
2
3 public class PermutationCipher
4 {
5     public static void main (String [] args){
6         Scanner sc= new Scanner (System.in);
7         String a;
8         System.out.println("Enter the plaintext which you want to encrypt:");
9         a=sc.nextLine();
10        System.out.println("Enter your preferred size of key 'm':");
11        int m;
12        String key="";
13        String value="";
14        m=sc.nextInt();
15
16        int[] array = new int[m];
17        int var=1;
18        for(int i=0;i<m;i++){
19            array[i]=var;
20            var++;
21            //System.out.print(array[i]);
22        }
23        int [] arrayRandomized = new int[m];
24        for(int i = 0; i<m; i++){
25            arrayRandomized[i]=array[i];
26        }
27        shuffleArray(arrayRandomized);
28
29        try{
30            PrintWriter writer = new PrintWriter("output_key.txt", "UTF-8");
31
32            Enter the plaintext which you want to encrypt:

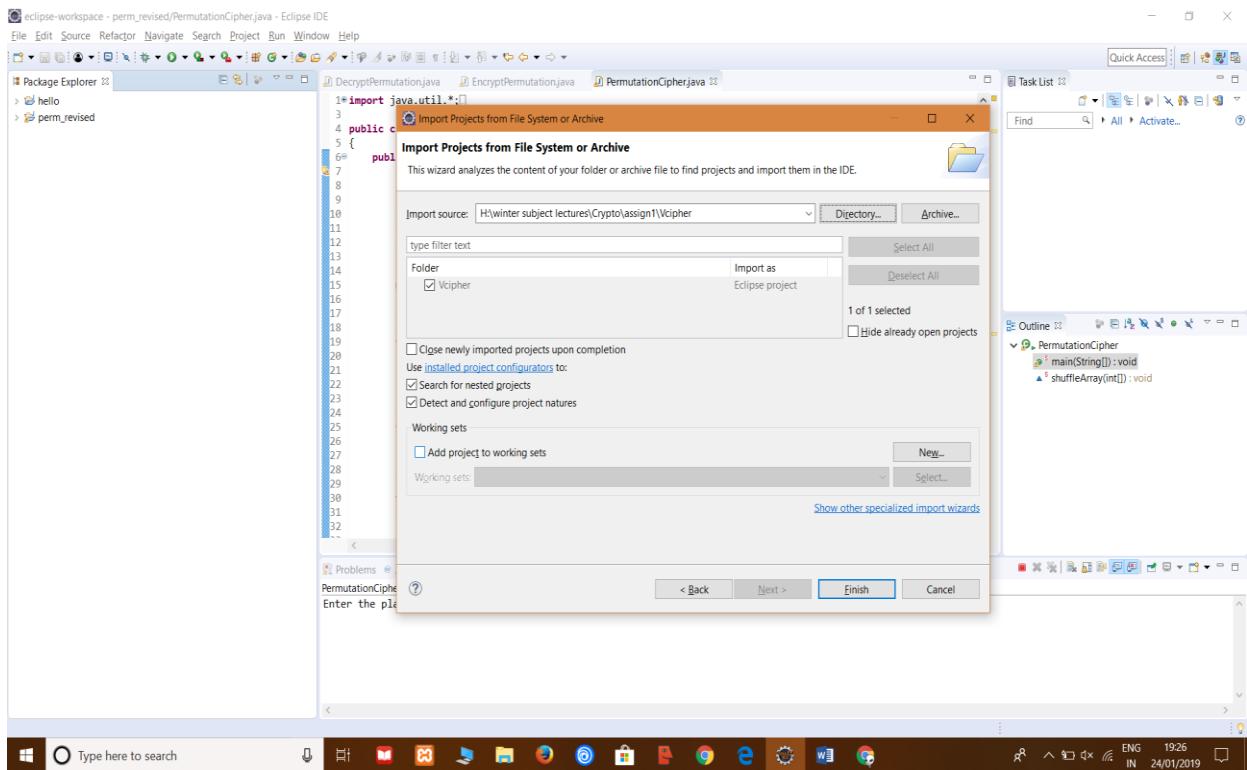
```

3. Go to Projects from Folder on Archive in Import wizard and proceed by selecting the folder provided with this draft i.e Vcipher

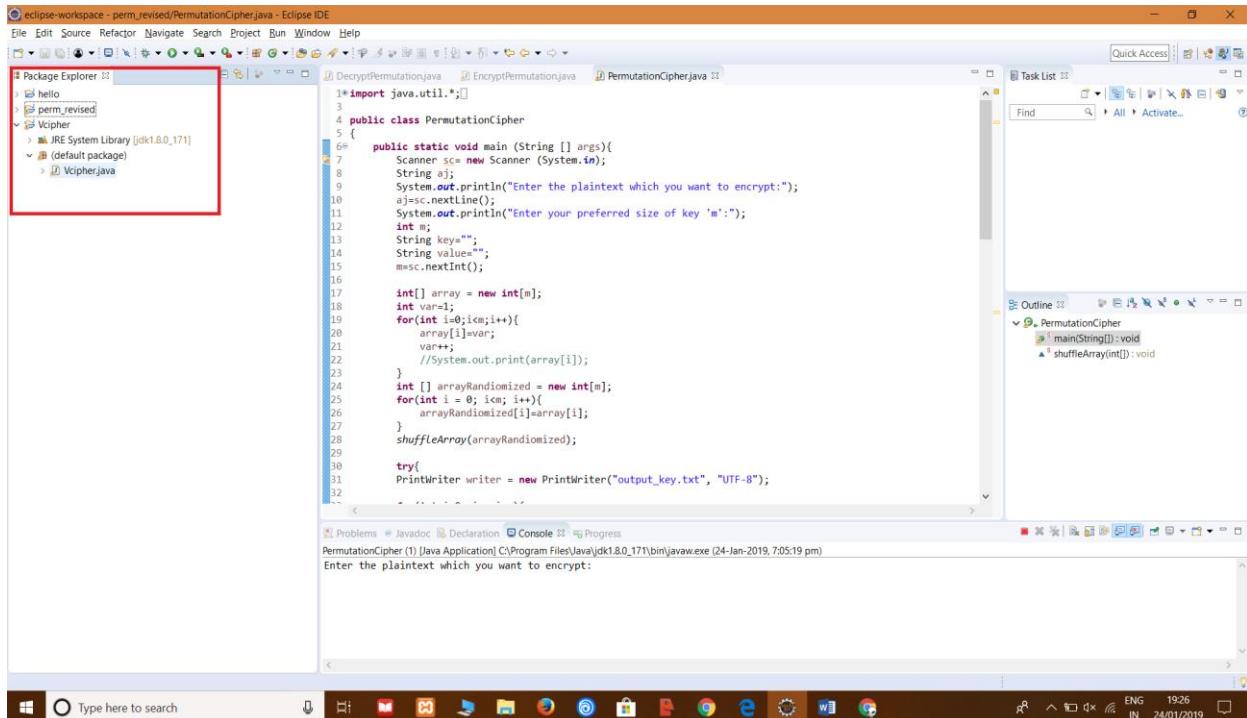


4. Select directory → location

