

- Konstantinos Filippou
- Ics23044

Exercise 1

Ποια η διαφορά των διαδικασιών κρυπτογράφησης (encryption) / αποκρυπτογράφησης (decryption) από τις διαδικασίες κωδικοποίησης (encoding) / αποκωδικοποίησης (decoding)? Αναπτύξτε την απάντησή σας με τη βοήθεια κειμένου και δικών σας κατάλληλων σχημάτων.

Solution

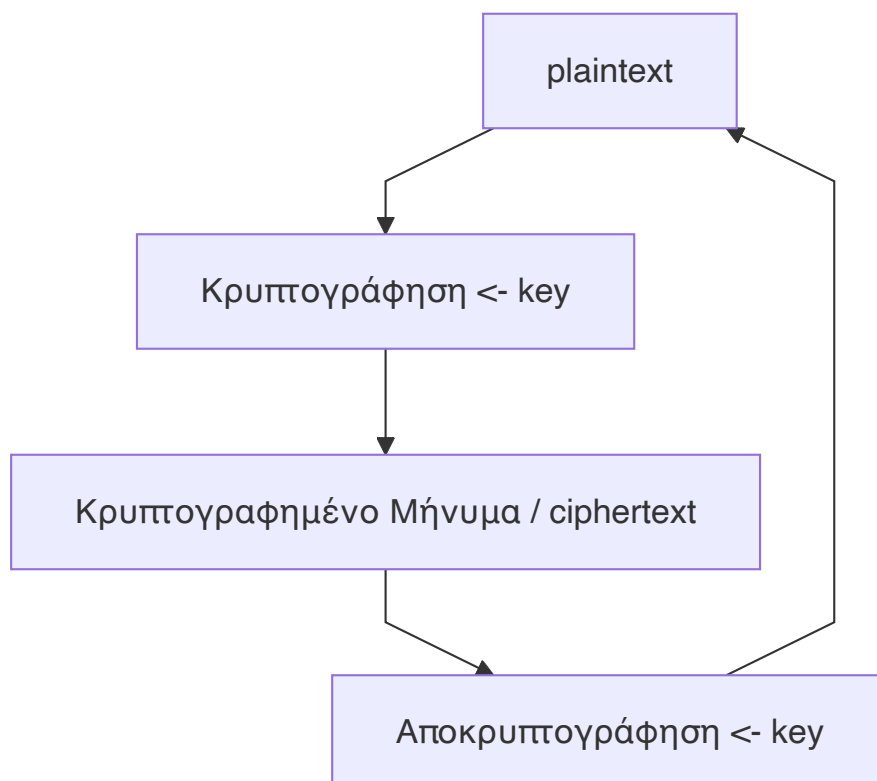
Κρυπτογράφηση / Αποκρυπτογράφηση.

Μετατροπή δεδομένων

Στόχος: Προστασία ασφάλειας & απορρήτου των δεδομένων

Μετατροπή των δεδομένων σε ένα **μη αναγνώσιμο format** (ciphertext), έτσι ώστε μόνο κάποιος με το σωστό **κλειδί** να μπορεί να τα διαβάσει.

- **Αρχικά:** εμπιστευτικότητα / ακεραιότητα / μη άρνηση
- Δηλαδή: Είναι η διαδικασία **κωδικοποίησης** ενός κειμένου (plaintext) σε **μη αναγνώσιμη μορφή** (ciphertext) έτσι ώστε να προστατευτεί η εμπιστευτικότητα των πληροφοριών.
- Αποκρυπτογράφηση: Αντίστροφη διαδικασία αποκωδικοποίησης (decryption). Είναι η πράξη με την οποία τα δεδομένα ξαναγίνονται γνωστά στον εξουσιοδοτημένο χρήστη. Έτσι, ο αποστολέας = **κρυπτογραφεί** και ο λήπτης = **αποκρυπτογραφεί**.



