Ανοικτό Πανεπιστήμιο Κύπρου

Σχολή Θετικών και Εφαρμοσμένων Επιστημών

Μεταπτυχιακή Διατριβή
στα Πληροφοριακά Συστήματα

Δημιουργία και Αξιοποίηση Ανοικτής Εκπαιδευτικής Πλατφόρμας για το Μάθημα της Κρυπτογραφίας

Ονούφριος Κωστάκης

Επιβλέπων Καθηγητής
Κωνσταντίνος Λιμνιώτης

Ιούνιος 2013

Ανοικτό Πανεπιστήμιο Κύπρου

Σχολή Θετικών και Εφαρμοσμένων Επιστημών

Δημιουργία και Αξιοποίηση Ανοικτής Εκπαιδευτικής Πλατφόρμας για το Μάθημα της Κρυπτογραφίας

Ονούφριος Κωστάκης

Επιβλέπων Καθηγητής
Κωνσταντίνος Λιμνιώτης

Η παρούσα μεταπτυχιακή διατριβή υποβλήθηκε
προς μερική εκπλήρωση των απαιτήσεων για απόκτηση

μεταπτυχιακού τίτλου σπουδών
στα Πληροφοριακά Συστήματα

από τη Σχολή Θετικών και Εφαρμοσμένων Επιστημών
του Ανοικτού Πανεπιστημίου Κύπρου

Ιούνιος 2013

Περίληψη

Η μεγάλη ανάπτυξη της πληροφορικής και των επικοινωνιών έχει επηρεάσει όλους τους τομείς της σύγχρονης εποχής. Δεν θα μπορούσε λοιπόν να μείνει ανεπηρέαστη και η εκπαιδευτική διαδικασία. Στόχος της παρούσας μεταπτυχιακής διατριβής είναι η κατασκευή εκπαιδευτικού λογισμικού, καθώς και μια σειρά μαθημάτων με αντικείμενο την θεματική ενότητα «Κρυπτογραφία». Αρχικά διερευνούνται θέματα σχετικά με το εκπαιδευτικό λογισμικό, όπως το τι είναι εκπαιδευτικό λογισμικό, τι προσφέρει στην διαδικασία μάθησης, ποιες αρχές διέπουν την σχεδίαση του, και πώς αξιολογείται. Στην συνέχεια παρουσιάζονται τα εργαλεία λογισμικού που χρησιμοποιήθηκαν για την κατασκευή τόσο της εφαρμογής αλλά και του υλικού των μαθημάτων. Έπειτα αναλύονται μαθηματικές έννοιες που χρειάζονται για την κατανόηση των κρυπτογραφικών αλγορίθμων. Μετά αναπτύσσονται θέματα που σχετίζονται με το αντικείμενο της κρυπτογραφίας και αποτελούν σημαντικό κομμάτι της ύλης που παρουσιάζεται μέσα από την εφαρμογή. Ακολούθως παρουσιάζεται η υλοποίηση των σημαντικότερων κρυπτογραφικών αλγορίθμων, καθώς και το περιβάλλον της εφαρμογής. Τέλος παρουσιάζεται το ερωτηματολόγιο που συμπληρώθηκε από τους φοιτητές της σχετικής Θεματικής Ενότητας του Ανοικτού Πανεπιστημίου της Κύπρου, με στόχο την τελική αποτίμηση του εκπαιδευτικού εργαλείου.

Summary

The rapid development of information technology and communications has greatly affected all areas of the modern era, including the educational process. The aim of this post graduate is the construction of educational software, in order to be used in a course covering the theme "Cryptography". Initially, issues relating to educational software are explored. What educational software is, what it offers the learning process, what the principles of its design are, and how it is evaluated. Then the software tools used in the construction of both the application and course material are presented. The next section analyzes mathematical concepts needed for the understanding of cryptographic algorithms. The following section focuses on issues related to the subject of cryptography, which constitute an important part of the material presented through the application. The next section presents the implementation of major cryptographic algorithms, and the application environment. In the last section, conclusions obtained from an appropriate questionnaire that has been completed by the students of the relevant Thematic Unit of Open University of Cyprus are presented, thus evaluating the effectiveness of the proposed educational tool.

Ευχαριστίες

Θα ήθελα να ευχαριστήσω τον καθηγητή μου και επιβλέπων της διατριβής κ. Λιμνιώτη Κωνσταντίνο, καθηγητή του Α.Π.Κ. για την πολύτιμη στήριξη και καθοδήγηση του.

Περιεχόμενα

Κεφάλαιο 1
Εισαγωγή

Η εποχή μας χαρακτηρίζεται από την εισαγωγή της πληροφορικής σε κάθε τομέα της καθημερινής μας ζωής. Κάθε οικογένεια, κάθε επιχείρηση και κάθε οργανισμός χρησιμοποιεί τους Ηλεκτρονικούς Υπολογιστές και τις εφαρμογές λογισμικού για διασκέδαση, για πιο παραγωγική εργασία, για επικοινωνία. Αυτή η νέα πραγματικότητα δεν θα έπρεπε να αφήσει ανεπηρέαστη και την εκπαίδευση. Φυσικά ο Η/Υ δεν μπορεί να αντικαταστήσει τον καθηγητή, μπορεί όμως να γίνει βοηθητικό μέσο ώστε να ενισχύσει τη διαδικασία της διδασκαλίας και να βοηθήσει τους εκπαιδευόμενους στην εκμάθηση των εννοιών. Ο εκπαιδευτής από απλός μετάδοσης της γνώσης εξελίσσεται σε συντονιστής, καθοδηγητής και υποστηριχτής της.

Η παραγωγή και η χρήση λοιπόν εκπαιδευτικού λογισμικού είναι το ζητούμενο προκειμένου η εκπαίδευση να εισέλθει στην νέα αυτή κατάσταση.

1.1 Αντικείμενο της Μεταπτυχιακής Διατριβής

Στο πλαίσιο της παρούσας Μεταπτυχιακής Διατριβής πραγματοποιήθηκε ανάπτυξη εκπαιδευτικού λογισμικού, με τη βοήθεια του οποίου δημιουργήθηκαν μια σειρά μαθημάτων ως υποστηρικτικό εργαλείο, με αντικείμενο την θεματική ενότητα «Κρυπτογραφία». Το σύνολο

αυτών των ηλεκτρονικών μαθημάτων απευθύνεται πρώτιστα σε φοιτητές. Περαιτέρω, επιχειρείται μία μελέτη για την αποτίμηση της χρησιμότητας του εν λόγω λογισμικού, αναφορικά με το βαθμό στον οποίο διευκολύνει η χρήση της ειδικής εκπαιδευτικής πλατφόρμας τους φοιτητές στην κατανόηση των βασικών αλγορίθμων της Θεματικής ενότητας.

1.2 Σκοπός

Το εκπαιδευτικό εργαλείο που αναπτύχθηκε, διανεμήθηκε στους σπουδαστές της Θεματικής Ενότητας «Κρυπτογραφία» του Ανοικτού Πανεπιστημίου της Κύπρου. Ο Σκοπός της διατριβής είναι η διερεύνηση των αποτελεσμάτων από την χρήση του.

1.3 Ερευνητικά Ερωτήματα

Μπορεί ειδικά διαμορφωμένο λογισμικό να υποβοηθήσει σε σημαντικό βαθμό την διαδικασία μάθησης; Μπορεί να κεντρίσει και να βελτιώσει την εμπειρία μάθησης; Τι αποτελέσματα έχει η χρήση του, στις ιδιαιτερότητες της εξ αποστάσεως εκπαίδευσης;

1.4 Δομή της Μεταπτυχιακής Διατριβής

Η παρούσα μεταπτυχιακή διατριβή είναι οργανωμένη στα ακόλουθα κεφάλαια.

1ο Κεφάλαιο: Εισαγωγή.

2ο Κεφάλαιο: Θέματα που αφορούν το Εκπαιδευτικό Λογισμικό.

3ο Κεφάλαιο: Τεχνολογίες και εργαλεία που χρησιμοποιήθηκαν για την ανάπτυξη της εφαρμογής και του εκπαιδευτικού υλικού.

4ο Κεφάλαιο: Το απαραίτητο μαθηματικό υπόβαθρο για την κατανόηση των θεμάτων της Κρυπτογραφίας.

5ο Κεφάλαιο: Θέματα κρυπτογραφίας για τα οποία δημιουργήθηκε εκπαιδευτικό υλικό.

6ο Κεφάλαιο: Περιγραφή της εφαρμογής και του σχετικού εκπαιδευτικού υλικού που δημιουργήθηκε.

7ο Κεφάλαιο: Παρουσίαση του ερωτηματολογίου και αποτίμηση του εκπαιδευτικού εργαλείου.

8ο Κεφάλαιο: Επίλογος.

Κεφάλαιο 2
Εκπαιδευτικό Λογισμικό

2.1 Τι ορίζουμε ως Εκπαιδευτικό Λογισμικό

"Εκπαιδευτικό λογισμικό" μπορεί να θεωρηθεί το λογισμικό που εξυπηρετεί εκπαιδευτικούς σκοπούς. Στην αυστηρή έννοια του όρου πρέπει να περιέχει διδακτικούς στόχους, ολοκληρωμένα σενάρια, interface και αλληγορίες με παιδαγωγική σημασία, και κυρίως επιφέρει συγκεκριμένα μαθησιακά αποτελέσματα ([61],[62]). Ο όρος εκπαιδευτικό λογισμικό συμπεριλαμβάνει συνήθως λογισμικό που βοηθά το έργο του εκπαιδευτικού. Σε άλλες περιπτώσεις ενισχύει την προσπάθεια του μαθητή παρέχοντας του εργαλεία για εξάσκηση, παραπομπές σε πηγές για αναζήτηση επιπρόσθετης γνώσης κ.λ.π. Υπάρχει εκπαιδευτικό λογισμικό που χρησιμοποιείτε για την συγκέντρωση και την οργάνωση του εκπαιδευτικού υλικού. Τέλος κάθε οργανωμένη πηγή γνώσης μπορεί να θεωρηθεί εκπαιδευτικό λογισμικό (ψηφιακές βιβλιοθήκες, ψηφιακές εγκυκλοπαίδειες καθώς και ψηφιακές συλλογές οπτικοακουστικού υλικού).

2.1.1 Είδη Εκπαιδευτικού Λογισμικού

Κατά τους Paterson και Strickland ([37],[57],[58]) το εκπαιδευτικό λογισμικό μπορεί να ταξινομηθεί με κριτήριο τη χρήση του στη μαθησιακή διαδικασία ως εξής :

- **Λογισμικό Παρουσίασης (Tutorial).** Αυτού του είδους το λογισμικό χρησιμοποιείται για να παρουσιάσει την διδαχθείσα ύλη. Κύριος στόχος είναι η εισαγωγή σε νέες έννοιες και η μετάδοση πληροφορίας στους εκπαιδευόμενους. Η μετάδοση της πληροφορίας γίνεται με χρήση κειμένου, παραδειγμάτων, animation, video, περιγραφής, ερωτήσεων και προβλημάτων.

- **Λογισμικό Εξάσκησης και Εμπέδωσης (Drill & Practice).** Το λογισμικό αυτό δίνει την δυνατότητα στον εκπαιδευόμενο να εξασκηθεί πάνω στην ύλη την οποία έχει διδαχθεί. Παρέχει ασκήσεις και ερωτήσεις σε τυχαία σειρά και με διαβάθμιση στην δυσκολία. Παρέχει επίσης ανατροφοδότηση, ενδεικτικές λύσεις και επεξηγήσεις σε ερωτήματα που εντοπίζονται αδυναμίες.

- **Λογισμικό Επίλυσης Προβλήματος (Problem solving).** Σε αυτό το είδος λογισμικού ο εκπαιδευόμενος καλείται να επιλύσει κάποιο πρόβλημα στηριζόμενος σε προηγούμενη γνώση. Το λογισμικό παρέχει το πλαίσιο και τα εργαλεία για διερευνητική μάθηση και συνήθως στοχεύει στην ανάπτυξη αλγοριθμικής σκέψης.

- **Λογισμικό Προσομοίωσης. (Simulation).** Στα συστήματα προσομοίωσης παρουσιάζεται ένα φαινόμενο του πραγματικού κόσμου στην οθόνη του Η/Υ. Η πραγματική εξέταση του φαινομένου μπορεί να είναι επικίνδυνη, πολυδάπανη, χρονοβόρα ή γενικά αδύνατη. Ο εκπαιδευόμενος ερευνά το φαινόμενο, αλλάζει παραμέτρους και παρατηρεί τα αποτελέσματα των επιλογών του.

- **Εκπαιδευτικά Παιχνίδια (Educational game)**. Ο εκπαιδευόμενος αποκτά δεξιότητες και γνώσεις παίζοντας. Αυξάνεται σίγουρα η κινητοποίηση, ο ενθουσιασμός αλλά και η προσοχή στην μαθησιακή διαδικασία. του εκπαιδευόμενου. Ένα «καλό» παιχνίδι θα πρέπει να ανταποκρίνεται στους μαθησιακούς στόχους που θέτει ο εκπαιδευτής.

- **Περιβάλλοντα Εικονικής Πραγματικότητας (Virtual Reality)**. Απαιτούν εξειδικευμένο εξοπλισμό και τεχνολογική υποδομή. Χρησιμοποιούνται για προσομοίωση πραγματικών η μη καταστάσεων. Παρέχουν ισχυρή αλληλεπίδραση επηρεάζοντας θετικά την εκπαιδευτική διαδικασία.

2.2 Σχεδίαση Εκπαιδευτικού Λογισμικού

2.2.1 Βασικές Αρχές Σχεδίασης Εκπαιδευτικού Λογισμικού

Ο Gagne ([18],[19],[20]) διατύπωσε μια στρατηγική 9 βασικών σημείων που αφορά την σχεδίαση εκπαιδευτικού λογισμικού. Σύμφωνα, λοιπόν, με τον Gagne το εκπαιδευτικό λογισμικό πρέπει να:

1. κερδίζει την προσοχή του χρήστη,
2. ενημερώνει τους χρήστες για τους μαθησιακούς στόχους του μαθήματος,
3. προκαλεί ανάκληση της προηγούμενης αποκτηθείσας γνώσης,
4. παρουσιάζει αποτελεσματικά το περιεχόμενο,
5. καθοδηγεί τον χρήστη στην διαδικασία μάθησης,
6. παρέχει κίνητρα χρήσης,
7. παρέχει ανατροφοδότηση,
8. αξιολογεί τις επιδόσεις,
9. αναπτύσσει τη μνήμη και μεταφέρει γνώση.

Τα τελευταία χρόνια η μεγάλη ανάπτυξη των πολυμέσων και του διαδικτύου επέβαλλαν τον εμπλουτισμό αυτών των βασικών σημείων. Επιπρόσθετα λοιπόν στοιχεία καλού σχεδιασμού εκπαιδευτικού λογισμικού μπορούν να θεωρηθούν και τα ακόλουθα.

- Να είναι θεμελιωμένο παιδαγωγικά.
- Να παρέχει διαβαθμισμένα επίπεδα δυσκολίας.
- Να επιτρέπει μη γραμμική μετάδοση της πληροφορίας.
- Να επιτρέπει εξατομικευμένη διδασκαλία.
- Να παρέχει βοήθεια όποτε ο χρήστης την χρειαστεί.
- Να διευκολύνει την συνεργατική μάθηση.
- Να προσφέρει την δυνατότητα επικοινωνίας σε τοπικό δίκτυο Η/Υ και στο διαδίκτυο.

- Να παρέχει την δυνατότητα επανάληψης μέρους του γνωστικού αντικειμένου.
- Να προωθεί την ανάπτυξη πνευματικών δεξιοτήτων.
- Να χρησιμοποιεί τα πολυμέσα για ενίσχυση της μαθησιακής διαδικασίας.
- Να παρέχει εναλλακτικούς τρόπους παρουσίασης της πληροφορίας.
- Να προωθεί την δημιουργικότητα.
- Να καταγράφει και να παρέχει ιστορικό της μαθησιακής πορείας του χρήστη.
- Να παρουσιάζει την ύλη μέσα από μια σειρά μαθημάτων.
- Να μπορεί να χρησιμοποιηθεί και από μη πεπειραμένους χρήστες Η/Υ.
- Να παρέχει την δυνατότητα εκτύπωσης του υλικού.

2.2.2 Σχεδιασμός υπερμεσικών εκπαιδευτικών εφαρμογών

Πολυμέσα

Τα Πολυμέσα είναι ο κλάδος της πληροφορικής τεχνολογίας ο οποίος ασχολείται με το συνδυασμό ψηφιακών δεδομένων πολλαπλών μορφών – δηλαδή κειμένου, γραφικών ακίνητης εικόνας, ήχου και βίντεο – για την αναπαράσταση, παρουσίαση, αποθήκευση, μετάδοση και επεξεργασία πληροφοριών [55].

Τα συστήματα πολυμέσων διαθέτουν τα παρακάτω βασικά χαρακτηριστικά:

- **Μη Γραμμική οργάνωση της πληροφορίας**: Η πληροφορία οργανώνεται όχι με γραμμικό τρόπο αλλά σε ένα δίκτυο από κόμβους. Κάθε κόμβος περιέχει την πληροφορία με μορφή πολλαπλών μορφών, ενώ ταυτόχρονα περιέχει και συνδέσμους προς άλλους κόμβους. Ο χρήστης ξεκινώντας από έναν αρχικό κόμβο μπορεί να εμβαθύνει σε σημεία που επιθυμεί, να προχωρήσει απορρίπτοντας σημεία που δεν τον ενδιαφέρουν κ.λ.π.

- **Αλληλεπιδραστικότητα:** Η μη γραμμική οργάνωση της πληροφορίας δημιουργεί μια ποικιλία διαφορετικών διαδρομών- επιλογών για την ροή της διαδικασίας. Ο χρήστης έχει την δυνατότητα να την ελέγχει διαμορφώνοντας την μορφή, την ταχύτητα και την σειρά στην ροή της πληροφορίας. Η ιδιότητα αυτή ονομάζεται αλληλεπιδραστηκότητα.

Υπερμέσα

Τα Υπερμέσα είναι ένα υπερσύνολο των πολυμέσων. Σε σύγκριση με τα πολυμέσα ενσωματώνουν μεγαλύτερο βαθμό διαδραστικότητας. Μια εφαρμογή υπερμέσων παρέχει

- Εύκολο και γρήγορο εντοπισμό της πληροφορίας.
- Ανατροφοδότηση στον χρήστη.
- Απαντήσεις στα ερωτήματα του χρήστη.
- Ελευθερία πλοήγησης, επιτρέποντας στον χρήστη να δημιουργεί τις δικές του διαδρομές.

2.3 Πλεονεκτήματα - Μειονεκτήματα Εκπαιδευτικού Λογισμικού

2.3.1 Πλεονεκτήματα

Η χρήση ειδικού λογισμικού κατά την εκπαιδευτική διαδικασία επιφέρει τα εξής πλεονεκτήματα:

- Η παρουσίαση του περιεχομένου γίνεται πλουσιότερη και ελκυστικότερη.
- Ο χρόνος αφομοίωσης της ύλης μειώνεται αισθητά.
- Η Εκπαίδευση μπορεί να πραγματοποιηθεί σε οποιοδήποτε χώρο και χρόνο.
- Υποστηρίζεται εξατομικευμένη εκπαίδευση.
- Προάγεται η συνεργατικότητα.

- Ενθαρρύνεται η δημιουργικότητα και η κριτική σκέψη των εκπαιδευόμενων.
- Ενισχύεται και βελτιώνεται η μάθηση.

