Department of Information Technology

Name of Student: Vishal Bangar
Student ID: 20104084

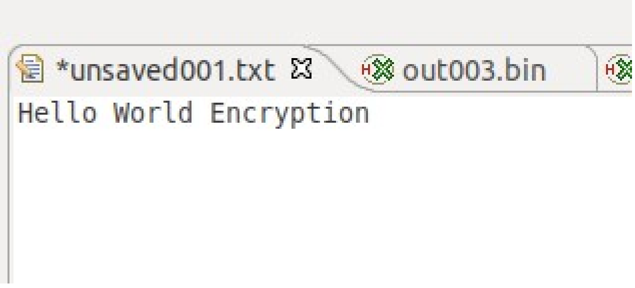
Semester: V
Academic Year: 2022-23
Class / Branch: TE IT
Subject: Security Lab (SL)
Name of Instructor: Prof. Apeksha Mohite

EXPERIMENT NO. 11

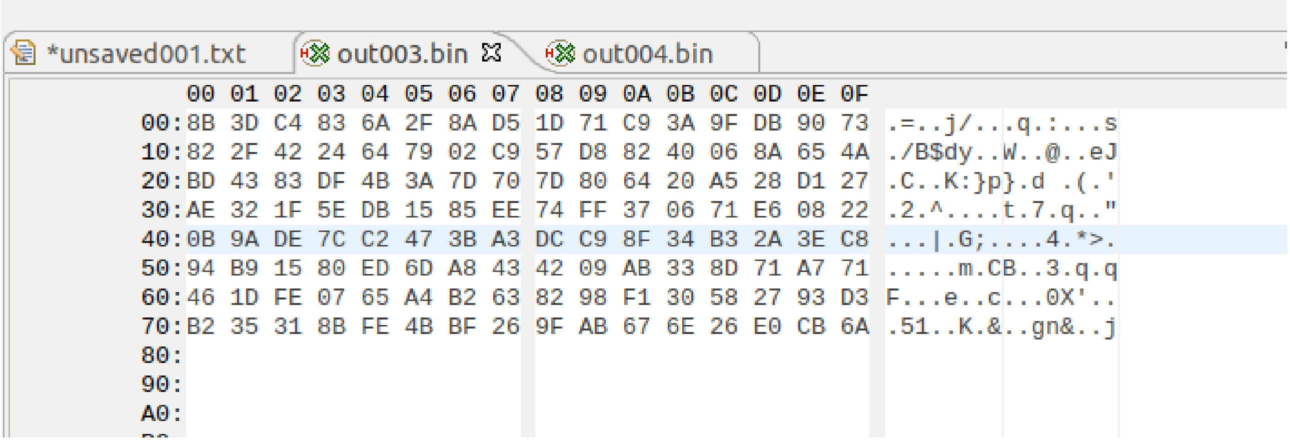
Aim: To study symmetric and asymmetric encryption methods using Cryptool.

Output:

