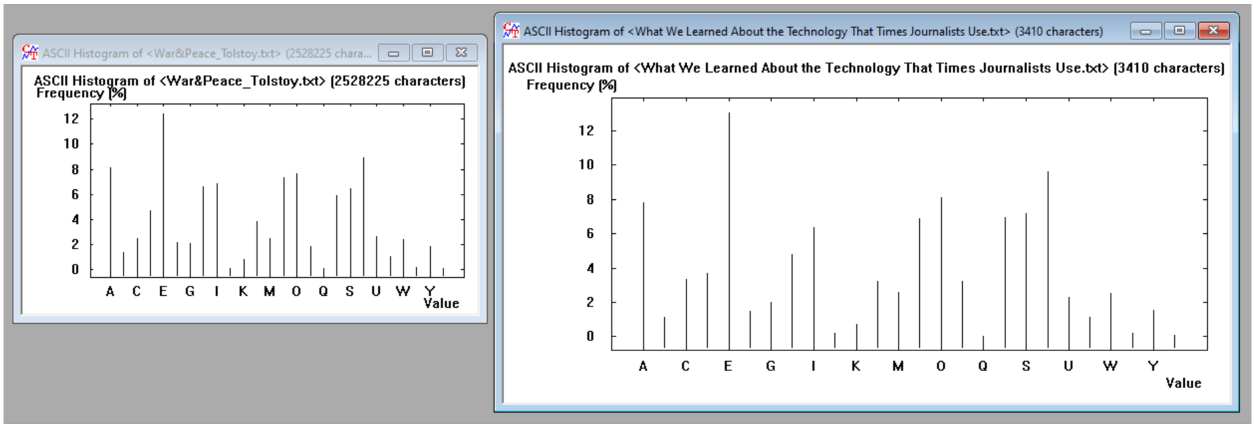
Homework 5 – Cryptography

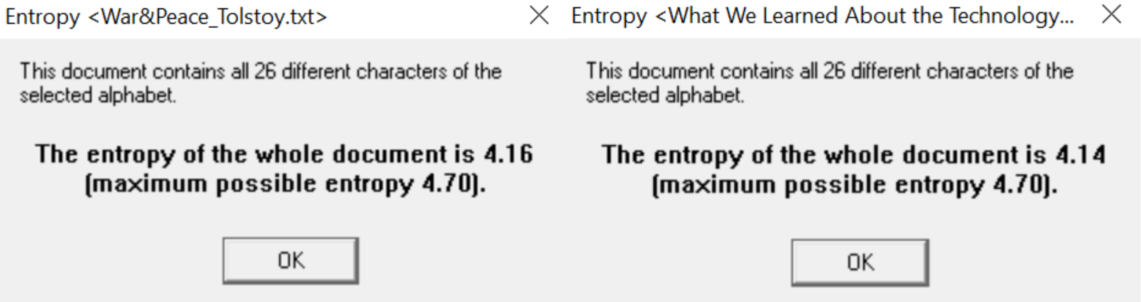
- This is an individual assignment, and is worth 20 points.
- The due date is Wednesday, October 7 midnight.
- You need to provide your answers using the Outcome file.
- Follow the usual naming convention.
- Do not make screenshots too small.

Task 1 (4 points)

- (1.5 points) Create a histogram for each text that display the relative frequency of letters in a graphical form. For this, go to Analysis > Tools for Analysis. Provide the two histograms in screenshots.


ASCII Histogram of <War&Peace_Tolstoy.txt> (2528225 chara...
ASCII Histogram of <War&Peace_Tolstoy.txt> (2528225 characters)
Frequency (%)
12
10
8
6
4
2
0
A C E G I K M O Q S U W Y
Value
ASCII Histogram of <What We Learned About the Technology That Times Journalists Use.txt> (3410 characters)
ASCII Histogram of <What We Learned About the Technology That Times Journalists Use.txt> (3410 characters)
Frequency (%)
12
10
8
6
4
2
0
A C E G I K M O Q S U W Y
Value

- (1.5 points) Do the two histograms depend significantly on the texts you have provided?
  - No, the English language has a letter frequency which is simply the amount of times letters of the alphabet appear on average in written language. The histograms look nearly identical despite being on different subjects and one being much longer in length.
- (1 point) Calculate the entropy of each text. For this, Analysis > Tools for Analysis > Entropy. What would you conclude from the comparison of the entropies?