2.3.2 Μειονεκτήματα

Η χρήση ειδικού λογισμικού κατά την εκπαιδευτική διαδικασία, εκτός των πλεονεκτημάτων της, παρουσιάζει και κάποια μειονεκτήματα. Συγκεκριμένα:

- Δυσκολίες από χρήστες χωρίς εξοικείωση στη χρήση των Η/Υ.
- Είναι σε πολλές περιπτώσεις απρόσωπος, τρόπος διδασκαλίας. Αυτό μπορεί να οδηγήσει στην απομόνωση του χρήστη.
- Σε κάποιες περιπτώσεις μπορεί να απαιτεί υψηλό κόστος εξοπλισμού (αν το λογισμικό έχει υψηλές τεχνικές απαιτήσεις).

2.4 Χαρακτηριστικά της εξ αποστάσεως Εκπαίδευσης

Η εξ αποστάσεως εκπαίδευση διαφοροποιείται της συμβατικής εκπαίδευσης κυρίως ως προς τον περιορισμό της φυσικής παρουσίας του εκπαιδευομένου σε συγκεκριμένους χώρους και σε καθορισμένους χρόνους. Η συμβατική εκπαίδευση παρουσιάζει ιδιαίτερες δυσκολίες σε περιπτώσεις εργαζομένων, σε περιπτώσεις που το πανεπιστήμιο βρίσκεται μακριά από την μόνιμη κατοικία του ενδιαφερομένου, κ.λ.π.

Το σύστημα της εξ' αποστάσεως εκπαίδευσης άρει αυτούς του περιορισμούς και τις δυσκολίες και δίνει την δυνατότητα πρόσβασης στην εκπαίδευση σε όλους. Φυσικά, η μη φυσική παρουσία του εκπαιδευομένου δημιουργεί ιδιαιτερότητες και δυσκολίες στην μετάδοση της γνώσης ([54],[60]). Αφού ο εκπαιδευτής και ο εκπαιδευόμενος δεν βρίσκονται στο ίδιο μέρος την ίδια στιγμή, πρέπει να βρεθούν άλλοι τρόποι μετάδοσης της γνώσης. Κατά συνέπεια, είναι απαραίτητο να υπάρχουν τεχνικά κανάλια επικοινωνίας μεταξύ τους για την μετάδοση της πληροφορίας και την αλληλεπίδραση μεταξύ τους.

Η χρήση λοιπόν της τεχνολογίας, Η/Υ και εξειδικευμένου λογισμικού είναι επιβεβλημένη για το συντονισμό, οργάνωση και εκτέλεση της εκπαιδευτικής διαδικασίας.

Οι ιδιαιτερότητες της εξ' αποστάσεως εκπαίδευσης αφορούν τόσο τον εκπαιδευτή, όσο και τον εκπαιδευόμενο, όπως αναλύεται στη συνέχεια.

2.4.1 Ιδιαιτερότητες για τον Εκπαιδευτή

Οι δυσκολίες στην επικοινωνία μεταξύ εκπαιδευτή και εκπαιδευόμενου δεν πρέπει να επηρεάσουν την εκπαιδευτική διαδικασία. Το εκπαιδευτικό υλικό λοιπόν πρέπει να έχει τέτοια δομή ώστε να συμπληρώνει το κενό αυτής της επικοινωνίας. Παράλληλα θα πρέπει να επιτελούνται όλες οι διδακτικές λειτουργίες της παραδοσιακής εκπαίδευσης.

Έτσι ο εκπαιδευτής θα πρέπει :

- Να καθοδηγεί τον εκπαιδευόμενο στην διαδικασία μάθησης και να οργανώνει την μελέτη του.
- Να επεξηγεί επαρκώς δύσκολα σημεία και έννοιες.
- Να του παρέχει συγκεκριμένες ασκήσεις και εργασίες.
- Να του προτείνει επιπλέον πηγές πληροφόρησης (για εμβάθυνση στην ύλη).
- Να αξιολογεί και να ενημερώνει το εκπαιδευόμενο για την πρόοδό του.
- Να τον ενθαρρύνει να συνεχίσει.
- Να του επιτρέπει να επιλέγει ελεύθερα τον τόπο, το χρόνο, καθώς και το ρυθμό της μελέτης του.

2.4.2 Ιδιαιτερότητες για τους Εκπαιδευόμενους

Οι εκπαιδευόμενοι προγραμμάτων εξ αποστάσεως εκπαίδευσης πρέπει να είναι γνώστες βασικού χειρισμού Η/Υ. Η πρόσβαση στο εκπαιδευτικό υλικό, η επικοινωνία και όλη η δομή της εκπαίδευσης στηρίζεται αποκλειστικά στην χρήση των Η/Υ και σχετικών τεχνολογιών.

Ορισμένοι μπορεί να αποδειχθούν ανεπαρκώς εκπαιδευμένοι και να χρειαστούν βοήθεια ώστε να προσαρμοστούν στον τρόπο αυτό μελέτης.

2.4.3 Το Εκπαιδευτικό Λογισμικό στην Εξ αποστάσεως Εκπαίδευση

Στην εξ αποστάσεως εκπαίδευση πέρα από το βασικό έντυπο διδακτικό υλικό, χρησιμοποιείται και εκπαιδευτικό λογισμικό για την οργάνωση, υποστήριξη, και επέκταση του. Συγκεκριμένα οι στόχοι που καλύπτει το εκπαιδευτικό λογισμικό είναι οι ακόλουθοι:

- Συμπληρώνει το έντυπο υλικό (παρουσιάζει πληροφορίες που είναι αδύνατο να ενταχθούν σε αυτό).
- Παρουσιάζει την πληροφορία με πολλαπλούς τρόπους (ήχο, εικόνα, γραφικά, βίντεο).
- Υποστηρίζει πολλαπλές μαθησιακές πηγές (βιβλία, διευθύνσεις κ.λ.π.).
- Καθοδηγεί, αλληλεπιδρά με τον χρήστη.
- Ενημερώνει για την πρόοδο του χρήστη.
- Παρέχει δραστηριότητες και ασκήσεις αυτοαξιολόγησης.
- Είναι οργανωμένο σε ενότητες, παρέχοντας ελεύθερη πλοήγηση.
- Ελέγχεται & οδηγείτε από τον χρήστη.
- Προάγει την εξατομικευμένη μάθηση.

2.5 Αξιολόγηση Εκπαιδευτικού Λογισμικού

Η αξιολόγηση του εκπαιδευτικού λογισμικού περιλαμβάνει δύο στάδια. ([54],[56]) της διαμορφωτικής αξιολόγησης (formative) και της τελικής αξιολόγησης (summative).

2.5.1 Διαμορφωτική Αξιολόγηση

Η διαμορφωτική αξιολόγηση υλοποιείται κατά το στάδιο σχεδίασης & υλοποίησης της εφαρμογής.

Αρχικά, μια ομάδα από επιλεγμένα άτομα (είτε ανήκουν στο κοινό που απευθύνεται το λογισμικό είτε είναι ειδικοί στο γνωστικό αντικείμενο που πραγματεύεται), διερευνούν για δυσλειτουργίες στην ροή εκτέλεσης της εφαρμογής. Ελέγχουν επίσης αν το περιεχόμενο ανταποκρίνεται στο επίπεδο των ικανοτήτων των εκπαιδευομένων. Τέλος καταγράφουν τις πρώτες αντιδράσεις των χρηστών του λογισμικού.

Στην δεύτερη φάση, η αξιολόγηση του λογισμικού γίνεται από εκπαιδευτές και εκπαιδευόμενους με τη χρήση αντίστοιχων ερωτηματολογίων. Το λογισμικό δοκιμάζεται (σε συνθήκες πραγματικής λειτουργίας) από εκπαιδευόμενους και εκπαιδευτές. Πρέπει να συμμετέχουν εκπαιδευόμενοι διαφορετικών δυνατοτήτων, και εκπαιδευτές με διαφορετική εμπειρία στην χρήση των Η/Υ. Οι παρατηρήσεις και οι αντιδράσεις των συμμετεχόντων χρησιμοποιούνται για την βελτίωση του λογισμικού.

2.5.2 Τελική Αξιολόγηση

Ο στόχος της τελικής αξιολόγησης είναι να ελεγχθεί η καταλληλότητα ή όχι του εκπαιδευτικού λογισμικού σε σχέση με την κάλυψη των εκπαιδευτικών στόχων που τέθηκαν κατά την δημιουργία του. Επίσης εντοπίζονται προβλήματα και τυχόν δυσκολίες της χρήση του από εκπαιδευτές και εκπαιδευόμενους (προβλήματα αποδοχής, αξιοποίησης κ.λ.π.).

Από τους σημαντικότερους παράγοντες στη διαδικασία παραγωγής του εκπαιδευτικού λογισμικού, αποτελεί η γνώμη εκπαιδευτών και εκπαιδευομένων. Με την χρήση ερωτηματολογίου μπορούμε να αποτυπώσουμε τη γνώμη τους και να συλλέξουμε σχετικά στοιχεία για περαιτέρω αξιοποίησή. Η χρήση του μας δίνει την δυνατότητα για μαζική επεξεργασία των στοιχείων (αποτελεί εργαλείο ποσοτικής έρευνας). Στο ερωτηματολόγιο όμως δεν είναι εύκολο να αποτυπωθούν οι ειδικές απαιτήσεις που θέτουν εκπαιδευτές και εκπαιδευόμενοι. Ομαδικές συζητήσεις με ομάδες εκπαιδευτικών και εκπαιδευομένων καθώς και προσωπικές συνεντεύξεις μπορούν να συμπληρώσουν αυτό το κενό (εργαλεία ποιοτικής έρευνας).

2.5.3 Ερωτηματολόγιο αξιολόγησης του λογισμικού

Το ερωτηματολόγιο αξιολόγησης του εκπαιδευτικού λογισμικού πρέπει να περιλαμβάνει την αξιολόγηση των απαιτήσεων του υλικού και του λογισμικού, των διδακτικών στόχων, του περιεχομένου, του περιβάλλοντος της εφαρμογής και του συνοδευτικού υλικού [56]. Αναλυτικά οι κατηγορίες αξιολόγησης αφορούν:

1) Υλικό και λογισμικό (Hardware & software) Απαιτήσεις σε τεχνολογία επεξεργαστή, σε μέγεθος βασικής και δευτερεύουσας μνήμης, σε απαιτήσεις δικτύωσης, σύνδεσης στο internet, ειδικό πολυμεσικό εξοπλισμό, απαιτήσεις συγκεκριμένου λειτουργικού συστήματος, κ.λ.π..

2) Τους διδακτικούς στόχους. Ελέγχουμε αν επιτυγχάνεται σε ικανοποιητικό βαθμό:

   i) Οικοδόμηση των εννοιών.

   ii) Ανάπτυξη δεξιοτήτων.

   iii) Αξιοποίηση διερευνητικής μάθησης.

   iv) Προώθηση ερευνητικής εργασίας.

   v) Ομαδική συνεργασία.

   vi) Ο επιδιωκόμενος στόχος κάθε μαθήματος.

   vii) Ο επιδιωκόμενος στόχος ολόκληρης της θεματικής ενότητας.

3) Εκπαιδευτικό περιεχόμενο.

   i) Τμηματική ενσωμάτωση της γνώσης σύμφωνα πάντα με τις δυνατότητες των εκπαιδευομένων.

   ii) Να ανταποκρίνεται στο προφίλ των εκπαιδευομένων που το χρησιμοποιούν.

   iii) Να ανταποκρίνεται στην χρήση του λογισμικού. (υλικό πολυμέσων, οδηγίες και υποδείξεις, απαντήσεις κ.λ.π.)

   iv) Η διδακτική στρατηγική να προωθεί τους μαθησιακούς στόχους που θέτει το λογισμικό.

v) Η ύλη να βρίσκεται σε αντιστοιχία με τους εκπαιδευτικούς στόχους.

vi) Να είναι ακριβές.

vii) Να είναι πλήρες.

viii) Να χρησιμοποιεί πολλαπλές αναπαραστάσεις.

ix) Να κεντρίζει το ενδιαφέρον του εκπαιδευομένου.

x) Να παρέχει πληροφορίες πως θα εκτελεστούν συγκεκριμένες διεργασίες.

xi) Να παρέχει δυνατότητα εξάσκησης μέσω ασκήσεων και δραστηριοτήτων.

xii) Να χρησιμοποιεί παραδείγματα για κατανόηση διαδικασιών.

xiii) Να μην παρουσιάζει ορθογραφικά και συντακτικά λάθη.

4) Περιβάλλον της εφαρμογής

i) Απλή και κατανοητή διασύνδεση με τον χρήστη

Κεφάλαιο 3
Τεχνολογίες & Εργαλεία

Για την κατασκευή της εκπαιδευτικής πλατφόρμας καθώς και του εκπαιδευτικού υλικού στο πλαίσιο της παρούσας εργασίας χρησιμοποιήθηκαν διάφορα εργαλεία λογισμικού. Στην συνέχεια του κεφαλαίου γίνεται αναφορά στα χαρακτηριστικά τους.

3.1 Γλώσσες Προγραμματισμού

3.1.1 HTML

Η HTML (HyperText Markup Language) είναι μια γλώσσα μορφοποίησης υπερκειμένου. Αποτελεί την βασική γλώσσα δόμησης των ιστοσελίδων στο Internet. Επιτρέπει την παρουσίαση πολυμεσικού περιεχομένου σε μια σελίδα (κείμενο, εικόνα, ήχο και βίντεο). Χρησιμοποιεί ένα σύνολο ετικετών (tags) για να περιγράψει την μορφοποίηση και την ενσωμάτωση του υλικού που υποστηρίζει. Οι ετικέτες περιγράφουν στο πρόγραμμα πλοήγησης (Browser) πώς θα παρουσιάσει αυτό το υλικό.

Μερικές βασικές ετικέτες είναι οι ακόλουθες [49]:

- <html> & </html>. Το <html> σημαίνει έναρξη εγγράφου html. Το </html> σημαίνει τέλος εγγράφου html. Ενδιάμεσα στις δυο αυτές ετικέτες τοποθετούμε τις πληροφορίες του εγγράφου

- <head> & </head>. Ανάμεσα σε αυτές τις δυο ετικέτες τοποθετούμε στοιχεία που αφορούν το έγγραφο, όπως το συγγραφέα, τον τίτλο κ.λ.π.

- <title> & </title> Ότι τοποθετούμε ανάμεσα σε αυτές τις δύο ετικέτες τοποθετείτε στην γραμμή τίτλου του παραθύρου που εμφανίζει την σελίδα.

- <body> & </body> Ανάμεσα στις δύο ετικέτες τοποθετείται όλο το περιεχόμενο της σελίδας μας.

- & . Ότι τοποθετηθεί ανάμεσα στις δύο ετικέτες εμφανίζεται με έντονα γράμματα.

- & . Ότι τοποθετηθεί ανάμεσα στις δύο ετικέτες εμφανίζεται με πλάγια γράμματα.

- <u> & </u>. Ότι τοποθετηθεί ανάμεσα στις δύο ετικέτες εμφανίζεται με υπογράμμιση.

- <tt> & </tt>. Ότι τοποθετηθεί ανάμεσα στις δύο ετικέτες εμφανίζεται με στυλ γραφομηχανής.

- <strike> & </strike>. Ότι τοποθετηθεί ανάμεσα στις δύο ετικέτες εμφανίζεται με στυλ διακριτής διαγραφής.

- [&]. Ότι τοποθετηθεί ανάμεσα στις δύο ετικέτες εμφανίζεται σαν εκθέτης.

- _&. Ότι τοποθετηθεί ανάμεσα στις δύο ετικέτες εμφανίζεται σαν δείκτης.

- <small> & </small>. Ότι τοποθετηθεί ανάμεσα στις δύο ετικέτες εμφανίζεται με μικρά γράμματα.

- <big> & </big>. Ότι τοποθετηθεί ανάμεσα στις δύο ετικέτες εμφανίζεται με μεγάλα γράμματα.

- & . Ότι τοποθετηθεί ανάμεσα στις δύο ετικέτες εμφανίζεται σαν μια ενιαία παράγραφος.

- <h1> & </h1>. Ότι τοποθετηθεί ανάμεσα στις δύο ετικέτες εμφανίζεται σαν επικεφαλίδα. Υποστηρίζονται ετικέτες 6 μεγεθών (1-6). Έαν θέλουμε μικρότερο μέγεθος ετικέτας επιλέγουμε <h2>….</h2> κ.ο.κ.

Μια ακόμα πολύ σημαντική ετικέτα είναι η ετικέτα font. Η σημαντική διαφορά σε αυτή την ετικέτα είναι ότι χρησιμοποιεί παραμέτρους (ιδιότητες) για να μορφοποιήσει το κείμενο. Για παράδειγμα η ακόλουθη σύνταξη:

 το κείμενο μας

έχει ως αποτέλεσμα να διαμορφώσει το «κείμενο μας» με γραμματοσειρά verdana μεγέθους 2 και χρώματος κόκκινου.

Για την εισαγωγή εικόνας χρησιμοποιείτε η ετικέτα image. Η ετικέτα Image δεν χρησιμοποιεί ετικέτα τέλους. Η σύνταξη της είναι η ακόλουθη: <img src=”xxxxx.jpg”> όπου xxxxx.jpg το όνομα του αρχείου της εικόνας.

Για την εισαγωγή συνδέσμου χρησιμοποιείται η ετικέτα <a>. Ένα παράδειγμα χρήσης της ετικέτας είναι

 το κείμενο του συνδέσμου .

Ο προορισμός του συνδέσμου δηλώνεται στην ιδιότητα href.

Για την εισαγωγή ενός Java Applet στην σελίδα μας χρησιμοποιείται η ετικέτα <APPLET> </APPLET>. Ένα παράδειγμα σύνταξης της ακόλουθης ετικέτας είναι <APPLET codebase="classes" code="crypto/DiffieHellmanApplet.class" width=800 height=600> </APPLET> όπου στην ιδιότητα code γράφουμε την διαδρομή για την βασική κλάση του applet, και στις ιδιότητες width & height το πλάτος & ύψος της επιφάνειας που θα καλύψει στην σελίδα μας.

3.1.2 Java

Η γλώσσα προγραμματισμού JAVA ([13],[23],[53]) είναι μια γλώσσα προγραμματισμού που γνωρίζει μεγάλη ανάπτυξη και αποδοχή τα τελευταία χρόνια. Διαθέτει ιδιαίτερα χαρακτηριστικά που τη διαφοροποιούν από τις παραδοσιακά γνωστές γλώσσες προγραμματισμού.