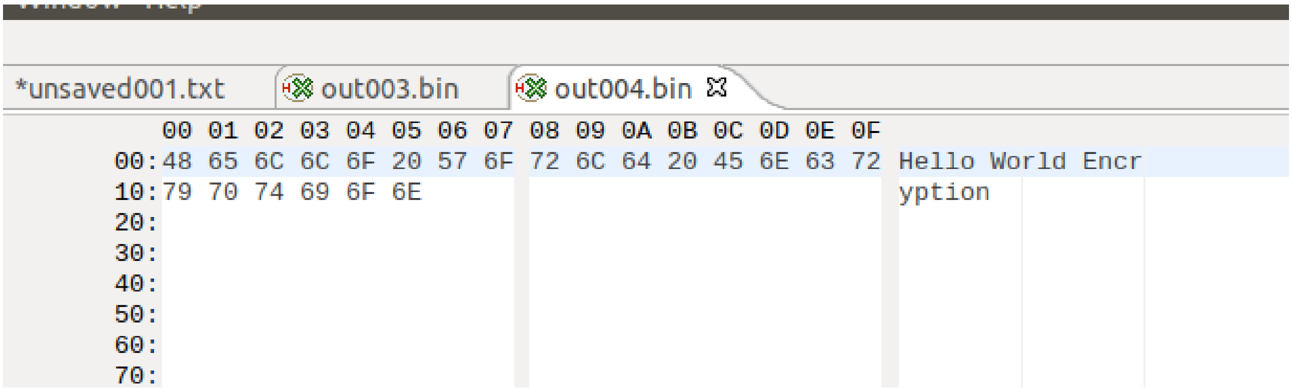
1) RSA



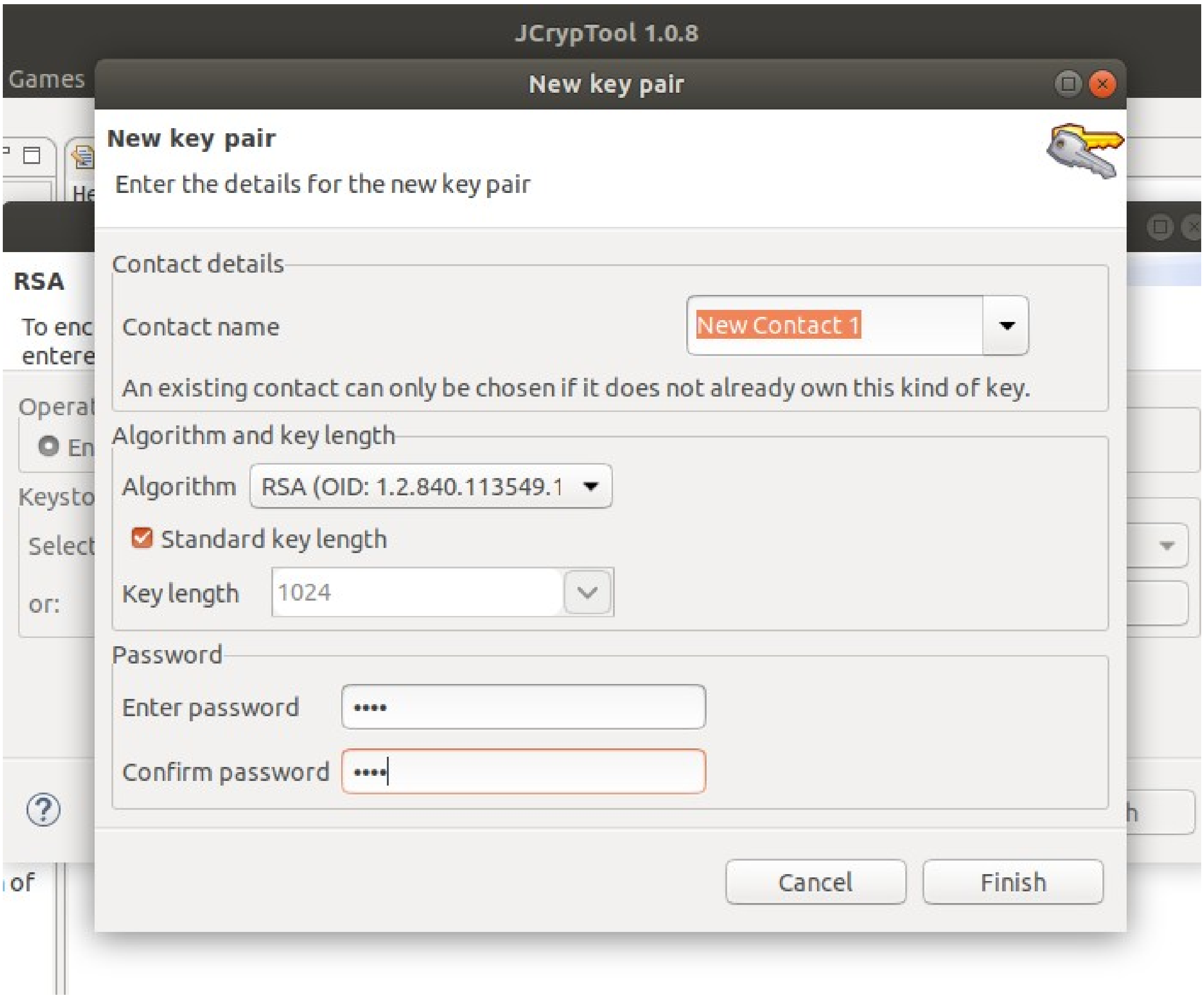
```
Hello World Encryption
```



```
     00 01 02 03 04 05 06 07 08 09 0A 0B 0C 0D 0E 0F
00:8B 3D C4 83 6A 2F 8A D5 1D 71 C9 3A 9F DB 90 73 .=..j/...q.:...s
10:82 2F 42 24 64 79 02 C9 57 D8 82 40 06 8A 65 4A ./B$dy..W..@..eJ
20:BD 43 83 DF 4B 3A 7D 70 7D 80 64 20 A5 28 D1 27 .C..K:}p}.d .(.'
30:AE 32 1F 5E DB 15 85 EE 74 FF 37 06 71 E6 08 22 .2.^....t.7.q.."
40:0B 9A DE 7C C2 47 3B A3 DC C9 8F 34 B3 2A 3E C8 ...|.G;....4.*>.
50:94 B9 15 80 ED 6D A8 43 42 09 AB 33 8D 71 A7 71 .....m.CB..3.q.q
60:46 1D FE 07 65 A4 B2 63 82 98 F1 30 58 27 93 D3 F...e..c...0X'..
70:B2 35 31 8B FE 4B BF 26 9F AB 67 6E 26 E0 CB 6A .51..K.&..gn&..j
80:
90:
A0:
```



```
     00 01 02 03 04 05 06 07 08 09 0A 0B 0C 0D 0E 0F
00:48 65 6C 6C 6F 20 57 6F 72 6C 64 20 45 6E 63 72 Hello World Encr
10:79 70 74 69 6F 6E                               yption
20:
30:
40:
50:
60:
70:
```



New key pair

Enter the details for the new key pair

Contact details

Contact name: New Contact 1

An existing contact can only be chosen if it does not already own this kind of key.

