# ΠΡΟΣΤΑΣΙΑ ΚΑΙ ΑΣΦΑΛΕΙΑ ΣΥΣΤΗΜΑΤΩΝ ΥΠΟΛΟΓΙΣΤΩΝ (Εργαστήριο)

## Ενότητα 1

## Κρυπτογράφηση μονοαλφαβητικής αντικατάστασης

## 1. Βασικές έννοιες κρυπτογράφησης

Με τον όρο κρυπτογραφία εννοούμε τη μελέτη τεχνικών που στοχεύουν στην εξασφάλιση μετάδοσης της πληροφορίας, όπως εμπιστευτικότητα, ακεραιότητα και διαθεσιμότητα (βλέπε Εικόνα 1).


Εικόνα 1: Τρίπτυχο ασφαλείας συστημάτων και δικτύων υπολογιστών (Πηγή: http://geraintw.blogspot.com/2012/09/cia-infosec.html)

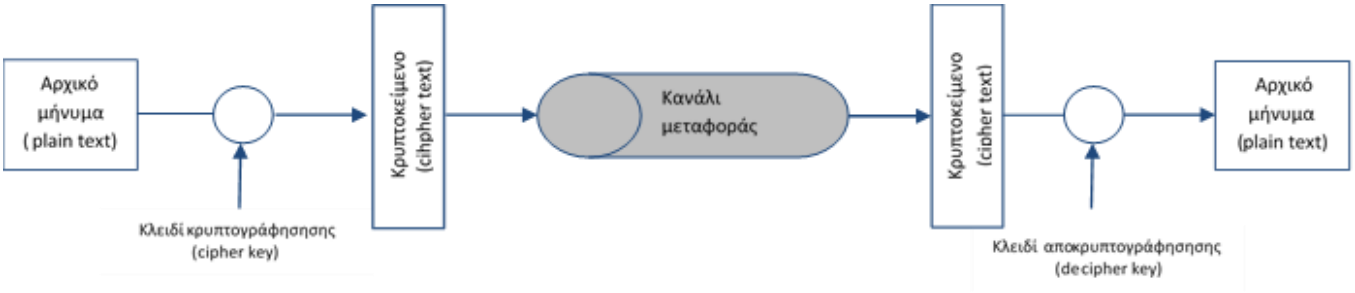
***Ορολογία:***

**Κρυπτογράφηση (Encryption)**: Η διαδικασία μετατροπής των δεδομένων σε μη αναγνώσιμη μορφή μέσω της εφαρμογής ενός **αλγορίθμου κρυπτογράφησης**, με στόχο να μην αναγνωρίζεται από ένα μη εξουσιοδοτημένο άτομο.

**Αποκρυπτογράφηση (Decryption):** Είναι η αντίστροφη διαδικασία, δηλαδή η μετατροπή του κρυπογραφημένου μηνύματος στην αρχική του μορφή.

**Κρυπτοσύστημα (cryptosystem):** Ένα σύστημα που υποστηρίζει και τις δύο διαδικασίες (δηλαδή κρυπτογράφηση – αποκρυπτογράφηση).

Ένα μοντέλο ασφάλειας επικοινωνιών παρουσιάζεται στην Εικόνα 2.




Εικόνα 2: Μοντέλο ασφάλειας επικοινωνιών. (Πηγή: W. Stallings, "Κρυπτογραφία και Ασφάλεια Δικτύων, Αρχές και εφαρμογές", εκδ. Ιων)

Το αρχικό μήνυμα (plaintext) μετατρέπεται με την εφαρμογή ενός αλγόριθμου κρυπτογράφησης σε ένα κρυπτοκείμενο (ciphertext, encrypted text), προκειμένου να μη μπορούν να το διαβάσουν μη εξουσιοδοτημένοι χρήστες, όταν στέλνεται στον παραλήπτη μέσα από ένα κανάλι μεταφοράς (π.χ. διαδίκτυο). Η κρυπτογράφηση του κειμένου λαμβάνει χώρα με τη βοήθεια ενός κλειδιού κρυπτογράφησης (encryption key, cipher key). Κατά την λήψη του μηνύματος ο δέκτης λαμβάνει το κρυπτοκείμενο και εφαρμόζει τον αλγόριθμο αποκρυπτογράφησης με τη βοήθεια ενός κλειδιού αποκρυπτογράφησης (decryption key, decipher key) για την εξαγωγή του αρχικού μηνύματος.

***Κατηγορίες αλγορίθμων:***

Αλγόριθμοι συμμετρικού (ή κρυφού) κλειδιού (symmetric key algorithms): Χρησιμοποιούν το ίδιο κλειδί για την κρυπτογράφηση και την αποκρυπτογράφηση. Το κλειδί αυτό θα πρέπει να διατηρείται μυστικό.

Αλγόριθμοι ασύμμετρου (ή δημοσίου) κλειδιού (asymmetric key algorithms): Χρησιμοποιούν δύο διαφορετικά κλειδιά για την κρυπτογράφηση και την αποκρυπτογράφηση. Ο αποστολέας χρησιμοποιεί το δημόσιο κλειδί για την κρυπτογράφηση του μηνύματος και ο παραλήπτης το αποκρυπτογραφεί χρησιμοποιώντας διαφορετικό κλειδί αποκρυπτογράφησης το οποίο θα πρέπει να παραμένει κρυφό.