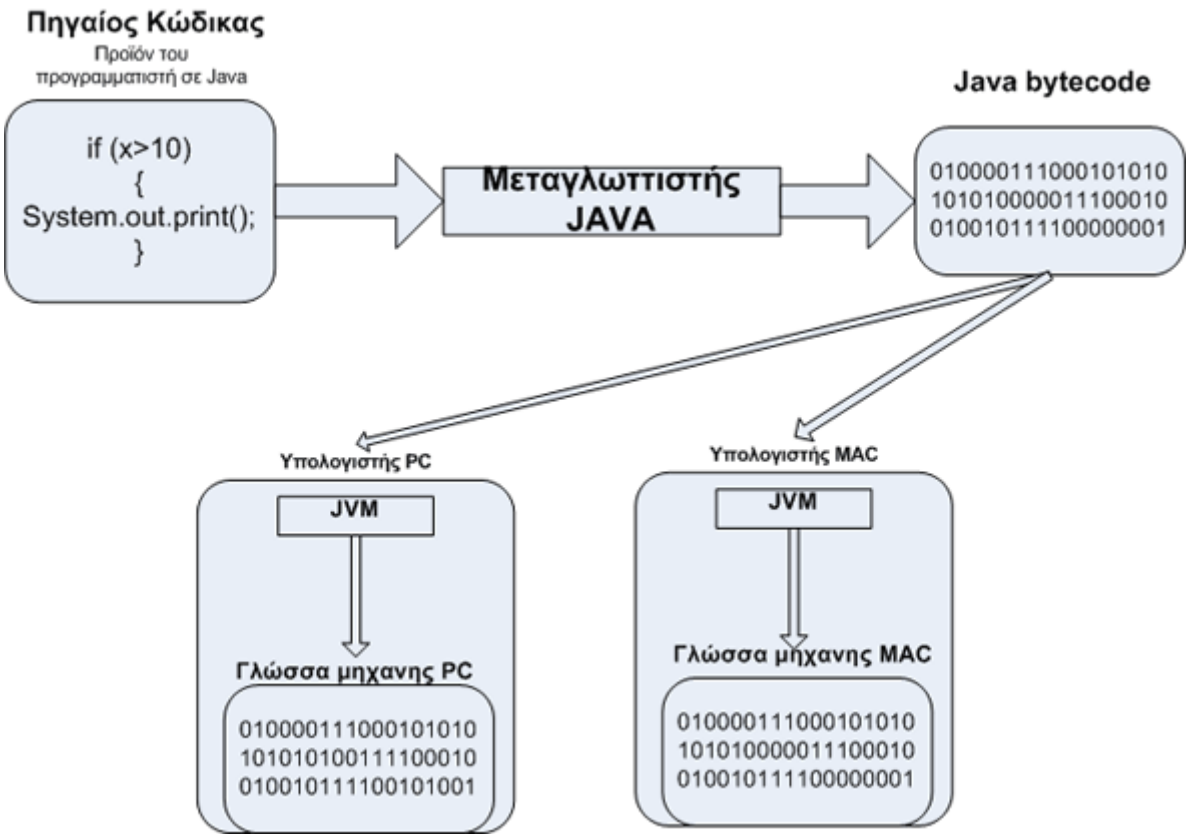
Τα χαρακτηριστικά της Java

Το ενδεχομένως πιο σημαντικό χαρακτηριστικό της Java είναι η ανεξαρτησία της από το λειτουργικό σύστημα αλλά και από την τεχνολογία του υλικού. Ένα πρόγραμμα σε JAVA εκτελείται ακριβώς το ίδιο σε περιβάλλον Windows, Linux, Unix και Macintosh, χωρίς να χρειάζεται διαδικασία μεταγλώττισης ή οποιαδήποτε μετατροπή πηγαίου κώδικα. Αντίστοιχα, προγράμματα java γραμμένα για κινητές συσκευές εκτελούνται αυτούσια σε συσκευές διαφορετικών κατασκευαστών.

Για να καταφέρει η JAVA να κάνει τα προγράμματα της ανεξάρτητα του λειτουργικού συστήματος και του υλικού πρόσθεσε ένα επίπεδο ανάμεσα στον πηγαίο κώδικα και τον εκτελέσιμο κώδικα. Το επίπεδο αυτό το διαχειρίζεται η Εικονική μηχανή της JAVA (Java virtual Machine)

Η εικονική μηχανή της Java

Η διαδικασία μεταγλώττισης σε κάποιο πρόγραμμα Java παράγει ένα πλήθος από αρχεία .class (bytecode). Τα αρχεία class δεν είναι άμεσα εκτελέσιμα. Για να εκτελεστούν απαιτούν ένα πρόγραμμα που πρέπει να είναι εγκατεστημένο, και αναλαμβάνει να διαβάσει και να εκτελέσει τα αρχεία class. Η εικονική μηχανή της JAVA (JAVA Virtual Machine) μεταφράζει τα αρχεία σε γλώσσα μηχανής που υποστηρίζεται από το λειτουργικό σύστημα και τον επεξεργαστή. Η εικονική μηχανή της JAVA εξαρτάτε από το λειτουργικό σύστημα και την αρχιτεκτονική του Η/Υ. Ο χρήστης που θέλει να εκτελεί εφαρμογές JAVA πρέπει προηγούμενα να έχει εγκαταστήσει το JVM που αντιστοιχεί στο λειτουργικό σύστημα και τον Η/Υ που χρησιμοποιεί.



Εικόνα 3.1 πηγή: http://static.greektuts.net [23]Διαδικασία Εκτέλεσης Προγράμματος JAVA

Ο προγραμματιστής και ο χρήστης του προγράμματος δεν έχει άμεση πρόσβαση στον Η/Υ που εκτελείται το πρόγραμμα. Όλες οι λειτουργίες διεκπεραιώνονται μέσω της εικονικής μηχανής της JAVA. Αυτό προσθέτει ένα επίπεδο ασφάλειας, αφού προβληματικός ή επιβλαβής κώδικας μπορεί να ανιχνευτεί από την εικονική μηχανή, η οποία δεν επιτρέπει την εκτέλεση του.

Επιδόσεις

Η χρήση της εικονικής μηχανής, παρά τα πλεονεκτήματα που προσφέρει, παρουσιάζει μειωμένες επιδόσεις σε σύγκριση με άλλες γλώσσες προγραμματισμού υψηλού επιπέδου (C η C++). Παρόλα αυτά η ταχύτητα της είναι ικανοποιητική.

Ολοκληρωμένο περιβάλλον ανάπτυξης (IDE)

Το μόνο που χρειάζεται κάποιος για να γράψει κώδικα σε java, είναι ένας επεξεργαστής κειμένου. (text editor). Υπάρχουν όμως ολοκληρωμένα περιβάλλοντα ανάπτυξης που διανέμονται ελεύθερα και διαθέτουν εργαλεία που διευκολύνουν τη συγγραφή και την αποσφαλμάτωση του κώδικα.

3.1.3 Java Applets

Ένα Java applet είναι μια βοηθητική εφαρμογή που ενσωματώνεται σε μια ιστοσελίδα. Ουσιαστικά, είναι πρόγραμμα java με κάποιους επιπλέον περιορισμούς σε σύγκριση με μια κλασική εφαρμογή Java. Εκτελείται από την εικονική μηχανή της Java (JVM) σε ξεχωριστή διαδικασία από το πρόγραμμα περιήγησης, παρουσιάζεται όμως μέσω αυτού. Το Java applet εκτελείται πολύ πιο γρήγορα από κώδικα Java Script, υπολείπεται όμως σε ταχύτητα από γλώσσες που χρησιμοποιούν compiler, όπως είναι για παράδειγμα η C++. Επιπλέον μπορεί να χρησιμοποιήσει 3D επιτάχυνση υλικού. Είναι λοιπόν ιδανικό για εφαρμογές με απαιτήσεις οπτικοποίησης φαινομένων (visualizations) που πρέπει να παρουσιαστούν σε μια ιστοσελίδα.

Όπως οι κλασικές εφαρμογές JAVA παρουσιάζει ανεξαρτησία από το λειτουργικό σύστημα και το υλικό.

Πλεονεκτήματα

Ένα Java applet έχει όλα τα ακόλουθα πλεονεκτήματα:

- Λειτουργεί χωρίς καμία μετατροπή σε όλα τα γνωστά λειτουργικά συστήματα Linux, Microsoft Windows and OS X.
- Υποστηρίζεται από τα περισσότερα προγράμματα περιήγησης.
- Το ίδιο Applet συνήθως συνεργάζεται με οποιαδήποτε έκδοση της Java είναι εγκατεστημένη στο μηχάνημα. Δεν απαιτείται δηλαδή συγκεκριμένη έκδοση της java. Ωστόσο, αν μια εφαρμογή απαιτεί μια νεότερη έκδοση του Java Runtime Environment (JRE), ο πελάτης θα αναγκαστεί να εγκαταστήσει την ενημερωμένη αυτή έκδοση.

- Τα περισσότερα προγράμματα περιήγησης μεταφέρουν το applet στην cache. Έτσι, μετά την 1η φορά που εκτελούμε το Applet, η φόρτωση γίνεται πολύ γρήγορα.

- Μπορεί να γίνει μεταφορά φορτίου εργασίας από τον Server στους Client (το Applet εκτελείται στους Clients). Με αυτόν τον τρόπο, μια WEB εφαρμογή γίνεται πιο επεκτάσιμη. Περισσότεροι χρήστες δεν επιβαρύνουν την απόδοση του συστήματος.

- Ένα «μη υπογεγραμμένο» Applet δεν έχει πρόσβαση σε τοπικούς πόρους στον Η/Υ. Έχει μόνο πρόσβαση στον Server από όπου το κατεβάσαμε. Αυτό το κάνει πιο ασφαλές από τα υπόλοιπα είδη εκτελέσιμων αρχείων. Ωστόσο, ένα υπογεγραμμένο Applet μπορεί να έχει πλήρη πρόσβαση στο μηχάνημα του χρήστη, εφόσον βέβαια αυτός το αποδεχτεί.

- Είναι γρήγορο και δεν υστερεί σημαντικά σε ταχύτητα σε σχέση με το συνηθισμένο εγκατεστημένο λογισμικό.

Μειονεκτήματα

Ένα Java applet έχει όλα τα ακόλουθα μειονεκτήματα:

- Απαιτεί το πρόσθετο της Java.

- Μερικά προγράμματα περιήγησης, κυρίως για κινητά που εκτελούν το iOS της Apple ή Android δεν υποστηρίζουν Applets.

- Κάποιοι οργανισμοί επιτρέπουν μόνο λογισμικό που είναι εγκατεστημένο από διαχειριστές των συστημάτων. Έτσι οι χρήστες μπορούν μόνο να εκτελούν applet μόνο αν ο διαχειριστής έχει εγκαταστήσει το πρόσθετο της Java. Οι ίδιοι σαν απλοί χρήστες δεν μπορούν να κάνουν εγκατάσταση του Java plug-in.

- Όπως και με κάθε client-side scripting, οι περιορισμοί ασφαλείας μπορεί να καταστήσουν δύσκολη ή ακόμα και αδύνατη για ένα μη υπογεγραμμένο applet, την επίτευξη των επιθυμητών στόχων. Ωστόσο, απλά με επεξεργασία του αρχείου java.policy στην εγκατάσταση Java JRE, μπορεί κανείς να επιτρέψει την πρόσβαση στους τοπικούς πόρους, ή σε άλλες πηγές του δικτύου, εκτός από την πηγή δίκτυου που εξυπηρετούσε το applet.

- Ορισμένα applets απαιτούν συγκεκριμένη έκδοση του JRE.

- Αν ένα applet απαιτεί νεότερη έκδοση του JRE από αυτήν που είναι εγκατεστημένη στο σύστημα, τότε ο χρήστης πρέπει να περιμένει μέχρι να ολοκληρωθεί το κατέβασμα και η εγκατάσταση της νεότερης έκδοσης.

3.2 Ολοκληρωμένα Περιβάλλοντα ανάπτυξης (IDE)

Η πιο απλή εφαρμογή JAVA μπορεί να υλοποιηθεί με την ακόλουθη διαδικασία. Αρχικά γράφουμε το πρόγραμμα χρησιμοποιώντας ένα απλό επεξεργαστή κειμένου (editor). Αποθηκεύουμε το αρχείο με κατάληξη «.java». Στην συνέχεια εκτελούμε την μεταγλώττιση από την γραμμή εντολών δημιουργώντας το αρχείο με το κώδικα bytecode, το αρχείο class. Τέλος, εκτελούμε το αρχείο class (μέσω της εικονικής μηχανής).

Ένα IDE εκτελεί όλες τις προηγούμενες εργασίες με το πάτημα ενός κουμπιού. Φυσικά δεν κάνει μόνο αυτό. Προσφέρει πολλές επιπλέον ευκολίες και χρήσιμα εργαλεία στους προγραμματιστές. Στόχος είναι να αυξηθεί η αποδοτικότητα και η παραγωγικότητα των προγραμματιστών. Είναι ουσιαστικά μια σουίτα λογισμικού που περιλαμβάνει κάποιον επεξεργαστή κειμένου για την συγγραφή του κώδικα, έναν μεταγλωττιστή, εργαλεία αυτόματης παραγωγής κώδικα, debugger για αποσφαλμάτωση του κώδικα, συνδέτη και εργαλεία κατασκευής γραφικού περιβάλοντος διασύνδεσης χρήστη (GUI).

3.2.1 NetBeans

Το NetBeans IDE επιτρέπει στους προγραμματιστές να αναπτύξουν γρήγορα και εύκολα εφαρμογές Java για Υπολογιστές, κινητά καθώς και εφαρμογές web ([25],[35]). Υποστηρίζει επίσης την ανάπτυξη εφαρμογών σε PHP, C / C + +. Είναι δωρεάν και ανοιχτού κώδικα (open source), ενώ επίσης έχει μια μεγάλη κοινότητα χρηστών και προγραμματιστών σε όλο τον κόσμο.

Ο επεξεργαστής κειμένου του NetBeans μπορεί να εντοπίσει συντακτικά λάθη κατά την πληκτρολόγηση και βοηθά με pop-up τεκμηρίωση και με έξυπνη συμπλήρωση κώδικα. Τονίζει τον πηγαίο κώδικα συντακτικά και σημασιολογικά. Ο συντάκτης υποστηρίζει πολλές γλώσσες,

όπως Java, C / C + +, XML, HTML, PHP, Groovy, Javadoc, Javascript και JSP. Μπορεί να επεκταθεί για να υποστηρίξει και άλλες γλώσσες.

Παρέχει δυνατότητα αυτόματης δημιουργίας κώδικα όπως μεθόδων setValue, getValue, δομές try – catch κ.λ.π. Σε περιπτώσεις λαθών προτείνει διορθώσεις στον κώδικα. Επίσης μορφοποιεί τον κώδικα με χρώματα και εσοχές ώστε να είναι εύκολος ο οπτικός έλεγχος του κώδικα.

Παρέχει στατικά εργαλεία ανάλυσης (FindBugs tool) για τον εντοπισμό και τον καθορισμό κοινών προβλημάτων σε κώδικα Java. Επιπλέον, το εργαλείο NetBeans Debugger επιτρέπει να τοποθετηθούν σημεία διακοπής στον κώδικα, να γίνει βηματική εκτέλεση, και να παρακολουθηθούν οι διάφορες μεταβλητές της εφαρμογής σε όλη την διάρκεια του ελέγχου.

Είναι το ίδιο γραμμένο σε Java. Έτσι μπορεί να εγκατασταθεί σε όλα τα λειτουργικά συστήματα που υποστηρίζουν Java (Windows, Linux & MacOS).

Η κοινότητα του NetBeans είναι μεγάλη και ενεργή. Πολλοί χρήστες συμμετέχουν στην ανάπτυξη νέων πρόσθετων χαρακτηριστικών συνεχώς. Έτσι, μόνιμα επεκτείνεται και βελτιώνεται.

3.3 Βάσεις Δεδομένων

3.3.1 Εισαγωγή στις Βάσεις Δεδομένων

Οι άνθρωποι σήμερα έχουν την δυνατότητα να ανταλλάσσουν και να μεταφέρουν πληροφορίες ελεύθερα, έχοντας άμεση πρόσβαση σε γνώσεις που θα ήταν δύσκολο ή αδύνατο να βρεθούν στο παρελθόν. Η εποχή μας χαρακτηρίζεται πλέον ως εποχή της πληροφορίας. Η αποδοτική διαχείριση της πληροφορίας μας κάνει πιο ανταγωνιστικούς και πιο παραγωγικούς στην εργασία μας. Τα συστήματα βάσεων δεδομένων [63] αναλαμβάνουν να διαχειριστούν αποδοτικά το τεράστιο όγκο των πληροφοριών που δημιουργούνται καθημερινά.

3.3.2 Προβλήματα στην Οργάνωση Αρχείων

Μια αρχική προσέγγιση στην διαχείριση της πληροφορίας ήταν να διατηρούνται ξεχωριστές εφαρμογές και ξεχωριστά αρχεία για κάθε διαφορετική πηγή. Για παράδειγμα, θα τηρούνταν ξεχωριστό αρχείο πελατών και διαφορετικό αρχείο για παραγγελίες πελατών. Τα δυο αρχεία λειτουργούσαν αυτόνομα και ανεξάρτητα. Αυτή η πρακτική διαπιστώθηκε ότι προκαλούσε διάφορα προβλήματα όπως:

- Πλεονασμός (data redundancy). Τα ίδια δεδομένα επαναλαμβάνονταν σε διαφορετικά αρχεία. Στο παράδειγμα που προαναφέραμε θα είχαμε κάποιες πληροφορίες που αφορούν τους πελάτες και στα δύο αρχεία (πχ η διεύθυνση του πελάτη).

- Ασυνέπεια (data inconsistency). Όταν κάποιες πληροφορίες τηρούνται σε δύο αρχεία, μια διόρθωση που θα γίνει στο ένα αρχείο θα δημιουργήσει ασυνέπεια, αν δεν εφαρμοστεί και στο άλλο αρχείο.

- Αδυναμία κοινής χρήσης (data sharing). Πολλαπλοί χρήστες ή εφαρμογές να μπορούν να προβάλουν και να ενημερώνουν την ίδια χρονική στιγμή το ίδιο αρχείο.

- Αδυναμία προτυποποίησης. Ο διαφορετικός τρόπος που οι προγραμματιστές τηρούσαν τα αρχεία (διαφορετικές αναπαραστάσεις και οργάνωση) προκαλούσε προβλήματα στην ανταλλαγή δεδομένων μεταξύ διαφορετικών συστημάτων.

3.3.3 Βάσεις Δεδομένων

Ένα σύστημα βάσης δεδομένων (Β.Δ.) είναι ένα ηλεκτρονικό σύστημα εγγραφών. Χρησιμοποιεί Η/Υ και λογισμικό για να αποθηκεύει, ενημερώνει και να αποδίδει πληροφορίες όταν του ζητηθεί.

Μία βάση δεδομένων είναι μια συλλογή ηλεκτρονικών αρχείων δεδομένων. Ο χρήστης αλληλεπιδρά με την Β.Δ. εκτελώντας συγκεκριμένες λειτουργίες. Οι σημαντικότερες από αυτές είναι οι εξής:

- προσθήκη νέων αρχείων.

- Διαγραφή υπαρχόντων αρχείων από την Β.Δ.

- Προσθήκη δεδομένων σε υπάρχον αρχείο.

- Ενημέρωση δεδομένων σε υπάρχον αρχείο.
- Ανάκτηση δεδομένων από αρχείο.
- Διαγραφή δεδομένων από αρχείο.

Τα πλεονεκτήματα ενός συστήματος βάσης δεδομένων (ΣΔΒΔ), σε σύγκριση με τις προηγούμενες προσπάθειες διαχείρισης της πληροφορίας είναι σημαντικά και κυρίως συνοψίζονται στα εξής:

- Ο πλεονασμός μειώνεται στο ελάχιστο. Εδώ τα δεδομένα αντιμετωπίζονται σαν συλλογές δεδομένων και όχι αυτόνομα αρχεία. Τα διάφορα αρχεία αλληλοσυσχετίζονται και αλληλεπιδρούν και δεν είναι πλέον απαραίτητη η επανάληψη της ίδιας πληροφορίας σε διαφορετικά αρχεία.
- Μπορεί να αποφευχθεί η ασυνέπεια των δεδομένων. Στο ΣΔΒΔ μπορούμε να θέσουμε κανόνες και να γίνεται αυτόματη διαδοχική ενημέρωση κατά την μεταβολή κοινής πληροφορίας που υπάρχει σε δύο διαφορετικά σημεία της βάσης δεδομένων.
- Τα δεδομένα πλέον είναι κοινόχρηστα. Πολλοί διαφορετικοί χρήστες αλλά και διαφορετικές εφαρμογές μπορούν να μοιράζονται τα δεδομένα της βάσης δεδομένων.
- Μπορούν να καθορίζονται πρότυπα, παρέχοντας την δυνατότητα για εύκολη ανταλλαγή δεδομένων.
- Εφαρμόζονται διαδικασίες & περιορισμοί ασφαλείας. Έχουν ενσωματωμένο σύστημα διαχείρισης χρηστών και δικαιωμάτων αποδίδοντας το επίπεδο πρόσβασης που απαιτείτε σε κάθε περίπτωση χρήστη.
- Διασφαλίζει την ακεραιότητα δεδομένων. Όταν ή ίδια πληροφορία υπάρχει σε δύο ή περισσότερα σημεία στη βάση δεδομένων, και επέλθει μεταβολή μόνο σε κάποια από τα σημεία αναφοράς της και όχι σε όλα, τότε έχουμε πρόβλημα ακεραιότητας δεδομένων. Αυτή η κατάσταση προέρχεται από τον πλεονασμό που αναφέρθηκε προηγουμένως. Η χρήση του συστήματος βάσεων δεδομένων περιορίζει στο ελάχιστο τον πλεονασμό, άρα και το πρόβλημα της ακεραιότητας.