Algorithm and key length

Algorithm: RSA (OID: 1.2.840.113549.1

☑ Standard key length

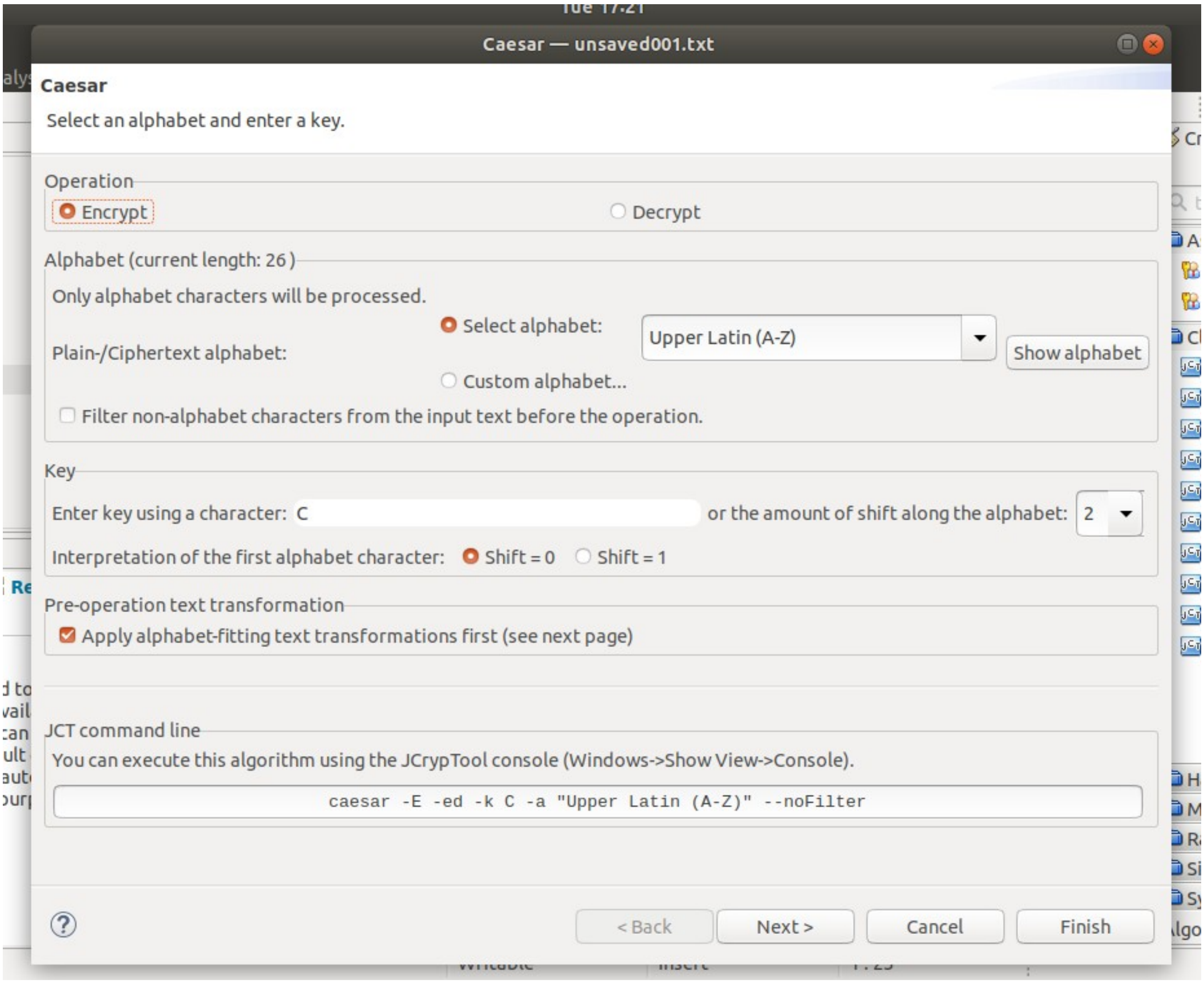
Key length: 1024

Password

Enter password: ••••

Confirm password: ••••

2) Caeser



Caesar — unsaved001.txt

Caesar

Select an alphabet and enter a key.

Operation

● Encrypt ○ Decrypt

Alphabet (current length: 26)

Only alphabet characters will be processed.

Plain-/Ciphertext alphabet: ● Select alphabet: Upper Latin (A-Z) Show alphabet

○ Custom alphabet...

□ Filter non-alphabet characters from the input text before the operation.