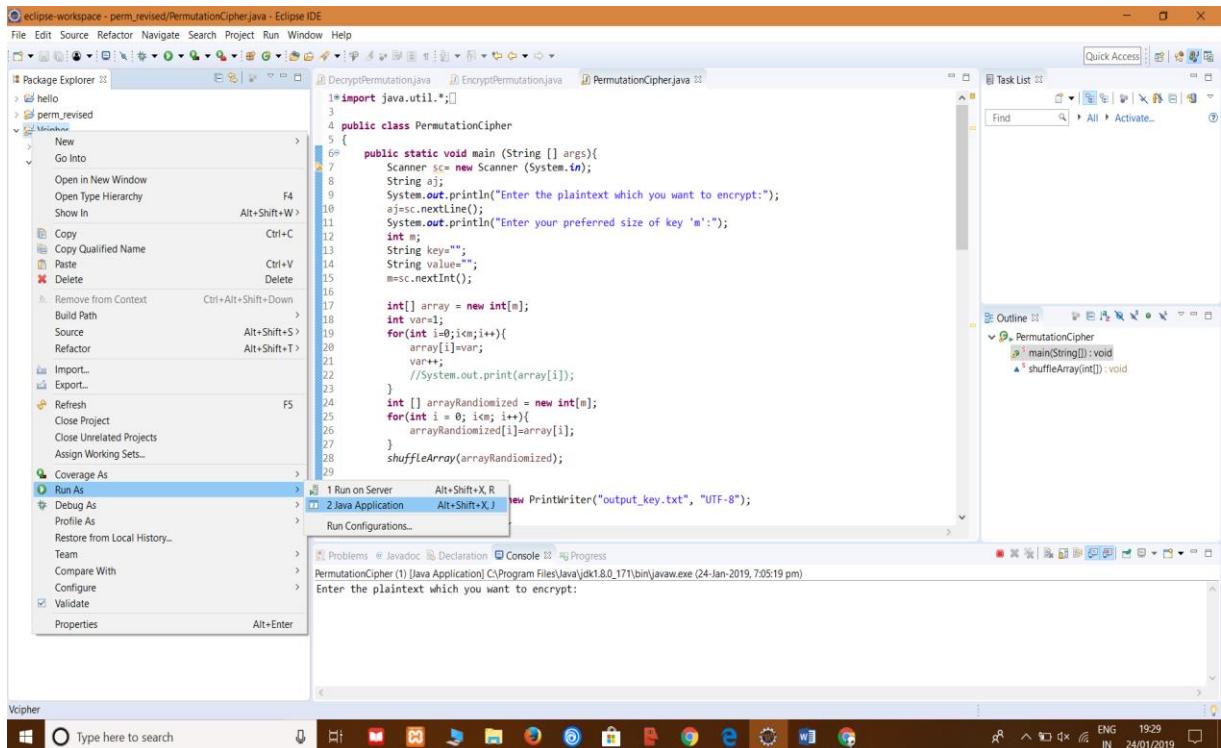




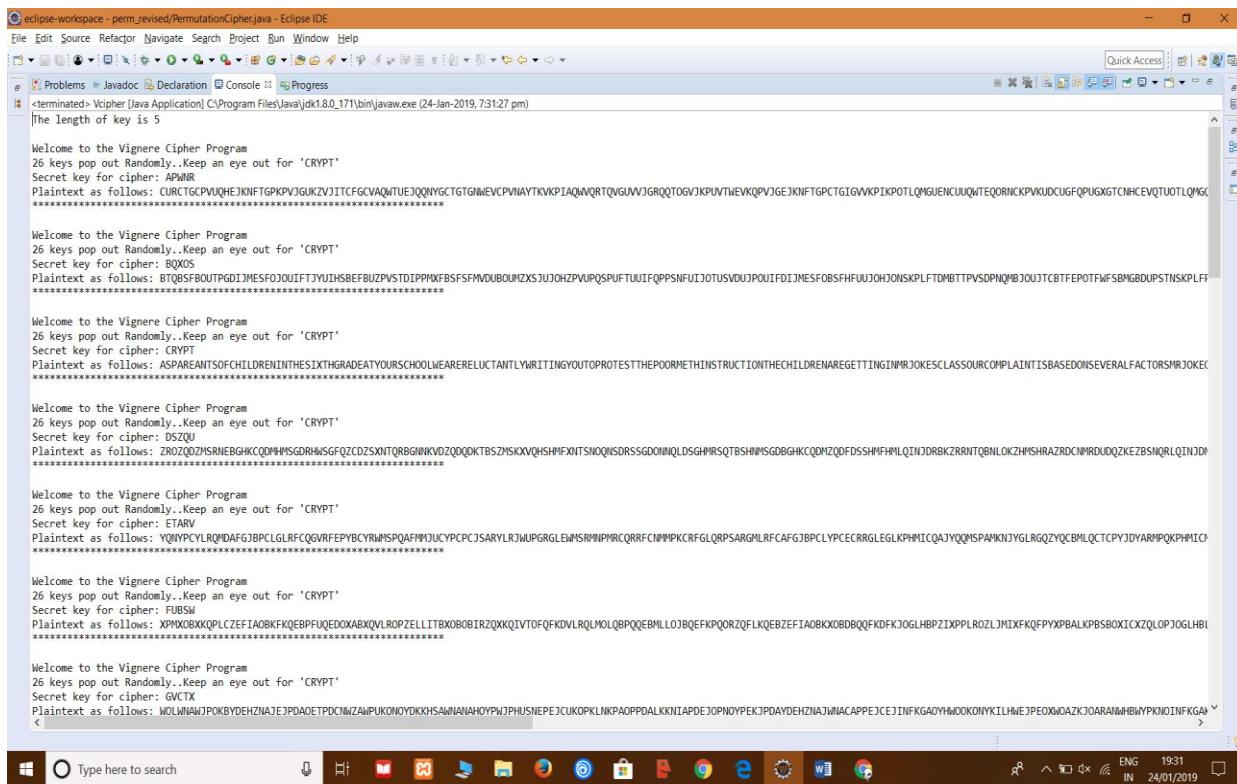
5. You will see the imported folder in the package explorer of Eclipse as shown below.



6. Right click on Vcipher → run as → java application



7. You can watch the output in the console at the bottom of the IDE



8. There are 26 keys popping out randomly in the output with all possible combinations. The length of key coded and found is 5 which is displayed at the start of the output.
9. Using this found key of size m=5, the plaintext is found from the given ciphertext in the assignment problem.