3.3.4 SQLite

Η SQLite είναι ένα σύστημα βάσεων δεδομένων συμβατό με το ISO SQL [47]. Σε αντίθεση με τις περισσότερες άλλες βάσεις δεδομένων SQL, η SQLite δεν έχει μια ξεχωριστή λειτουργία διακομιστή (Server). Η SQLite διαβάζει και γράφει κατευθείαν σε συνηθισμένα αρχεία στο δίσκο. Μια πλήρης βάση δεδομένων SQL με πολλαπλούς πίνακες, δείκτες, προβολές, περιέχεται σε ένα ενιαίο αρχείο στο δίσκο. Η μορφή του αρχείου βάσης δεδομένων παρουσιάζει χαρακτηριστικά ανεξαρτησίας από το υλικό και το λειτουργικό σύστημα (cross-platform). Μπορεί να μεταφερθεί τόσο σε συστήματα 32-bit όσο και σε 64-bit ή μεταξύ μηχανημάτων διαφορετικών αρχιτεκτονικών. Αυτά τα χαρακτηριστικά καθιστούν την SQLite μια δημοφιλής επιλογή.

Η SQLite είναι μια συμπαγής βιβλιοθήκη. Με όλα τα χαρακτηριστικά ενεργοποιημένα, το μέγεθος της βιβλιοθήκης μπορεί να είναι μικρότερο από 350KiB, ανάλογα με την πλατφόρμα-για την οποία προορίζεται. Η SQLite μπορεί επίσης να τρέξει με ελάχιστες απαιτήσεις σε μνήμη RAM., κάνοντας την μια δημοφιλής επιλογή για μηχανισμό διαχείρισης βάσεων δεδομένων σε συσκευές με περιορισμένη μνήμη όπως κινητά τηλέφωνα, PDAs, και MP3 players. Γενικά όσο περισσότερη διαθέσιμη μνήμη υπάρχει τόσο ταχύτερα τρέχει η SQLite. Παρ 'όλα αυτά, οι επιδόσεις είναι αρκετά καλές ακόμα και σε περιβάλλοντα με χαμηλή μνήμη.

Η SQLite πριν από κάθε έκδοση ελέγχεται διεξοδικά και γενικώς θεωρείται αξιόπιστη βάση δεδομένων. Φυσικά μπορεί να διαπιστωθούν διάφορα bugs, όμως, σε αντίθεση με κάποιες άλλες λύσεις (κυρίως εμπορικούς ανταγωνιστές) οι διορθώσεις είναι άμεσες.

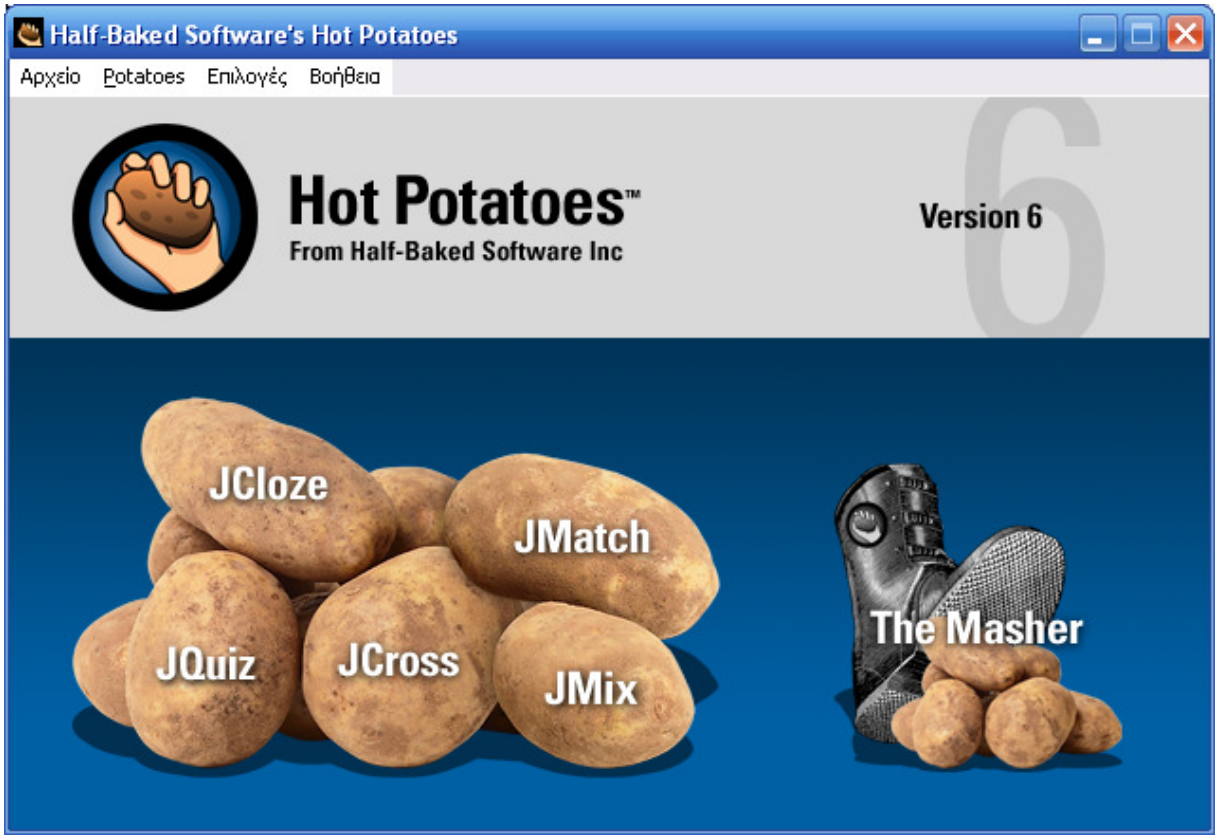
Η SQLite υποστηρίζεται από μια διεθνή ομάδα από προγραμματιστές. Οι προγραμματιστές συνεχίζουν να επεκτείνουν τις δυνατότητες της SQLite ενισχύοντας την αξιοπιστία και τις επιδόσεις της, διατηρώντας παράλληλα συμβατότητα προς τα πίσω όσο αφορά την σύνταξη της SQL και την μορφή του αρχείου της βάσης δεδομένων. Ο πηγαίος κώδικας είναι απολύτως ελεύθερος σε όποιον θέλει. Επίσης είναι διαθέσιμη και με επαγγελματική υποστήριξη.

Σίγουρα η SQLite δεν αποτελεί αντίπαλο δέος της Oracle, αλλά είναι ιδανική για desktop και embedded εφαρμογές. Μάλιστα χρησιμοποιείται από το Adobe Air, Firefox, Safari, iPhone, Skype κλπ. Είναι αρκετά καλή και για χρήση σε web εφαρμογές με μικρή προς μέτρια επισκεψιμότητα.

3.4 Εργαλεία Λογισμικού

3.4.1 Hot Potatoes

Το HotPotatoes [24] είναι ένα πρόγραμμα δημιουργίας διαφόρων μορφών ασκήσεων. Το πρόγραμμα διανέμεται ελεύθερα για εκπαιδευτική ή μη εμπορική χρήση. Χαρακτηρίζεται από μεγάλη φιλικότητα., και ευκολία στην χρήση του. Το πρόγραμμα μπορούμε να το κατεβάσουμε από την διεύθυνση **http://hotpot.uvic.ca/index.htm#downloads**



Εικόνα 3.2 Η Βασική Οθόνη της Εφαρμογής Hot Potatoes.

Το Hotpotatoes αποτελείται από 5 επιμέρους προγράμματα που παράγουν διαφορετικά είδη ασκήσεων:

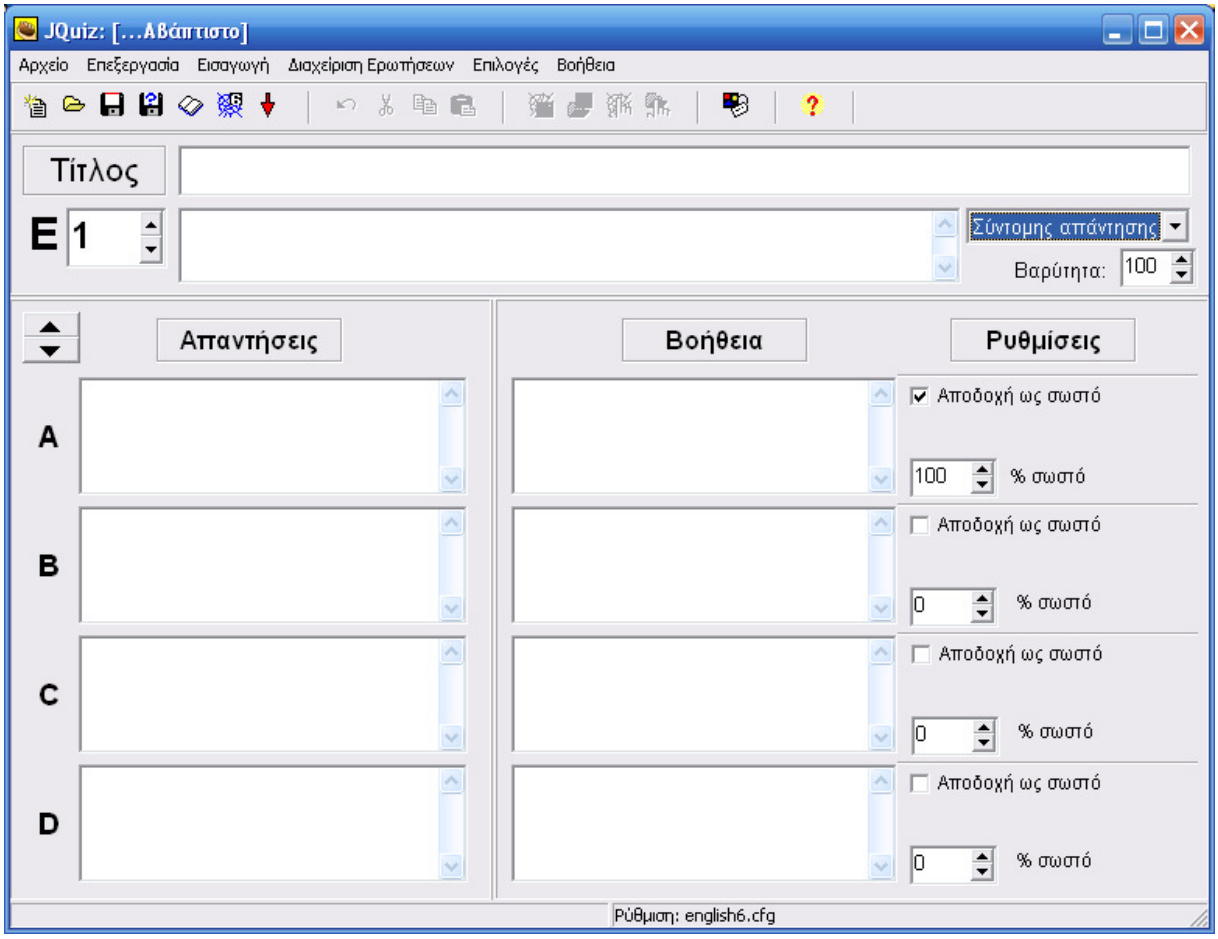
- JQUIZ (σύντομη απάντηση)
- JMIX (μπερδεμένη πρόταση)
- JCROSS (σταυρόλεξο)
- JMATCH (αντιστοίχιση)

- JCLOZE (συμπλήρωση κενών)

Με το Hotpotatoes ο εκπαιδευτικός μπορεί να φτιάξει εύκολα πολλά και διαφορετικά είδη ασκήσεων με τη μορφή ιστοσελίδων (html). Οι εκπαιδευόμενοι έπειτα έχουν πρόσβαση στις ασκήσεις χρησιμοποιώντας ένα πρόγραμμα περιήγησης ιστού (Web Browser). Το πρόγραμμα προσφέρει την δυνατότητα παροχής βοήθειας και υποδείξεων, ενώ βαθμολογεί και τις επιδόσεις του εκπαιδευόμενου. Υπάρχει τέλος η δυνατότητα αποστολής των ολοκληρωμένων ασκήσεων σε κάποιο email. Είναι ένα εργαλείο που μπορεί να χρησιμοποιηθεί για αξιολόγηση και ανατροφοδότηση.

JQUIZ (ασκήσεις πολλαπλής επιλογής, σύντομης απάντησης κ.λ.π.)

Άσκηση σύντομης απάντησης



Εικόνα 3.3 JQuiz

1) Στο 1ο πτυσσόμενο πλαίσιο δεξιά επιλέγουμε το είδος της άσκησης. Υπάρχουν 4 επιλογές:

   - Πολλαπλής Επιλογής
   - Σύντομης απάντησης
   - Υβριδικές
   - Πολλών Επιλογών

2) Στο παράδειγμα έχει γίνει η επιλογή «σύντομης απάντησης»

3) Πληκτρολογούμε τον τίτλο της Άσκησης στη θέση «Τίτλος».

4) Πληκτρολογούμε την πρότασή μας στο πλαίσιο δίπλα από τη θέση «Ε1»(Ερώτηση1).

5) Πληκτρολογούμε τις πιθανές απαντήσεις της ερώτησης στη θέση «Απαντήσεις». Τσεκάρουμε την επιλογή «αποδοχή ως σωστό» για την σωστή απάντηση. Εναλλακτικά μπορούμε να γράψουμε υποδείξεις για βοήθεια στα αντίστοιχα πλαίσια. Επίσης μπορούμε να δώσουμε ξεχωριστό ποσοστό ακρίβειας απάντησης για κάθε περίπτωση αλλάζοντας το ποσοστό δεξιά.

6) Μπορούμε να προσθέσουμε 2η πρόταση πατώντας το πάνω βελάκι στο «Ε1» (θα γίνει Ε2) και επαναλαμβάνουμε την ίδια διαδικασία.

7) Μπορούμε να ενσωματώσουμε βοηθητικό κείμενο μέσα στην άσκηση πατώντας «Αρχείο» → «Προσθήκη Βοηθητικού Κειμένου».

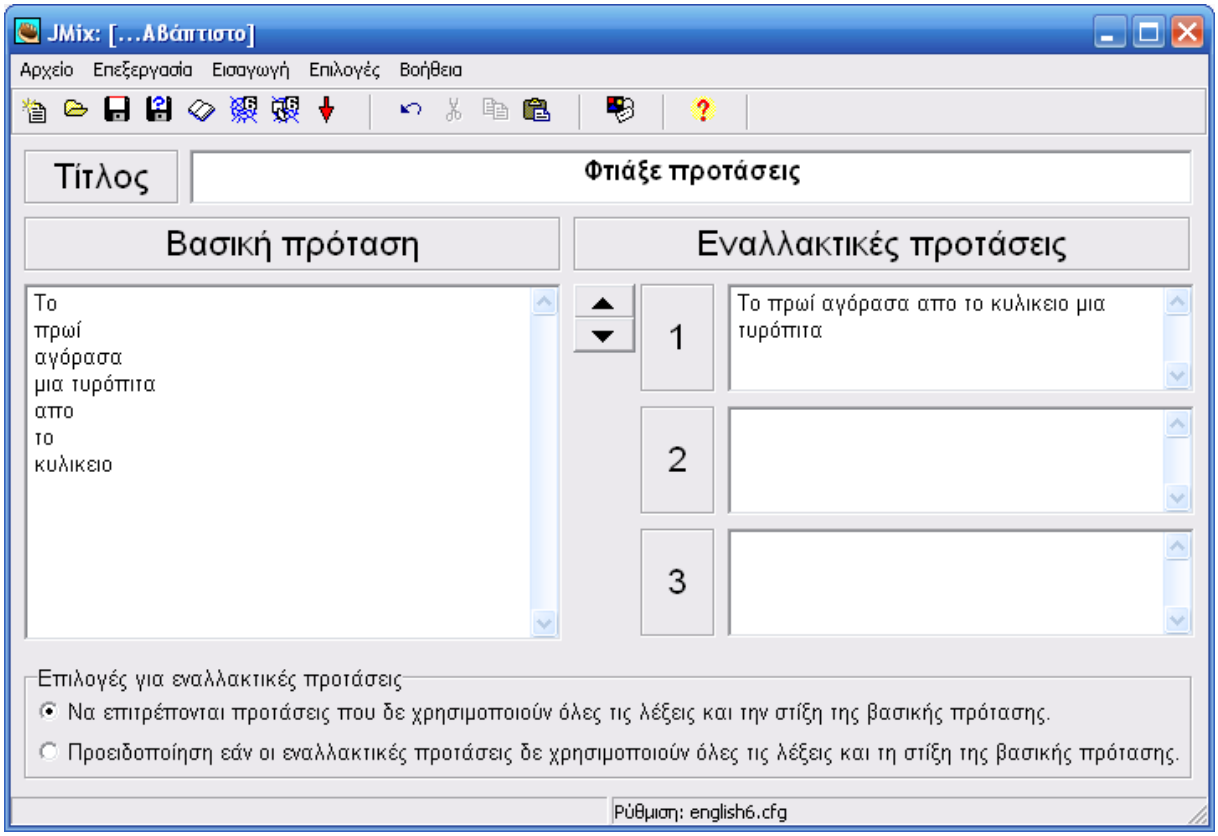
8) Από το μενού «Εισαγωγή» μπορούμε επίσης να ενσωματώσουμε εικόνες, links ή πίνακες.

9) Αποθηκεύουμε την άσκηση: «Αρχείο» → «Αποθήκευση ως» (για πιθανές μελλοντικές διορθώσεις).

10) Πατάμε το πλήκτρο  για να εξάγουμε την άσκηση σε μορφή ιστοσελίδας (html), επιλέγοντας όνομα.

Με αντίστοιχη διαδικασία εργαζόμαστε και στις υπόλοιπες δυνατότητες του JQUIZ (Πολλαπλής Επιλογής, Υβριδικές, Πολλών Επιλογών)

JMIX (μπερδεμένη πρόταση)



Εικόνα 3.4 JMix.

1) Πληκτρολογούμε τον τίτλο της Άσκησης στη θέση «Τίτλος».

2) Στην θέση «Βασική πρόταση» πληκτρολογούμε τον πρότασή μας χωρίζοντας την πατώντας ENTER στα σημεία που επιθυμούμε.

3) Στην θέση «Εναλλακτικές προτάσεις» πληκτρολογούμε παραλλαγές της πρότασης.