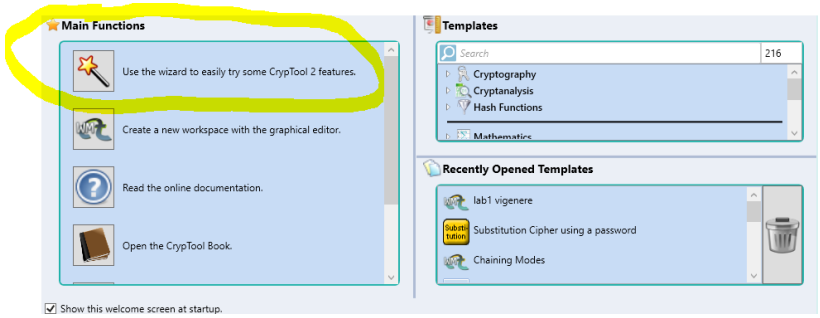
# 2. Εισαγωγή στο Cryptool 2

Το CrypTool 2 (CT2) είναι ένα γραφικό περιβάλλον ανοικτού λογισμικού το οποίο έχει αναπτυχθεί με στόχο την εξοικείωση και εκμάθηση βασικών εννοιών της κρυπτογραφίας. Παρέχεται δωρεάν στη σελίδα https://www.cryptool.org/en/ct2-downloads

Είναι πολύ απλό στη χρήση του και ευρύτατα διαδεδομένο λογισμικό ηλεκτρονικής μάθησης στον τομέα της κρυπτογραφίας. Μέσα σε αυτό ένας μεγάλος αριθμός εργαλείων ανάλυσης και αλγόριθμοι έχουν υλοποιηθεί αποτελεσματικά. Η γραφική διεπαφή και η πλούσια ηλεκτρονική του τεκμηρίωση δίνει στο χρήστη τη δυνατότητα, να γνωρίσει τη κρυπτογραφία, δημιουργώντας δικές του διατάξεις, δοκιμάζοντας αλγορίθμους και μελετώντας τα αποτελέσματα.

*Περιβάλλον εργασίας*

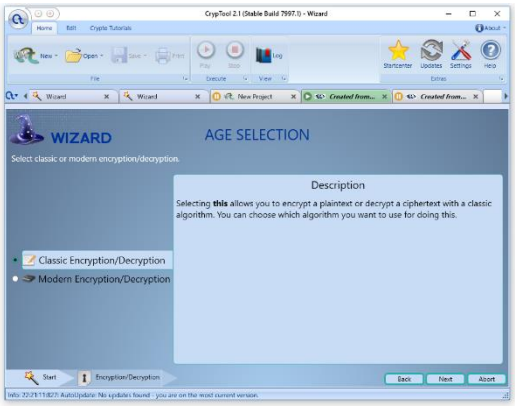
Η Εικόνα 3 δείχνει την αρχική εικόνα του προγράμματος όταν το CT2 ξεκινά. Το **startcenter** είναι η πρώτη εικόνα που εμφανίζεται και από εδώ ο χρήστης μπορεί να μεταφερθεί σε οποιαδήποτε άλλη λειτουργία επιλέγοντάς την.




Εικόνα 3: Η πρώτη εικόνα του προγράμματος κατά την έναρξη του CT2

## 2.1. ΤΟ ΕΡΓΑΛΕΙΟ WIZARD

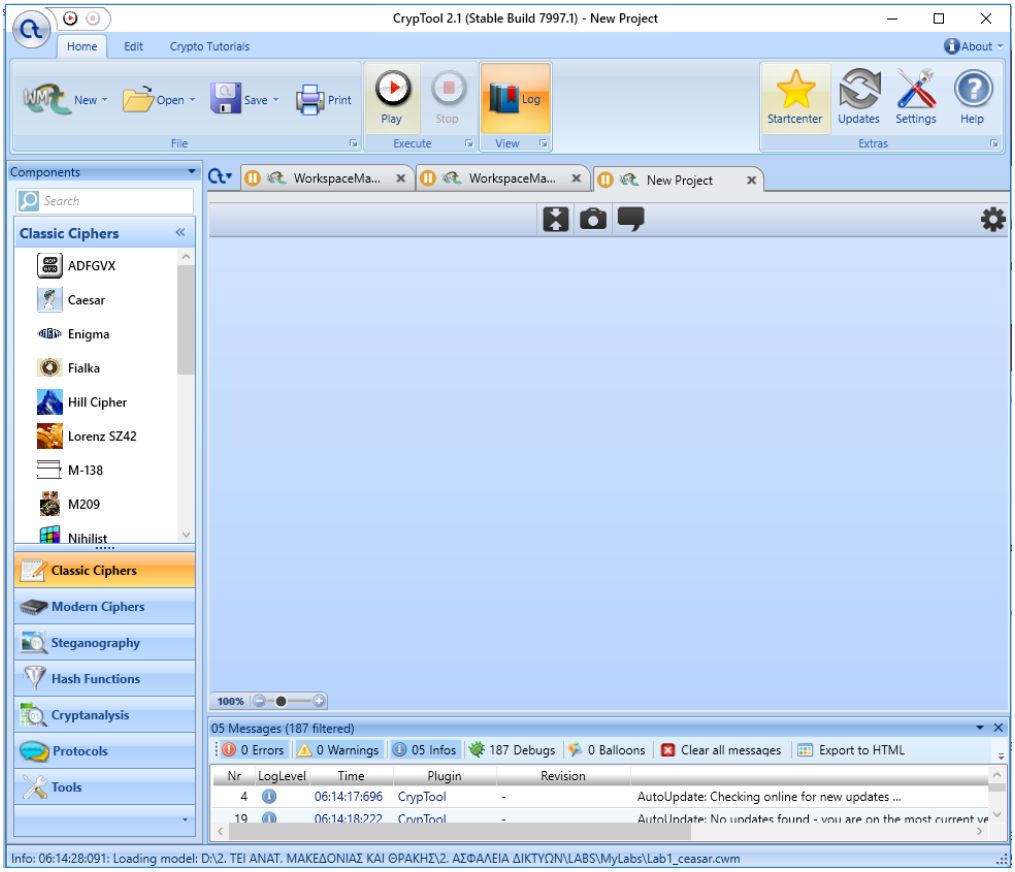
Ο απλούστερος τρόπος χρήσης και εξοικείωσης με το CT2 είναι από το εργαλείο Wizard: Startcenter -> Use the wizard (βλέπε Εικόνα 3, πρώτη επιλογή). Ο χρήστης συμπληρώνει βήμα – προς – βήμα επιλέγοντας τις βασικές λειτουργίες από μια διαθέσιμη λίστα επιλογών (βλέπε Εικόνα 4)




Εικόνα 4: Επιλέγοντας αλγόριθμο κρυπτογράφησης στο CT με το εργαλείο Wizard

## 2.2. ΤΟ WORKSPACE

Το Workspace (βλέπε Εικόνα 3, δεύτερη επιλογή) αποτελεί το βασικό χώρο εργασίας του CT2, καθώς επιτρέπει στον χρήστη να δημιουργεί διάφορα σενάρια κρυπτογράφησης (βλέπε Εικόνα 5).

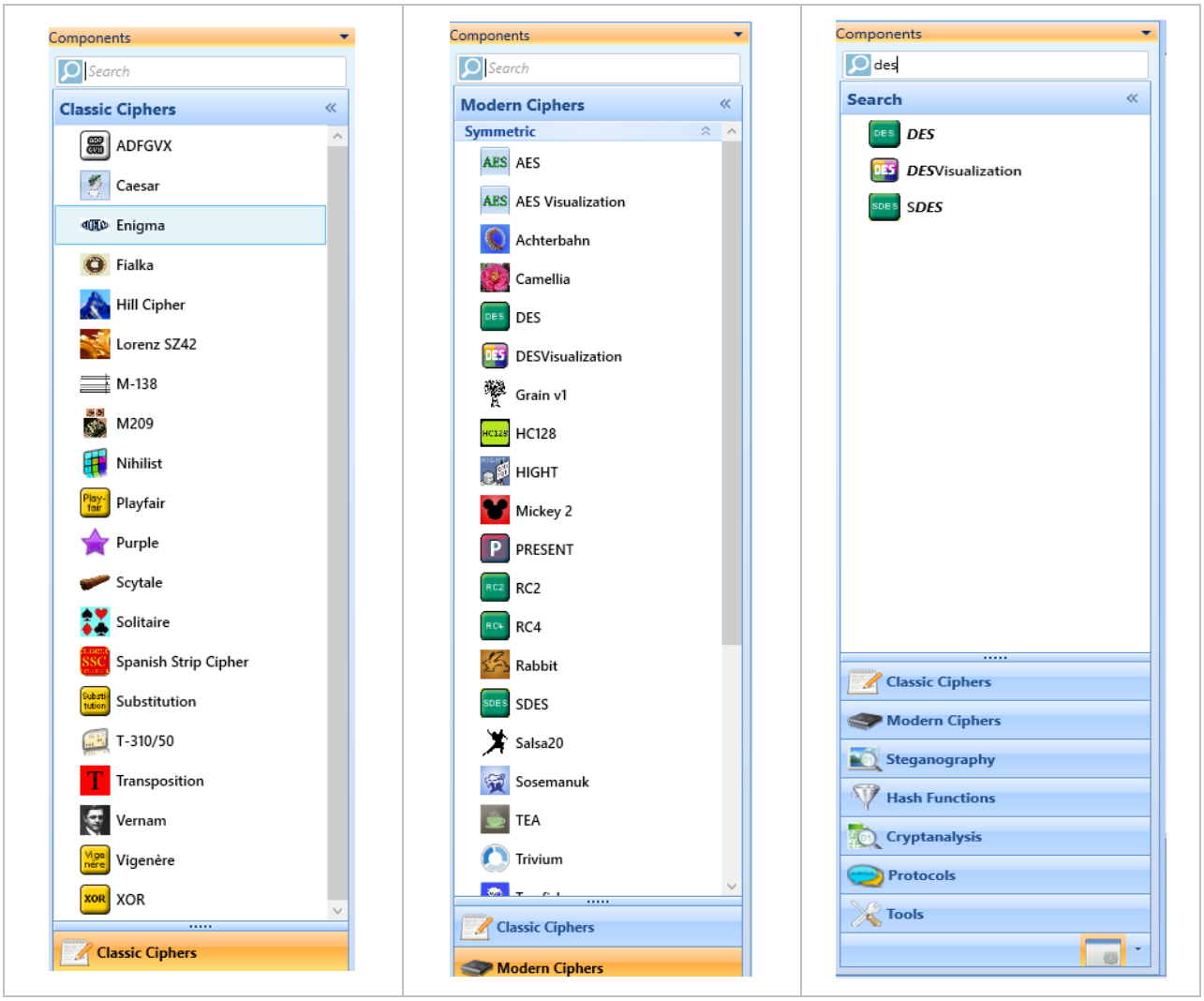



Εικόνα 5: Το περιβάλλον εργασίας του CT2

Ο οριζόντιος χώρος στην επάνω πλευρά είναι οι επιλογές μενού στις βασικές λειτουργίες (αποθήκευση, επιλογή αρχείων, ενημερώσεις, ρυθμίσεις και εκτέλεση του σεναρίου). Η κάθετη αριστερή πλευρά είναι η εργαλειοθήκη των επιλογών, ενώ ο υπόλοιπος χώρος είναι η περιοχή εργασίας για την υλοποίηση της σύνδεσης των απαραίτητων μερών.

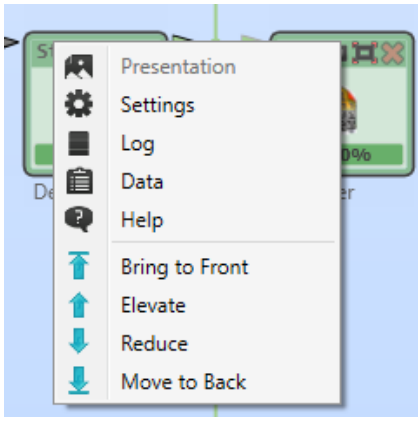
Για τη δημιουργία ενός σεναρίου, ο χρήστης ακολουθεί τα παρακάτω βήματα:

1. Επιλογή και τοποθέτηση των στοιχείων (components) που απαιτούνται για να εκτελεστεί το σενάριο, από μια λίστα διαθέσιμων επιλογών (drag and drop) (βλέπε Εικόνα 6). Επιπλέον, είναι εύκολη η αναζήτηση πληκτρολογώντας τα αρχικά γράμματα του αλγόριθμου.
2. Δημιουργία των κατάλληλων συνδέσεων μεταξύ των στοιχείων αυτών.