```

Welcome to the Vignere Cipher Program
26 keys pop out Randomly..Keep an eye out for 'CRYPT'
Secret key for cipher: APWNR
Plaintext as follows: CURTCGCPVUQHEJONFTGPKPVJGUZVJITFCFGVAQWTEJQQNYGCTGTGNMEVCVPVAYTKVKPIAQWQRTQVGUVVJGRQQTOGVJKPUVTWEVKQPVJGEJKNFTGCTGIGVVKPIKPOTLQMGUENCUIUQWTEQRORICKPVKUDCUGFQPUUGXTCNIHCEVQUTOLQNGC*****
*****
```

```

Welcome to the Vignere Cipher Program
26 keys pop out Randomly..Keep an eye out for 'CRYPT'
Secret key for cipher: BOXOS
Plaintext as follows: BTB85FBOUTPGD1MEFSOJUIFTYUJHSBEFBUZPVSDFPPMXFB5F5FMWDUBOMIXSJUJ0H2PVUPQSPUFTUUJFOPPSNFUJOTUSVDUJPOLIFD1MESF08SFHFUJ0HJ0NSKPLFTDMBTTPVSDPNQMBJOUJTCBTFEPOTFWSBMGBDUPSTNSKPLFF*****
*****
```

```

Welcome to the Vignere Cipher Program
26 keys pop out Randomly..Keep an eye out for 'CRYPT'
Secret key for cipher: CRYPT Key of size 5 - CRYPT
Plaintext as follows: ASPEARANTOCHILDRENINTHESEXTGRADEATYOURCHOOLWEARERELUCTANTLYWRITINGYOUTOPROTESTTHEPOORMETHINSTRUCTIONTHECHILDRENAREGETTINGINMRJOKECLASSOURCOMPLAINTISBASEDONSEVERALFACTORSMRJOKE*****
*****
```

```

Welcome to the Vignere Cipher Program
26 keys pop out Randomly..Keep an eye out for 'CRYPT'
Secret key for cipher: DSZQJ
Plaintext as follows: ZRQZQDZHNRNIEBGHKCDHMISGDHMSGFQZCDZSNTQRBGINVKDZQDDQKTBZMSKIAVQSHMFXTSIIQNSDRSSGDQINQLDSGHMRSQTBSHMSGDBGHKCDMZQDFSSHMFHMLQINJDRBKZRRNTQBZKHZMSHRAZRCNMRDUDQZKEBSNQRLQINJDN*****
*****
```

```

Welcome to the Vignere Cipher Program
26 keys pop out Randomly..Keep an eye out for 'CRYPT'
Secret key for cipher: ETARV
Plaintext as follows: YQNPVPCYLQRQMDAGFJBPCLGLRFCQGVRFEPYBCYRWMSPQAFMNUJCYPCCJSARYLRJWUPGRGLEHNSRMNPHRCQRRFCNMMPKCRFGLQRPSSARGHLRCFAGJBPCLYPCERRGLEGLKPHMTCQAJYQQMSPAKNUYGLRGQZYQCBMLQTCPYDYARMQPKHMC*****
*****
```

```

Welcome to the Vignere Cipher Program
26 keys pop out Randomly..Keep an eye out for 'CRYPT'
Secret key for cipher: FUBSW
Plaintext as follows: XPHXOBXKQPLCZEFIAOBKFQJBPQEDOXABXQVLRQZELLITBXOB0BIRZQXKQIVTOFQFKDVLRLQMLQLBQPBQEBMLLQJBBQEFKQORZQFLKQEZEFAOBXOB0BQKFDFKJ0GLHBPZIXPPLR0ZLJMIXFKQFYPXBALKPB5BOICXZQLOPJOGLHBI*****
*****
```