Key

Enter key using a character: C or the amount of shift along the alphabet: 2

Interpretation of the first alphabet character: ● Shift = 0 ○ Shift = 1

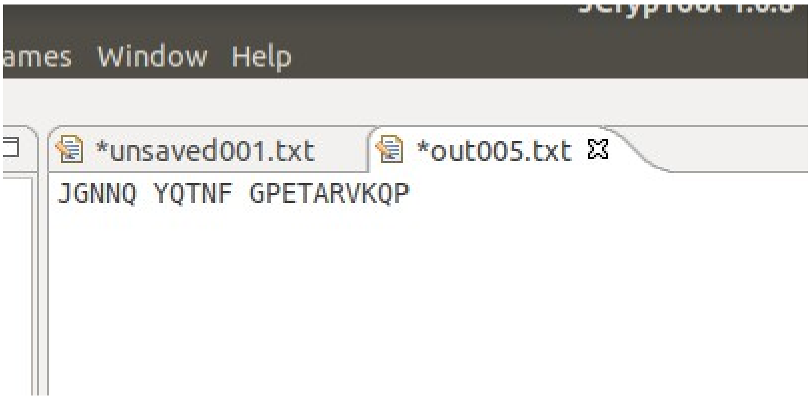
Pre-operation text transformation

☑ Apply alphabet-fitting text transformations first (see next page)

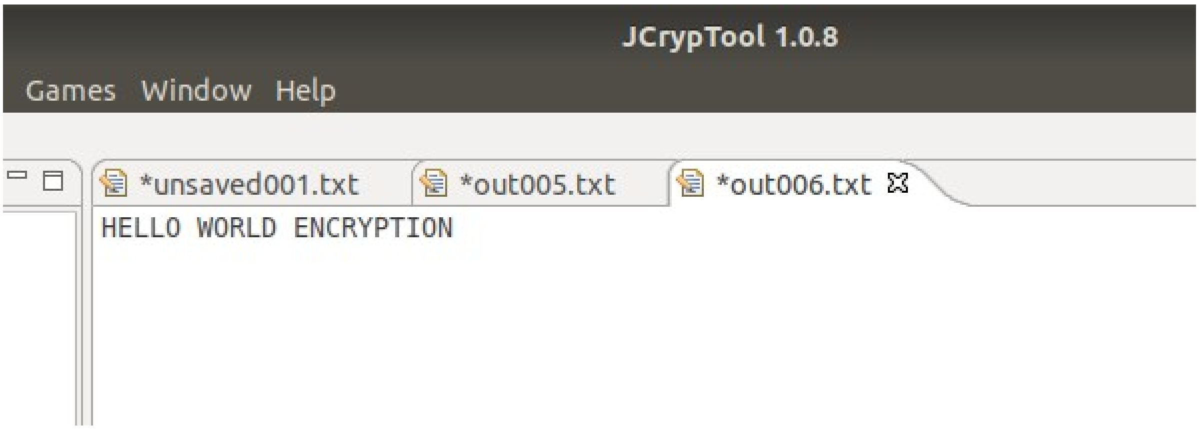
JCT command line

You can execute this algorithm using the JCrypTool console (Windows->Show View->Console).

```
caesar -E -ed -k C -a "Upper Latin (A-Z)" --noFilter
```