Κωδικοποίηση / Αποκωδικοποίηση

Μετατροπή δεδομένων

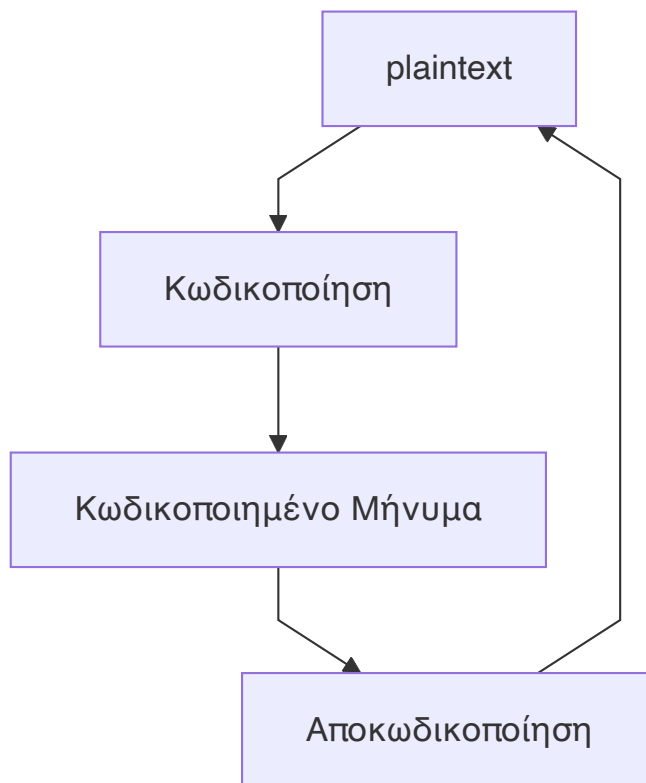
Στόχος: Διασφάλιση **ακεραιότητας** και σωστής **μετάδοσης** των δεδομένων (όχι ασφάλειας).

Μετατροπή των δεδομένων σε μια μορφή που μπορεί να αποθηκευτεί ή να μεταδοθεί πιο εύκολα σε όλα τα συστήματα.

- Παράδειγμα: ASCII, Base64, Unicode
- Δεν υπάρχει καμία ασφάλεια πέρα από ακεραιότητα και σωστή μετάδοση.
Άρα η ασφάλεια είναι **τεχνική**.

Χωρίς ασφάλεια

Αναγνώσιμα σε άλλη μορφή



Συμπέρασμα

Η **κρυπτογράφηση** προστατεύει τα πληροφορία από μη εξουσιοδοτημένη πρόσβαση, ενώ η **κωδικοποίηση** απλώς αλλάζει τη μορφή της πληροφορίας ώστε να μπορεί να αποθηκευτεί και να μεταφερθεί πιο εύκολα.

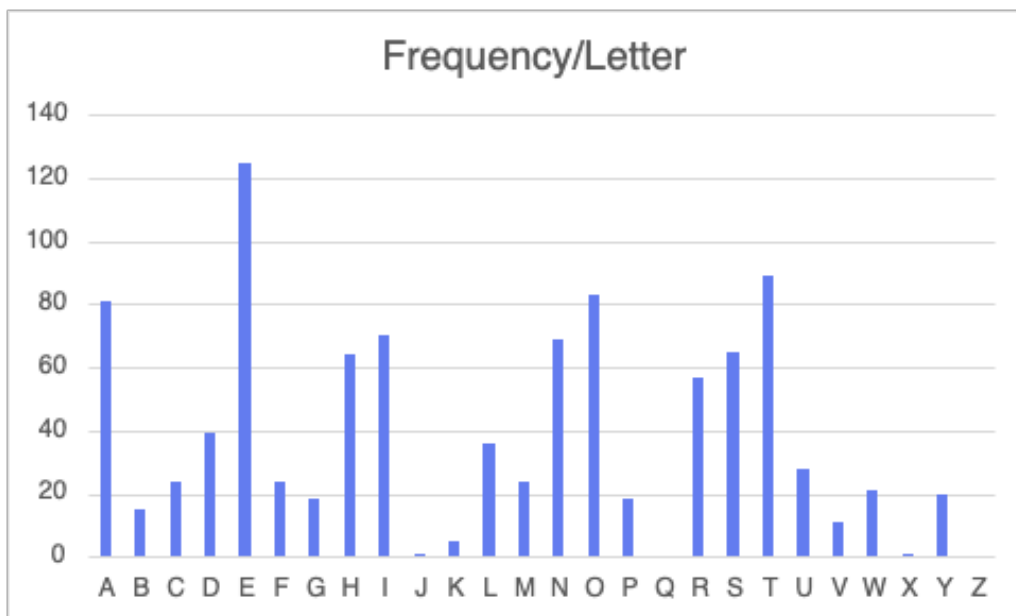
Τέλος, και τα δύο χρησιμοποιούνται για μεταφορά δεδομένων, αλλά έχουν διαφορετικό σκοπό και μηχανισμό λειτουργίας.

Exercise 2

Επισκεφθείτε τη σελίδα <https://www.gutenberg.org/> και κατεβάστε ένα οποιοδήποτε βιβλίο της αρεσκείας σας ως αρχείο κειμένου (.txt). Στη συνέχεια με τη βοήθεια του κώδικα που παρουσιάζεται παραπάνω υπολογίστε τις συχνότητες των γραμμάτων που περιέχονται σε ολόκληρο το βιβλίο και απεικονίστε τις σε ένα γράφημα του excel. Ποιες είναι οι παρατηρήσεις σας λαμβάνοντας υπόψη το δοθέν γράφημα συχνοτήτων που αφορά το βιβλίο "The Room with the Little Door";

Solution

Επισκέπτηκα την σελίδα και επέλεξα το "Συμπόσιο" του Πλάτωνα και το αποθήκευσα μέσω Plain Text UTF-8. Παρακάτω βλέπουμε τις συχνότητες των γραμμάτων:



Παρατηρούμε πως οι συχνότητες των γραμμάτων είναι ίδιες με τις συχνότητες που μιλήσαμε στο εργαστήριο (Ε το πιο συχνό γράμμα, Ζ και Q το λιγότερο κ.ο.κ).

Exercise 3

Το κρυπτοκείμενο που ακολουθεί έχει κρυπτογραφηθεί χρησιμοποιώντας κρυπταλγόριθμο **μετατόπισης**. Κρυπταναλύστε το και βρείτε το αρχικό κείμενο παραθέτοντας τον τρόπο εργασίας σας. Πόσα είναι τα λιγότερα δυνατά γράμματα που πρέπει να αναγνωρίσετε προκειμένου να ανακτήσετε το κλειδί κρυπτογράφησης? Πώς θα ερμηνεύατε την δήλωση του μηνύματος αυτού? Σημείωση: **μην χρησιμοποιήσετε επίθεση εξανλητικής δοκιμής**.

**** QTCDE ESP DPYEPYNP LYO ESPY ESP PGTOPYNP ****

Solution

Χρησιμοποίησα τον αλγόριθμο Caesar Cipher του εργαστηρίου και ως input έβαλα το δοθέν μήνυμα και ως output μου έβγαλε τα εξής:

```
0 QTCDEESPDYEPYNPLYOESPYESP PGTOPYNP
1 PSBCDDROCOXDOXMOKXNDROXDROOFSNOXMO
2 ORABCCQNBNCNWL NJWMCQNCQNNERMNWL N
3 NQZABBP MAMVBMVKMIVLBPMVBPMMDQLMVKM
4 MPYZAAOLZLUALUJLHUKAOLUAOLLCPKLUJL
5 LOXYZZNKYKTZKTIKGTJZNKTZNKKBOJKTIK
6 KNWXYJM JXJSYJSHJFSIYMJSY MJJANIJS HJ
7 JMVWXXLIWIRXIRGIERHXLIRXLIIZMHIRGI
8 ILUVWWKHVHQWHQFHDQGWKHQWKHHYLGHQFH
9 HKTUVVJGUGPVGPEGCPFVJGPVJGGXKFGPEG
10 GJSTUUIFTFOUFODFBOEUIFOUIFFWJEFODF
11 FIRSTTHESENTENCEANDTHEENTHEEVIDENCE
12 EHQRSSGDRDMSDMDZMCSGDMSGDDUHCMDBD
13 DGPQRRFCQCLRCLACYLBRFCLRFCCTGBCLAC
14 CFOPQQEBPBKQBKZBXKAQEBKQEBBSFABKZB
15 BENOPPDAAJPAJYAWJZPDAJPDAAAREZAJYA
16 ADMNOOCZNZIOZIXZVIYOCZIOCZZQDYZIXZ
17 ZCLMNNBYMYHNYHWYUHXNBYHNBYYPCXYHWY
18 YBKLMMAXLXGMXGVXTGWMAXGMAXXOBWXGVX
19 XAJKLLZWKWFLWFUWSFVLZWFLZWNNAVWFWU
20 WZIJKKYVJVEKVETVREUKYVEKYVVMZUVETV
21 VYHIJJXUIUDJUDSUQDTJXUDJXUULYTUDSU
22 UXGHIIWTHTCITCRTPCSIWTCIWTTKXSTCRT
23 TWFGHHVSGSBHSBQSBRHVSBBHVSSJWRBQS
24 SVEFGGURFRAGRAPRNAQGURAGURRIVQRAPR
25 RUDEFFTQEZFQZQZMZPFTQZFTQZHUPQZQZ
```