3. Εκτέλεση (Play) και εμφάνιση των αποτελεσμάτων της εκτέλεσης. Τα αποτελέσματα που λαμβάνονται στη συνέχεια μελετώνται και συγκρίνονται ή χρησιμοποιούνται σε νέα κρυπτογράφηση ή αποκρυπτογράφηση.




Εικόνα 6: Εργαλειοθήκη διαθέσιμων επιλογών του CT2

Δύο σημαντικές βοηθητικές λειτουργίες του CT2 είναι το δεξί "κλικ" πάνω σε αυτό. Σε αυτήν την περίπτωση το πρόγραμμα δίνει περισσότερες πληροφορίες σχετικά με τον τρόπο χρήσης και λειτουργίας τους (βλέπε Εικόνα 7).




Εικόνα 7: Μενού διαθέσιμων επιλογών ενός στοιχείου (επιλογή δεξί κλικ πάνω στο στοιχείο)

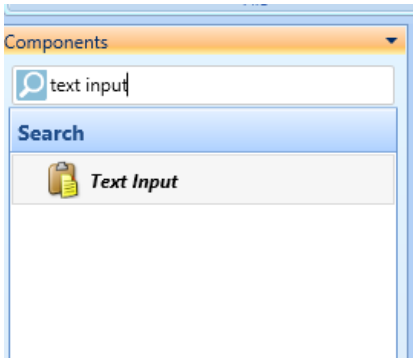
Επιπλέον, πατώντας το πλήκτρο F1 ενώ έχει επιλεχθεί κάποιο στοιχείο, εμφανίζεται η σχετική βοήθεια (online help) για το στοιχείο αυτό.

## 2.3. ΠΑΡΑΔΕΙΓΜΑ ΔΗΜΙΟΥΡΓΙΑΣ ΣΕΝΑΡΙΟΥ ΜΕ ΤΟ CRYPTOOL2

Στο παρακάτω παράδειγμα θα δούμε πως μπορούμε να υλοποιήσουμε ένα σενάριο χρήσης της συνάρτησης κατακερματισμού (hash function) MD5. Η συγκεκριμένη συνάρτηση λαμβάνει ως τιμή εισόδου ένα string τυχαίου μήκους και επιστρέφει μία «σύνοψη» (digest).

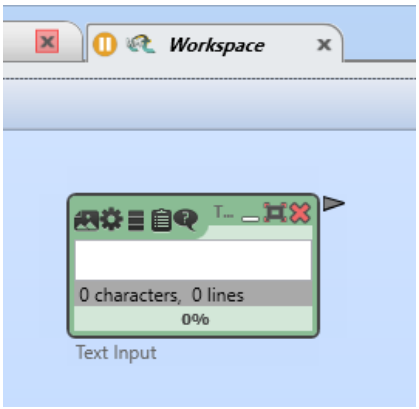
Σημειωτέον ότι μια συνάρτηση κατακερματισμού δεν χρησιμοποιείται για κρυπτογράφηση αλλά για την «υπογραφή» αρχείων με τέτοιο τρόπο ώστε να εντοπίζεται οποιαδήποτε μετατροπή τους ώστε να διασφαλίζεται η Ακεραιότητα (Integrity) των δεδομένων.

1. Πληκτρολογήστε «Text Input» στο πεδίο *Search* που βρίσκεται στην εργαλειοθήκη *Components* ώστε να εμφανιστεί η αντίστοιχη επιλογή (βλέπε Εικόνα 8).



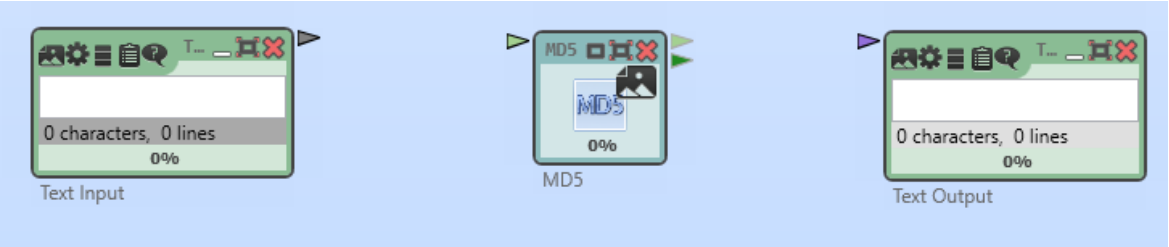

Εικόνα 8: Αναζήτηση στο πεδίο Search

2. Τραβήξτε (με drag and drop) την επιλογή «Text Input» μέσα σε ένα κενό Workspace (βλέπε Εικόνα 9).



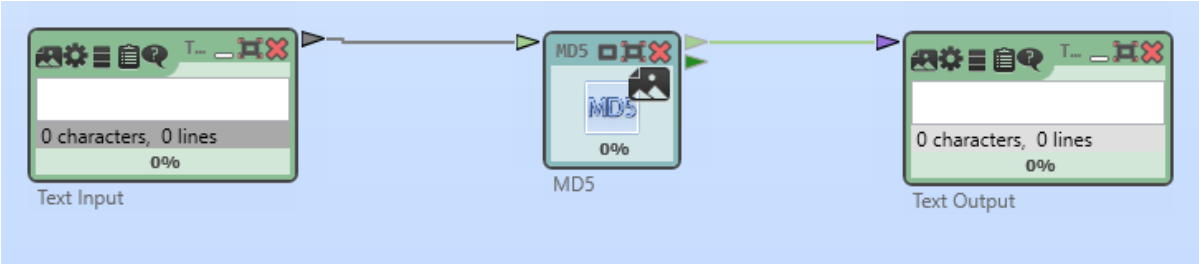

Εικόνα 9: Εισαγωγή εργαλείου στο Workspace

3. Με τον ίδιο τρόπο, τοποθετήστε μέσα στο ίδιο Workspace τα εργαλεία «Text Output» και «MD5» (βλέπε Εικόνα 10).



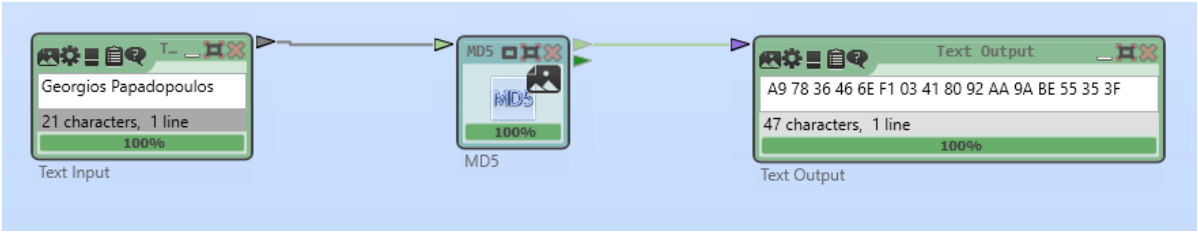

Εικόνα 10: Εισαγωγή όλων των εργαλείων στο Workspace

4. Ενώστε τα εργαλεία με τον τρόπο που εμφανίζεται στην Εικόνα 11. Προσέξτε ότι όλα τα «βέλη» δεν είναι ίδια. Ακουμπήστε το δείκτη του ποντικιού πάνω από κάθε βέλος ώστε να διαπιστώσετε τις διαφορετικές λειτουργικότητες του κάθε βέλους.




Εικόνα 11: Ένωση των εργαλείων

5. Εισάγετε στο εργαλείο «Text Input» το ονοματεπώνυμο σας με λατινικούς χαρακτήρες και πατήστε το κουμπί «Play» στην εργαλειοθήκη «Execute». Θα παρατηρήσετε την «σύνοψη» που παράγεται από τη συνάρτηση κατακερματισμού στο εργαλείο «Text Output» (βλέπε Εικόνα 12).




Εικόνα 12: Εκτέλεση του σεναρίου

6. Για να διακόψετε την εκτέλεση του σεναρίου, πατήστε το κουμπί «Stop» στην εργαλειοθήκη «Execute».

## 3. Κρυπτογράφηση Μονοαλσφαβητικής Αντικατάστασης

***Ορισμός - Κλασικοί αλγόριθμοι μονοαλφαβητικής αντικατάστασης***

Οι αλγόριθμοι μονοαλφαβητικής αντικατάστασης (monoalphabetic substitution) αντικαθιστούν κάθε γράμμα του αρχικού μηνύματος από ένα άλλο γράμμα χρησιμοποιώντας κάποιο συγκεκριμένο αλφάβητο για την αντιστοίχιση

***1ο Παράδειγμα αλγόριθμου μονοαλφαβητικής αντικατάστασης. Ο αλγόριθμος του Καίσαρα.***

Στον αλγόριθμο του Καίσαρα (**Caesar** cipher) έχουμε ολίσθηση των γραμμάτων του αλφαβήτου κατά 3 γράμματα:

Αλφαβήτο αρχικού μηνύματος: 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

Αλφάβητο κρυπτογραφήματος : d e f g h I j k l m n o p q r s t u v w x y z a b c

Παράδειγμα:

Αρχικό μήνυμα: hello world

Κρυπτογραφημένο μήνυμα: khoor zruog

Γενίκευση του αλγόριθμου του Καίσαρα: Ολίσθηση των γραμμάτων του αλφαβήτου κατά k γράμματα.

***2ο Παράδειγμα αλγόριθμου μονοαλφαβητικής αντικατάστασης***

Στον αλγόριθμο απλής αντικατάστασης έχουμε τυχαία αντιστοίχηση των γραμμάτων του αλφαβήτου:

Αλφαβήτα αρχικού μηνύματος: abcdefghijklmnopqrstuvwxyz

Αλφαβήτα αντιστοίχησης: joenaizrdmwhcqvbtlkpugysfx

Παράδειγμα:

Αρχικό μήνυμα: hello world

Κρυπτογραφημένο μήνυμα: rahhv yvlhn

## 4. Κρυπτανάλυση Μονοαλφαβητικής Αντικατάστασης

**Κρυπτανάλυση (cryptoanalysis)**: Η μελέτη και κατανόηση των μεθόδων που οδηγούν στην εύρεση του κλειδιού αποκρυπτογράφησης ή μέρους του, με στόχο την δυνατότητα αποκρυπτογράφησης του αρχικού μηνύματος

***Ασφάλεια Μονοαλφαβητικής αντικατάστασης***

Η μονοαλφαβητική αντικατάσταση έχει μια σοβαρή αδυναμία, αφού ο αντίπαλος μπορεί να ανακαλύψει με σχετική ευκολία το κείμενο, ακόμη και χωρίς τη χρήση ηλεκτρονικού υπολογιστή.

Η αδυναμία της μονοαλφαβητικής αντικατάστασης αφορά στη διατήρηση της πληροφορίας σχετικά με τη συχνότητα εμφάνισης των γραμμάτων σε μια γλώσσα.

Το πιο συχνό γράμμα στην ελληνική γλώσσα είναι το **α**, και ακολουθούν το **ο**, το **ε** και το **ι**. Αντίστοιχα στην αγγλική γλώσσα είναι τα **e, t** και **a** (βλέπε πίνακα 1).

Ο αντίπαλος μπορεί να κατασκευάσει έναν πίνακα συχνοτήτων του κρυπτοκειμένου και να αντιπαραθέσει τις συχνότητες εμφάνισης του κρυπτοκειμένου με αυτές της ελληνικής γλώσσας. Για τα πιο συχνά γράμματα μπορεί να βρει τις αντιστοιχίες των συμβόλων του απλού κειμένου με το κρυπτοκείμενο.

Βασική παράμετρος στην επιτυχία της μεθόδου αυτής αποτελεί το μέγεθος του κρυπτοκειμένου. Το κρυπτοκείμενο θα πρέπει να είναι αρκετά μεγάλο ώστε να μπορέσουν να διακριθούν τα γράμματα τα οποία έχουν μεγάλη συχνότητα εμφάνισης.

| Γράμμα | Συχνότητα εμφάνισης (%) | Γράμμα | Συχνότητα εμφάνισης (%) |
|---|---|---|---|
| **a** | 8.167 | **n** | 6.749 |
| **b** | 1.492 | **o** | 7.507 |
| **c** | 2.782 | **p** | 1.929 |
| **d** | 4.253 | **q** | 0.095 |
| **e** | 12.702 | **r** | 5.987 |
| **f** | 2.228 | **s** | 6.327 |
| **g** | 2.015 | **t** | 9.056 |
| **h** | 6.094 | **u** | 2.758 |
| **i** | 6.966 | **v** | 0.978 |
| **j** | 0.153 | **w** | 2.360 |
| **k** | 0.772 | **x** | 0.150 |
| **l** | 4.025 | **y** | 1.974 |
| **m** | 2.406 | **z** | 0.074 |

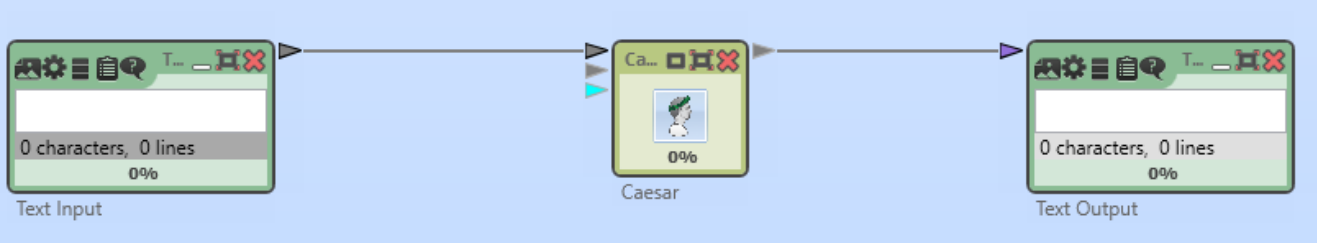
**Πίνακας 1:** Συχνότητα εμφάνισης των γραμμάτων της Αγγλικής γλώσσας. (Πηγή: Κάτος, Β. "Τεχνικές Κρυπτογραφίας και Κρυπτανάλυσης", εκδ. Ζυγός, 2003).

