ΠΡΟΣΤΑΣΙΑ ΚΑΙ ΑΣΦΑΛΕΙΑ ΣΥΣΤΗΜΑΤΩΝ ΥΠΟΛΟΓΙΣΤΩΝ (Εργαστήριο)

Ενότητα 2

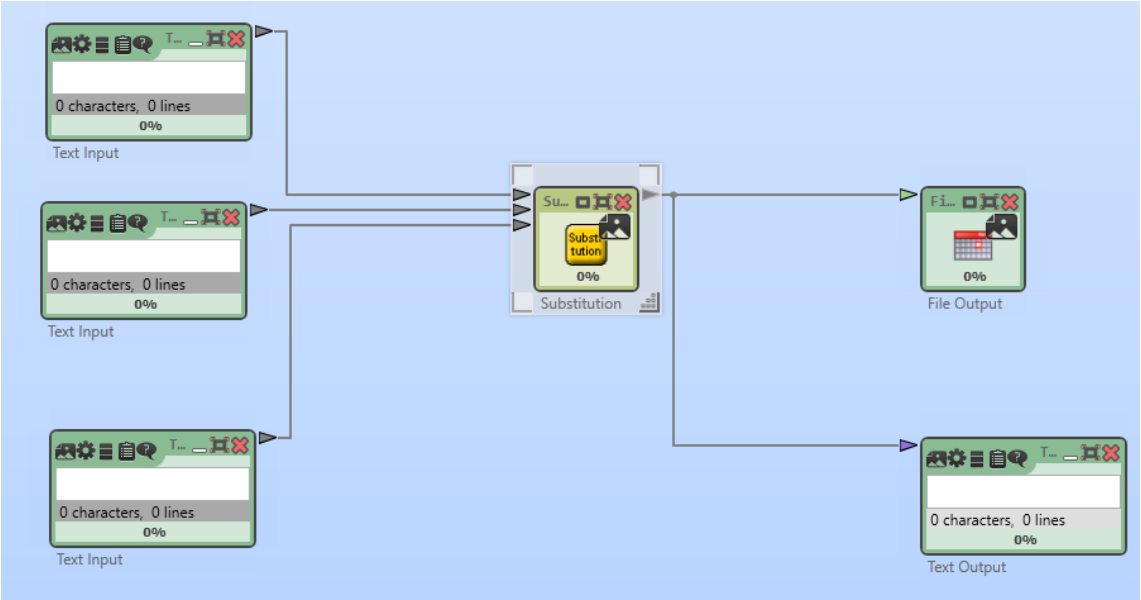
Κρυπτογράφηση μονοαλφαβητικής αντικατάστασης

Εργαστηριακή Άσκηση 2.Α: Κρυπτογράφηση απλής αντικατάστασης

1. Υλοποιήστε στο CT2 το σενάριο που εμφανίζεται στην Εικόνα 1 για την κρυπτογράφηση του ονοματεπώνυμου σας σύμφωνα με τον αλγόριθμο απλής αντικατάστασης. Χρησιμοποιήστε για την κρυπτογράφηση τα παρακάτω στοιχεία

```
Αρχικό μήνυμα:          το ονοματεπώνυμο σας, π.χ. Ioannis Papadopoulos
Αλφαβήτα εισόδου:       ABCDEFGHIJKLMNOPQRSTUVWXYZabcdefghijklmnopqrstuvwxyz
Αλφαβήτα εξόδου:        JOENAIZRDMWHCQVBTLKPUGYSFXjoenaizrdmwhcqvbtlkpugysfx
```

Λαμβάνοντας υπόψη τις απαιτήσεις του συγκεκριμένου component/αλγορίθμου θα πρέπει να δώστε και την κατάλληλη είσοδο στα αντίστοιχα text components. Εξάγετε το αποτέλεσμα της κρυπτογράφησης είτε σε κάποιο αρχείο, είτε σε ένα text component.



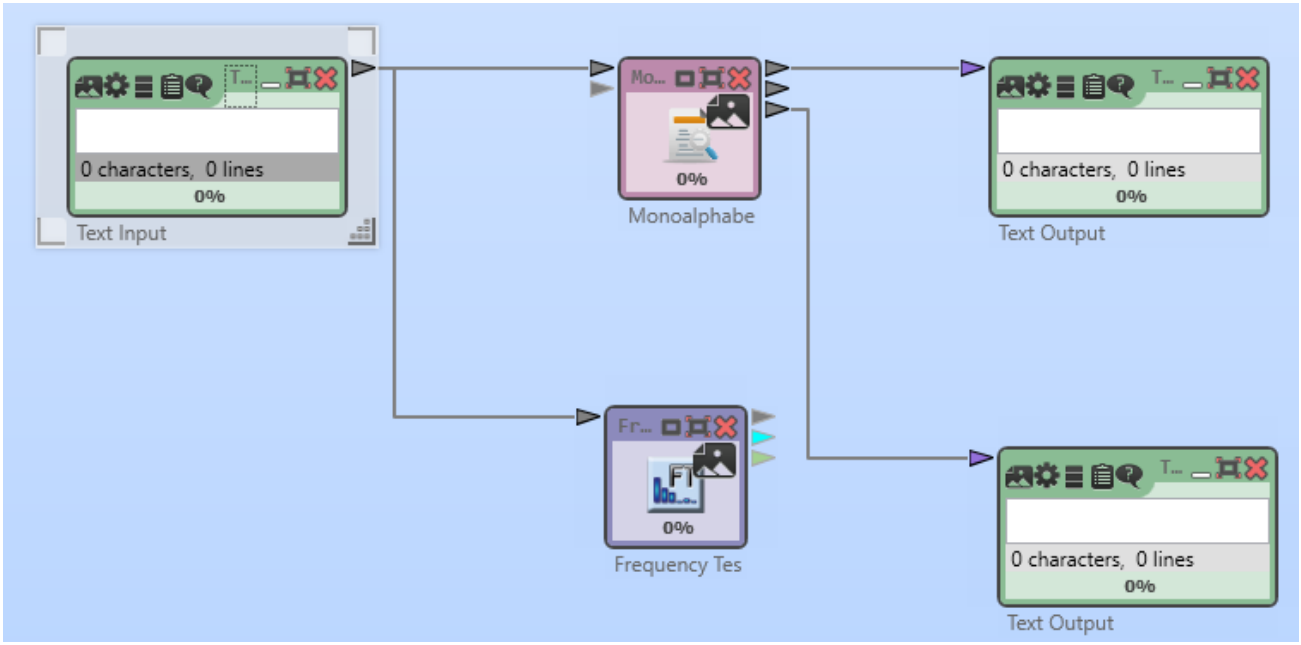
Εικόνα 1: Σενάριο υλοποίησης της Εργαστηριακής άσκησης 2Α (κρυπτογράφηση απλής αντικατάστασης).

2. Υλοποιήστε το αντίστοιχο σενάριο αποκρυπτογράφησης ως συνέχεια του προηγούμενου. Εμφανίστε το αποκρυπτογραφημένο κείμενο ως απλό κείμενο και επιβεβαιώστε ότι το ονοματεπώνυμό σας έχει αποκρυπτογραφηθεί σωστά.

Εργαστηριακή Άσκηση 2.Β: Κρυπτανάληση αλγορίθμου απλής αντικατάστασης

1. Υλοποιήστε το σενάριο που εμφανίζεται στην Εικόνα 2 για την κρυπτανάλυση του αλγορίθμου απλής αντικατάστασης. Ως είσοδο χρησιμοποιήστε το κρυπτογραφημένο κείμενο που εμφανίζεται παρακάτω:

Elfbpjqjhfkdk dk pra kpunf vi jqjhfxdqz dqivlcjpdvq kfkpack dq vlnal pv kpunf pra rdnnaq jkbaepk vi pra kfkpack. Elfbpjqjhfkdk dk ukan pv olajer elfbpvzljbrde kaeuldpf kfkpack jqn zjdq jeeakk pv pra evqpaqpk vi aqelfbpan cakkjzak, agaq di pra elfbpvzljbrde waf dk uqwqvyq



Εικόνα 2: Σενάριο υλοποίησης στης εργαστηριακής άσκησης 2Β (κρυπτανάλυση αλγορίθμου απλής αντικατάστασης)

Εμφανίστε το αποτέλεσμα της κρυπτανάλυσης σε ένα text component.

Γράμμα αλφαβήτου κρυπτοκειμένου	**Συχνότητα εμφάνισης γράμματος (%)**	**Αντιστοίχιση με γράμμα αλφαβήτου κρυπτοκειμένου σύμφωνα με τον πίνακα 1**	**Αντιστοίχιση με γράμμα αλφαβήτου κρυπτοκειμένου σύμφωνα με το πρόγραμμα**

Πίνακας 1: Πίνακας συχνοτήτων εμάνισης του γραμμάτων στο κρυπτοκείμενο

1. Συμπληρώστε τον παραπάνω πίνακα για τα τρία πρώτα γράμματα του κρυπτογραφημένου μηνύματος και ελέγξτε αν το αλφάβητο αντιστοίχισης συμπίπτει με

αυτό που υπολογίστηκε από το πρόγραμμα (έξοδος του στοιχείου Monoalphabetic analyser).

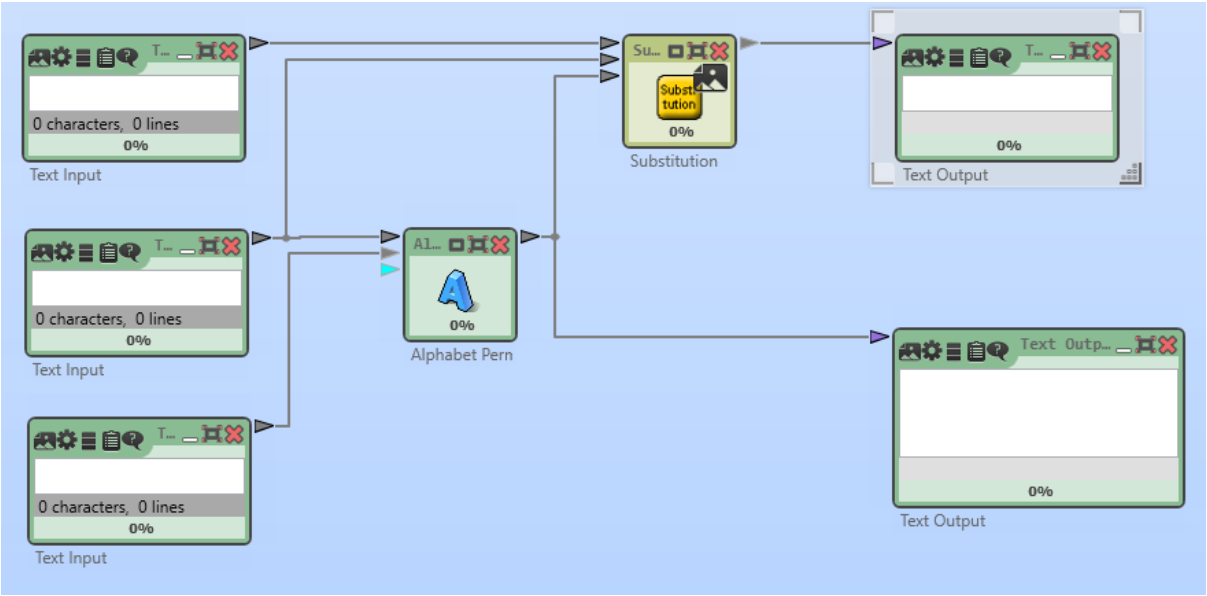
2. Εξηγήστε που μπορεί να οφείλονται τυχόν διαφοροποιήσεις μεταξύ της στήλης 3 και 4 του πίνακα.

Εργαστηριακή Άσκηση 2.Γ: Κρυπτογράφηση απλής αντικατάστασης με λέξη κλειδί

Ο Alphabet Permutator είναι component που σας επιτρέπει να δημιουργήσετε μια αντιμετάθεση του αλφάβητου με τη χρήση κάποιου κλειδιού. Σε αυτή την περίπτωση, τα μοναδικά γράμματα της λέξης κλειδί που θα χρησιμοποιηθεί θα είναι τα πρώτα γράμματα του αλφάβητου αντικατάστασης, ακολουθούμενα από τα εναπομείναντα γράμματα του αλφάβητου. Το αλφάβητο που θα δημιουργηθεί θα χρησιμοποιηθεί ως αλφάβητο αντικατάστασης.

1. Υλοποιήστε στο CT2 το σενάριο που εμφανίζεται στην για να κρυπτογραφήσετε το παρακάτω κείμενο χρησιμοποιώντας για παράδειγμα το μικρό σας όνομα ως κλειδί.

In cryptography, a substitution cipher is a method of encryption by which units of plaintext are replaced with ciphertext, according to a regular system; the "units" may be single letters (the most common), pairs of letters, triplets of letters, mixtures of the above, and so forth. The receiver deciphers the text by performing an inverse substitution.



Εικόνα 3: Σενάριο υλοποίησης της Εργαστηριακής άσκησης 2Γ (κρυπτογράφηση απλής αντικατάστασης με λέξη κλειδί).

2. Υλοποιήστε το αντίστοιχο σενάριο αποκρυπτογράφησης του αλγορίθμου. Εμφανίστε το αποκρυπτογραφημένο κείμενο ως απλό κείμενο και επιβεβαιώστε πως το plaintext αντιστοιχεί στο αρχικό κείμενο.

Εργαστηριακή Άσκηση 2.Δ: Πολλαπλή κρυπτογράφηση

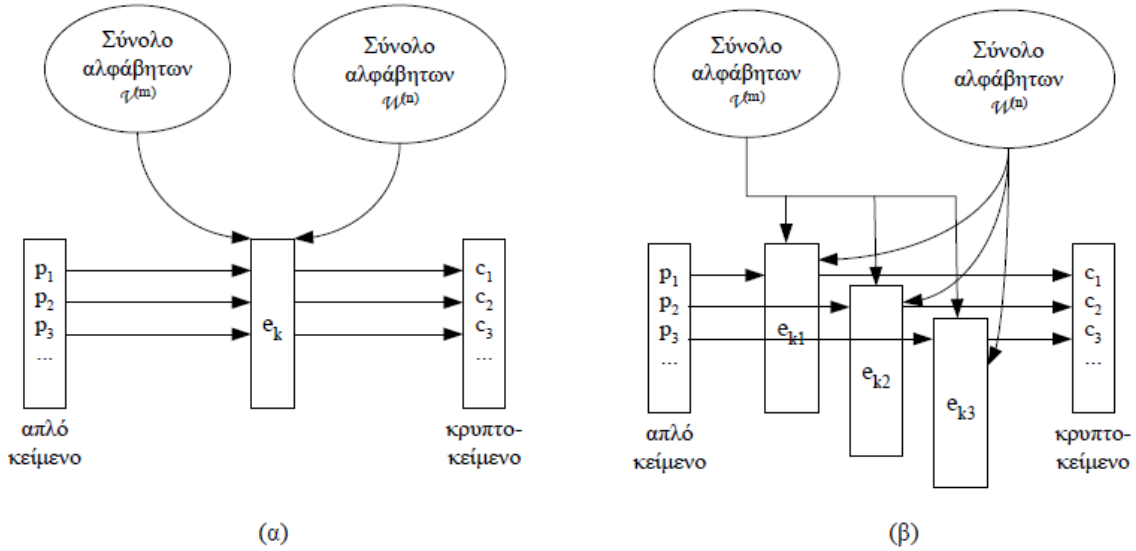
Ένας από τους μηχανισμούς που μπορούν να χρησιμοποιηθούν για την αντιμετώπιση της κρυπτανάλυσης είναι η επανακρυπτογράφηση του ήδη κρυπτογραφημένου κειμένου. Παράδειγμα τέτοιας προσέγγισης είναι και ο επαναληπτικός κώδικας Feistel.
Ως συνέχεια της άσκησης 2.Γ, υλοποιήστε ένα κρυπτοσύστημα μονοαλφαβητικής αντικατάστασης όπου το κρυπτογραφημένο κείμενο ξανακρυπτογραφείται με ένα διαφορετικό ciphertext alphabet και ελέγξτε αν και κατά πόσο ο monoalphabetic analyzer μπορεί να αποκρυπτογραφήσει το μήνυμα σας.
Για τις ανάγκες της άσκησης χρησιμοποιήστε ως αρχικό κείμενο αυτό της άσκησης 2.Γ.
Για την εκ νέου κρυπτογράφηση του κειμένου μπορείτε να χρησιμοποιήσετε και πάλι το Alphabet Permutator.

Κρυπτογράφηση πολυαλφαβητικής αντικατάστασης

Βασική αρχή

Η τεχνική της πολυαλφαβητικής αντικατάστασης βελτιώνει την απλή μονοαλφαβητική αντικατάσταση, διότι εφαρμόζει διαφορετική αντικατάσταση για κάθε ίδιο χαρακτήρα, καθώς προχωράμε κατά μήκος του κειμένου.

Σε αντίθεση με τη μονοαλφαβητική αντικατάσταση όπου η κρυπτογραφική πράξη e_k επιλέγει μια αντιστοιχία του αλφάβητου του απλού κειμένου με ένα συγκεκριμένο αλφάβητο του κρυπτοκειμένου, στην πολυαλφαβητική αντικατάσταση η κρυπτογράφηση μεταπηδά μεταξύ πολλών αλφάβητων του κρυπτοκειμένου όπως φαίνεται στην Εικόνα 4. Έτσι ένα γράμμα του απλού κειμένου μπορεί να αντιστοιχισθεί σε περισσότερα από ένα γράμματα του κρυπτοκειμένου. Αυτό έχει ως αποτέλεσμα όλες οι συχνότητες εμφάνισης των γραμμάτων να προσεγγίζουν την τιμή *1/n* (*n* το σύνολο των αλφάβητων), δηλαδή αίρεται η έμφυτη αδυναμία του μονοαλφαβητικού κρυπταλγόριθμου να κρύψει την πληροφορία περί συχνότητας των γραμμάτων.



Εικόνα 4: (α) Μονοαλφαβητική και (β) πολυαλφαβητική αντικατάσταση (Πηγή: Κάτος, Β. "Τεχνικές Κρυπτογραφίας και Κρυπτανάλυσης", εκδ. ΖΥΓΟΣ, 2003).

Ο αλγόριθμος ***VIGENERE***

Για την κατανόηση του αλγορίθμου και για την καλύτερη εφαρμογή του κατασκευάζεται ένας πίνακας γνωστός σαν πίνακας Vigenère (Πίνακας 2). Κάθε ένας από τους 24 μονοαλφαβητικούς αλγόριθμους τοποθετείται οριζόντια. Αριστερά τοποθετείται το γράμμα-κλειδί που περιγράφει τον κάθε αλγόριθμο. Στην κορυφή του πίνακα βρίσκεται το αλφάβητο στην κανονική του διάταξη.

Η διαδικασία της κρυπτογράφησης είναι η εξής: Δοθέντων ενός γράμματος-κλειδιού ***x*** και ενός γράμματος ***y*** του μηνύματος, το αντίστοιχο γράμμα του κρυπτοκειμένου προκύπτει από την τομή της γραμμής με ετικέτα ***x*** και της στήλης με ετικέτα ***y.*** Επειδή το κλειδί πρέπει να είναι τόσο μεγάλο όσο και το αρχικό μήνυμα, αυτή η μυστική λέξη συνεχώς επαναλαμβάνεται.

p / κλειδί	α β γ δ ε ζ η θ ι κ λ μ ν ξ ο π ρ σ τ υ φ χ ψ ω
Α	ΑΒΓΔΕΖΗΘΙΚΛΜΝΞΟΠΡΣΤΥΦΧΨΩ
Β	ΒΓΔΕΖΗΘΙΚΛΜΝΞΟΠΡΣΤΥΦΧΨΩΑ
Γ	ΓΔΕΖΗΘΙΚΛΜΝΞΟΠΡΣΤΥΦΧΨΩΑΒ
Δ	ΔΕΖΗΘΙΚΛΜΝΞΟΠΡΣΤΥΦΧΨΩΑΒΓ
Ε	ΕΖΗΘΙΚΛΜΝΞΟΠΡΣΤΥΦΧΨΩΑΒΓΔ
Ζ	ΖΗΘΙΚΛΜΝΞΟΠΡΣΤΥΦΧΨΩΑΒΓΔΕ
Η	ΗΘΙΚΛΜΝΞΟΠΡΣΤΥΦΧΨΩΑΒΓΔΕΖ
Θ	ΘΙΚΛΜΝΞΟΠΡΣΤΥΦΧΨΩΑΒΓΔΕΖΗ
Ι	ΙΚΛΜΝΞΟΠΡΣΤΥΦΧΨΩΑΒΓΔΕΖΗΘ
Κ	ΚΛΜΝΞΟΠΡΣΤΥΦΧΨΩΑΒΓΔΕΖΗΘΙ
Λ	ΛΜΝΞΟΠΡΣΤΥΦΧΨΩΑΒΓΔΕΖΗΘΙΚ
Μ	ΜΝΞΟΠΡΣΤΥΦΧΨΩΑΒΓΔΕΖΗΘΙΚΛ
Ν	ΝΞΟΠΡΣΤΥΦΧΨΩΑΒΓΔΕΖΗΘΙΚΛΜ
Ξ	ΞΟΠΡΣΤΥΦΧΨΩΑΒΓΔΕΖΗΘΙΚΛΜΝ
Ο	ΟΠΡΣΤΥΦΧΨΩΑΒΓΔΕΖΗΘΙΚΛΜΝΞ
Π	ΠΡΣΤΥΦΧΨΩΑΒΓΔΕΖΗΘΙΚΛΜΝΞΟ
Ρ	ΡΣΤΥΦΧΨΩΑΒΓΔΕΖΗΘΙΚΛΜΝΞΟΠ
Σ	ΣΤΥΦΧΨΩΑΒΓΔΕΖΗΘΙΚΛΜΝΞΟΠΡ
Τ	ΤΥΦΧΨΩΑΒΓΔΕΖΗΘΙΚΛΜΝΞΟΠΡΣ
Υ	ΥΦΧΨΩΑΒΓΔΕΖΗΘΙΚΛΜΝΞΟΠΡΣΤ
Φ	ΦΧΨΩΑΒΓΔΕΖΗΘΙΚΛΜΝΞΟΠΡΣΤΥ
Χ	ΧΨΩΑΒΓΔΕΖΗΘΙΚΛΜΝΞΟΠΡΣΤΥΦ
Ψ	ΨΩΑΒΓΔΕΖΗΘΙΚΛΜΝΞΟΠΡΣΤΥΦΧ
Ω	ΩΑΒΓΔΕΖΗΘΙΚΛΜΝΞΟΠΡΣΤΥΦΧΨ

Πίνακας 2: Πίνακας Vigenère (Πηγή: Κάτος, Β. "Τεχνικές Κρυπτογραφίας και Κρυπτανάλυσης", εκδ. ΖΥΓΟΣ, 2003]).

Παράδειγμα 1

Εστω το απλό κείμενο P = [ναζεικανεισηναμηζει] και το κλειδί k=[αμλετ].

Σχηματίζουμε τον πίνακα Vigenère από τα αλφαβήτα της λέξης κλειδί (5 συνολικά). Το κρυπτοκείμενο προκύπτει από το συνδυασμό αυτών των δύο.

	α	β	γ	δ	ε	ζ	η	θ	ι	κ	λ	μ	ν	ξ	ο	π	ρ	ς	τ	υ	φ	χ	ψ	ω
Α	Α	Β	Γ	Δ	Ε	Ζ	Η	Θ	Ι	Κ	Λ	Μ	Ν	Ξ	Ο	Π	Ρ	Σ	Τ	Υ	Φ	Χ	Ψ	Ω
Μ	Μ	Ν	Ξ	Ο	Π	Ρ	Σ	Τ	Υ	Φ	Χ	Ψ	Ω	Α	Β	Γ	Δ	Ε	Ζ	Η	Θ	Ι	Κ	Λ
Λ	Λ	Μ	Ν	Ξ	Ο	Π	Ρ	Σ	Τ	Υ	Φ	Χ	Ψ	Ω	Α	Β	Γ	Δ	Ε	Ζ	Η	Θ	Ι	Κ
Ε	Ε	Ζ	Η	Θ	Ι	Κ	Λ	Μ	Ν	Ξ	Ο	Π	Ρ	Σ	Τ	Υ	Φ	Χ	Ψ	Ω	Α	Β	Γ	Δ
Τ	Τ	Υ	Φ	Χ	Ψ	Ω	Α	Β	Γ	Δ	Ε	Ζ	Η	Θ	Ι	Κ	Λ	Μ	Ν	Ξ	Ο	Π	Ρ	Σ

απλό κειμ.	ν	α	ζ	ε	ι	κ	α	ν	ε	ι	σ	η	ν	α	μ	η	ζ	ε	ι
κλειδί	α	μ	λ	ε	τ	α	μ	λ	ε	τ	α	μ	λ	ε	τ	α	μ	λ	ε
κρυπτοκ.	Ν	Μ	Π	Ι	Γ	Κ	Μ	Ψ	Ι	Γ	Σ	Σ	Ψ	Ε	Ζ	Η	Ρ	Ο	Ν

Πίνακας 3: Ο πίνακας Vigenère του παραδείγματος 1 (χρησιμοποιούνται 5 αλφάβητα, όσοι και οι χαρακτήρες του κλειδιού

Επειδή το κλειδί είναι συνήθως μικρότερο από το απλό κείμενο, αυτό θα πρέπει να επαναλαμβάνεται προκειμένου να κρυπτογραφηθεί όλο το απλό κείμενο. Στο παράδειγμά μας, ο κρυπταλγόριθμος Vigenère εκτελέστηκε τέσσερις φορές. Το τελευταίο τμήμα του απλού κειμένου που κρυπτογραφήθηκε ήταν μικρότερο από το κλειδί κατά ένα γράμμα, οπότε παραλήφθηκε και το τελευταίο γράμμα του κλειδιού. Επίσης το **α** κρυπτογραφήθηκε τις δυο

φορές σε **Μ** και τη μια φορά σαν **Ε**. Παρόμοια, το **ε** κρυπτογραφήθηκε δυο φορές ως **Ι** και μια φορά ως **Ο**.

Ασφάλεια του VIGENERE

Η ασφάλεια του Vigenère εξαρτάται από το μήκος του κλειδιού, όχι μόνον για την αποτροπή της επίθεσης της εξαντλητικής αναζήτησης, γεγονός το οποίο ισχύει σε όλα τα κρυπτοσυστήματα, αλλά και για την απόκρυψη της κατανομής συχνοτήτων των γραμμάτων. Στο παράδειγμά μας χρησιμοποιήθηκαν 5 αλφάβητα από κάποιο σύνολο αλφάβητων. Η κρυπτογραφική πράξη e_k περιορίζει το σύνολο αυτό στα αλφάβητα τα οποία προκύπτουν με μετατόπιση του αρχικού αλφάβητου (e_0). Επομένως στο παράδειγμα διατίθενται συνολικά 24 διαφορετικά αλφάβητα όπως φαίνεται στον Πίνακα 1 και η ακολουθία του κλειδιού καθορίζει τη σειρά που θα επιλεχθούν τα αλφάβητα αυτά.

Κρυπτανάλυση του VIGENERE

Το πρώτο βήμα στην προσπάθεια εύρεσης του κλειδιού ενός κρυπταλγόριθμου Vigenère, είναι να βρεθεί το μέγεθος του κλειδιού αυτού. Εάν βρεθεί το μέγεθος, τότε το πρόβλημα μπορεί να αναχθεί σε πολλές μονοαλφαβητικές απλές αντικαταστάσεις, αφού σε ένα κρυπτοκείμενο, όλα τα σύμβολα που απέχουν ίση απόσταση μεταξύ τους θα ανήκουν στο ίδιο αλφάβητο.

Ο έλεγχος του Kasiski εκμεταλλεύεται το γεγονός ότι συχνά επαναλαμβανόμενα μοτίβα του απλού κειμένου θα τύχουν κρυπτογράφησης με τμήματα του κλειδιού, παραπάνω από μια φορά. Στην περίπτωση που συμβεί αυτό, το επαναλαμβανόμενο μοτίβο θα είναι φανερό και στο κρυπτοκείμενο. Για παράδειγμα, στην ελληνική γλώσσα τα μοτίβα «οσ», «στο», «απο», «νοσ», «του» συναντώνται αρκετά συχνά σε ένα κείμενο. Εάν κάποιο από τα μοτίβα αυτά τύχει να κρυπτογραφηθεί δυο φορές από το ίδιο τμήμα του κλειδιού, τα αντίστοιχα τμήματα του κρυπτοκειμένου θα είναι τα ίδια. Έτσι παρατηρώντας το κρυπτοκείμενο, ο αντίπαλος σημειώνει τις θέσεις των μοτίβων που εμφανίζονται παραπάνω από μια φορά. Μικρά σε μέγεθος μοτίβα (των δύο γραμμάτων) είναι πιθανότατα τυχαία, αλλά οποιοδήποτε μοτίβο μεγαλύτερο των τριών γραμμάτων είναι σχεδόν βέβαιο ότι δεν είναι τυχαίο και αντιστοιχεί σε μοτίβο του απλού κειμένου. Πράγματι, η πιθανότητα ενός μοτίβου τριών γραμμάτων να είναι τυχαία είναι ίση με $1/(24^3) \cong 0.0007$ και τεσσάρων γραμμάτων είναι ίση με $1/(24^4) \cong 0.00003$.
Έχοντας σημειώσει τις θέσεις του επαναλαμβανόμενου μοτίβου, ο αντίπαλος υπολογίζει τις διαδοχικές αποστάσεις που εμφανίζεται το μοτίβο αυτό. Γνωρίζοντας ότι το κλειδί θα πρέπει να είναι υποπολλαπλάσιο των αποστάσεων αυτών, παραγοντοποιεί τις αποστάσεις, οπότε το κλειδί θα είναι κάποιο από τους κοινούς αυτούς παράγοντες.

Παράδειγμα 2

Ο έλεγχος του Kasiski. Θεωρούμε το ακόλουθο κρυπτο-κείμενο:

[ΔΘΒΚΗΤΤΓΨΗ**ΓΓΘ**ΘΔΥΘΜ**ΨΧΤ**ΥΥΙΚΥΜΔ**ΨΧΤ**ΑΧΓΩΜΞ
ΟΜΝΑΞΦΠΝΛΔΨΜΕΜΞΦΠΥΘΗΞΣΕΜΝΝΨΑΥΥΖΔΘΤΥΠΣΘΥΞΝ
ΟΡΚΥΙΘΦΧΕΨΜΗΞΨΣΠΝΤΒΡΚΖΔΟΠΚΖΑΥΣΧΤΒΒΒΜΔΣΒΨΤΡΠ
ΜΗΔΔΧΟΚΔΖΨΩΟΜΗΩΔΑΨΕΠΑΓΜΝΨΚΞΔΑΒΚΣΝΝΠΘΨΟΝΟΚ
ΣΠΝΨΚΨΨΗΞΞΕΛΝΓΗΨΦΗΞΓΤΕΞΝΕΤΜΑΘΨΖΑΗΜΗΦ**ΓΓΘ**ΡΣ
ΑΜΥΣΧΓΒΚΣΦΕΣΩΞΣΑΒΥΠΧΓΥΞΝΤΓΟΩΡΚΩΜΘΝΔΑΘΗΓΦΝΑ
ΩΚΜΝΘΛΓΜΕΠΥΘΔΦΜΘΨΧΦΨΚΡΔΧΠΘΕΦΤΑΥΛΔΩΜΝΨΦΡΤΔ
ΨΔΔΜΔ**ΟΜΝ**ΡΥΗΘΑΘΞΗΤΓΒΥΤΥΓΥΚΣ]

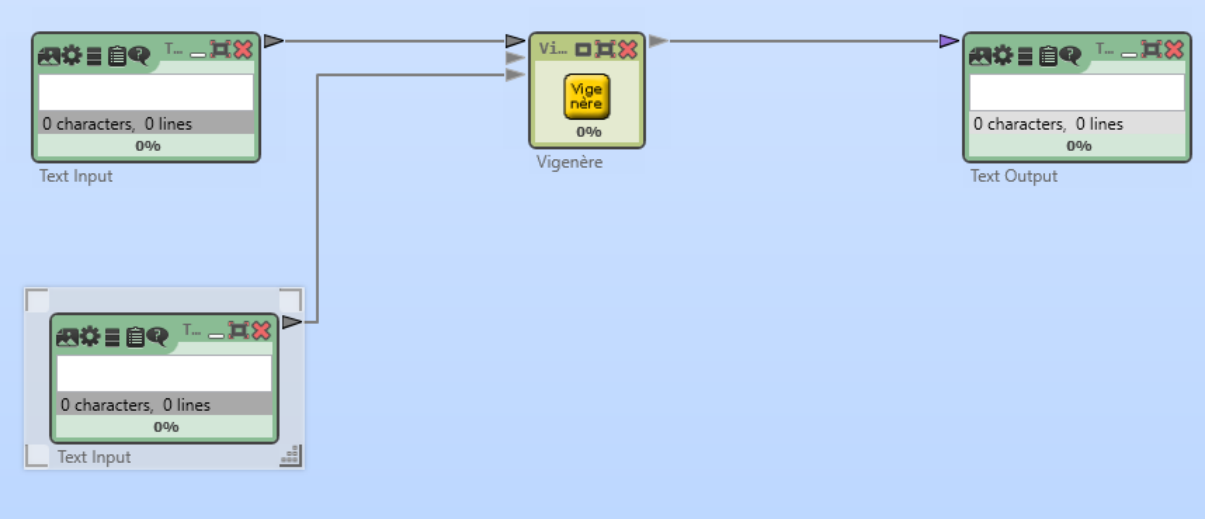
Το πρώτο στάδιο είναι η ανακάλυψη των μοτίβων. Όσο περισσότερες επαναλήψεις ενός μοτίβου και όσο μεγαλύτερο το μέγεθος του μοτίβου, τόσο μεγαλύτερη και η πιθανότητα να ανακαλύψουμε το μήκος του κλειδιού. Στο κρυπτοκείμενο του παραδείγματος είναι υπογραμμισμένα ορισμένα μοτίβα τριών χαρακτήρων. Για να θεωρηθεί μια ακολουθία χαρακτήρων ως μοτίβο, θα πρέπει η ακολουθία αυτή να εμφανισθεί στο κείμενο τουλάχιστον δύο φορές. Για τα μοτίβα που ανακαλύψαμε, υπολογίζουμε τις αποστάσεις τους:

μοτίβο	απόσταση	παράγοντες
ΓΓΘ	190	19,10,5,2
ΨΧΤ	10	10,5,2
ΟΜΝ	255	85,51,17,15,5,3

Οι παράγοντες είναι πολλαπλάσια της απόστασης. **Το μήκος του κλειδιού θα πρέπει να είναι κοινό πολλαπλάσιο όλων των αποστάσεων.** Από τα πρώτα δύο μοτίβα, το «ΓΓΘ» και το «ΨΧΤ», τα υποψήφια μήκη είναι τρία σε πλήθος (10,5,2). Ωστόσο, το 2 απορρίπτεται διότι είναι πολύ μικρό. Εάν το μήκος του κλειδιού ήταν ίσο με 2, τότε θα εμφανιζόταν πολύ περισσότερα (και μεγαλύτερα σε μέγεθος) μοτίβα. Η κατάσταση ξεκαθαρίζει με το τρίτο μοτίβο το οποίο έχει μόνο ένα κοινό παράγοντα με τα άλλα δυο, το 5. Ανακαλύπτοντας το μέγεθος του κλειδιού, ανάγουμε το κρυπτοσύστημα σε 5 κρυπτοσυστήματα μονοαλφαβητικής αντικατάστασης.

Εργαστηριακή Άσκηση 2.Ε: Κρυπτογράφηση πολυαλφαβητικής αντικατάστασης

1. Υλοποιήστε στο CT2 τις απαραίτητες τροποποιήσεις στο σενάριο που εμφανίζεται στην Εικόνα 5 προκειμένου να κρυπτογραφήστε και να αποκρυπτογραφήσετε το ονοματεπώνυμό σας χρησιμοποιώντας τον αλγόριθμο κρυπτογράφησης Vigenère. Ως κλειδί κρυπτογράφησης χρησιμοποιήστε π.χ. το επώνυμο σας με λατινικούς χαρακτήρες. Τι παρατηρείτε αναφορικά με την κρυπτογράφηση των ίδιων γραμμάτων αρχικού κειμένου;



Εικόνα 5: Σενάριο υλοποίησης της Εργαστηριακής άσκησης 2Ε (κρυπογράφηση – αποκρυπτογράφηση Vigenère).

2. Επαληθεύστε ότι οι κρυπτογραφημένοι χαρακτήρες προκύπτουν σύμφωνα με τον **Πίνακα 2** (σελίδα 7). Κατόπιν υλοποιήστε το σενάριο αποκρυπτογράφησης.
   Υπόδειξη: Για την αποκρυποκρυπτογάφηση συνδέστε ένα νέο στοιχείο *vigenère*, με την έξοδο του κρυπτογραφητή. Ρυθμίστε κατάλληλα τις παραμέτρους του στοιχείου (Action, Shift key, Alphabet)

Εργαστηριακή Άσκηση 2.Z: Κρυπτανάλυση πολυαλφαβητικής αντικατάστασης

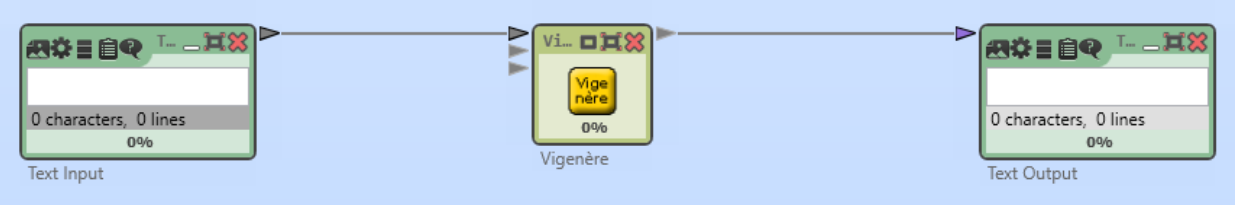
1. Εφαρμόστε τη μέθοδο ελέγχου Kasiski για την εύρεση του κλειδιού του κρυπτογραφημένου μηνύματος που σας δίνεται:

Fvvbhxla: Ixa qq txct vhb aty rfc'ox oide. Rfc hgva eofvbebuk. Ihtk gln rraw, rfc ztu'x qxicifg, iyf yhl nbxs mf. Yhl nbea mf yhlz bgamde eznb. Moide'l jwjxalunz'j eohuk iimy bex dsdlw. Pwr wvr'f kgfe tahx, num zb'p moide. Ezsb t ztxigkmo bu cauk dqkw, kvuvbeo vhb qmd. Bk qp mome fxvtfgn xtam yip uysggak gln as ye. Wf gln rraw pyiq B't xmldzvd tisgt?Gvw: Qal Qmtkzf.Jhyttenj: Ll rvy iagk bl dusi warb fm pw?[Zeh ewal]Tsdpavcp: Moi Yamiqu bz ihekpeexyi. Ut bj iie hvaugu cp. Xciz nhn, qk mome vxig ohvq. Kon tik lli ut pymk rvy xohb wrm fsgr pzvahd, sd wavv vhb xgrg fv vhbv feevdflpsz. Yhl kxg miql bk eexu cau zf bl pvvw, wavv vhb ka th tprkjl, ihxe gln wek yhlz qteie. Im za qal aareu beta lms uvmk ibpxew fdbk fsgr xpmp mv fxigu gln mvam mym qkbxt.Nxf: Eeta xdumy?Ulkwlqul: Kpxm fsg akv i pehzq. Lbbm bolvkogv mill, cau pvzb uvvz igkw yhuhmgx, swog prfo t gzflvr fhtk gln jeznhk ajxsp ar mraqx vv fontp. X iymeog wwo rvyd mbel.

Χρησιμοποιήστε το online εργαλείο που είναι διαθέσιμο στην παρακάτω διεύθυνση για την πραγματοποίηση των υπολογισμών σας.

http://www.brianveitch.com/maze-runner/frequency-analysis-vigenere/index.html

2. Εχοντας υπολογίσει το κλειδί στο προηγούμενο βήμα, υλοποιήστε το σενάριο αποκρυπτογράφησης που εμφανίζεται στην Εικόνα 6, χρησιμοποιώντας το κλειδί που υπολογίσατε στο προηγούμενο βήμα, προκειμένου να εξακριβώσετε εάν η κρυπτανάλυσή σας ήταν επιτυχής.



Εικόνα 6: Σενάριο υλοποίησης της Εργαστηριακής άσκησης 4Β (αποκρυπτογράφηση Vigenère).