Entropy <War&Peace_Tolstoy.txt>
OK
Entropy <What We Learned About the Technology...
OK

This document contains all 26 different characters of the selected alphabet.

The entropy of the whole document is 4.16 (maximum possible entropy 4.70).

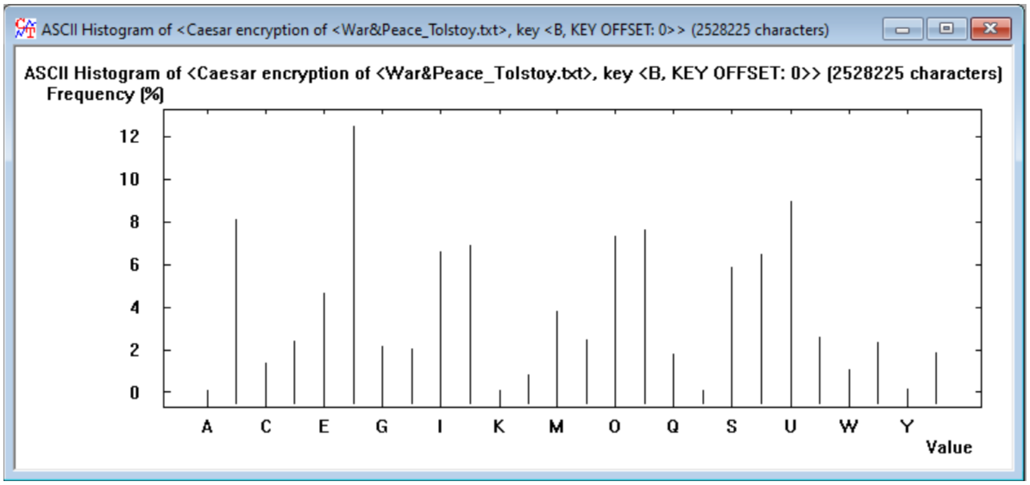
This document contains all 26 different characters of the selected alphabet.

The entropy of the whole document is 4.14 (maximum possible entropy 4.70).

  - The chosen texts are 0.2 points apart. War & Peace is longer and has a higher entropy, this means it is harder to convert into bits. It's interesting because it is considerably longer, but not far off from the NYT article.

Task 2 (4 points)

- (2 points) What are the characteristic features of the obtained distribution compared with the original text? Provide a screenshot to support your answer.

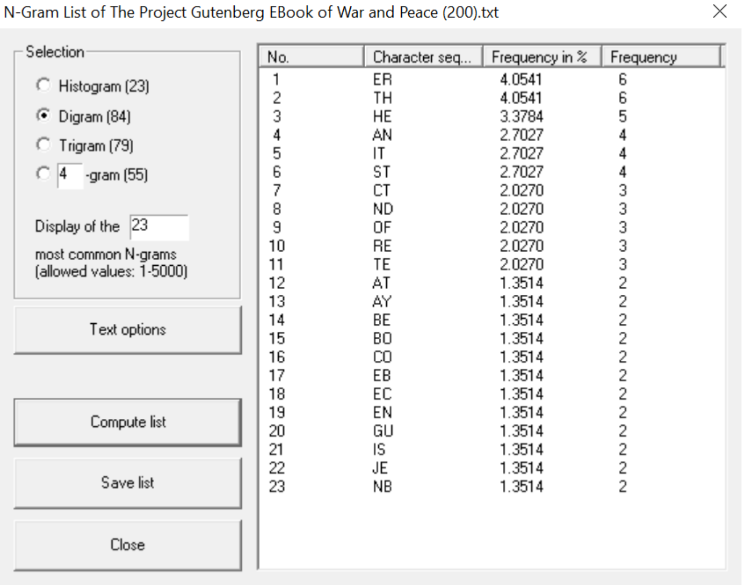


  - Everything shifted over one place to the right because I selected B as the key entry. This explains everything moving over by one since one was the number value of the shift.

- (2 points) How would you apply the features you have discovered in cracking the key?
  - Visually you can see that the frequencies have shifted, cracking a simple encryption attempt like this wouldn't be too difficult with the assistance of both histograms. Without both, this tool does not provide much help.

Task 3 (4 points)

- (1.5 points for War&Peace_Tolstoy.txt) Summarize your observation of the frequency distribution. Also, provide a screenshot of the frequency distribution.



N-Gram List of The Project Gutenberg EBook of War and Peace (200).txt

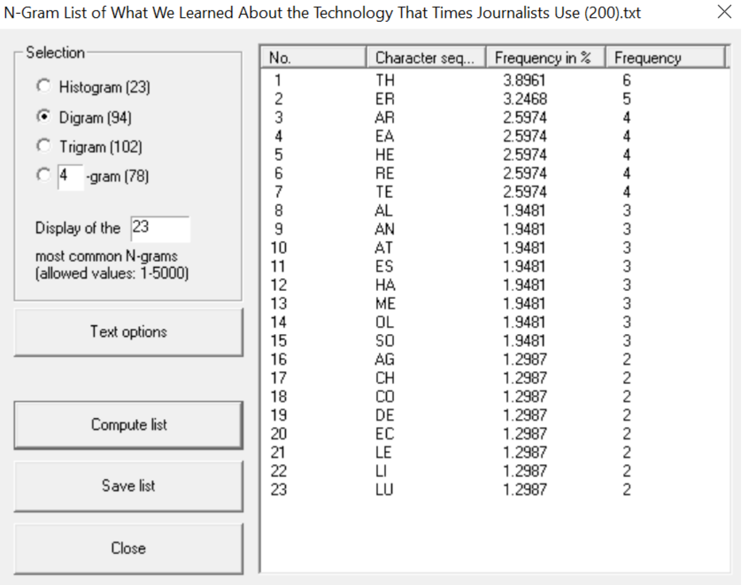
Selection
○ Histogram (23)
● Digram (84)
○ Trigram (79)
○ 4 -gram (55)

Display of the 23 most common N-grams (allowed values: 1-5000)

No.	Character seq...	Frequency in %	Frequency
1	ER	4.0541	6
2	TH	4.0541	6
3	HE	3.3784	5
4	AN	2.7027	4
5	IT	2.7027	4
6	ST	2.7027	4
7	CT	2.0270	3
8	ND	2.0270	3
9	OF	2.0270	3
10	RE	2.0270	3
11	TE	2.0270	3
12	AT	1.3514	2
13	AY	1.3514	2
14	BE	1.3514	2
15	BO	1.3514	2
16	CO	1.3514	2
17	EB	1.3514	2
18	EC	1.3514	2
19	EN	1.3514	2
20	GU	1.3514	2
21	IS	1.3514	2
22	JE	1.3514	2
23	NB	1.3514	2

-
  - I'm surprised ER has the greatest frequency, I thought it would be SE.

- (1.5 points for a NYT article) Summarize your observation of the frequency distribution. Also, provide a screenshot of the frequency distribution.



N-Gram List of What We Learned About the Technology That Times Journalists Use (200).txt

Selection

○ Histogram (23)
● Digram (94)
○ Trigram (102)
○ 4 -gram (78)

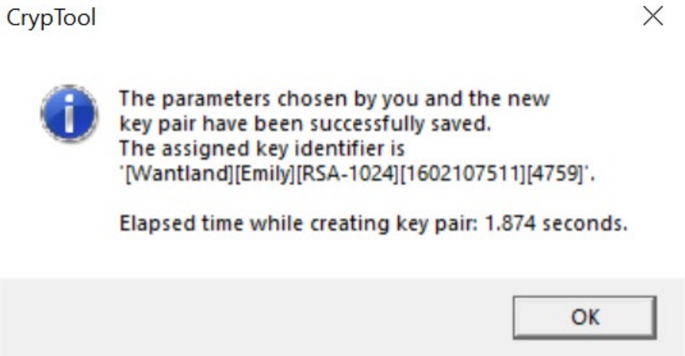
Display of the 23 most common N-grams (allowed values: 1-5000)

No.	Character seq...	Frequency in %	Frequency
1	TH	3.8961	6
2	ER	3.2468	5
3	AR	2.5974	4
4	EA	2.5974	4
5	HE	2.5974	4
6	RE	2.5974	4
7	TE	2.5974	4
8	AL	1.9481	3
9	AN	1.9481	3
10	AT	1.9481	3
11	ES	1.9481	3
12	HA	1.9481	3
13	ME	1.9481	3
14	OL	1.9481	3
15	SO	1.9481	3
16	AG	1.2987	2
17	CH	1.2987	2
18	CO	1.2987	2
19	DE	1.2987	2
20	EC	1.2987	2
21	LE	1.2987	2
22	LI	1.2987	2
23	LU	1.2987	2

  - TH makes sense to me, "the" is an extremely common word so it being the most frequent is understandable.
- (1 point) Compare and contrast the two frequency distributions.
  - These are similar to the histograms, in the top five "ER", "TH", and "HE" appear in both. The letter combinations present are the letters that appear to have higher columns in the histograms. Even though both texts are very different, they still have similar character sequences, though the frequency differs.

Task 4 (4 points)

- (2 points) Attach a screen shot that shows the successful creation of the key pair.

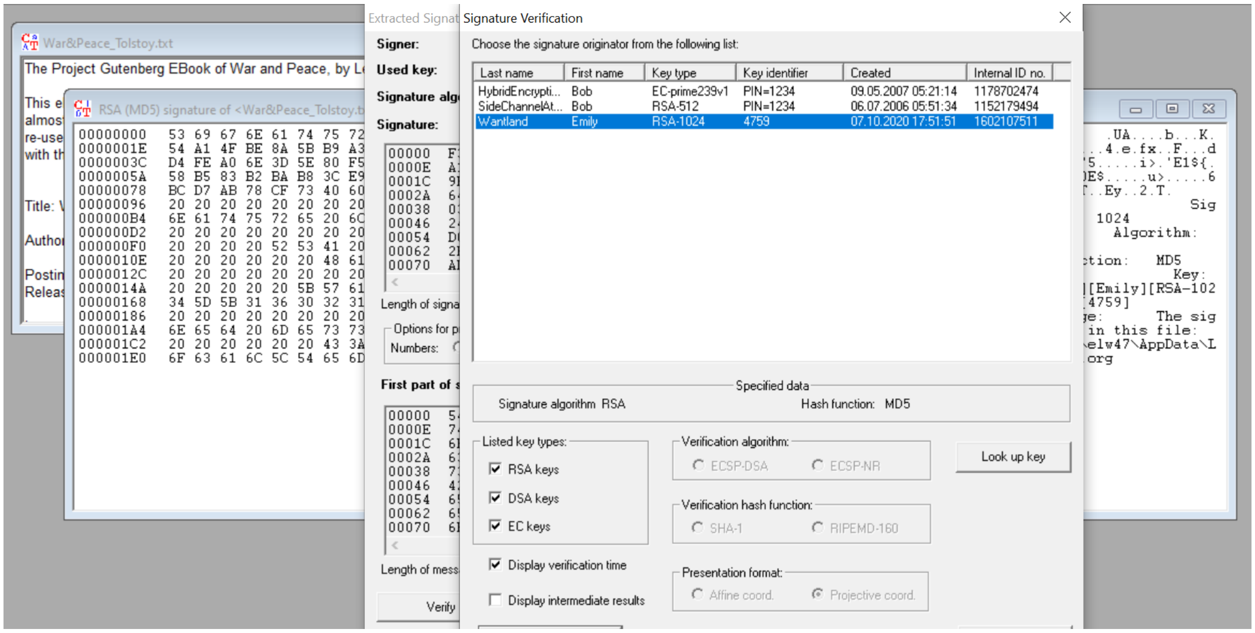


CrypTool

The parameters chosen by you and the new key pair have been successfully saved.
The assigned key identifier is '[Wantland][Emily][RSA-1024][1602107511][4759]'.

Elapsed time while creating key pair: 1.874 seconds.

-
- (2 points) Attach a screenshot that displays the signature verification.



War&Peace_Tolstoy.txt

The Project Gutenberg EBook of War and Peace, by L

RSA (MD5) signature of <War&Peace_Tolstoy.t

```
00000000   53 69 67 6E 61 74 75 72
0000001E   54 A1 4F BE 8A 5B B9 A3
0000003C   D4 FE A0 6E 3D 5E 80 F5
0000005A   58 B5 83 B2 BA B8 3C E9
00000078   BC D7 AB 78 CF 73 40 60
00000096   20 20 20 20 20 20 20 20
000000B4   6E 61 74 75 72 65 20 6C
000000D2   20 20 20 20 20 20 20 20
000000F0   20 20 20 20 52 53 41 20
0000010E   20 20 20 20 20 20 48 61
0000012C   20 20 20 20 20 20 20 20
0000014A   20 20 20 20 20 5B 57 61
00000168   34 5D 5B 31 36 30 32 31
00000186   20 20 20 20 20 20 20 20
000001A4   6E 65 64 20 6D 65 73 73
000001C2   20 20 20 20 20 20 43 3A
000001E0   6F 63 61 6C 5C 54 65 6D
```

Signature Verification

Choose the signature originator from the following list:

Last name	First name	Key type	Key identifier	Created	Internal ID no.
HybridEncrypti...	Bob	EC-prime239v1	PIN=1234	09.05.2007 05:21:14	1178702474
SideChannelAt...	Bob	RSA-512	PIN=1234	06.07.2006 05:51:34	1152179494
Wantland	Emily	RSA-1024	4759	07.10.2020 17:51:51	1602107511

Specified data

Signature algorithm RSA   Hash function: MD5

Listed key types:
☑ RSA keys
☑ DSA keys
☑ EC keys

☑ Display verification time
□ Display intermediate results

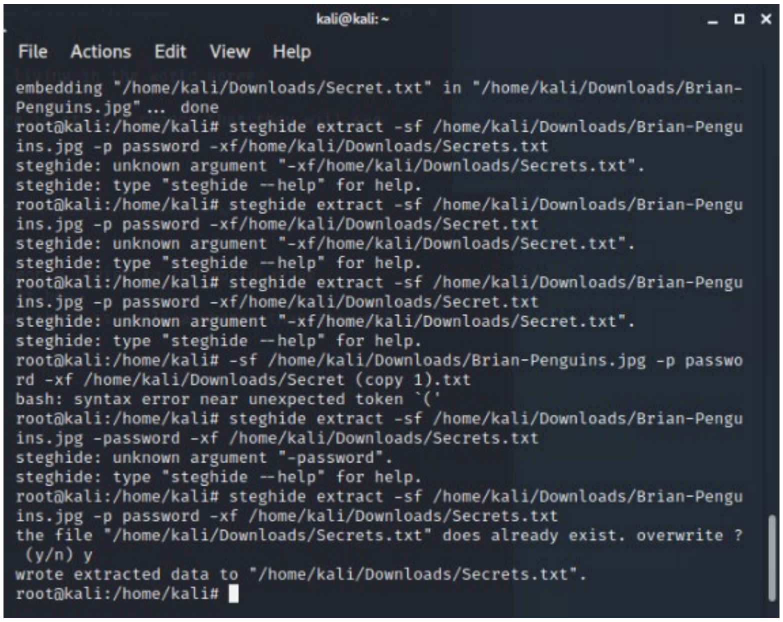
Verification algorithm: ○ ECSP-DSA ○ ECSP-NR

Verification hash function: ○ SHA-1 ○ RIPEMD-160

Presentation format: ○ Affine coord. ● Projective coord.

Task 5 (4 points)

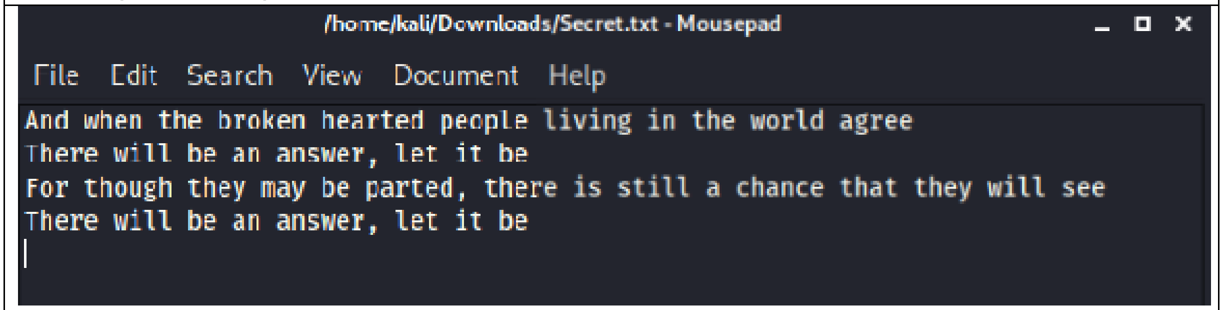
- (2 points) Follow the steps in the video and show the recovered secret text file as below.



```
embedding "/home/kali/Downloads/Secret.txt" in "/home/kali/Downloads/Brian-
Penguins.jpg"... done
root@kali:/home/kali# steghide extract -sf /home/kali/Downloads/Brian-Pengu
ins.jpg -p password -xf/home/kali/Downloads/Secrets.txt
steghide: unknown argument "-xf/home/kali/Downloads/Secrets.txt".
steghide: type "steghide --help" for help.
root@kali:/home/kali# steghide extract -sf /home/kali/Downloads/Brian-Pengu
ins.jpg -p password -xf/home/kali/Downloads/Secret.txt
steghide: unknown argument "-xf/home/kali/Downloads/Secret.txt".
steghide: type "steghide --help" for help.
root@kali:/home/kali# steghide extract -sf /home/kali/Downloads/Brian-Pengu
ins.jpg -p password -xf/home/kali/Downloads/Secret.txt
steghide: unknown argument "-xf/home/kali/Downloads/Secret.txt".
steghide: type "steghide --help" for help.
root@kali:/home/kali# -sf /home/kali/Downloads/Brian-Penguins.jpg -p passwo
rd -xf /home/kali/Downloads/Secret (copy 1).txt
bash: syntax error near unexpected token `('
root@kali:/home/kali# steghide extract -sf /home/kali/Downloads/Brian-Pengu
ins.jpg -password -xf /home/kali/Downloads/Secrets.txt
steghide: unknown argument "-password".
steghide: type "steghide --help" for help.
root@kali:/home/kali# steghide extract -sf /home/kali/Downloads/Brian-Pengu
ins.jpg -p password -xf /home/kali/Downloads/Secrets.txt
the file "/home/kali/Downloads/Secrets.txt" does already exist. overwrite ?
 (y/n) y
wrote extracted data to "/home/kali/Downloads/Secrets.txt".
root@kali:/home/kali# █
```

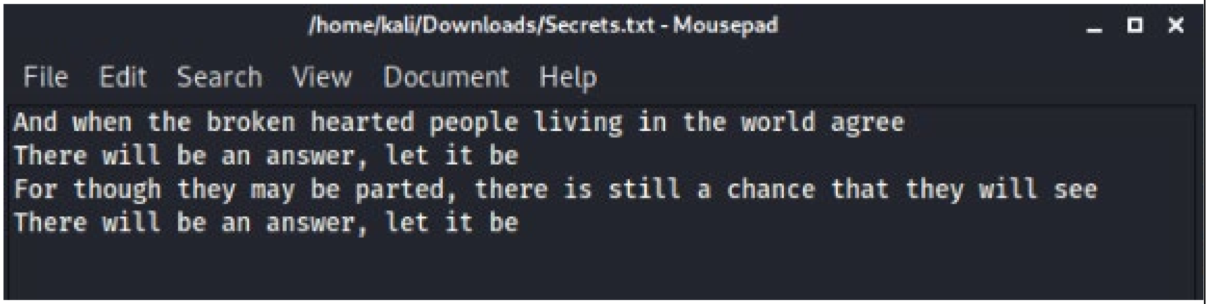
- (2 points) Show in screenshots that the contents of the two files are the same.

The image of the original file


/home/kali/Downloads/Secret.txt - Mousepad
File Edit Search View Document Help

```
And when the broken hearted people living in the world agree
There will be an answer, let it be
For though they may be parted, there is still a chance that they will see
There will be an answer, let it be
```

The image of the recovered file


/home/kali/Downloads/Secrets.txt - Mousepad
File Edit Search View Document Help

```
And when the broken hearted people living in the world agree
There will be an answer, let it be
For though they may be parted, there is still a chance that they will see
There will be an answer, let it be
```