```

Welcome to the Vignere Cipher Program
26 keys pop out Randomly..Keep an eye out for 'CRYPT'
Secret key for cipher: GVCTK
Plaintext as follows: WOLWMAWJPOKBYDEHZNAJE3PD0AEETPDCIMZAIPUKONODYKKHSANAH0YWPJPHUSNEPEJCUOKPLNKPAOPPDALKKNIAPDEJOPNOYPEKJPDAYDEHZNAJWACAPPEJCEJINFKA0YH0OKONYKILHWEJPEOXGIOAZKJ0ARANWHBWPKN0INFKGAH*****
*****
```

10. The key ‘CRYPT’ is seen in first few iterations of the output. The screenshot given below displays rest of the keys out of 26.

eclipse-workspace - perm_revised/PermutationCipher.java - Eclipse IDE

File Edit Source Refactor Navigate Search Project Run Window Help

Problems Javadoc Declaration Console Progress

<terminated> Vcipher [Java Application] C:\Program Files\Java\jdk1.8.0_171\bin\javaw.exe (24-Jan-2019, 7:31:27 pm)

Welcome to the Vignere Cipher Program
26 keys pop out Randomly..Keep an eye out for 'CRYPT'
Secret key for cipher: HxDUY
Plaintext as follows: VNVKmVZV(OH)AXCDGVMZIDOCZNDSOCMVYZOTJPNUWCJGRZVMZGPXOVIOTGRMDODIBTPOJOMJZHOOCZKJMHZCDINOMPXOD)IOCZXCDCGYMZIVMZBZODIBDHEFZIXGVNIPM0CHGVDOONWVIZYJNZQZMVGAZOJNHMEFZ*****

Welcome to the Vignere Cipher Program
26 keys pop out Randomly..Keep an eye out for 'CRYPT'
Secret key for cipher: IXEVZ
Plaintext as follows: UHJULYUHNWIZWBFCFLYHCNBYNCRNBALUXYUNISIOLMWBIFFQYULYLYFOWNUHNSQLCNHASIONIJLINVNNBHYJIIILGYNBCHMILAWNCHNBYWBCFLXLYHULAYNNCHACHGLDIEYMFUMMIOLWIGJFUCHICNVMYXHJYPLUFZUNNILMGLDIEY*****

Welcome to the Vignere Cipher Program
26 keys pop out Randomly..Keep an eye out for 'CRYPT'
Secret key for cipher: JYFAA
Plaintext as follows: TLITKXTGMILHYVABEWXQGBGMAXLBQNAZKTWXRHNLVVAHEPXTOKXXEIVMTGMRPKBMGBZRHNWHIKHMXLMMAXIHKFXVABGLMKVNBHGMXAVBEWOKGTOKXWIMBGZBFKCHDXLVEETLHINKVHFETBGBLUTLXWHLGXOKTEYTVMHKLFKHDH*****

Welcome to the Vignere Cipher Program
26 keys pop out Randomly..Keep an eye out for 'CRYPT'
Secret key for cipher: KZGK8
Plaintext as follows: SKHSJWSFLKGXKUZADWVJWFAFLZKAPLZYJZWSLQGMJUKZGDDWSWJDWDLMSFLDQOJALAFYQGMILGHJGLWLKLZMNGGEWLZAFKLJMULAGFLZNUZADVJWFSJWYLLAFYAFEBGCWUDSKKGJUJEHDSAFLAKTSKAVGFKNWJSDXSULGKEJBGCW*****

Welcome to the Vignere Cipher Program
