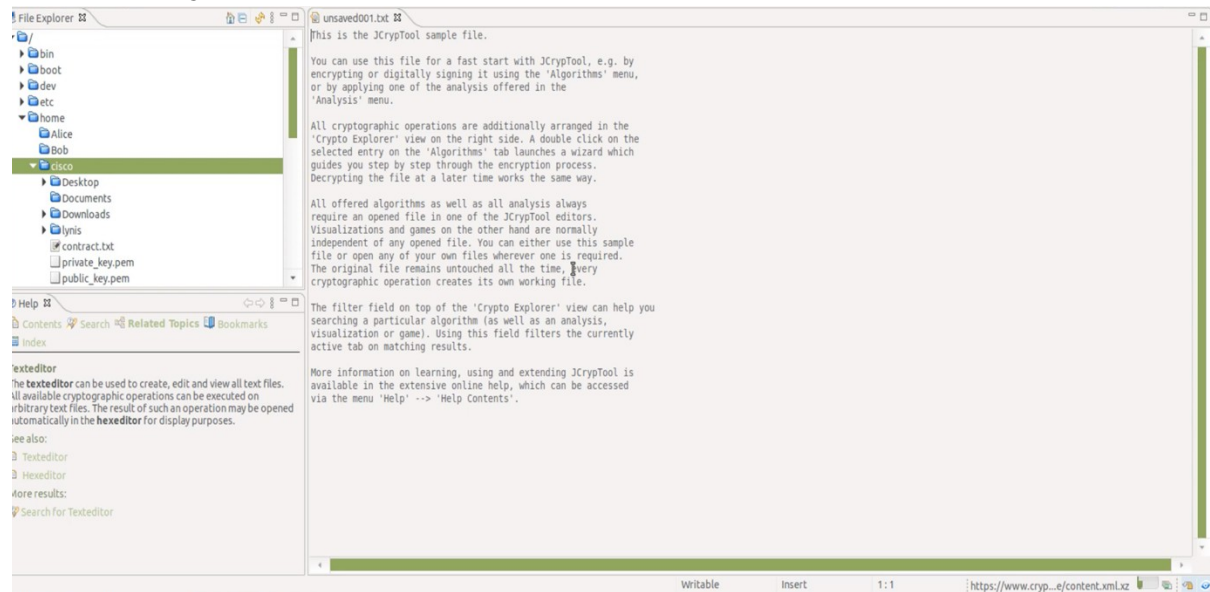


Completed by Gaaze Verena, 22B030332



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)
☐ Custom alphabet...

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

Key
Enter key using a character: K or the amount of shift along the alphabet: 10
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 K -a "Upper Latin (A-Z)" --noFilter`

? < Back Next > Cancel Finish

Algorithms Analysis Visuals Games

Caesar

Select an alphabet and enter a key.

Operation

☐ Encrypt

☒ Decrypt

Alphabet (current length: 26)

Only alphabet characters will be processed.

☒ Select alphabet:

Upper Latin (A-Z)

Show alphabet

Plain-/Ciphertext alphabet:

☐ Custom alphabet...

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

Key

Enter key using a character: K

or the amount of shift along the alphabet: 10

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 -D -ed -k K -a "Upper Latin (A-Z)" --noFilter
```



< Back

Next >

Cancel

Finish

*unsaved001.txt *out001.txt
MBIZDYQBKZRI SC PEX. MKX IYE BOKN DRSC COMBOD WOCCKQ0?

Crypto Explorer *out002.txt
CRYPTOGRAPHY IS FUN. CAN YOU READ THIS SECRET MESSAGE?

Writable

Insert

1:1

Caesar

Select an alphabet and enter a key.

Operation

☒ Encrypt

☐ Decrypt

Alphabet (current length: 52)

Only alphabet characters will be processed.

☒ Select alphabet:

Upper and lower Latin (A-Z,a-z)

Show alphabet

Plain-/Ciphertext alphabet:

☐ Custom alphabet...

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

Key

Enter key using a character: N

or the amount of shift along the alphabet: 1

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 N -a "Upper and lower Latin (A-Z,a-z)" --noFilter
```