# Εργαστηριακή Άσκηση 1.Α: Κρυπτογράφηση του Αλγορίθμου Καίσαρα

***Κρυπτογράφηση του αλγορίθμου Καίσαρα***

1. Υλοποιήστε στο CT2 το σενάριο που απεικονίζεται στη Εικόνα 13 για την κρυπτογράφηση κειμένου σύμφωνα με τον αλγόριθμο Καίσαρα. Χρησιμοποιείστε ως κλειδί κρυπτογράφησης του αλγόριθμου το λατινικό γράμμα που αντιστοιχεί στο πρώτο γράμμα του επώνυμού σας. Το (plaintext) κείμενο που θα κρυπτογραφήσετε είναι το εξής:

*Lorem ipsum dolor sit amet, consectetur adipiscing elit, sed do eiusmod tempor incididunt ut labore et dolore magna aliqua. Ut enim ad minim veniam, quis nostrud exercitation ullamco laboris nisi ut aliquip ex ea commodo consequat. Duis aute irure dolor in reprehenderit in voluptate velit esse cillum dolore eu fugiat nulla pariatur. Excepteur sint occaecat cupidatat non proident, sunt in culpa qui officia deserunt mollit anim id est laborum.*




Εικόνα 13: Σενάριο υλοποίησης της Εργαστηριακής άσκησης 1.Α (κρυπτογράφηση Καίσαρα).

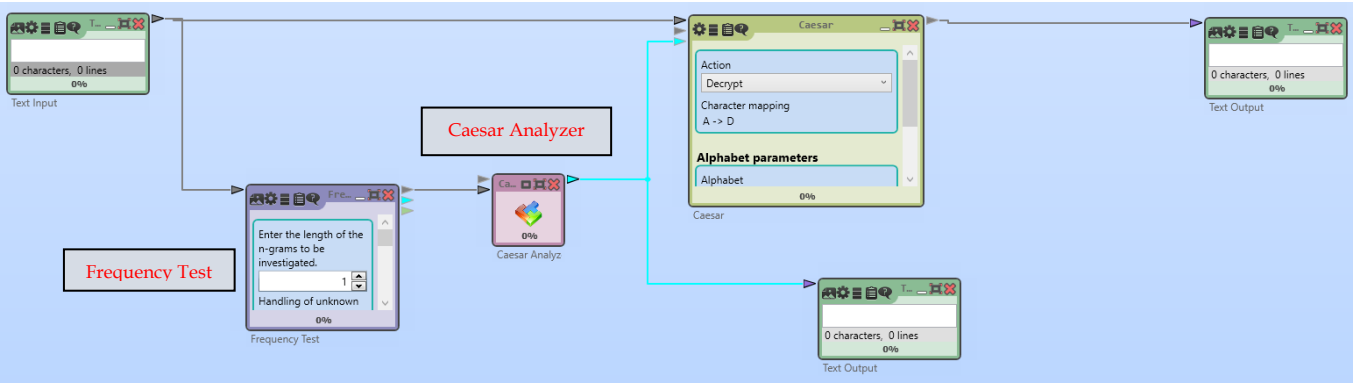
2. Τροποποιήστε το παραπάνω σενάριο για την αποκρυπτογράφηση του μηνύματος που κρυπτογραφήσατε στο προηγούμενο βήμα. Ως κείμενο εισόδου (Text Input) επιλέξετε το κρυπτογραφημένο κείμενο του προηγούμενου βήματος. Χρησιμοποιείστε ως κλειδί αποκρυπτογράφησης του αλγόριθμου το λατινικό γράμμα που αντιστοιχεί στο πρώτο γράμμα του επώνυμού σας.

3. Επιβεβαιώστε ότι η αποκρυπτογράφηση ήταν επιτυχής (δηλαδή ότι το παραγόμενο αποκρυπτογραφημένο κείμενο είναι ίδιο με το αρχικό από το υποερώτημα 1.