26 keys pop out Randomly..Keep an eye out for 'CRYPT'
Secret key for cipher: LAHYC
Plaintext as follows: R3JGTVREKJFMWTYZCUIVEZEKYJZOKYKIRUVRKPFJTYFCHVNRIVICLTKRECPNIZKZEXPFLKFJFVKJKKYJGFFIDVKYJEKJLITKZFEKYVYZCUIVERIVXVKKZEXEDIAFBVJTCRJFLITFDGCRZEKJSRJUFEJVMVIRCWRTKFJJDIAFBV*****

Welcome to the Vignere Cipher Program
26 keys pop out Randomly..Keep an eye out for 'CRYPT'
Secret key for cipher: MBIZD
Plaintext as follows: QFQHQUOJIEVSXBTHUDYDQJXIJNQXHQHOUQJOEKHISXEEMQHJQHUUHUKSJDQJBOHMYJYDWOEKJEFHEJUJJXJXUEEEHCUJXYD1JHKSYEDJXJSXYBTHUDQHUMJJYDCHZEAUISQIIEKHSECFCBQDQJYIRQIUTEDIULUJHQBVQSEHICHZEAU*****

Welcome to the Vignere Cipher Program
26 keys pop out Randomly..Keep an eye out for 'CRYPT'
Secret key for cipher: NCJAE
Plaintext as follows: PHEPGTPCJHOURWKA5GTXCINTH001WVGPTSPINDGHRWDALTPGTGTAJRIPCIANLGIXCVDNJDIDEOTHITHIWTEDDGBTIWXCHIGJRIXDCIWTIXA5GTCPTVIIIXCVXCBGYZTHRAPHHDJGRDBEAPXCIXHQPHTSDCHTKTGPAPRIDGHGBGYDZTC*****

Windows Type here to search ENG 19:39 IN 24/01/2019

eclipse-workspace - perm_revised/PermutationCipher.java - Eclipse IDE

File Edit Source Refactor Navigate Search Project Run Window Help

Problems Javadoc Declaration Console Progress

<terminated> Vcipher [Java Application] C:\Program Files\Java\jdk1.8.0_171\bin\javaw.exe (24-Jan-2019, 7:31:27 pm)

Welcome to the Vignere Cipher Program
26 keys pop out Randomly..Keep an eye out for 'CRYPT'
Secret key for cipher: ODKBF
Plaintext as follows: OGDOFSOBHGETQWZFSBWHSGWLHIVFORSHQHCKIFGQVCZKSOSFSZIQLQOBHZMKFWMBUMCJHCFCHSGHHVSOCFCASHWBGFIQHBCBHSQWZRSBFSUSHMBUNBAFXCYSGQZOGGCFQCADZ0BHNGPOGSRCBGSJSFOZTOQHCFGAFXCYSC*****

Welcome to the Vignere Cipher Program
26 keys pop out Randomly..Keep an eye out for 'CRYPT'
Secret key for cipher: PELCG
Plaintext as follows: NFCNERNAGFBSPUNVYQERAVAGURFVKGUTEINQRNGLBLHEFPUBBYJRNERERYHPGNAGYLJEVGVATLBHGBCEBRGGURCBBEZRGUJAVGEHPPGVAGURPVVYQERANERTRGGVATVAZENBXRFPNFFBHEPBZCYINAVGFFONFRQBAFRIRENYSNPGBEFZENBXRE*****

Welcome to the Vignere Cipher Program
26 keys pop out Randomly..Keep an eye out for 'CRYPT'
Secret key for cipher: QFMHD