< Back

Next >

Cancel

Finish

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

Custom key

Key length: 128

Key (hex): AA 00 00 00 00 00 00 00 00 00 00 00 00 00 00 FF

Mode and padding scheme

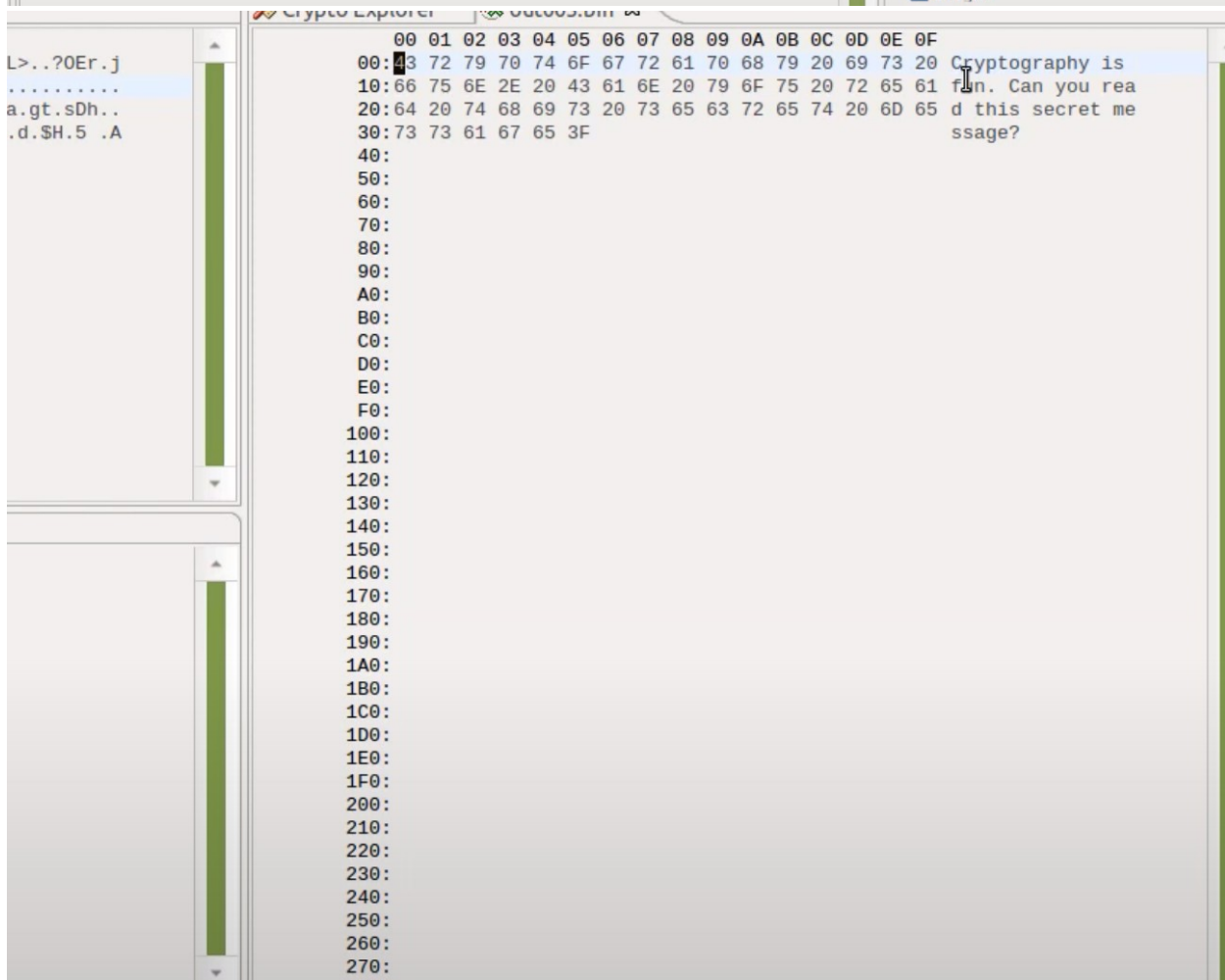
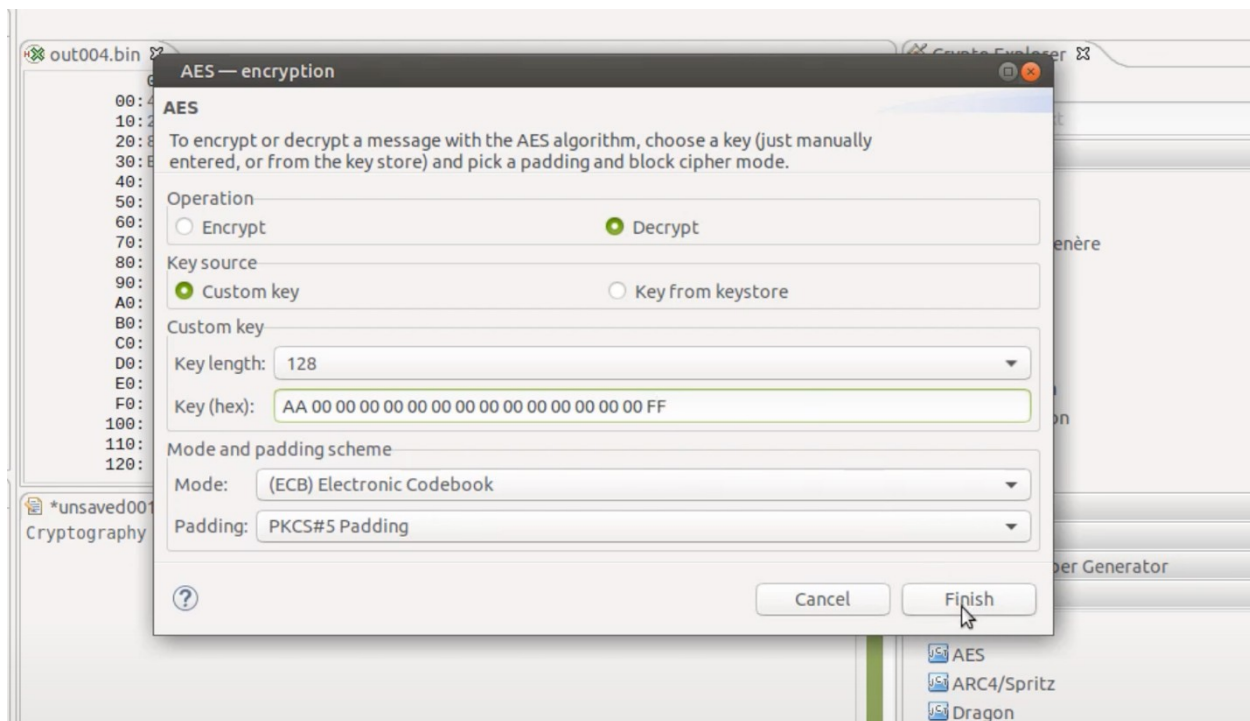
Mode: (ECB) Electronic Codebook