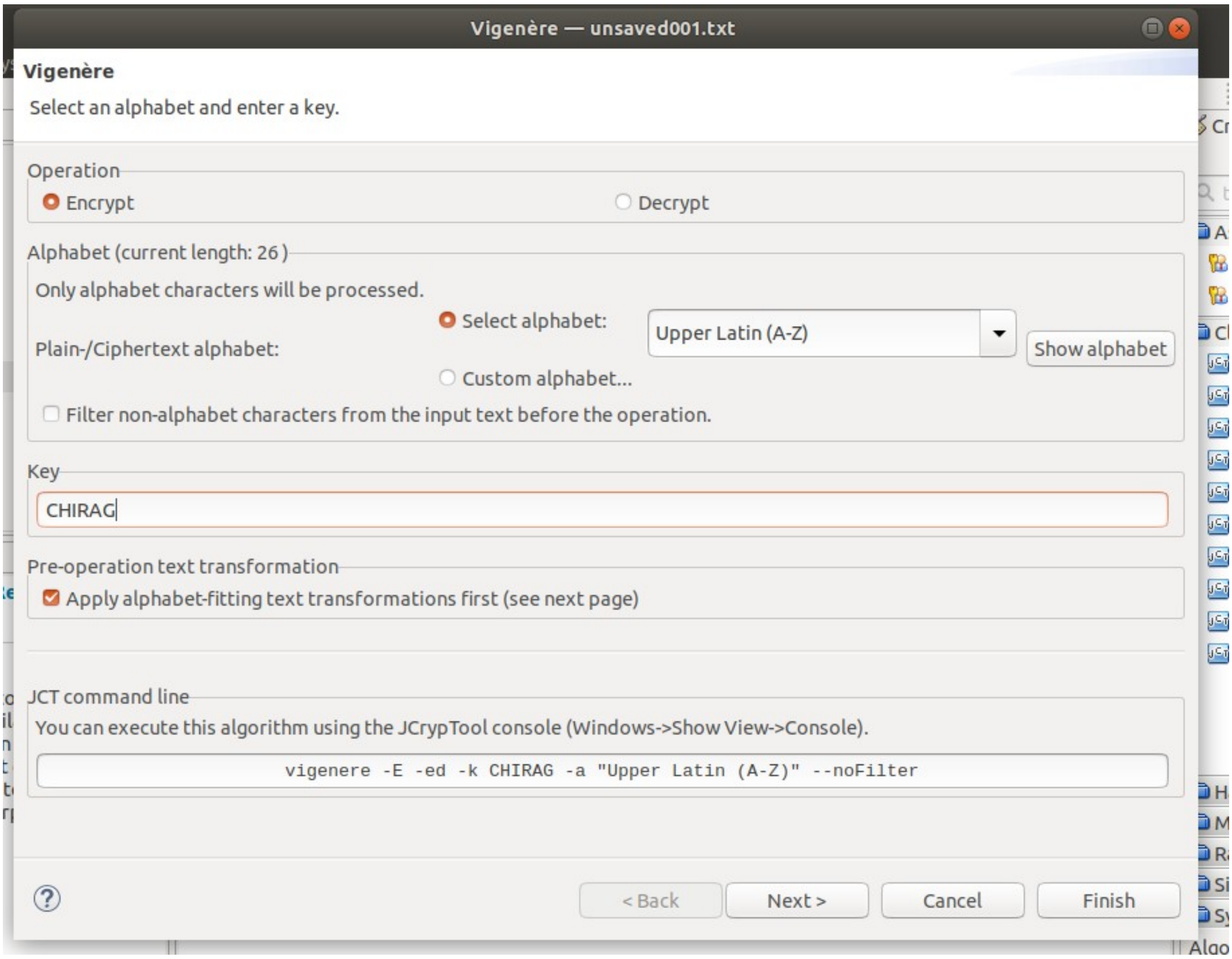


```
JGNNQ YQTNF GPETARVKQP
```



```
HELLO WORLD ENCRYPTION
```

3) Vigenere



Vigenère — unsaved001.txt

Vigenère

Select an alphabet and enter a key.

Operation

● Encrypt ○ Decrypt

Alphabet (current length: 26)

Only alphabet characters will be processed.

Plain-/Ciphertext alphabet: ● Select alphabet: Upper Latin (A-Z)

○ Custom alphabet...

□ Filter non-alphabet characters from the input text before the operation.

Key

CHIRAG

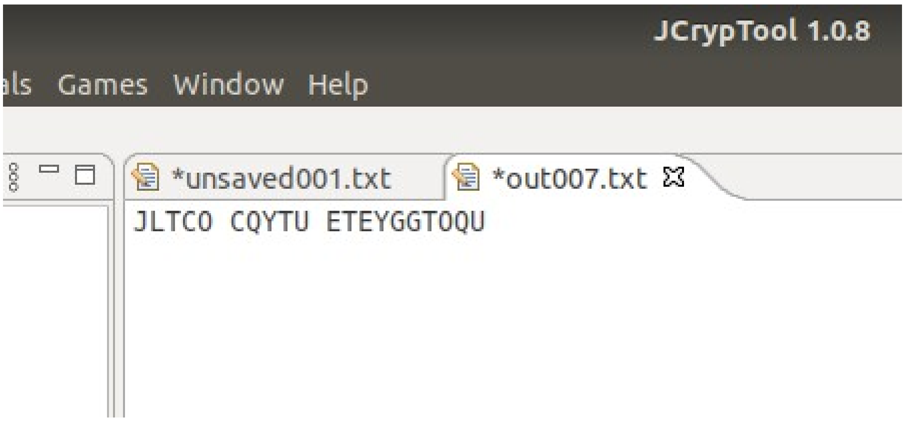
Pre-operation text transformation

☑ Apply alphabet-fitting text transformations first (see next page)

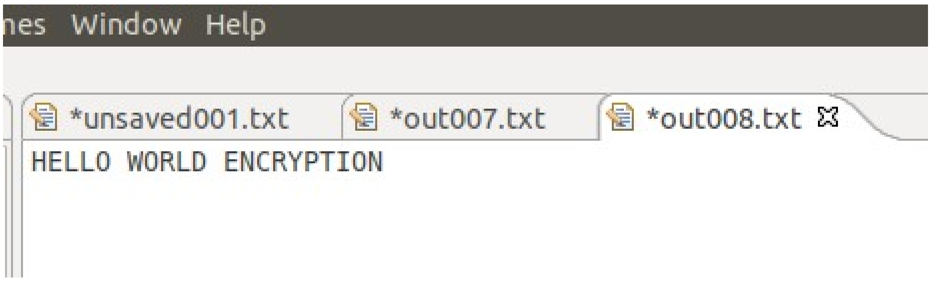
JCT command line

You can execute this algorithm using the JCrypTool console (Windows->Show View->Console).

```
vigenere -E -ed -k CHIRAG -a "Upper Latin (A-Z)" --noFilter
```

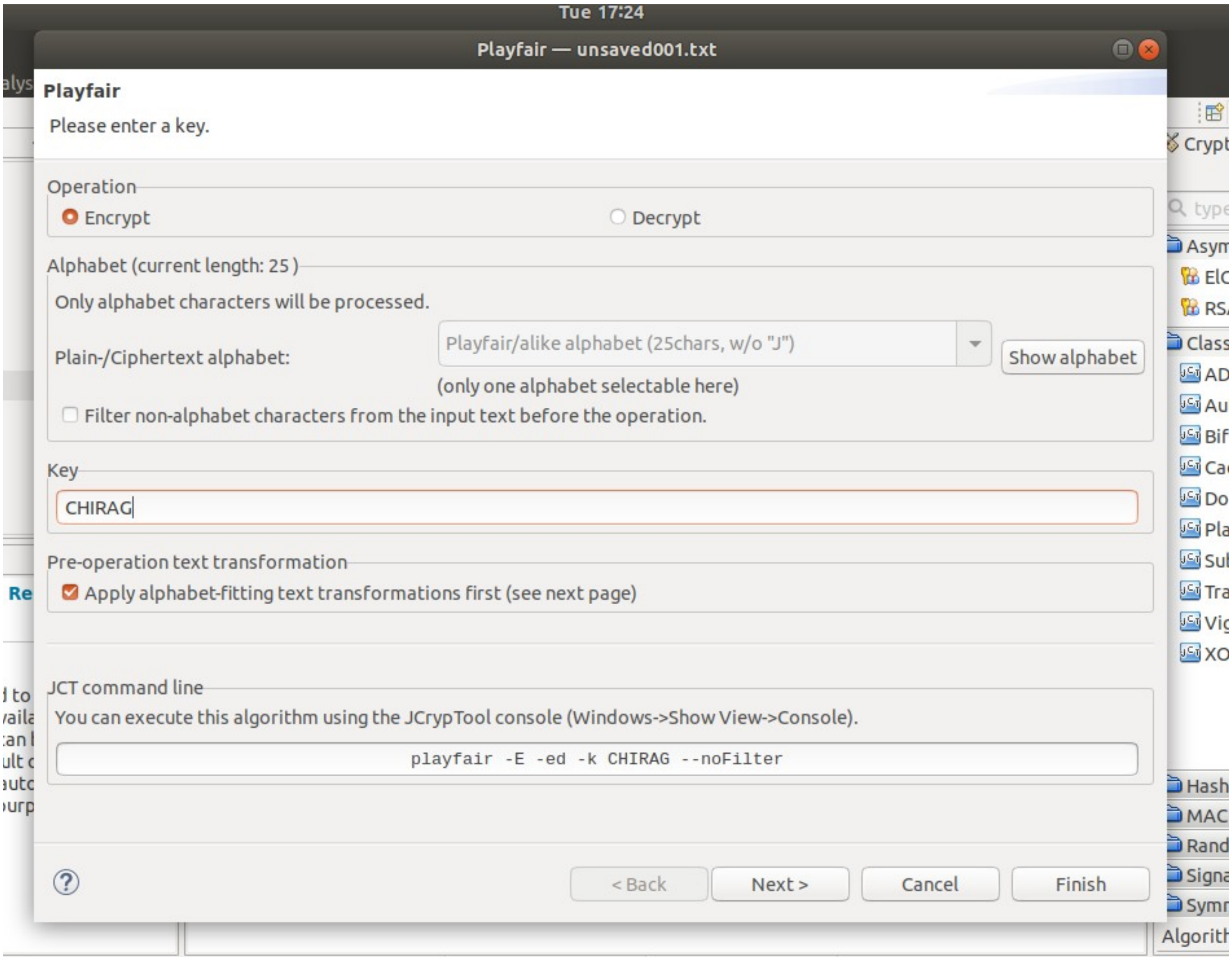


```
JLTCO CQYTU ETEYGGTOQU
```



```
HELLO WORLD ENCRYPTION
```

4) PlayFair



Playfair

Please enter a key.

Operation

● Encrypt ○ Decrypt

Alphabet (current length: 25)

Only alphabet characters will be processed.

Plain-/Ciphertext alphabet: Playfair/alike alphabet (25chars, w/o "J")

(only one alphabet selectable here)

□ Filter non-alphabet characters from the input text before the operation.

Key

CHIRAG

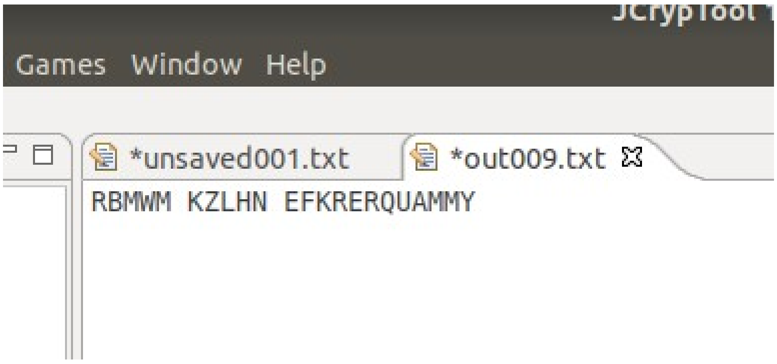
Pre-operation text transformation

☑ Apply alphabet-fitting text transformations first (see next page)

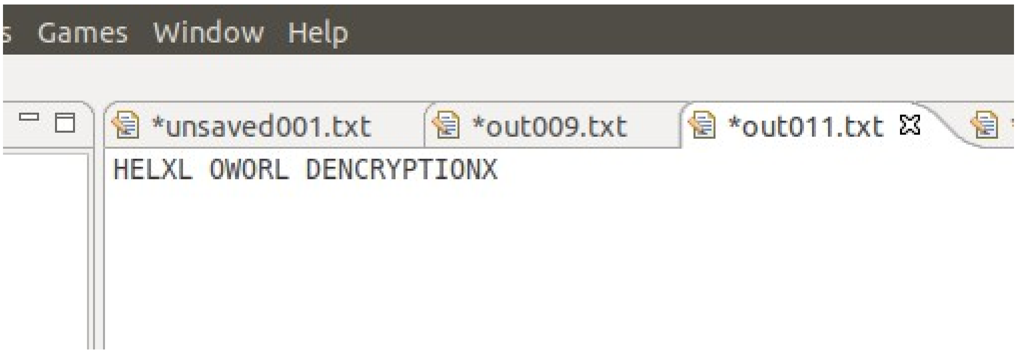
JCT command line

You can execute this algorithm using the JCrypTool console (Windows->Show View->Console).

```
playfair -E -ed -k CHIRAG --noFilter
```

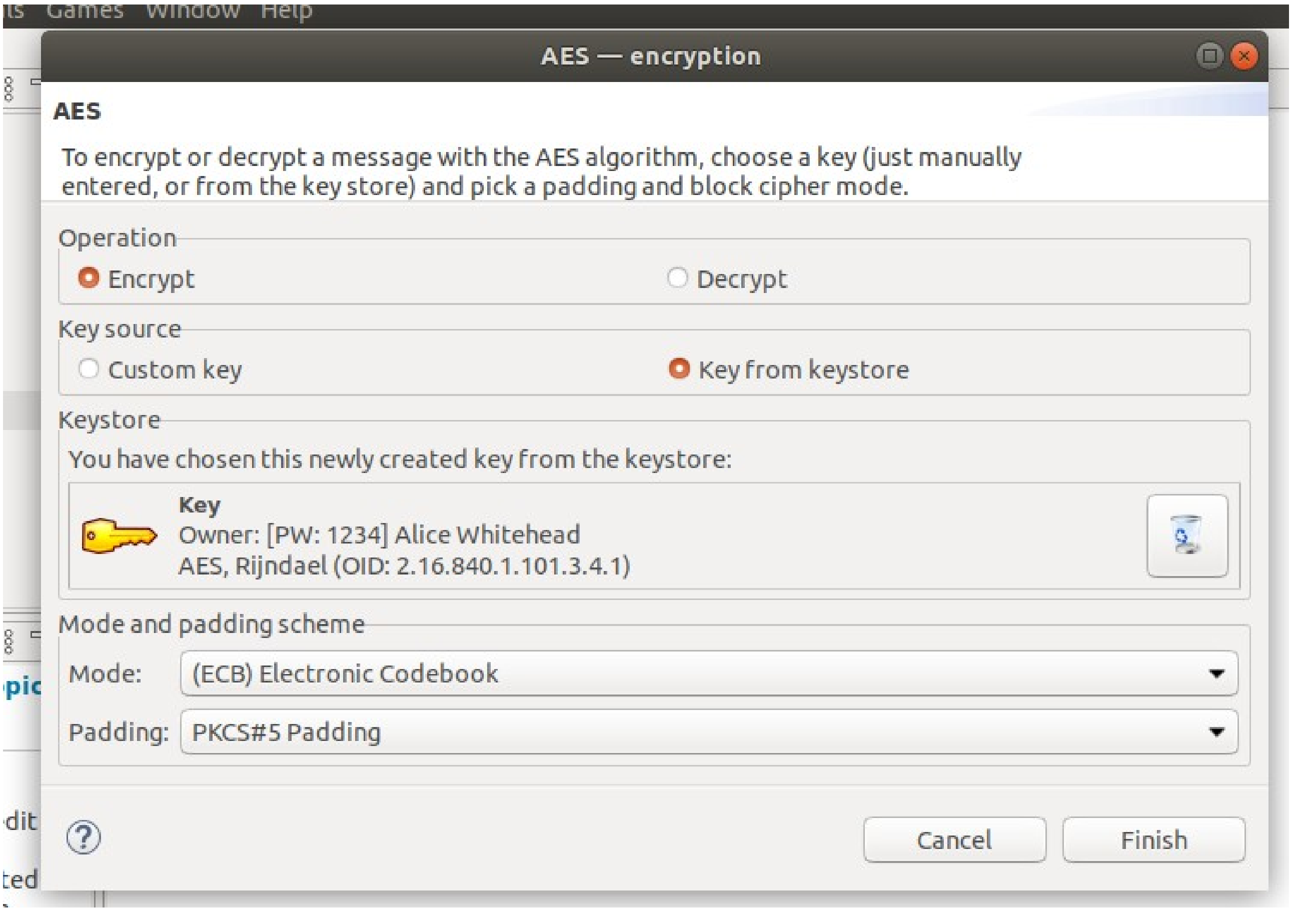


```
RBMWM KZLHN EFKRERQUAMMY
```



```
HELXL OWORL DENCRYPTIONX
```

5) AES



AES

To encrypt or decrypt a message with the AES algorithm, choose a key (just manually entered, or from the key store) and pick a padding and block cipher mode.