Plaintext as follows: MEBMDQNFZEAROTUXPDQZUFTQEIJFTSDMPQMFKAQDEOTAAXIQMDQDXQGFMZXKIDUFSKAGFABDAFQEFFTQBAADYQFTUZEFDFGUFUAZFTQOTUXPDQZHDQSFFUZSUZYDVAQE0XMEEGD0AYBXWIZFUEUNMQPAZEQHQDMXRM0FADEYDVWQ*****

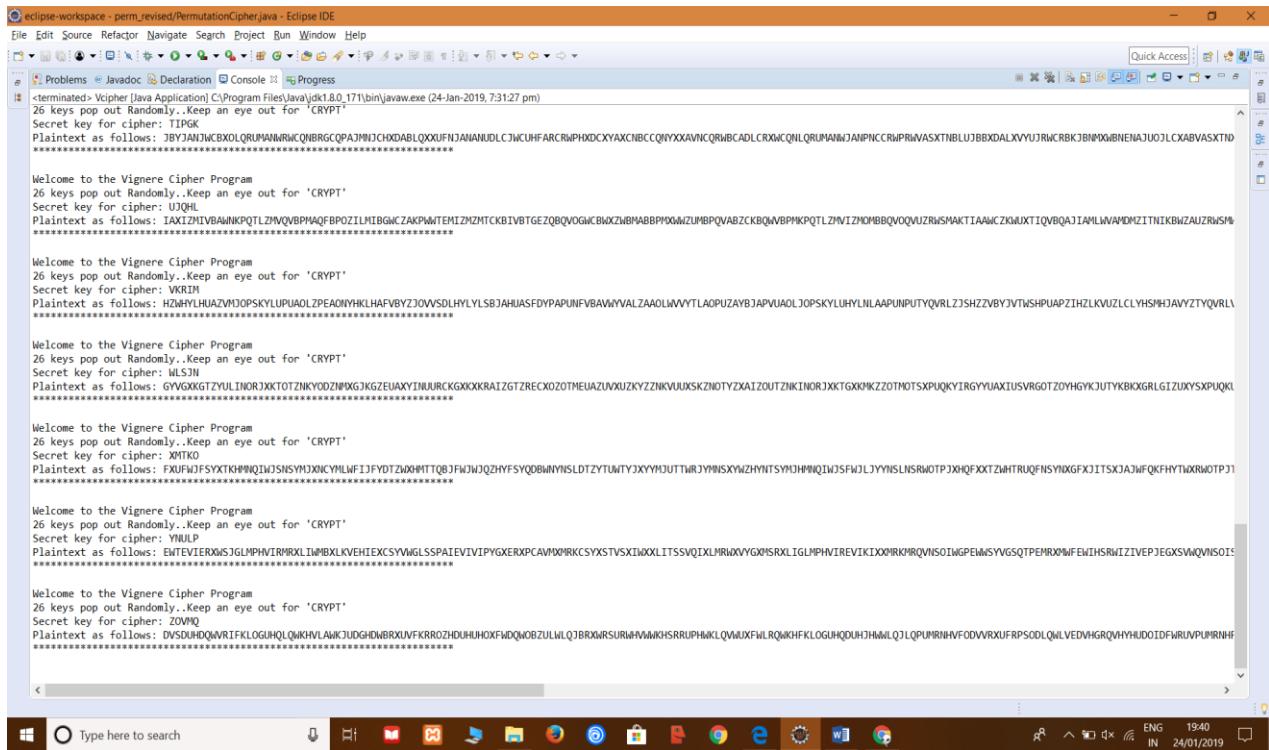
Welcome to the Vignere Cipher Program
26 keys pop out Randomly..Keep an eye out for 'CRYPT'
Secret key for cipher: RGNEI
Plaintext as follows: LDAICPLYEDZONTWQCPYTESPDTESRCOLPLEJZFCDSZSZZHPLCPCPWFNLEYWJHCTETYRJZFZECZPDEESPNTWQCPYLCPRPEETYRTYXCUZVDPNWLDDZFCNZXAHLYETDMLDPOZYDPPGCLWQLNEZCDXCUZVP*****

Welcome to the Vignere Cipher Program
26 keys pop out Randomly..Keep an eye out for 'CRYPT'
Secret key for cipher: SHOFJ
Plaintext as follows: KCZBK0KDCYPMBSVNBOKSDROCSHEDPKNOHDJYEBCHIRYYGOKBOBOVEMDKD0VIGBDSXQJYEDYZBYDCCDR0ZYBWDORSXDBEMDSYXDR0MRSVNBOKBQ0QDOSXQ5XB7YUOCJVKCCYEBMIVZVKSXDSCLKCONYXCOFOBKVKNDYBCWBTYUO*****

Welcome to the Vignere Cipher Program
26 keys pop out Randomly..Keep an eye out for 'CRYPT'
Secret key for cipher: TIPGK
Plaintext as follows: JBVJADNJCX0LQRUHABHRWCQNBRCGQPA2MNJCHXDABLQXXUHJANANUDLCJNUHFARCRWPHDXCXYAXNCBCQNYXAVICQWBCADLRCXNCQNLQRUMANWJANPNCCRIPRIVASXTNBLUJBBDALXVYUJRWCRBKJBNM0WBNENAJUOJLCXAVVASXTD*****

Welcome to the Vignere Cipher Program
26 keys pop out Randomly..Keep an eye out for 'CRYPT'
Secret key for cipher: U3QHL
Plaintext as follows: IAXCIZMIVBAWNPQTLZMVQBPMAQFBPQZILMBGWCZAKPWNITEMIZMZMTCKBIVBTGEZQBQVQGWCBIKZWBMABBPMXGZUMBQPVBZCKBQWBPQKPTLZMV1ZM0MBQVQVUZRWSMAKTIAAWCZKWXTIQVBQAJIAMLWVANDM2ITNIKBWZAUZRWSM*****

Windows Type here to search ENG 19:39 IN 24/01/2019



eclipse-workspace - perm_revised/PermutationCipher.java - Eclipse IDE

File Edit Source Refactor Navigate Search Project Run Window Help

Problems Javadoc Declaration Console Progress

<terminated> Vcipher [Java Application] C:\Program Files\Java\jdk1.8.0_171\bin\javaw.exe (24-Jan-2019, 7:31:27 pm)

26 keys pop out Randomly..Keep an eye out for 'CRYPT'

Secret key for cipher: TIPCK

Plaintext as follows: JBVJANJWCXQLOQRUMANRWCQNRGCOPAZMNDCHXDABLOXXUFN)ANANUDLCJWCUHFARCRWPHDXCYAXCNBCQIRYXXAVNCQRWBACDLRXWCQNLQRUMANINJANPNCCRWPRIWA5XTNBLUJBBDALXVYUJRWCRBKJBNPQWBNEAJUJLCXABVASXTD

Welcome to the Vigenere Cipher Program