Padding: PKCS#5 Padding



Cancel

Finish



fun **New key pair** 

Enter the details for the new key pair

Contact details

Contact name

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

Algorithm and key length

Algorithm

☒ Standard key length

Key length

Password

Enter password

Confirm password

SA

to enc

ntere

opera

En

eysto

Sele

or:

enère

on

m Number Gene

Signature

Symmetric

AES

```

00 01 02 03 04 05 06 07 08 09 0A 0B 0C 0D 0E 0F
00: 1B 3B AD 14 8E D6 6E 95 8B 82 E3 DB 6B 9D 50 67 .;...n....k.Pg
10: 10 C8 88 5F 66 D2 02 1B 90 D1 DD E0 D8 13 1B B2 ..._f.....
20: B6 9D E8 6D B4 81 04 57 5E 0B B3 8F 23 23 66 82 ...m...W^...##f.
30: 38 1E 10 9A 57 2E 86 25 7C 8E 6A 1F B2 A2 38 25 8...W...%|.j...8%
40: E7 2B BE 37 D2 5C AF C9 52 05 43 68 41 34 DD E6 .+.7.\...R.ChA4..
50: FB 14 98 8A A6 CE 69 11 55 A6 13 40 BF D6 37 0F .....i.U..@..7.
60: B3 20 5C A6 88 1E DB 76 AA F7 29 9C 4D BA CC 72 . \....v..).M..r
70: 15 77 75 A0 F7 E1 65 72 88 BB 4E 13 98 DD 2F 60 .wu...er..N.../`
80:
90:
A0:
B0:
C0:
D0:
E0:
F0:
100:
110:
120:
130:
140:
150:
160:
170:
180:
190:
1A0:
1B0:
1C0:
1D0:
1E0:
1F0:
200:
210:
220:
230:
240:
250:
260:

```