Βλέπουμε ότι η λύση είναι στην 11η γραμμή και το κρυπτοκείμενο είναι η φράση "FIRST THE SENTENCE AND THEN THE EVIDENCE". Τα λιγότερα δυνατά γράμματα είναι έξι καθώς αν και η πρώτη λέξη είναι FIRST (5 γραμμάτων), παρατηρούμε ότι στην τελευταία γραμμή προκύπτει και μια άλλη πρώτη λέξη (RUDE) και για να καταλάβουμε ότι απλώς ήταν σύμπτωση χρειάζεται να δούμε ότι στο 5ο και 6ο γράμμα υπάρχουν δύο σύμφωνα μαζί και σε συνδυασμό ότι βρίσκουμε την λέξη FIRST, καταλήγουμε ότι από το 6ο γράμμα είμαστε σίγουροι ότι η γραμμή 11 είναι η σωστή γραμμή με την υπόλοιπη φράση. Το μήνυμα μου θυμίζει δύο πράγματα, την άσκηση μας που κυριολεκτικά παραθέτω την πρόταση - sentence και μετά τον τρόπο εύρεσης - evidence, καθώς και το αντίθετο από αυτό που εφαρμόζεται στον νόμο και σε μία δίκη (δηλαδή πρώτα τα στοιχεία - evidence και μετά η ετυμηγορία - sentence).

Exercise 4

Το κρυπτοκείμενο που ακολουθεί έχει κρυπτογραφηθεί χρησιμοποιώντας κρυπταλγόριθμο **αντικατάστασης**. Κρυπταναλύστε το, παραθέτοντας τον τρόπο εργασίας σας.

**** ZFFD BXWE QEUFPCY TIXYF JWA BXWE FCFSUFY TIXYFE ****

Solution

Στην αρχή προσπάθησα μέσω Frequency Analysis αν θα έβρισκα κάποια ομοιότητα, ωστόσο μόνο το E ήταν αρκετά πιθανό ζεύγος καθώς στο αρχικό μας μήνυμα το γράμμα F εμφανίζεται πιο συχνά (8 φορές) ωστόσο τα υπόλοιπα γράμματα εμφανιζόντουσαν παρόμοιες φορές μεταξύ τους, σε συνδυασμό με το γεγονός ότι έχουμε ένα μικρού μήκους κρυπτοκείμενο είναι δύσκολο να βρούμε το αντίστοιχο με αυτόν τον τρόπο. Ωστόσο ένας πολύ απλός τρόπος είναι online μέσω του Mono-Alphabetic Cipher που προκύπτει η φράση "KEEP YOUR FRIENDS CLOSE BUT YOUR ENEMIES CLOSER".



Search for a tool

★ [SEARCH A TOOL ON dCODE](#)

e.g. type 'caesar'

★ [BROWSE THE FULL dCODE TOOLS' LIST](#)

Results

dCode tried to find the correct alphabet and its substitution automatically. The result is a draft that should allow you to perform the decryption manually by indicating letters in each cell.

KEEP YOUR FRIENDS CLOSE BUT YOUR ENEMIES CLOSER



dCode is preparing a new interface. Come test and give your feedback on the **new page: Mono-alphabetic Substitution!**

MONO-ALPHABETIC SUBSTITUTION

[Cryptography](#) > [Substitution Cipher](#) > [Mono-alphabetic Substitution](#)



[Learn more](#)

MONOALPHABETIC SUBSTITUTION DECODER

★ **ALPHABETIC SUBSTITUTION CIPHERTEXT**

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	Z
T	Y	N	P	R	E	A	H	L	B	G	M	W	J	Q	D	F	X	M	C	I	Z	U	O	S	K

= GJTPFQKHUNZILSCXDOEYAWMRBV (Original Encryption Alphabet)

= TYNPREAHLBGWJQDFXMCIZUOSK (Reciprocal & Decryption Alphabet)

Z	F	F	D	B	X	W	E	Q	E	U	F	C	P	Y	T	I	X	Y	F	J	W
K	E	E	P	Y	O	U	R	F	R	I	E	N	D	S	C	L	O	S	E	B	U
A	B	X	W	E	F	C	F	S	U	F	Y	T	I	X	Y	F	E				
T	Y	O	U	R	E	N	E	M	I	E	S	C	L	O	S	E	R				

★ SPACES ☒ ARE RELEVANT AND MUST BE KEPT (ARISTOCRAT CIPHER)

☐ CAN BE IGNORED OR ARE MISSING (PATRISTOCRAT CIPHER)

★ PLAINTEXT LANGUAGE

[▶ DECRYPT AUTOMATICALLY](#)