26 keys pop out Randomly..Keep an eye out for 'CRYPT'

Secret key for cipher: U7QHL

Plaintext as follows: IAXIZMTVBAWIKPQTJZHQVBPMQFBPOZTLMIBGWZAKCPWTEMIZHZMTCKBIVBTGEZQBQVOGWCBXZWBMABBP0XWZUMBHQVABZCKBQWBPMPKPTLZMVIZHOMBBQVQVUZRWSMAKTIAAWCZKNUXTIQUVQAJIAMLWVAMONZITNIKBWZAUZRWSM

Welcome to the Vigenere Cipher Program

26 keys pop out Randomly..Keep an eye out for 'CRYPT'

Secret key for cipher: VKRJM

Plaintext as follows: HZWHYLHUAZVJOPSKYLUUQAUOLJPEAQNYHKLHAFVBYZJOWVSDLHYLYLSBJAHIASFDYPAPUNFV8AWVALZAOLWVYTALAOUPAZBJAOPVUAOLJOPSKYLUUHYNLAAPUNPUTYQVRLZJSHZZBVYJVTSWHPUAPZIHZLKVKUZLCYHSHHJAVYZTYQVRL

Welcome to the Vigenere Cipher Program

26 keys pop out Randomly..Keep an eye out for 'CRYPT'

Secret key for cipher: WLSJN

Plaintext as follows: GYWXKGKGTZVULINORJXKTTZKHYODZNIGJKGZEUAXYINJURCKGXKXKRAIZGTZRECXOZOTMEUAZUVXUZYZZNKVUUXSKZNOTYZXAIZOUTZNKINORJXKTXGK9KZZOTMOTSXPUQKYIRGGYUAXIUSVRGOTZOYHGKJUTYKBXGRLGIZUXYSXPQKL

Welcome to the Vigenere Cipher Program

26 keys pop out Randomly..Keep an eye out for 'CRYPT'

Secret key for cipher: XMTKO

Plaintext as follows: FXJUJFJSYTKHMNQIWJSNSNMYJXNCYMLWFJFYTDTZKQHMTTQBJFWQWZQZHYSYQDBWNYNSLDTZYTUWITYJXYMMQUTTWIRJYMMNSXWZHNTSYHJHMNQIWJSFWQJLJYMMNSLRWOTPJKHQFXXTZWHTRUQFNSYIXGFJXITSXJAJWIFQKFHYTWXRWOTPJT

Welcome to the Vigenere Cipher Program

26 keys pop out Randomly..Keep an eye out for 'CRYPT'

Secret key for cipher: YNULP

Plaintext as follows: ENTEVIERXWISJGLMPHIVIRMRLXIMMBXLKVHEIEXCSYVGWLSSPAIEVIVIPYGERXPCA\W\W\RKCSYXSTVSXI\W\XLITSSVQIXLMR\W\Y\GXMSRXLIGLMPHVIREVIKIXXMRKMRQVNSOIWGPEW\W\Y\GSQTPEM\W\%FEWIHSRWIZIVEP\EGXSVWQVNSOIS

Welcome to the Vigenere Cipher Program

26 keys pop out Randomly..Keep an eye out for 'CRYPT'

Secret key for cipher: ZOVHQ

Plaintext as follows: DVSDUHDQ\W\RTFKLOGUQLQ\KHVLAWIKJUDGHWDWRXUVFKRROZHDUHUOXFWDQWOBZULWQJBRXMRSURHVMKHSRRUPH\KLVQWLFRLRQWKFKLOGUHQDH\H\H\W\LQJLQPU\RNHVFOD\W\RXUFRPSOLQWLVEDVHGRQVHYHDDOIDFWRUVPU\RNHF

Windows Start Type here to search Back Home Task View Taskbar ENG 1940 IN 24/01/2019

Thank You!

Name – Ajinkya Kunjir

Student ID- 0876835

Subject- Cryptography & Network Security

Assignment 1