Operation

● Encrypt ○ Decrypt

Key source

○ Custom key ● Key from keystore

Keystore

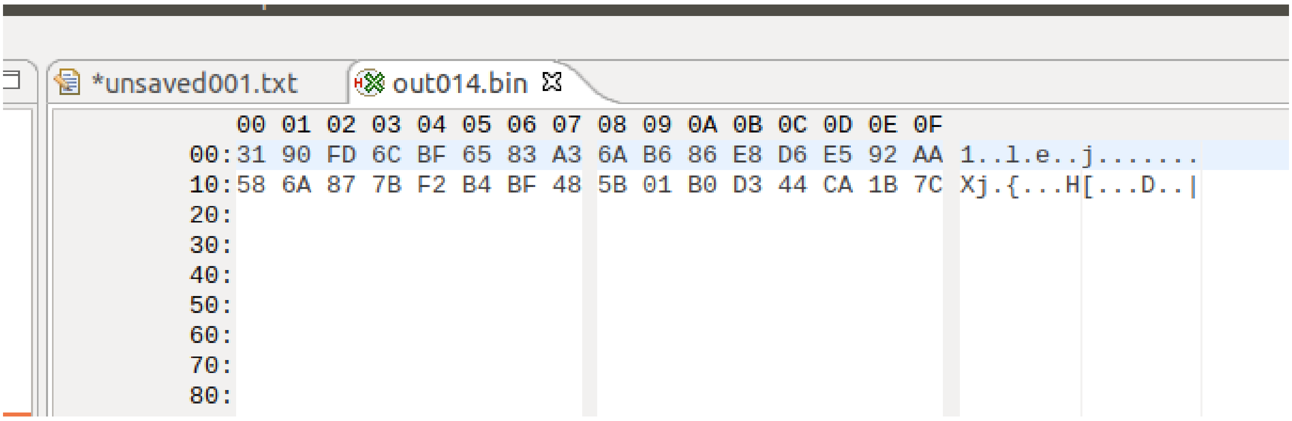
You have chosen this newly created key from the keystore:

Key
Owner: [PW: 1234] Alice Whitehead
AES, Rijndael (OID: 2.16.840.1.101.3.4.1)

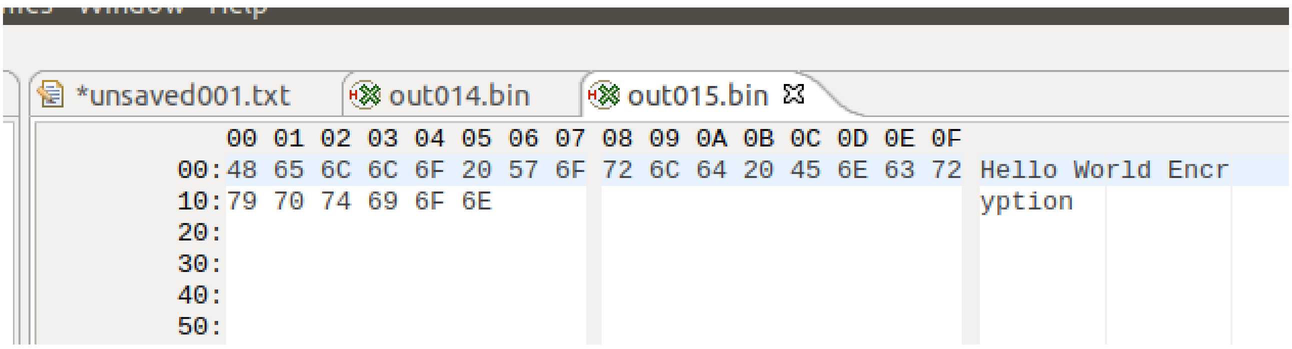
Mode and padding scheme

Mode: (ECB) Electronic Codebook

Padding: PKCS#5 Padding



```
     00 01 02 03 04 05 06 07 08 09 0A 0B 0C 0D 0E 0F
 00:31 90 FD 6C BF 65 83 A3 6A B6 86 E8 D6 E5 92 AA 1..l.e..j.......
 10:58 6A 87 7B F2 B4 BF 48 5B 01 B0 D3 44 CA 1B 7C Xj.{...H[...D..|
 20:
 30:
 40:
 50:
 60:
 70:
 80:
```



```
     00 01 02 03 04 05 06 07 08 09 0A 0B 0C 0D 0E 0F
 00:48 65 6C 6C 6F 20 57 6F 72 6C 64 20 45 6E 63 72 Hello World Encr
 10:79 70 74 69 6F 6E                               yption
 20:
 30:
 40:
 50:
```