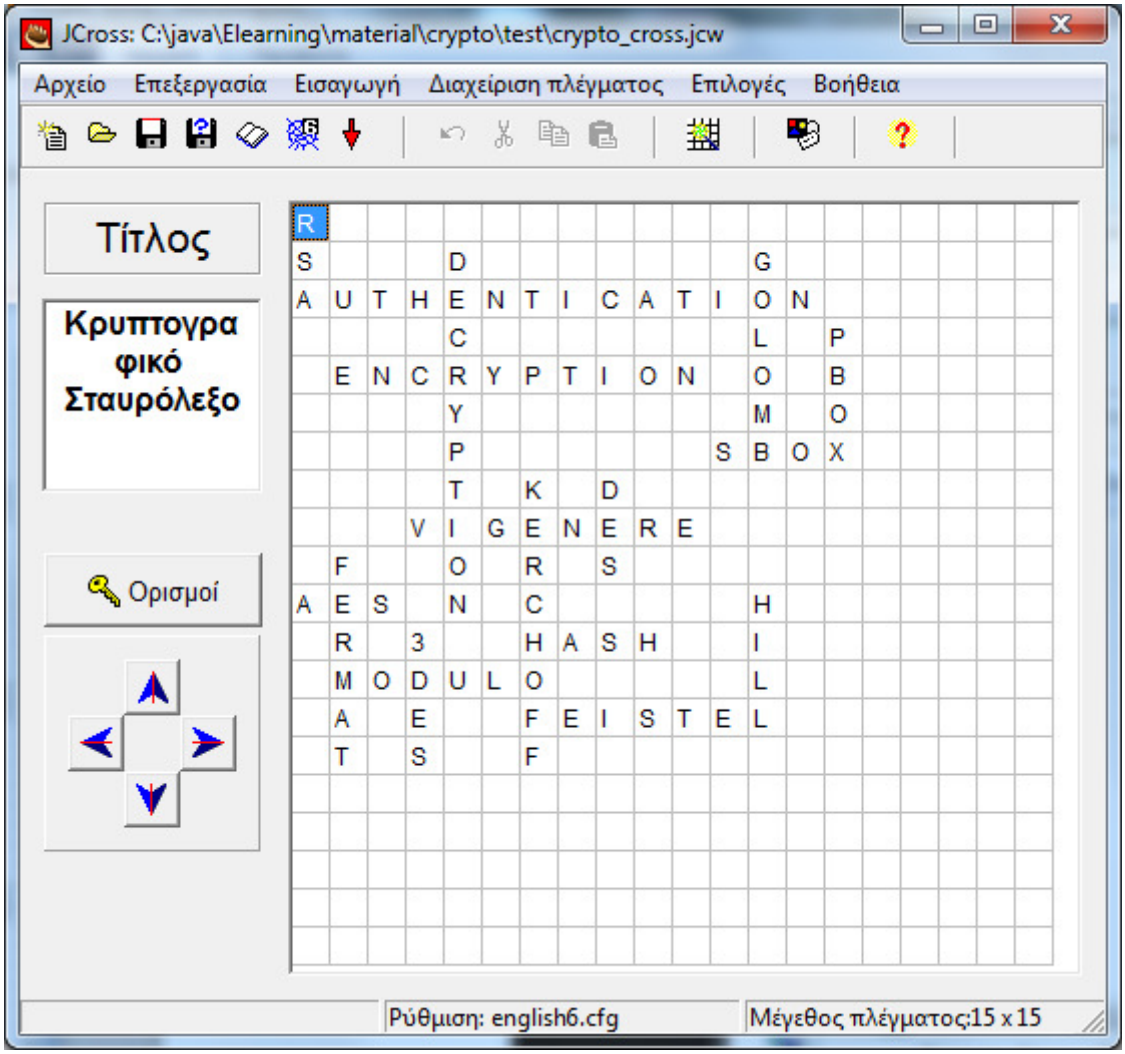
4) Μπορούμε να ενσωματώσουμε βοηθητικό κείμενο μέσα στην άσκηση πατώντας «Αρχείο» → «Προσθήκη Βοηθητικού Κειμένου».

5) Από το μενού «Εισαγωγή» μπορούμε επίσης να ενσωματώσουμε εικόνες, links ή πίνακες.

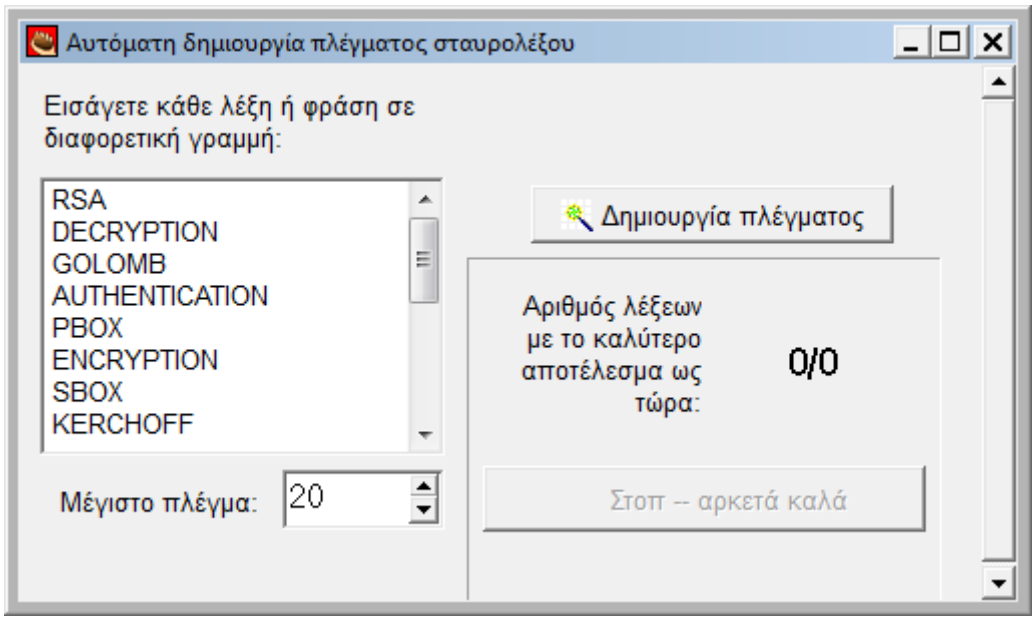
6) Αποθηκεύουμε την άσκηση: «Αρχείο» → «Αποθήκευση ως» (για πιθανές μελλοντικές διορθώσεις).

7) Πατάμε το πλήκτρο  για να εξάγουμε την άσκηση σε μορφή ιστοσελίδας (html) επιλέγοντας όνομα.

JCROSS (σταυρόλεξο)



Εικόνα 3.5 JCross



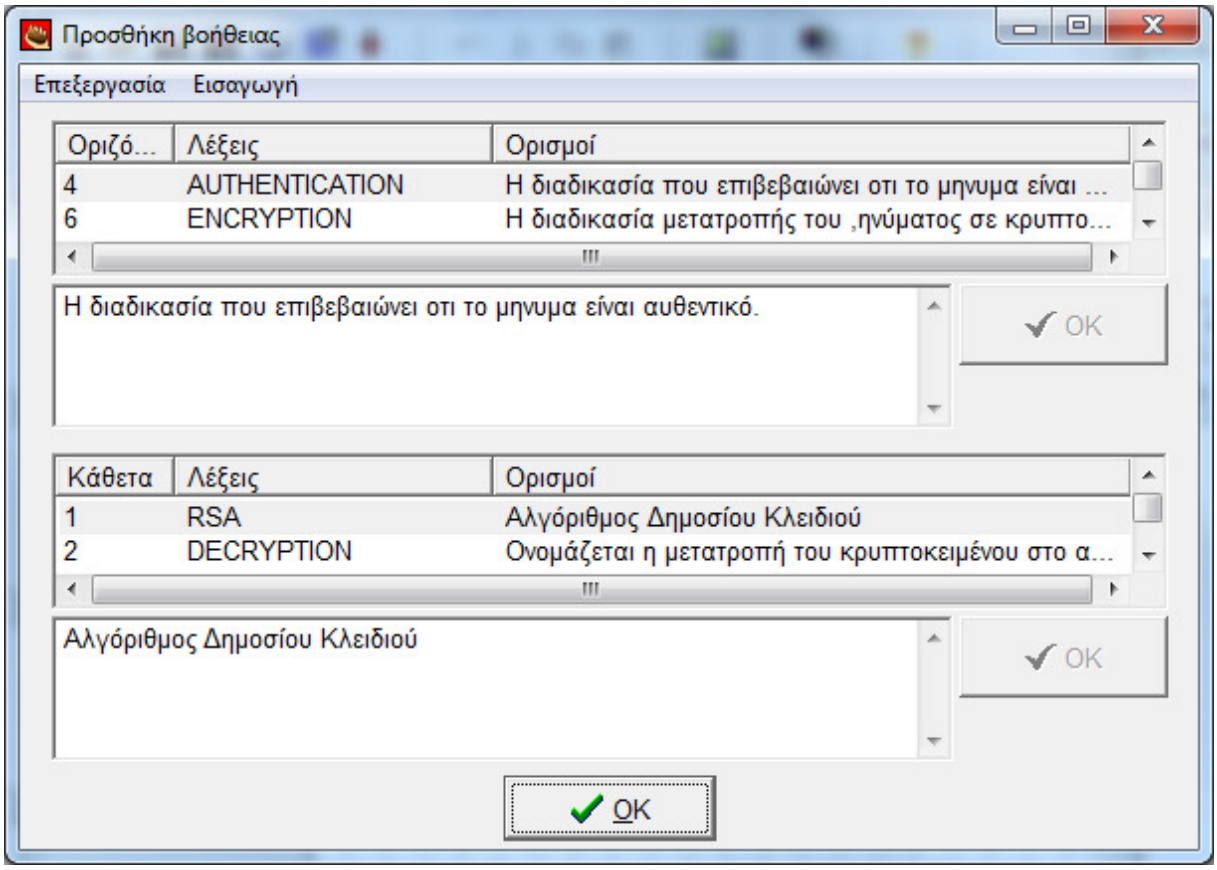
Εικόνα 3.6 JCross. Αυτόματη Δημιουργία Σταυρολέξου.

1) Πληκτρολογούμε τον τίτλο της Άσκησης στη θέση «Τίτλος».

2) Πατάμε το πλήκτρο «Διαχείριση Πλέγματος» → «Αυτόματη δημιουργία πλέγματος».

3) Πληκτρολογούμε τις λέξεις που θέλουμε να συμπεριλάβουμε στο σταυρόλεξο καθεμιά σε ξεχωριστή σειρά.

4) Πατάμε στο πλήκτρο «Δημιουργία πλέγματος».



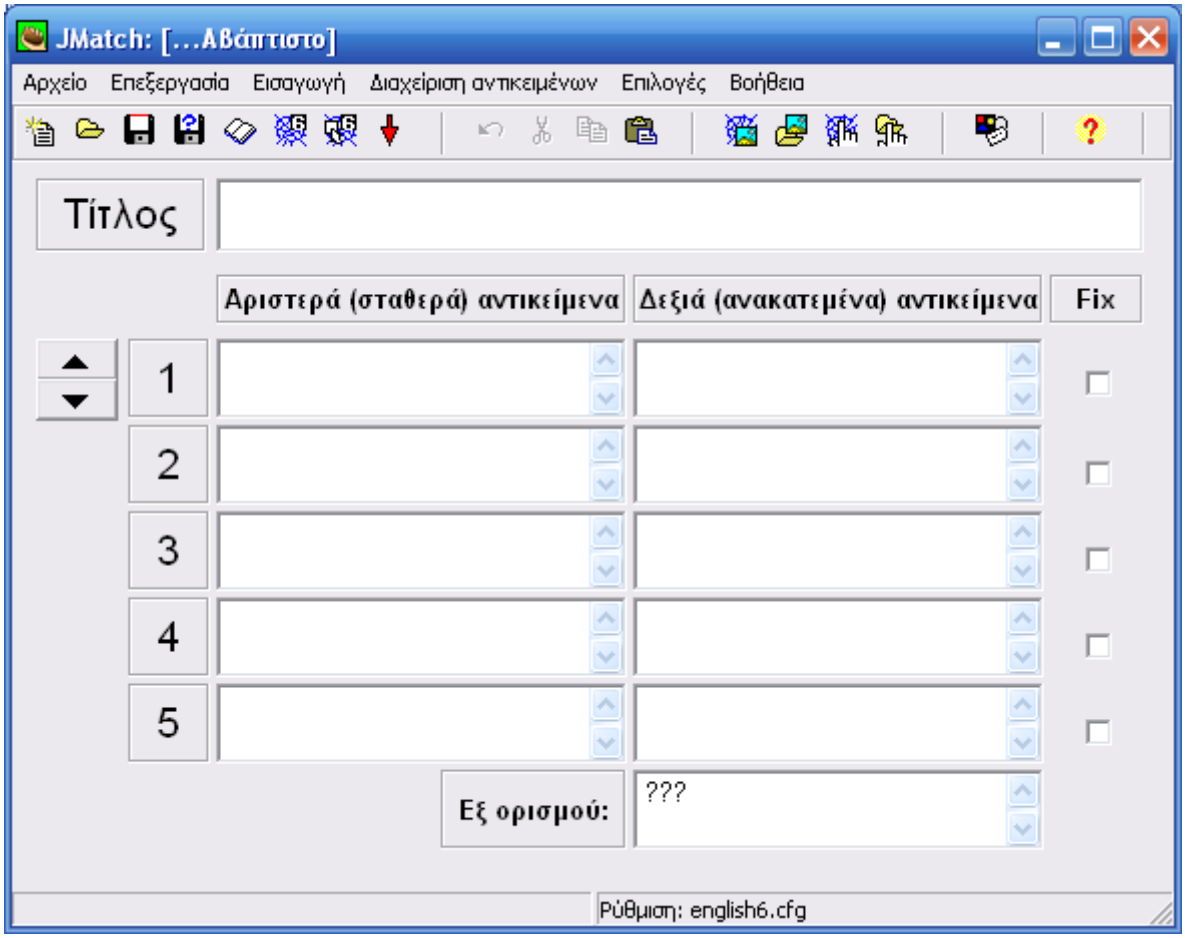
Εικόνα 3.7 JCross. Καθορισμός Ορισμών Σταυρόλεξου.

5) Στο αρχικό παράθυρο πατάμε «Ορισμοί» και πληκτρολογούμε τους ορισμούς των λέξεων. Πηγαίνοντας στο μενού «Εισαγωγή», μπορούμε να προσθέσουμε εικόνες, συνδέσμους ή πολυμεσικό υλικό.

6) Αποθηκεύουμε την άσκηση: «Αρχείο» → «Αποθήκευση ως» (για πιθανές μελλοντικές διορθώσεις).

7) Πατάμε το πλήκτρο για να εξάγουμε την άσκηση σε μορφή ιστοσελίδας (html) επιλέγοντας όνομα.

JMATCH (αντιστοίχιση)



Εικόνα 3.8 JMatch

1) Πληκτρολογούμε τον τίτλο στη θέση «Τίτλος».

2) Στο αριστερό τμήμα πληκτρολογούμε την αριστερή στήλη των αντιστοιχίσεων.

3) Στο δεξιό τμήμα πληκτρολογούμε τις αντιστοιχίσεις τους. Οι δεξιές επιλογές κατά την διενέργεια της άσκησης ανακατεύονται.

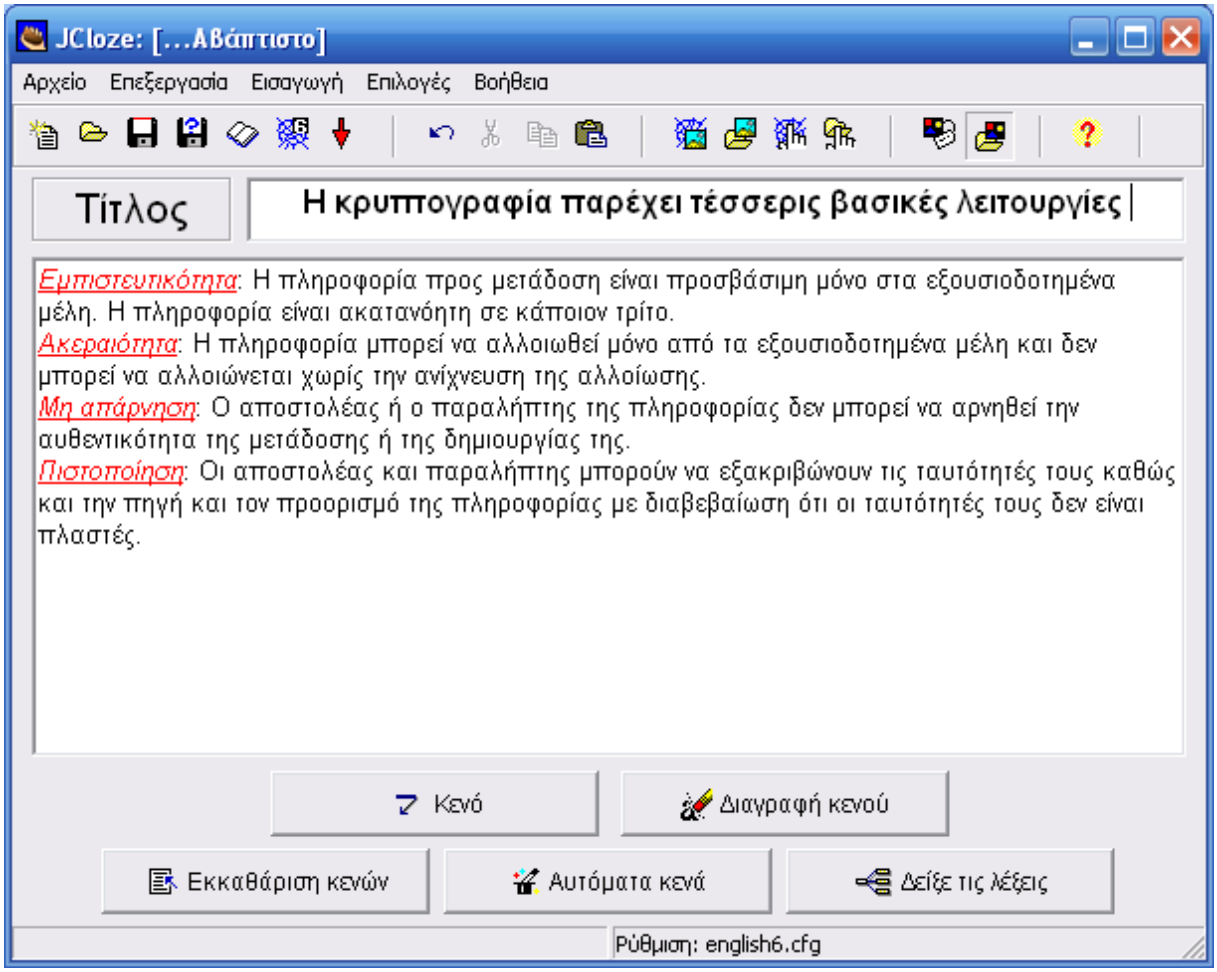
4) Μπορούμε να ενσωματώσουμε βοηθητικό κείμενο μέσα στην άσκηση πατώντας «Αρχείο» → «Προσθήκη Βοηθητικού Κειμένου».

5) Από το μενού «Εισαγωγή» μπορούμε επίσης να ενσωματώσουμε εικόνες, links ή πίνακες.

6) Αποθηκεύουμε την άσκηση: «Αρχείο» → «Αποθήκευση ως» (για πιθανές μελλοντικές διορθώσεις)

7) Πατάμε το πλήκτρο η το διπλανό του για να εξάγουμε την άσκηση σε μορφή ιστοσελίδας (html) επιλέγοντας όνομα. Στην συγκεκριμένη άσκηση έχουμε 2 μορφές εξαγωγής. Η 2η προσφέρει αντιστοίχιση σε μορφή drag and drop.

JCLOZE (συμπλήρωση κενών)



Εικόνα 3.9 JCloze

1) Πληκτρολογούμε τον τίτλο στη θέση «Τίτλος».

2) Πληκτρολογούμε στο πλαίσιο το κείμενό μας.

3) Επιλέγουμε τη λέξη στην οποία θα εμφανιστεί κενό προς συμπλήρωση, και πατάμε το πλήκτρο «Κενό». Μπορούμε στο παράθυρο που ανοίγει, να προσθέσουμε βοήθεια για την λέξη, ή να προσθέσουμε εναλλακτικές σωστές απαντήσεις.

4) Από το μενού «Εισαγωγή» μπορούμε επίσης να ενσωματώσουμε εικόνες, links ή πίνακες.

5) Αποθηκεύουμε την άσκηση: «Αρχείο» → «Αποθήκευση ως» (για πιθανές μελλοντικές διορθώσεις).

6) Πατάμε το πλήκτρο  για να εξάγουμε την άσκηση σε μορφή ιστοσελίδας (html) επιλέγοντας όνομα.

Κεφάλαιο 4
Μαθηματικό Υπόβαθρο

Η κατασκευή ισχυρών κρυπτογραφικών συναρτήσεων βασίζεται σε συγκεκριμένες μαθηματικές ιδιότητες. Κατά συνέπεια, για τη μελέτη της κρυπτογραφίας απαιτείται η εμβάθυνση σε συγκεκριμένες μαθηματικές έννοιες. Στο κεφάλαιο αυτό παρουσιάζεται το απαραίτητο μαθηματικό υπόβαθρο, το οποίο και αποτέλεσε τον «κορμό» του εκπαιδευτικού λογισμικού.

4.1 Αριθμητική Modulo

Η αριθμητική modulo (υπολοίπου) στηρίζεται στον τελεστή mod και στις ιδιότητές του. Ο τελευτής mod υπολογίζει το ακέραιο υπόλοιπο της διαίρεσης δύο ακεραίων. Για παράδειγμα, η πράξη 11 mod 5 επιστρέφει το αριθμό 1. Μια ιδιότητα του ακέραιου υπολοίπου είναι ότι υπάρχουν άπειροι αριθμοί που αν διαιρεθούν με το 5 μας δίνουν υπόλοιπο 1. Π.χ. 1 mod 5 = 1, 6 mod 5 = 1, 11 mod 5 = 1, 16 mod 5 = 1 κ.λ.π. Δύο αριθμοί θεωρούνται ισοδύναμοι mod N, αν αφήνουν το ίδιο υπόλοιπο όταν διαιρεθούν με το N. Η ισοδυναμία αυτή εκφράζεται με το σύμβολο ≡. Έτσι για στο προηγούμενο παράδειγμα θα λέγαμε $6 \equiv 11 \bmod 5$.

Μια άλλη ιδιότητα που ισχύει είναι η ακόλουθη. Αν ισχύει a ≡ b mod N, τότε ισχύει επίσης ότι a + λn ≡ b mod n όπου λ ένας οποιοσδήποτε ακέραιος.

-21	-20	-19	-18	-17	-16	-15	(-3 * 7 = -21)
-14	-13	-12	-11	-10	-9	-8	(-2 * 7 = -14)
-7	-6	-5	-4	-3	-2	-1	(-1 * 7= -7)
0	***1***	***2***	***3***	***4***	***5***	***6***	(a)
7	8	9	10	11	12	13	(+1 * 7=7)
14	15	16	17	18	19	20	(+2 * 7=14)
21	22	23	24	25	26	27	(+3 * 7=21)
28	29	30	31	32	33	34	(+4 * 7=28)
							(+λ * N)

Έτσι οι αριθμοί κάθε στήλης είναι ισοδύναμοι μεταξύ τους mod 7. Σε μια μαθηματική έκφραση mod N, οποιοσδήποτε αριθμός μπορεί να αντικατασταθεί από έναν ισοδύναμο του mod N, χωρίς να επηρεαστεί το αποτέλεσμα της έκφρασης. Οι πράξεις πρόσθεση, αφαίρεση και πολλαπλασιασμός ορίζονται όπως στην κλασική αριθμητική, με την προσθήκη βέβαια της ιδιότητας της χρήσης ισοδυνάμων.

Για μια πλήρη αριθμητική, θα πρέπει να οριστεί και η διαίρεση. Εν προκειμένω, η πράξη a/ b mod N Ορίζεται ως ο πολλαπλασιασμός του διαιρετέου (a) με τον αντίστροφο (κατά mod N) του διαιρέτη. Δηλαδή a/ b mod N = $\alpha^* \beta^{-1}$ mod N. Αντίστροφος ενός αριθμού mod N θεωρείτε αυτός που αν πολλαπλασιαστεί (mod N) μας δίνει την μονάδα. Για παράδειγμα αντίστροφος του 2 (mod 7)=2^{-1} mod 7 = 4 αφού 2 * 4 mod 7 = 8 mod 7 = 1. Άρα για την πράξη της διαίρεσης απαιτείται διαδικασία εύρεσης του αντιστρόφου του διαιρέτη.

Μια απλή τεχνική εύρεσης του αντιστρόφου είναι μέσω δοκιμών. Συνολικά απαιτούνται μέχρι N-1 δοκιμές για να εντοπιστεί (αν υπάρχει) ο αντίστροφος. Έτσι, για την εύρεση του αντιστρόφου του 2 mod 7 δοκιμάζουμε

1 * 2 (mod 7) = 2

2*2 (mod 7) = 4

3* 2 (mod 7) = 6

4* 2 (mod 7) = 1 Άρα το 4 είναι ο αντίστροφος.

Ο αντίστροφος ενός αριθμού στην αριθμητική υπολοίπων, δεν υπάρχει πάντα. Για να υπάρχει ο αντίστροφος ενός αριθμού a mod N πρέπει οι αριθμοί a και N να είναι πρώτοι μεταξύ τους. Δυο αριθμοί είναι πρώτοι μεταξύ τους όταν ο μέγιστος κοινός διαιρέτης τους (Μ.Κ.Δ.) είναι η μονάδα.

4.2 Αλγόριθμος του Ευκλείδη

Ο αλγόριθμος του Ευκλείδη είναι ένας αποδοτικός αλγόριθμος εύρεσης του Μ.Κ.Δ. (Μέγιστου Κοινού Διαιρέτη) 2 αριθμών. Βασίζεται την ιδιότητα ότι ο Μ.Κ.Δ. διαιρεί εκτός των 2 αριθμών, και το υπόλοιπο της διαίρεσης τους. Εφαρμόζει μια επαναληπτική διαδικασία που κατά την ολοκλήρωσή της εντοπίζει τον Μ.Κ.Δ.. Αρχικά γράφουμε την σχέση μεταξύ των a,b στην μορφή a= λ * b + υπ. Σε κάθε επόμενο βήμα αντικαταστούμε το a από το β, το β από το υπ, και υπολογίζουμε το νέο υπόλοιπο υπ. Η διαδικασία επαναλαμβάνεται μέχρι να μηδενιστεί το υπόλοιπο. Το τελευταίο μη μηδενικό υπόλοιπο είναι ο μέγιστος κοινός διαιρέτης. Παράδειγμα εύρεση του ΜΚΔ (792,92)

a		b		υπόλοιπο	
792	=	8 * 90	+	72	(1)
90	=	1 * 72	+	18	(2)
72	=	4 * 18	+	0	

Το τελευταίο μη μηδενικό υπόλοιπο είναι το 18 που είναι ο Μ.Κ.Δ. των 792, 90

4.3 Επεκταμένος Αλγόριθμος του Ευκλείδη

Για μεγάλο ακέραιο N, η μέθοδος της δοκιμής για την εύρεση του αντιστρόφου a^{-1} mod N είναι χρονοβόρα. Υπάρχουν πιο αποδοτικές τεχνικές εύρεσης του αντιστρόφου. Μια τέτοια μέθοδος είναι ο εκτεταμένος αλγόριθμος του Ευκλείδη. Αρχικά εκτελούμε τον αλγόριθμο του Ευκλείδη για την εύρεση του ΜΚΔ (a,N). Π.Χ. Για την εύρεση του 43^{-1} mod 1752.

1752 = 40 * 43 + 32 (1)
43 = 1 * 32 + 11 (2)

32 = 2 * 11 + 10 (3)
11 = 1 * 10 + 1 (4)

Ο μέγιστος κοινός διαιρέτης είναι:1

Συνεχίζουμε γράφοντας την σχέση (4) ως προς το υπόλοιπο, δηλαδή το 1

1=11- 1*10 (5)

λύνοντας την (3) ως προς το υπόλοιπο, δηλαδή το 10 και αντικαθιστώντας το 10 στην (5)

έχουμε 1=11-1*(32-2*11)=3*11 -1*32 (6)

λύνοντας την (2) ως προς το υπόλοιπο, δηλαδή το 11 και αντικαθιστώντας το 11 στην (6)

έχουμε 1=3*(43-1*32)-1*32=3*43-4*32(7)

λύνοντας την (1) ως προς το υπόλοιπο, δηλαδή το 32 και αντικαθιστώντας το 32 στην (7)

έχουμε 1=3*43-4*(1752-40*43)=-4*1752+163*43 (8)

Από την τελευταία σχέση βλέπουμε ότι 163*43 mod 1752 =1

Άρα ο αντίστροφος του 43 mod 1752 είναι το 163.

4.4 Πρώτοι Αριθμοί

Ένας αριθμός λέγεται πρώτος αν διαιρείται μόνο από τον εαυτό του και την μονάδα. Οι πρώτοι αριθμοί είναι πολύ σημαντικοί για την κρυπτογραφία. Χρησιμοποιούνται στους περισσότερους κρυπτογραφικούς αλγορίθμους. Δυο θέματα σχετικά με τους πρώτους αριθμούς σχετικά με την κρυπτογραφία είναι

- η εύρεση μεγάλων πρώτων αριθμών
- η ανάπτυξη ενός αριθμού ως γινόμενο πρώτων (παραγοντοποίηση)

Και τα δύο θέματα αποτελούν δύσκολα προβλήματα. Δεν υπάρχει δηλαδή αποδοτικός αλγόριθμος αντιμετώπισης τους.

4.5 Γεννήτορες

Ένας ακέραιος αριθμός g ονομάζεται **γεννήτορας** mod p (όπου p πρώτος αριθμός) αν όλες οι δυνάμεις g^1 (mod p), g^2 (mod p), …, g^{p-1} (mod p) είναι ανά δύο διαφορετικές μεταξύ τους. Για παράδειγμα αν p=7, ο αριθμός g=3 είναι γεννήτορας mod p γιατί:

$3^6 \pmod 7 = 1$

$3^5 \pmod 7 = 5$

$3^4 \pmod 7 = 4$

$3^3 \pmod 7 = 6$

$3^2 \pmod 7 = 2$

$3^1 \pmod 7 = 3$

Αντίστοιχα αν p=7, ο αριθμός g=2 **δεν** είναι γεννήτορας mod p γιατί:

$2\text{^}6 \pmod 7 = 1$

$2\text{^}3 \pmod 7 = 1$

(εμφανίστηκε η τιμή 1 δύο φορές)

Σε σχέση με τους πρώτους αριθμούς και τους γεννήτορες ισχύουν τα εξής:

- Για κάθε ακέραιο g και πρώτο αριθμό p ισχύει $g^{p-1} \pmod p = 1$ (Θεώρημα του Fermat)

- Αν p είναι πρώτος αριθμός και ισχύει $g^k \pmod p = 1$, τότε ο k είναι διαιρέτης του p-1.

Από αυτά συμπεραίνουμε ότι για να ελέγξουμε αν ένας αριθμός είναι γεννήτορας mod p, αρκεί να εξετάσουμε τα $g^k \pmod p$ για όλα τα k που είναι διαιρέτες του p-1. Αν κανένα $g^k \pmod p$ δεν ισούται με 1, τότε το g είναι γεννήτορας mod p.

Κεφάλαιο 5
Κρυπτογραφία

Στην σημερινή εποχή οι άνθρωποι έχουν την δυνατότητα να ανταλλάσουν και να μεταφέρουν πληροφορίες ελεύθερα έχοντας εύκολη πρόσβαση σε γνώσεις όπως ποτέ άλλοτε στο παρελθόν. Στην εποχή αυτή της πληροφορίας, τα δεδομένα μας χάνουν την ιδιωτικότητά τους αποκτώντας δημόσια χαρακτηριστικά. Κρατικές Υπηρεσίες, επιχειρήσεις, μηχανές αναζήτησης, κακόβουλο λογισμικό μπορούν να παρακολουθούν τα δεδομένα που μεταφέρονται. Η ασφαλής επικοινωνία είναι πλέον το ζητούμενο σε πολλές δραστηριότητες της καθημερινής μας ζωής (συναλλαγές με τράπεζες & δίκτυα ATM, κινητή τηλεφωνία, σταθερή τηλεφωνία, διασφάλιση εταιρικών πληροφοριών, στρατιωτικά δίκτυα, ηλεκτρονικές επιχειρήσεις, έξυπνες κάρτες, ασύρματα δίκτυα κ.λ.π.).

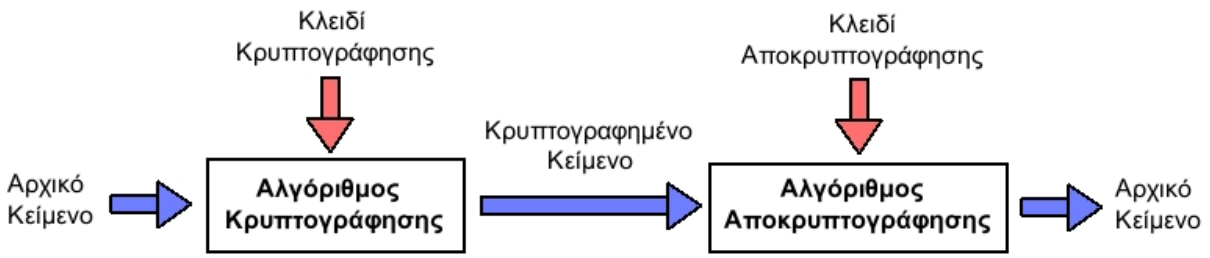
5.1 Κρυπτογραφία - Κρυπτανάλυση

5.1.1 Εισαγωγή – Βασικοί όροι

Με τον όρο ***κρυπτογραφία*** αναφερόμαστε στη μελέτη μαθηματικών τεχνικών που σχετίζονται με πλευρές της ασφάλειας πληροφοριών όπως ([33],[59]):

- Εμπιστευτικότητα (confidentiality). Η πληροφορία γίνεται αντιληπτή μόνο από εξουσιοδοτημένα μέλη. Είναι ακατανόητη σε κάποιον τρίτο.
- Πιστοποίηση ταυτότητας του αποστολέα (authentication). Ο παραλήπτης είναι σίγουρος ότι ο αποστολέας του μηνύματος είναι αυτός που ισχυρίζεται.
- Διασφάλιση του αδιάβλητου (ακεραιότητας) της πληροφορίας (integrity). Η πληροφορία μπορεί να μεταβληθεί μόνο από τα εξουσιοδοτημένα μέλη. Οποιαδήποτε μεταβολή από τρίτο ανιχνεύεται.
- Μη απάρνηση. Αποτρέπει μια οντότητα να αρνηθεί ενέργειες που έκανε. Για παράδειγμα μια οντότητα μπορεί να δώσει εξουσιοδότηση για την αγορά αγαθού από άλλη οντότητα, και σε μεταγενέστερο χρόνο να το αρνηθεί.

Η κρυπτογραφία γεννήθηκε από την ανάγκη αποστολής μυστικών μηνυμάτων. Ο αποστολέας τροποποιούσε το αρχικό μήνυμα εφαρμόζοντας κάποια διαδικασία, ώστε να μην είναι κατανοητό από τρίτους. Ο παραλήπτης εφαρμόζοντας κάποια αντίστροφη διαδικασία, επανέφερε το μήνυμα στην αρχική του μορφή. Η χρήση μυστικής διαδικασίας για κρυπτογράφηση των μηνυμάτων, διαπιστώθηκε ότι δεν ήταν αποτελεσματική μέθοδος για την διαδικασία κρυπτογράφησης (δεν μπορεί να διασφαλιστεί ότι ο αλγόριθμος δεν θα διαρρεύσει). Αυτό που εφαρμόζεται είναι η χρήση μιας μυστικής ποσότητας που ονομάζεται κλειδί και επηρεάζει το αποτέλεσμα της διαδικασίας κρυπτογράφησης.
Η ασφάλεια έγκειται μόνο στη μυστικότητα του κλειδιού – οι ίδιοι οι αλγόριθμοι κρυπτογράφησης και αποκρυπτογράφησης μπορούν να είναι ευρέως γνωστοί και δημοσιεύονται στο ευρύ κοινό (Αρχή του Kerchoff [59]).
Η διαδικασία κρυπτογράφησης – αποκρυπτογράφησης μπορεί να περιγραφεί από το ακόλουθο σχήμα.

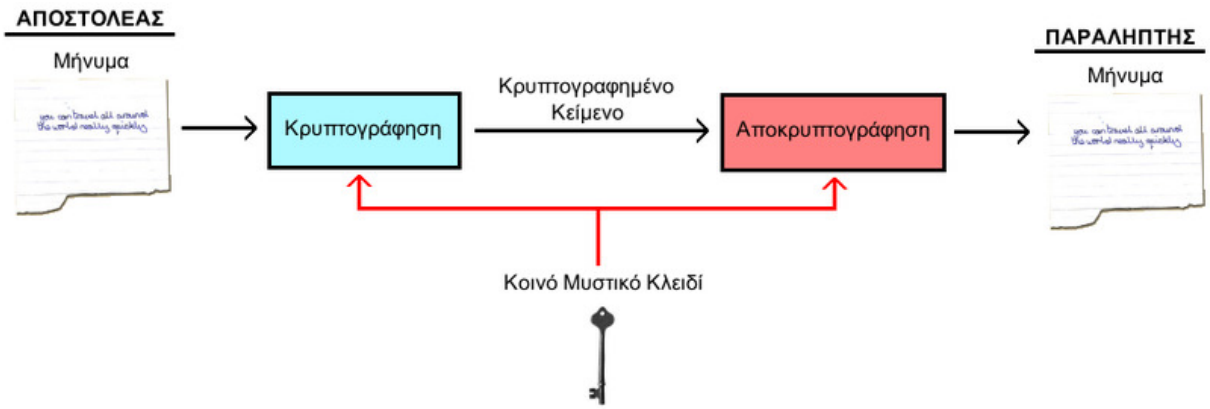


Εικόνα 5.1 πηγή: Wikipedia, Διαδικασία Κρυπτογράφησης – Αποκρυπτογράφησης.

Το μήνυμα (αρχικό κείμενο) κρυπτογραφείται με τη βοήθεια ενός μυστικού κλειδιού και ενός αλγόριθμου κρυπτογράφησης. Το κρυπτογραφημένο κείμενο ακολούθως μεταδίδεται/αποστέλλεται στον προορισμό του. Ο αλγόριθμος αποκρυπτογράφησης επαναφέρει το αρχικό μήνυμα χρησιμοποιώντας έναν αλγόριθμο αποκρυπτογράφησης και το κλειδί αποκρυπτογράφησης.

Οι αλγόριθμοι κρυπτογράφησης χωρίζονται σε δύο μεγάλες κατηγορίες ως ακολούθως:

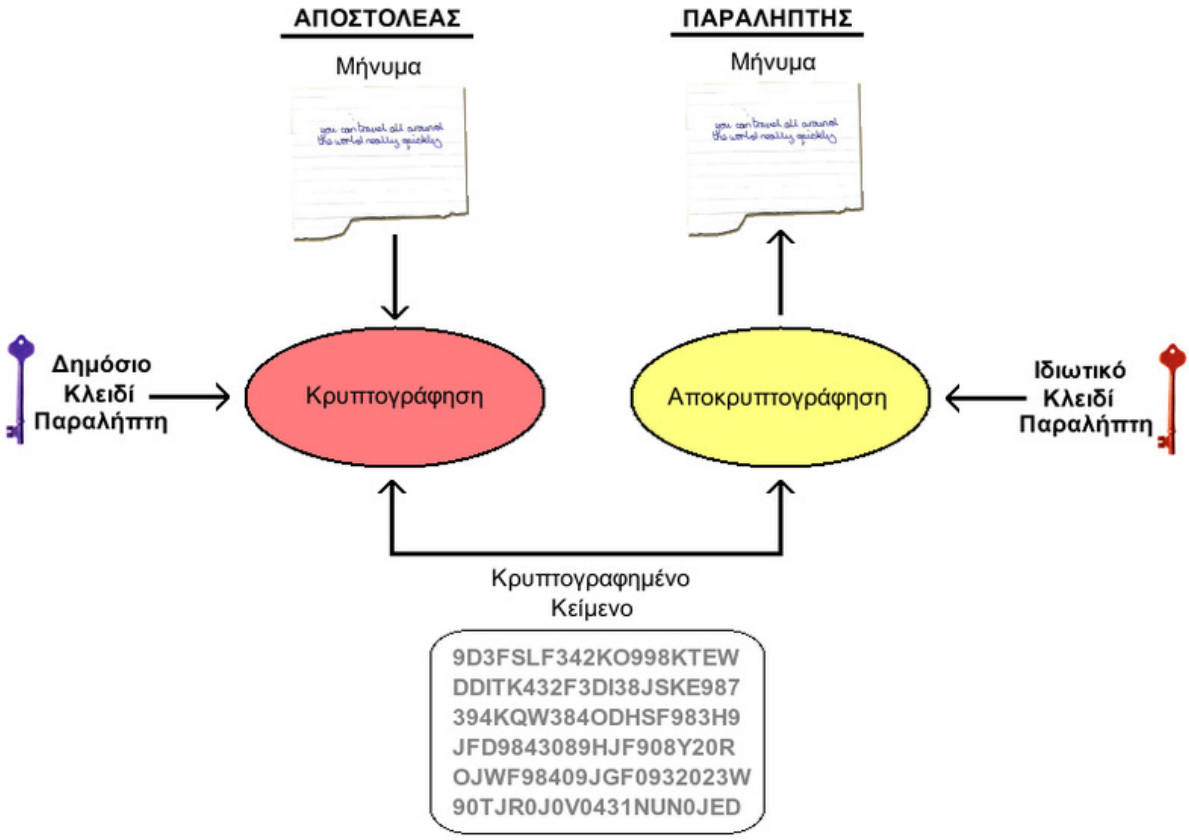
- **Αλγόριθμοι συμμετρικού ή ιδιωτικού κλειδιού.**



Εικόνα 5.2 πηγή: Wikipedia Αλγόριθμοι Συμμετρικού Κλειδιού.

Στην κρυπτογράφηση συμμετρικού κλειδιού χρησιμοποιείται το ίδιο κλειδί, τόσο κατά την διαδικασία κρυπτογράφησης, όσο και κατά την διαδικασία αποκρυπτογράφησης. Το κοινό κλειδί πρέπει να είναι γνωστό σε αποστολέα και παραλήπτη ώστε να ολοκληρωθεί επιτυχώς η διαδικασία. Οι διαδικασίες κρυπτογράφησης και αποκρυπτογράφησης υλοποιούνται εύκολα και γρήγορα. Η ταχύτητα αυτή αποτελεί και το συγκριτικό πλεονέκτημα αυτών των αλγορίθμων σε σχέση με τους αλγόριθμους δημοσίου κλειδιού. Παρουσιάζουν όμως και μια αδυναμία. Απαραίτητη προϋπόθεση είναι η ασφαλής ανταλλαγή του κλειδιού ανάμεσα σε αποστολέα και παραλήπτη. Είναι εξαιρετικά δύσκολο να υπάρχει ασφαλές κανάλι επικοινωνίας μέσω του οποίου να διακινηθεί το κλειδί. Γνωστοί αλγόριθμοι αυτής της κατηγορίας είναι οι DES, Triple DES, AES.

- **Αλγόριθμοι ασύμμετρου ή δημοσίου κλειδιού**.



Εικόνα 5.3 πηγή: Wikipedia Αλγόριθμοι Δημοσίου Κλειδιού.

Στην κρυπτογράφηση Δημοσίου κλειδιού ο αποστολέας και ο παραλήπτης δεν μοιράζονται ένα κοινό κλειδί όπως στους αλγόριθμους συμμετρικού κλειδιού. Εδώ το κάθε μέλος της επικοινωνίας διαθέτει ένα ζευγάρι κλειδιών (ιδιωτικό, δημόσιο). Το δημόσιο κλειδί χρησιμοποιείται στη διαδικασία της κρυπτογράφησης, ενώ το ιδιωτικό κατά την αποκρυπτογράφηση. Το δημόσιο κλειδί είναι γνωστό σε όλους, ενώ το ιδιωτικό παραμένει κρυφό. Η επιτυχία της διαδικασίας βασίζεται στην αδυναμία υπολογισμού του ιδιωτικού κλειδιού από το δημόσιο. Οι αλγόριθμοι αυτοί συγκριτικά με τους συμμετρικούς αλγόριθμους είναι αρκετά πιο αργοί. Δεν παρουσιάζουν όμως το πρόβλημα της μετάδοσης του μυστικού κλειδιού.

Στην πράξη οι δυο κατηγορίες αλγορίθμων χρησιμοποιούνται συνδυαστικά ώστε να αρθούν οι περιορισμοί τους. Δηλαδή χρησιμοποιείται κάποιος αλγόριθμος συμμετρικού κλειδιού για γρήγορη κρυπτογράφηση-αποκρυπτογράφηση της πληροφορίας, ενώ για την αρχική ανταλλαγή του μυστικού κλειδιού χρησιμοποιείται κάποιος αλγόριθμος δημοσίου κλειδιού.

Με τον όρο ***κρυπτανάλυση*** αναφερόμαστε στη μελέτη μαθηματικών τεχνικών που στοχεύουν στην "ακύρωση" των κρυπτογραφικών μεθόδων, προκειμένου να πληγεί η ασφάλεια [33].

Οι κρυπταναλυτικές επιθέσεις χωρίζονται στους ακόλουθους τύπους:

- ***Ciphertext-only attack*** (γνωστού κρυπτοκειμένου). Ο κρυπταναλυτής γνωρίζει Ν πλήθος κρυπτοκειμένων, καθώς και τον αλγόριθμο που χρησιμοποιήθηκε, και προσπαθεί να εξάγει το κλειδί και τελικά το μήνυμα. Παρουσιάζει μεγάλη δυσκολία επιτυχούς ολοκλήρωσης. Παράδειγμα τέτοιας διαδικασίας είναι η εξαντλητική αναζήτηση κλειδιών (brute-force).

- ***Known-plaintext attack*** (γνωστού μηνύματος). Ο κρυπταναλυτής γνωρίζει ζευγάρια πληροφορίας (μήνυμα, κρυπτοκείμενο). Για παράδειγμα αρχεία τύπου Postscript έχουν στην αρχή ένα συγκεκριμένο pattern. Έχει λοιπόν ο κρυπταναλυτής στην διάθεση του, ένα ζεύγος πληροφορίας (postscript_pattern, κρυπτοκείμενο). Αξιοποιώντας αυτή την πληροφορία προσπαθεί να εντοπίσει το κλειδί και να ανακτήσει το μήνυμα.

- ***Chosen-plaintext attack*** (επιλεγμένου μηνύματος). Ο κρυπταναλυτής είναι σε θέση να επιλέξει ο ίδιος συγκεκριμένα τμήματα του αρχικού μηνύματος για τα οποία είναι σε θέση να γνωρίσει πώς κρυπτογραφούνται. Παρατηρώντας τα αντίστοιχα κρυπτογραφήματα που προκύπτουν προσπαθεί να εντοπίσει το κλειδί και - κατ' επέκταση - να ανακτήσει το αρχικό μήνυμα.

- ***Chosen-ciphertext attack*** (επιλεγμένου κρυπτοκειμένου). Ο κρυπταναλυτής επιλέγει συγκεκριμένα κρυπτοκείμενα για τα οποία είναι σε θέση να γνωρίζει τα αρχικά μηνύματα (δηλαδή πώς αυτά θα αποκρυπτογραφούνταν αν γνώριζε το μυστικό κλειδί). Μελετώντας την συμπεριφορά του αλγορίθμου στην αποκρυπτογράφηση προσπαθεί να εντοπίσει το κλειδί και – κατ' επέκταση - να ανακτήσει το αρχικό μήνυμα.

Οι δύο τελευταίοι τύποι επιθέσεων είναι πρακτικά δύσκολο να εφαρμοστούν στην πράξη και έχουν περισσότερο θεωρητικό ενδιαφέρον. Εν τούτοις, χρησιμοποιούνται για την αποτίμηση της ασφάλειας ενός κρυπτογραφικού αλγόριθμου.

5.2 Ιστορικοί Αλγόριθμοι

Στην παράγραφο αυτή θα παρουσιαστούν οι βασικοί αλγόριθμοι κρυπτογράφησης που έχουν χρησιμοποιηθεί κατά τα πρώιμα στάδια της κρυπτογραφίας. Παρόλο που οι αλγόριθμοι αυτοί έχουν, κυρίως ιστορικό ενδιαφέρον, αναδεικνύουν – μέσω της ανάλυσής τους - τις βασικές αρχές και ιδιότητες που πρέπει να έχει ένα ασφαλές κρυπτοσύστημα.

5.2.1 Αλγόριθμος Μονοαλφαβητικής Αντικατάστασης

Στους αλγόριθμους μονοαλφαβητικής αντικατάστασης ο κάθε χαρακτήρας του κειμένου αντικαθίσταται από κάποιον άλλον συγκεκριμένο: με άλλα λόγια, ορίζεται εξ αρχής μία αντιστοίχιση (δηλ. από ποιον χαρακτήρα θα αντικαθίσταται το «Α», από ποιον το «Β» κ.ο.κ.). Στην ουσία, το μυστικό κλειδί για την κρυπτογράφηση και αποκρυπτογράφηση είναι αυτή ακριβώς η αντιστοίχιση. Κάνοντας τις ως άνω αντικαταστάσεις σε κάθε χαρακτήρα, προκύπτει το κρυπτοκείμενο.

Πχ για το μήνυμα 'ΑΒΓΑ' και τον ακόλουθο πίνακα αντιστοίχησης

Α	Β	Γ	Δ	Ε	Ζ	Η	Θ	Ι	Κ	Λ	Μ	Ν	Ξ	Ο	Π	Ρ	Σ	Τ	Υ	Φ	Χ	Ψ	Ω
Ν	Α	Ξ	Β	Ο	Γ	Π	Δ	Ρ	Ε	Σ	Ζ	Τ	Η	Υ	Θ	Φ	Ι	Χ	Κ	Ψ	Λ	Ω	Μ

Πίνακας 5.1 Πίνακας Αντιστοίχισης.

Το κρυπτοκείμενο που προκύπτει είναι 'ΝΑΞΝ'.

Το πλήθος των πιθανών κλειδών για μια επίθεση εξαντλητικής αναζήτησης είναι πολύ μεγάλο. Επίθεση εξαντλητικής αναζήτησης θεωρείτε η κατάσταση που ο επιτιθέμενος δοκιμάζει όλους τους πιθανούς συνδυασμούς των αντιστοιχήσεων των γραμμάτων. Οι πιθανοί συνδυασμοί εδώ είναι 24! (παραγοντικό) – γενικότερα, αν Ν είναι το πλήθος των συμβόλων του αλφαβήτου της γλώσσας του μηνύματος, τότε το πλήθος των πιθανών κλειδιών είναι Ν! Είναι λοιπόν πρακτικά (υπολογιστικά) αδύνατο να ελεγχθούν όλοι αυτοί οι συνδυασμοί.

Όμως τα αρχικά μηνύματα έχουν συνήθως κάποια χαρακτηριστικά που μπορούν να οδηγήσουν σε εύρεση του πίνακα αντιστοίχησης, άρα και στην ανάκτηση του μηνύματος. Το σημαντικότερο είναι η συχνότητα εμφάνισης του κάθε γράμματος. Για παράδειγμα, σε ένα μεγάλο μήνυμα του

ελληνικού αλφαβήτου, το πλέον συχνά εμφανιζόμενο γράμμα είναι το γράμμα Α. Αν λοιπόν στο κρυπτοκείμενο το πιο συχνό γράμμα είναι το γράμμα Ξ, τότε το πιο πιθανό το Ξ να αντιστοιχίζεται στο Α. Μια τέτοια στατιστική ανάλυση (ιδίως δε αν λάβει κανείς υπόψη και τη συχνή εμφάνιση διφθόγγων και τριφθόγγων, όπως «το», «οι», «και» κτλ.) μπορεί να αποκαλύψει την αντιστοίχιση και να οδηγήσει στην κατάρρευση της μυστικότητας του μηνύματος.

Γράμμα	Συχνότητα Εμφάνισης (%)	Γράμμα	Συχνότητα Εμφάνισης (%)
Α	12	Λ	3,3
Ο	9,8	Η	2,9
Τ	9,1	Γ	2
Ε	8	Δ	1,7
Ν	7,9	Ω	1,6
Ι	7,8	Χ	1,4
Π	5,024	Θ	1,3
Ρ	5,09	Φ	1,2
Σ	4,9	Β	0,8
Μ	4,4	Ξ	0,6
Υ	4,3	Ζ	0,5
Κ	4,2	Ψ	0,2

Πίνακας 5.2 Συχνότητες εμφάνισης γραμμάτων σε λέξεις της ελληνικής αλφαβήτου.

5.2.2 Αλγόριθμος Πολυαλφαβητικής Αντικατάστασης

Για να αντιμετωπιστεί η αδυναμία της μονοαλφαβητικής αντικατάστασης σε επιθέσεις βάσει της ανάλυσης της συχνότητας εμφάνισης των συμβόλων, προτάθηκαν οι αλγόριθμοι πολυαλφαβητικής αντικατάστασης. Εδώ κάθε χαρακτήρας που εμφανίζεται πολλές φορές στο

μήνυμα, δεν αντικαθίσταται πάντοτε με τον ίδιο χαρακτήρα στο κρυπτοκείμενο. Παράδειγμα τέτοιου αλγορίθμου είναι ο αλγόριθμος Vigenere.

Έστω το μήνυμα KWSTAKHSONOUFRIOS
Αντικαταστούμε κάθε γράμμα με τον αριθμό που αντιστοιχεί στην θέση του στο αλφάβητο. Το Α είναι στην θέση 0, το Β είναι στην θέση 1 κ.λ.π. Έτσι το μήνυμα γίνεται
10,22,18,19,0,10,7,18,14,13,14,20,5,17,8,14,18
Χρησιμοποιούμε και για μυστικό κλειδί μία λέξη πχ ONOUFRIOS. Ακλουθούμε την ίδια μετατροπή όπως προηγουμένως και το κλειδί γίνεται 14,13,14,20,5,17,8,14,18. Επειδή το κλειδί είναι μικρότερο του μηνύματος, το επαναλαμβάνουμε συνεχώς μέχρι το μέγεθος του να γίνει ίσο με το μήνυμα.
Σε κάθε θέση αθροίζουμε (mod 26) τον αριθμό που αντιστοιχεί στο γράμμα του μηνύματος και στο γράμμα του κλειδιού. Προκύπτουν δηλαδή οι αριθμοί 24,9,6,13,5,1,15,6,6,1,1,8,25,22,25,22,6. Ο αριθμοί αυτοί αντιστοιχούν στην θέση στο αλφάβητο των χαρακτήρων του κρυπτοκειμένου.

KWSTAKHSONOUFRIOS	K	W	S	T	A	K	H	S	O	N	O	U	F	R	I	O	S
ONOUFRIOS	O	N	O	U	F	R	I	O	S	O	N	O	U	F	R	I	O
ΜΗΝΥΜΑ	10	22	18	19	0	10	7	18	14	13	14	20	5	17	8	14	18
ΚΛΕΙΔΙ	14	13	14	20	5	17	8	14	18	14	13	14	20	5	17	8	14
ΑΘΡΟΙΣΜΑ	24	35	32	39	5	27	15	32	32	27	27	34	25	22	25	22	32
ΑΘΡ MOD 26	24	9	6	13	5	1	15	6	6	1	1	8	25	22	25	22	6
ΚΡΥΠΤΟΜΗΝΥΜΑ	Y	J	G	N	F	B	P	G	G	B	B	I	Z	W	Z	W	G

Παρότι είναι πολύ ισχυρότερος αλγόριθμος κρυπτογράφησης από τους αλγόριθμους μονοαλφαβητικής αντικατάστασης, παρουσιάζει κάποια αδυναμία λόγω της επανάληψης του κλειδιού. Ειδικά αν ο επιτιθέμενος εντοπίσει το μέγεθος του κλειδιού, τότε μπορεί να εφαρμόσει την επίθεση με ανάλυση της συχνότητας εμφάνισης των συμβόλων.

5.2.3 Γραμμικός (Affine) Αλγόριθμος

Η κρυπτογράφηση κάθε χαρακτήρα m γίνεται εφαρμόζοντας τον τύπο $c = a*m + b \ (mod\ N)$ (όπου N το πλήθος των χαρακτήρων του αλφάβητου που χρησιμοποιείτε στο μήνυμα. Για το ελληνικό αλφάβητο δηλαδή 24, για το αγγλικό 26) για κάθε χαρακτήρα του μηνύματος. Ο κάθε χαρακτήρας αντικαθίσταται από την θέση του στο αλφάβητο και εφαρμόζεται η μαθηματική

έκφραση. Κάθε φορά προκύπτει ένας αριθμός c. Αντικαταστούμε το c με τον χαρακτήρα που βρίσκεται στην θέση c στο αλφάβητο, και προκύπτει ο αντίστοιχος χαρακτήρας κρυπτοκειμένου.

Π.χ. Θέλουμε να κωδικοποιήσουμε το μήνυμα icantdoit με κλειδί (a,b) (3,2)
Ο χαρακτήρας 'i' αντιστοιχεί στον ακέραιο 8, c=a*x+b --> c=3 * 8 + 2 = 26 (mod26) =0 --> a
Ο χαρακτήρας 'c' αντιστοιχεί στον ακέραιο 2, c=a*x+b --> c=3 * 2 + 2 = 8 (mod26) =8 --> i
Ο χαρακτήρας 'a' αντιστοιχεί στον ακέραιο 0, c=a*x+b --> c=3 * 0 + 2 = 2 (mod26) =2 --> c
Ο χαρακτήρας 'n' αντιστοιχεί στον ακέραιο 13, c=a*x+b --> c=3 * 13 + 2 = 41 (mod26) =15 --> p
Ο χαρακτήρας 't' αντιστοιχεί στον ακέραιο 19, c=a*x+b --> c=3 * 19 + 2 = 59 (mod26) =7 --> h
Ο χαρακτήρας 'd' αντιστοιχεί στον ακέραιο 3, c=a*x+b --> c=3 * 3 + 2 = 11 (mod26) =11 --> l
Ο χαρακτήρας 'o' αντιστοιχεί στον ακέραιο 14, c=a*x+b --> c=3 * 14 + 2 = 44 (mod26) =18 --> s
Ο χαρακτήρας 'i' αντιστοιχεί στον ακέραιο 8, c=a*x+b --> c=3 * 8 + 2 = 26 (mod26) =0 --> a
Ο χαρακτήρας 't' αντιστοιχεί στον ακέραιο 19, c=a*x+b --> c=3 * 19 + 2 = 59 (mod26) =7 --> h
Άρα το κρυπτοκείμενο είναι το «aicphlsah».

Η αποκρυπτογράφηση γίνεται λύνοντας την σχέση τύπο c = a*m + b ως προς m.
$m=a^{-1}(c-b) \pmod N$ (2). Η αντίστοιχη διαδικασία που χρησιμοποιεί τον τύπο (2) μας δίνει το αρχικό μήνυμα.
Θέλουμε να Αποκωδικοποιήσουμε το μήνυμα aicphlsah
1ο βήμα. Εύρεση του $a^{-1} \pmod N$
26 = 8 * 3 + 2
3 = 1 * 2 + 1
Ο μέγιστος κοινός διαιρέτης είναι:1 (Αρα υπάρχει ο αντίστροφος)
Ο αντίστροφος είναι 9 αφού 1 = (9) (3) + (-1) (26)
Ο χαρακτήρας 'a' αντιστοιχεί στον ακέραιο 0, $m= a^{-1} *(c-b) \pmod{26}$ --> $m=9 * (0 - 2) \pmod{26} =-18 \pmod{26} =8$ --> i
Ο χαρακτήρας 'i' αντιστοιχεί στον ακέραιο 8, $m= a^{-1} *(c-b) \pmod{26}$ --> $m=9 * (8 - 2) \pmod{26} =2$ --> c
Ο χαρακτήρας 'c' αντιστοιχεί στον ακέραιο 2, $m= a^{-1} *(c-b) \pmod{26}$ --> $m=9 * (2 - 2) \pmod{26} =0$ --> a
Ο χαρακτήρας 'p' αντιστοιχεί στον ακέραιο 15, $m= a^{-1}*(c-b) \pmod{26}$ --> $m=9 * (15 - 2) \pmod{26} =13$ --> n
Ο χαρακτήρας 'h' αντιστοιχεί στον ακέραιο 7, $m= a^{-1} *(c-b) \pmod{26}$ --> $m=9 * (7 - 2) \pmod{26} =19$ --> t
Ο χαρακτήρας 'l' αντιστοιχεί στον ακέραιο 11, $m= a^{-1} *(c-b) \pmod{26}$ --> $m=9 * (11 - 2) \pmod{26} =3$ --> d

Ο χαρακτήρας 's' αντιστοιχεί στον ακέραιο 18, m= a^{-1} *(c-b) (mod 26) --> m=9 * (18 - 2) (mod 26) =14 --> o

Ο χαρακτήρας 'a' αντιστοιχεί στον ακέραιο 0, m= a^{-1} *(c-b) (mod 26) --> m=9 * (0 - 2) (mod 26) =-18 (mod 26) =8 --> i

Ο χαρακτήρας 'h' αντιστοιχεί στον ακέραιο 7, m= a^{-1} *(c-b) (mod 26) --> m=9 * (7 - 2) (mod 26) =19 --> t

Το αρχικό μήνυμα είναι το «icantdoit».

Το πλήθος των πιθανών κλειδιών στον γραμμικό αλγόριθμο είναι πολύ μικρό. Υπολογίζεται από την σχέση πλήθος_πιθανών_a * πλήθος_πιθανών_b. Πχ για το αγγλικό αλφάβητο που το N=26 τα πιθανά b είναι 26 ενώ τα πιθανά a είναι 12. Ο λόγος που τα πιθανά a είναι 12 και όχι 26 είναι επειδή για να μπορεί να γίνει αποκρυπτογράφηση θα πρέπει να υπάρχει το a^{-1}. Επιτρεπτές τιμές για το α είναι αυτές που ικανοποιούν τη σχέση ΜΚΔ(a,N)=1 (εν προκειμένω, το a και το 26 είναι πρώτοι μεταξύ τους). Το πλήθος λοιπόν των πιθανών κλειδιών (για αλφάβητο 26 συμβόλων) είναι 12*26=312, το οποίο προφανώς είναι πολύ μικρό, συνεπώς ο αλγόριθμος είναι ευάλωτος σε επιθέσεις εξαντλητικής αναζήτησης.

5.2.4 Αλγόριθμος Hill

Μπορεί να θεωρηθεί σαν επέκταση του γραμμικού αλγορίθμου. Το μήνυμα χωρίζεται σε τμήματα (block) σταθερού μήκους. Το κλειδί (K) είναι ένας τετραγωνικός πίνακας L χ L (όπου L το μέγεθος του Block. Σε κάθε Block του μηνύματος εφαρμόζεται η σχέση $C = K * M \pmod{p}$ (όπου C: Block Κρυπτοκειμένου, M: Block Μηνύματος, K : Πίνακας κλειδί, p : μέγεθος του αλφάβητου πχ 24 για ελληνικά, 26 για λατινικά)

Έστω ότι θέλουμε να κρυπτογραφήσουμε το μήνυμα “icantdoit” χρησιμοποιώντας το ακόλουθο κλειδί (K).

$$K = \begin{bmatrix} 9 & 18 & 10 \\ 16 & 21 & 1 \\ 5 & 12 & 23 \end{bmatrix}$$

Το μέγεθος του πίνακα κλειδί είναι 3 χ 3, άρα το μέγεθος του τμήματος είναι 3. Το πρώτο τμήμα είναι το ica. Τα γράμματα μετατρέπονται σε αριθμούς από το 0 έως 25 αναλόγως της θέσης τους στο αλφάβητο. Έτσι το i γίνεται 8, το c γίνεται 2, το α γίνεται 0. Το Block (M) είναι το ακόλουθο:

$$M = \begin{bmatrix} i \\ c \\ a \end{bmatrix} = \begin{bmatrix} 8 \\ 2 \\ 0 \end{bmatrix}$$

Εκτελώντας τον τύπο $C = K * M \pmod{p}$ προκύπτει το ακόλουθο Block κρυπτοκειμένου (C).

$$C = \begin{bmatrix} 9 & 18 & 10 \\ 16 & 21 & 1 \\ 5 & 12 & 23 \end{bmatrix} x \begin{bmatrix} 8 \\ 2 \\ 0 \end{bmatrix} = \begin{bmatrix} 4 \\ 14 \\ 12 \end{bmatrix} = \begin{bmatrix} e \\ o \\ m \end{bmatrix}$$

Αντικαθιστώντας τους αριθμούς με τα αντίστοιχα γράμματα του λατινικού αλφάβητου προκύπτει το κρυπτομήνυμα eom

Επαναλαμβάνουμε για την επόμενη τριάδα γραμμάτων μέχρι να ολοκληρωθεί το μήνυμα.

Για την αποκρυπτογράφηση χρειαζόμαστε τον αντίστροφο του πίνακα κλειδιού Mod 26. Αντίστροφος θεωρείτε αυτός που αν τον πολλαπλασιάσουμε (mod 26) με τον πίνακα κλειδί θα μας δώσει τον μοναδιαίο πίνακα. Στο παράδειγμα μας ο αντίστροφος K^{-1} είναι ο

$$K^{-1} = \begin{bmatrix} 11 & 14 & 24 \\ 21 & 21 & 25 \\ 7 & 12 & 1 \end{bmatrix}$$

Για την αποκρυπτογράφηση ισχύει η σχέση $M = K^{-1} * C \pmod{p}$

(όπου C: Block Κρυπτοκειμένου, M: Block Μηνύματος, K^{-1} : Αντίστροφος mod p για τον πίνακα κλειδί, p : μέγεθος του αλφάβητου πχ 24 για ελληνικά, 26 για λατινικά)

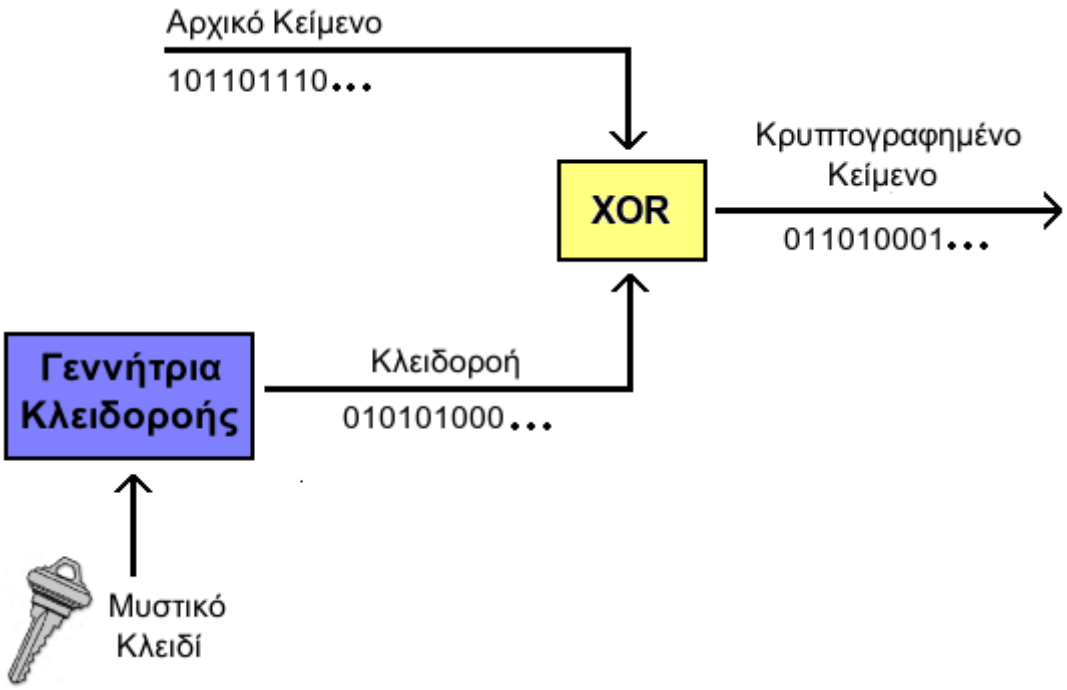
Εφαρμόζοντας τον τύπο προκύπτει M (8,2,0) που είναι το πρώτο Block του μηνύματος.

$$M = \begin{bmatrix} 11 & 14 & 24 \\ 21 & 21 & 25 \\ 7 & 12 & 1 \end{bmatrix} x \begin{bmatrix} 4 \\ 14 \\ 12 \end{bmatrix} = \begin{bmatrix} 8 \\ 2 \\ 0 \end{bmatrix} = \begin{bmatrix} i \\ c \\ a \end{bmatrix}$$

5.3 Κρυπταλγόριθμοι Ροής (Stream Ciphers)

Οι κρυπταλγόριθμοι ροής (ή stream ciphers) αποτελούν μία σύγχρονη, ευρέως χρησιμοποιούμενη, κατηγορία κρυπτογραφικών αλγορίθμων. Συναντώνται ιδίως σε εφαρμογές ασύρματης ή κινητής επικοινωνίας, λόγω του ότι προσφέρονται για κρυπτογραφήσεις υψηλής ταχύτητας και μικρής κατανάλωσης ισχύος.

Οι κρυπταλγόριθμοι ροής κρυπτογραφούν δεδομένα που είναι σε μορφή συνεχόμενης ροής bit ([22],[28],[29],[41]). Μια γεννήτρια κλειδοροής παράγει στην έξοδό της μια ψευδοτυχαία ακολουθία από Bits. Η κλειδοροή αυτή εξαρτάται από ένα μυστικό κλειδί που τροφοδοτεί την γεννήτρια: συνήθως το κλειδί εκφράζει την αρχική κατάσταση της γεννήτριας. Στην συνέχεια εφαρμόζεται ανάμεσα σε κάθε bit του μηνύματος και της κλειδοροής η πράξη XOR (πρόσθεση στο δυαδικό σώμα GF(2)). Το αποτέλεσμα της XOR αποτελεί τα bits του κρυπτοκειμένου. Η διαδικασία αποτυπώνεται στο σχήμα της εικόνας 5.4.



Εικόνα 5.4 πηγή: Wikipedia Διαδικασία Παραγωγής Κρυπτοκειμένου στους Κρυπταλγόριθμους Ροής.

Για την αποκρυπτογράφηση εφαρμόζεται η ίδια ακριβώς διαδικασία. Λόγω του ότι η πρόσθεση XOR είναι μία αυτο-αντιστρεπτή πράξη: αυτήν τη φορά η πράξη XOR γίνεται μεταξύ της κλειδοροής και του κρυπτοκειμένου. Εφόσον η κλειδοροή που δημιουργεί η γεννήτρια είναι ίδια

με αυτή που δημιουργήθηκε κατά την αποστολή του μηνύματος, τότε ανακτάται το αρχικό μήνυμα. Για να δημιουργηθεί η ίδια κλειδοροή απαιτείται φυσικά να τροφοδοτήσουμε την γεννήτρια στην παραλαβή με το ίδιο μυστικό κλειδί που χρησιμοποιήθηκε κατά την αποστολή του μηνύματος.

Η κλειδοροή που δημιουργείτε από την γεννήτρια πρέπει να ικανοποιεί κάποια κριτήρια.

1. Να έχει αρκετά μεγάλη περίοδο επανάληψης. Μια κλειδοροή με μικρή περίοδο επανάληψης είναι ευάλωτη σε επιθέσεις κρυπτανάλυσης.

2. Να είναι «τυχαία». Μια προβλέψιμη, μη τυχαία ακολουθία είναι επίσης ευάλωτη σε επιθέσεις κρυπτανάλυσης.

Η παραγωγή τελείως τυχαίων ακολουθιών από ντετερμινιστικά συστήματα είναι μη εφικτή[1]: ο απώτερος στόχος είναι η κατασκευή ψευδοτυχαίων ακολουθιών, ήτοι ακολουθιών που προσομοιάζουν τυχαίες ακολουθίες. Υπάρχουν διάφορα κριτήρια για την αποτίμηση της τυχαιότητας μίας ακολουθίας: τα ακόλουθα προτάθηκαν από τον Golomb :

1. Να έχουν ισοκατανεμημένο πλήθος από 0 και 1 (***Balance Property***)

2. Σε μια περίοδο, οι μισές διαδρομές να έχουν μήκος 1, Το ¼ των διαδρομών μήκος 2. Το 1/8 των διαδρομών μήκος 3, …, Το $1/2^{\nu}$ των διαδρομών μήκος ν (***Run Property***). Σαν διαδρομή ορίζεται ένα τμήμα μιας ακολουθίας που αποτελείτε μόνο από 0, ή μόνο από 1.

3. Η συνάρτηση αυτόσυσχέτισης

$$C(\tau) = \sum_{i=0}^{N-1} (-1)^{a_i \oplus a_{i+\tau}}$$

για την ακολουθία a0,a1,… περιόδου N μπορεί να πάρει μόνο δύο τιμές: να είναι σταθερή (ίση με K) για $\tau \neq 0$, και τιμή N για $\tau=0$. (***two-level autocorrelation property***).

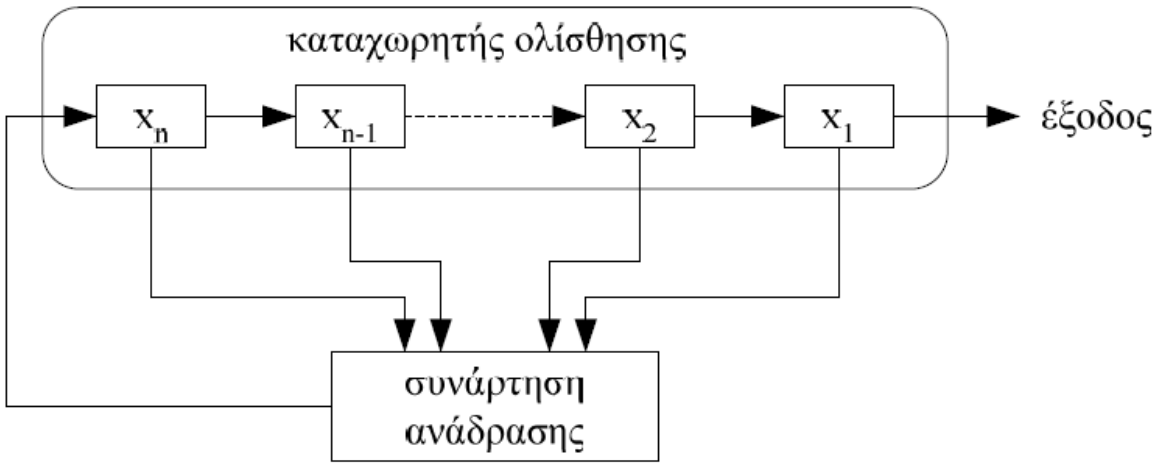
[1] Χαρακτηριστική είναι και η ρήση του J. N. Neumann: "Any one who considers arithmetical methods of producing random digits is, of course, in a state of sin"

Όπως όμως θα καταδείξουμε στη συνέχεια, τα ανωτέρω κριτήρια δεν είναι αρκετά.

5.3.1 Καταχωρητές ολίσθησης με ανάδραση (Linear Feedback Shift Register)

Για γεννήτρια παραγωγής κλειδοροής χρησιμοποιούνται αρκετά συχνά, καταχωρητές ολίσθησης με ανάδραση (LFSR).

Οι καταχωρητές ολίσθησης με ανάδραση είναι αυτοί των οποίων η έξοδος τροφοδοτείται από μια συνάρτηση της οποίας το αποτέλεσμα τροφοδοτείται με τη σειρά του στην είσοδο του καταχωρητή, όπως φαίνεται στην Εικόνα 5.5.



Εικόνα 5.5 πηγή: [59] Κάτος. Καταχωρητής ολίσθησης με ανάδραση.

Ο καταχωρητής ολίσθησης έχει την ικανότητα αποθήκευσης n δυαδικών στοιχείων (μνήμη των n bits). Ανά τακτά χρονικά διαστήματα, το κάθε στοιχείο αποθήκευσης x_i, μεταφέρει το περιεχόμενό του στο γειτονικό x_{i-1}. Το περιεχόμενο του x_1 παρουσιάζεται στην έξοδο της γεννήτριας, ενώ το xn αποθηκεύει το αποτέλεσμα της συνάρτησης ανάδρασης με είσοδο το διάνυσμα $(x_1,x_2,\ldots,x_n)$ [59]

Οι LFSR παρουσιάζουν τις ακόλουθες ιδιότητες:

- Το πλήθος των διαφορετικών καταστάσεων από τις οποίες μπορεί να διέλθει είναι το πολύ από 2^n -1: όλοι οι πιθανοί συνδυασμοί εκτός της μηδενικής κατάστασης (η μηδενική κατάσταση είναι μη αποδεκτή αφού εγκλωβίζει το κύκλωμα να παράγει συνεχώς μηδενικά). Η μέγιστη περίοδος της κλειδοροής είναι δηλαδή 2^n -1.

- Αν ένας LFSR επιτυγχάνει τη μέγιστη δυνατή περίοδο τότε καλείται πρωταρχικός (primitive). Ένας πρωταρχικός LFSR παράγει ακολουθίες μέγιστου μήκους. Η ακολουθία που παράγεται από έναν LFSR ικανοποιεί πάντα τα 3 κριτήρια τυχαιότητας του Golomb.

- Η ακολουθία εξόδου ενός LFSR εξαρτάται από την αρχική του κατάσταση (στις κρυπτογραφικές υλοποιήσεις αποτελεί το μυστικό κλειδί), καθώς και από την ανάδραση του.

- Η ανάδραση καθορίζει αν ένας LFSR είναι πρωταρχικός ή όχι.

Η χρήση των LFSR (ειδικά των πρωταρχικών) για γεννήτριες κλειδοροής παρουσιάζει τα ακόλουθα πλεονεκτήματα:

- Εύκολη υλοποίηση.

- Γρήγορη λειτουργία.

- Καλά χαρακτηριστικά τυχαιότητας.

- Παρέχει ακολουθίες μεγάλης περιόδου.

Παρόλα αυτά ο LFSR είναι ευάλωτος σε επιθέσεις τύπου Known-plain-text (ακόμα και αν το σύστημα παραγωγής της κλειδοροής κρατείται μυστικό). