- Konstantinos Filippou
- Ics23044

Exercise 1

What is the difference between the processes of encryption / decryption and the processes of encoding / decoding? Develop your answer with the help of text and your own appropriate diagrams.

Solution

Encryption / Decryption

Data transformation

Goal: Protection of security & confidentiality of data

Transformation of data into an **unreadable format** (ciphertext), so that only someone with the correct **key** can read it.

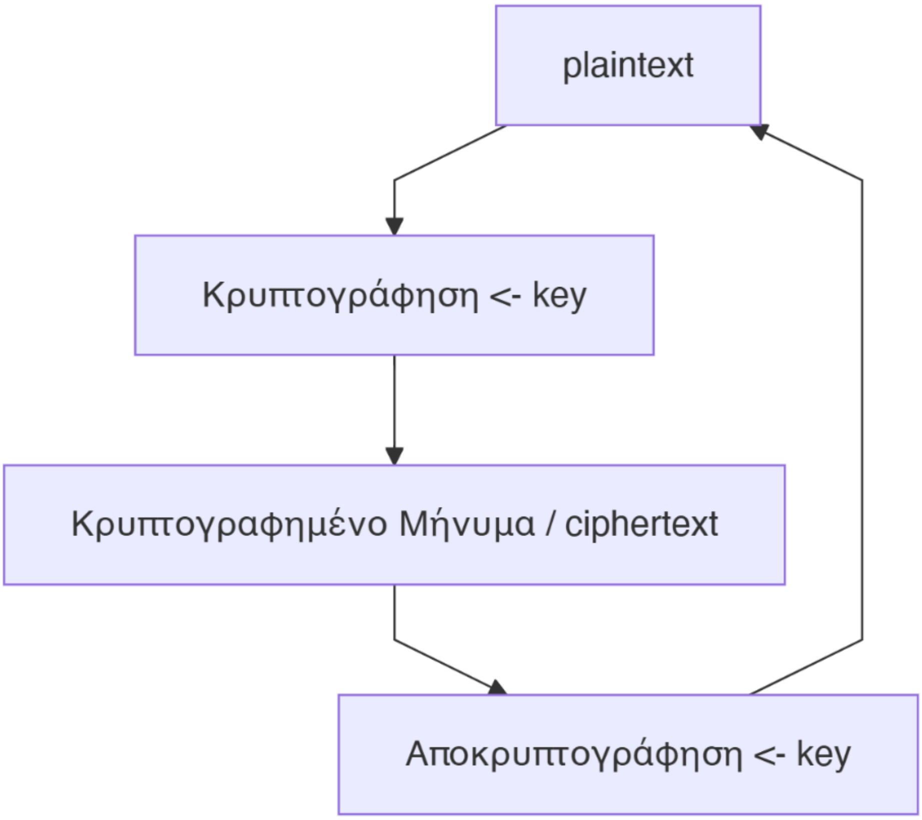
Primarily: confidentiality / integrity / non-repudiation

That is: It is the process of **converting** a text (plaintext) into an **unreadable form** (ciphertext) in order to protect the confidentiality of information.

Decryption: The reverse decoding process (decryption).

It is the act by which data becomes known again to the authorized user.

Thus, the sender = **encrypts** and the receiver = **decrypts**



Encoding / Decoding

Data transformation

Goal: Ensuring **integrity** and correct **transmission** of data (not security).

Transformation of data into a form that can be stored or transmitted more easily across systems.

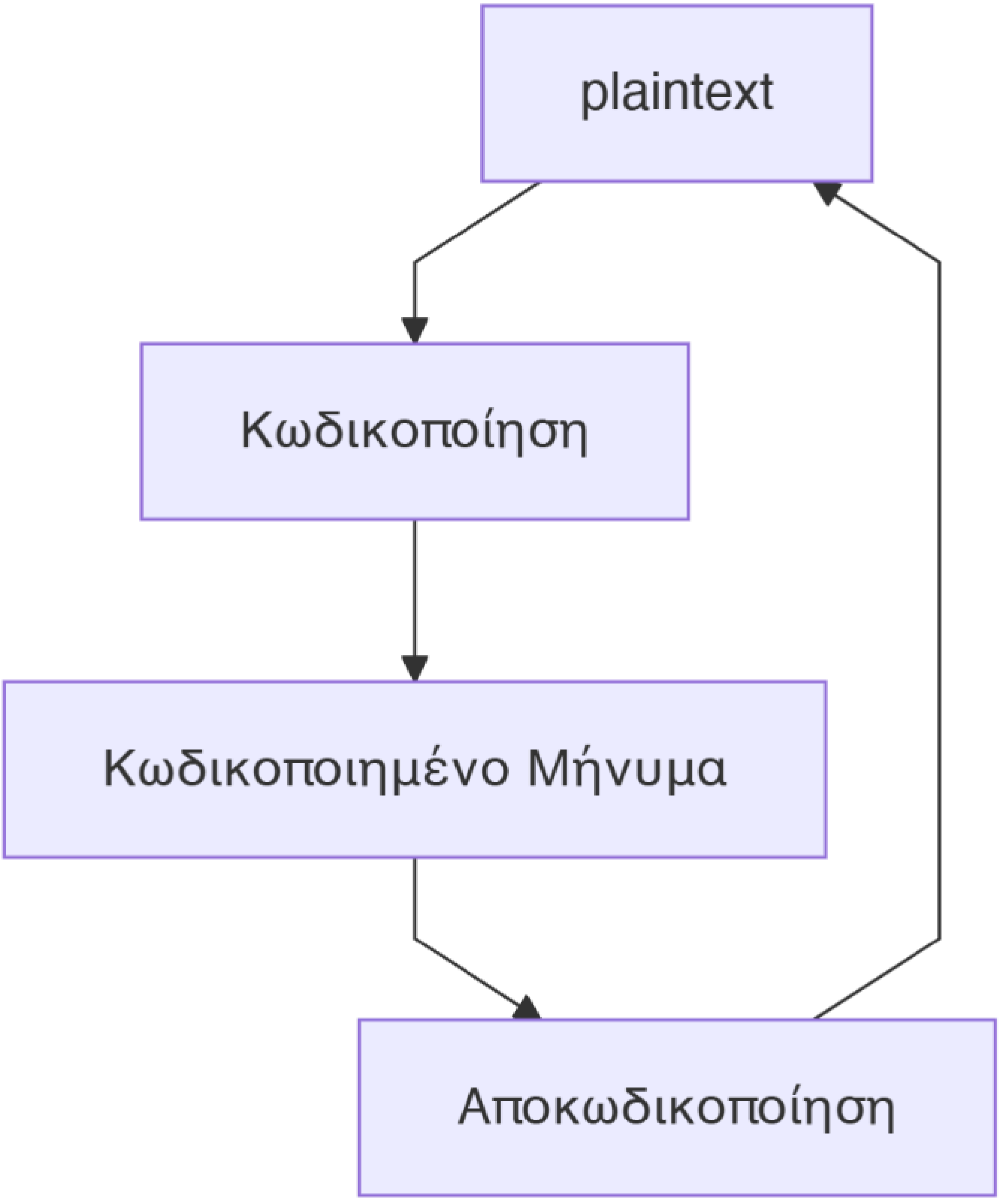
Example: ASCII, Base64, Unicode

There is no security beyond integrity and correct transmission.

Therefore, security is **technical**.

Without security

Readable in another form



Conclusion

Encryption protects information from unauthorized access,
whereas **encoding** simply changes the form of information so that it can be stored and transferred more easily.

Finally, both are used for data transfer, but they have different purposes and operating mechanisms.

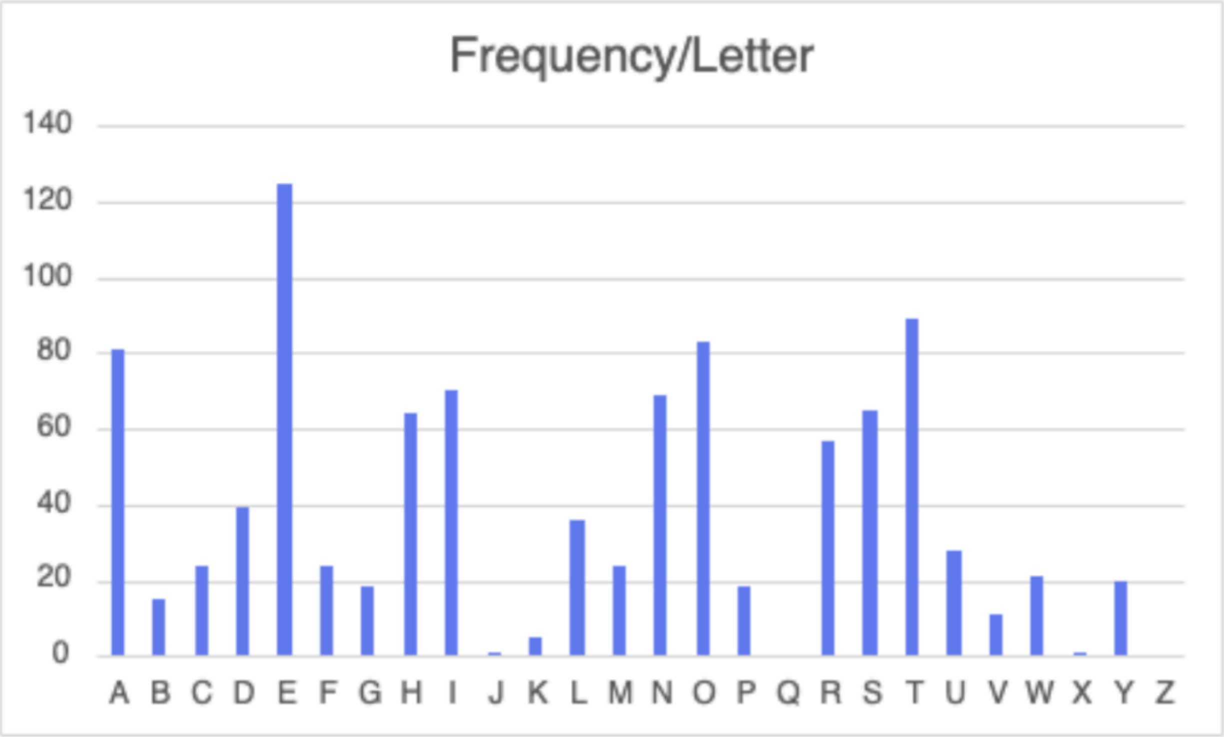
Exercise 2

Visit the website https://www.gutenberg.org/ and download any book of your choice as a text file (.txt). Then, using the code presented above, calculate the frequencies of the letters contained in the entire book and display them in an Excel graph. What are your observations considering the given frequency graph that concerns the book *"The Room with the Little Door"*?

Solution

I visited the website and chose Plato’s *“Symposium”* and saved it as Plain Text UTF-8.

Below we see the letter frequencies:



We observe that the letter frequencies are the same as the frequencies we discussed in the lab (E the most frequent letter, Z and Q the least frequent, etc.).

Exercise 3

The following ciphertext has been encrypted using a shift cipher algorithm.
Cryptanalyze it and find the original text, presenting your method.
What is the minimum number of letters that must be recognized in order to recover the encryption key?
How would you interpret the statement of this message?
Note: do not use a brute-force attack.

QTCDE ESP DPYEPYNP LYO ESPY ESP PGTOPYNP

Solution

I used the Caesar Cipher algorithm from the lab and as input I entered the given message, and as output it produced the following:

(shift table omitted for brevity — solution found at shift 11)

```
0 QTCDEESPDPYEPYNPLYOESPYESPPGTOPYNP
1 PSBCDDROCOXDOXMOKXNDROXDROOFSNOXMO
2 ORABCCQNBNWCNWLNJWMCQNWCQNNERMNWLN
3 NQZABBPMAMVBMVKMIVLBPMVBPMMDQLMVKM
4 MPYZAAOLZLUALUJLHUKAOLUAOLLCPKLUJL
5 LOXYZZNKYKTZKTIKGTJZNKTZNKKBOJKTIK
6 KNWXYYMJXJSYJSHJFSIYMJSYMJJANIJSHJ
7 JMVWXXLIWIRXIRGIERHXLIRXLIIZMHIRGI
8 ILUVWWKHVHQWHQFHDQGWKHQWKHHYLGHQFH
9 HKTUVVJGUGPVGPEGCPFVJGPVJGGXKFGPEG
10 GJSTUUIFTFOUFODFBOEUIFOUIFFWJEFODF
11 FIRSTTHESENTENCEANDTHENTHEEVIDENCE
12 EHQRSSGDRDMSDMBDZMCSGDMSGDDUHCDMBD
13 DGPQRRFCQCLRCLACYLBRFCLRFCCTGBCLAC
14 CFOPQQEBPBKQBKZBXKAQEBKQEBBSFABKZB
15 BENOPPDAOAJPAJYAWJZPDAJPDAAREZAJYA
16 ADMNOOCZNZIOZIXZVIYOCZIOCZZQDYZIXZ
17 ZCLMNNBYMYHNYHWYUHXNBYHNBYYPCXYHWY
18 YBKLMMAXLXGMXGVXTGWMAXGMAXXOBWXGVX
19 XAJKLLZWKWFLWFUWSFVLZWFLZWWNAVWFUW
20 WZIJKKYVJVEKVETVREUKYVEKYVVMZUVETV
21 VYHIJJXUIUDJUDSUQDTJXUDJXUULYTUDSU
22 UXGHIIWTHTCITCRTPCSIWTCIWTTKXSTCRT
23 TWFGHHVSGSBHSBQSOBRHVSBHVSSJWRSBQS
24 SVEFGGURFRAGRAPRNAQGURAGURRIVQRAPR
25 RUDEFFTQEQZFQZOQMZPFTQZFTQQHUPQZOQ
```

We see that the solution is on line 11 and the ciphertext corresponds to the phrase:

“FIRST THE SENTENCE AND THEN THE EVIDENCE”

The minimum number of letters is six, because although the first word is FIRST (5 letters), we observe that in the last line another first word (RUDE) appears, and in order to understand that this was just a coincidence we need to see that in the 5th and 6th letters there are two consonants together. In combination with finding the word FIRST, we conclude that from the 6th letter we are certain that line 11 is the correct line with the rest of the phrase.

The message reminds me of two things:
our exercise where I literally state the sentence first and then the method of finding (evidence), as well as the opposite of what is applied in law and in a trial (that is, first the evidence and then the sentence/verdict).

Exercise 4

The following ciphertext has been encrypted using a substitution cipher algorithm.
Cryptanalyze it, presenting your method.

ZFFD BXWE QEUFCPY TIXYF JWA BXWE FCFSUFY TIXYFE

Solution

At first I tried using Frequency Analysis to see if I could find any similarity; however, only E was a fairly likely pair since in the original message the letter F appears most frequently (8 times). However, the remaining letters appeared a similar number of times, and combined with the fact that we have a short ciphertext, it is difficult to find the correspondence in this way.

However, a very simple method is to use an online Mono-Alphabetic Cipher tool, from which the phrase emerges:

“KEEP YOUR FRIENDS CLOSE BUT YOUR ENEMIES CLOSER”