## Εργαστηριακή Άσκηση 1.Β: Κρυπτανάλυση του Αλγορίθμου Καίσαρα

1. Υλοποιήστε το σενάριο που εμφανίζεται στην Εικόνα 14 για την κρυπτανάλυση του αλγορίθμου του Καίσαρα. Το κείμενο που θα αποκρυπτογραφήσετε είναι το εξής:

LQ FUBSWRJUDSKB, HQFUBSWLRQ LV WKH SURFHVV RI HQFRGLQJ D PHVVDJH RU LQIRUPDWLRQ LQ VXFK D ZDB WKDW RQOB DXWKRULCHG SDUWLHV FDQ DFFHVV LW DQG WKRVH ZKR DUH QRW DXWKRULCHG FDQQRW. HQFUBSWLRQ GRHV QRW LWVHOI SUHYHQW LQWHUIHUHQFH EXW GHQLHV WKH LQWHOOLJLEOH FRQWHQW WR D ZRXG-EH LQWHUFHSWRU. LQ DQ HQFUBSWLRQ VFKHPH, WKH LQWHQGHG LQIRUPDWLRQ RU PHVVDJH, UHIHUUHG WR DV SODLQWHAW, LV HQFUBSWHG XVLQJ DQ HQFUBSWLRQ DOJRULWKP–D FLSKHU–JHQHUDWLQJ FLSKHUWHAW WKDW FDQ EH UHDG RQOB LI GHFUBSWHG.




Εικόνα 14: Σενάριο υλοποίησης της Εργαστηριακής άσκησης 1Β (κρυπτανάλυση Αλγορίθμου Απλής Αντικατάστασης).

2. Παρατηρήστε το κείμενο που παράγεται και σκεφτείτε αν η κρυπτανάλυση ήταν επιτυχής Υπόδειξη: Θέστε στον κρυπταναλυτή (Casear Analyzer) ως επιλογή για τη γλώσσα του κρυπτοκειμένου την αγγλική (English)

Στο τέλος της άσκησης θα πρέπει να παράξετε ένα αρχείο με το σενάριο κρυπτανάλυσης που υλοποιήσατε στο CT2 με το ΑΕΜ σας, π.χ. lab1b_caesar_cryptanalysis_<AM>.cwm χωρίς τα <>.

3. Χρησιμοποιώντας τα αποτελέσματα του σεναρίου που εκτελέσατε, καταγράψτε τη συχνότητα των γραμμάτων του κρυπτογραφημένου μηνύματος και κατόπιν υπολογίστε το κλειδί κρυπτογράφησης που προκύπτει από τον **πίνακα 1** και συγκρίνετέ τον με αυτόν που υπολογίστηκε από το πρόγραμμα.

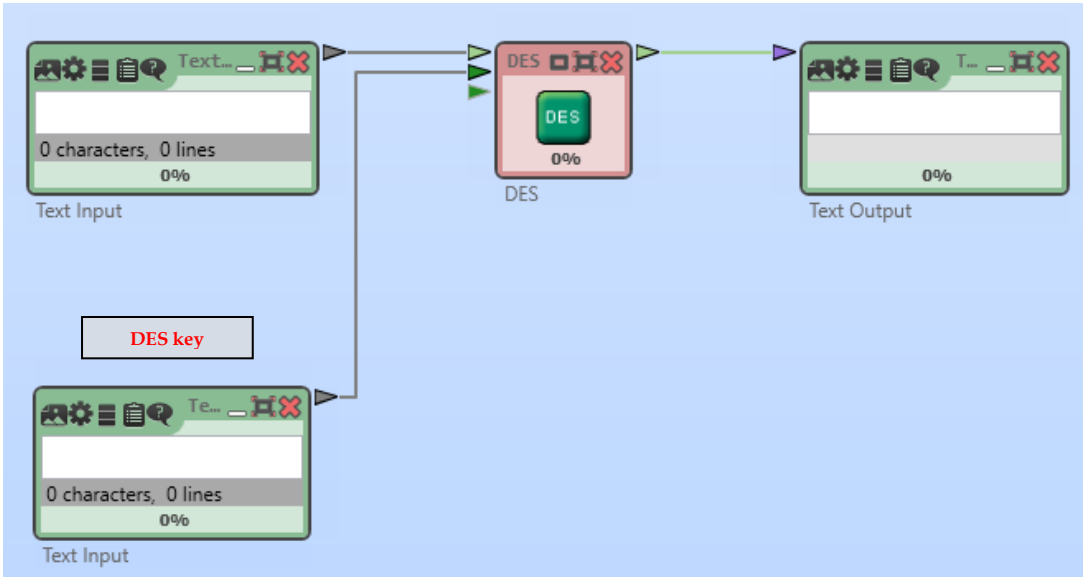
| **Γράμμα αλφαβήτου κρυπτοκειμένου** | **Συχνότητα εμφάνισης γράμματος** | **Αντιστοίχιση με γράμμα αλφαβήτου κρυπτοκειμένου (σύμφωνα με τον πίνακα 1)** | **Πιθανό κλειδί** |
|---|---|---|---|
| | | | |
| | | | |
| | | | |

**Πίνακας 2:** Πίνακας συχνοτήτων εμφάνισης του γραμμάτων στο κρυπτοκείμενο

4. Ελέγξτε αν η τιμή του κλειδιού που υπολογίσατε για τα τρια πρώτα γράμματα συμπίπτει με αυτήν που υπολογίστηκε από το πρόγραμμα. Που μπορεί να οφείλονται τυχόν διαφοροποιήσεις;

## Εργαστηριακή Άσκηση 1.Γ: Αλγόριθμος Data Encryption Standard

1. Υλοποιήστε στο CT2 το σενάριο που εμφανίζεται στην Εικόνα 15 για την κρυπτογράφηση του ονοματεπωνύμου σας σύμφωνα με τον αλγόριθμο DES.




Εικόνα 15: Σενάριο υλοποίησης της Εργαστηριακής άσκησης 1.Γ (κρυπτογράφηση DES).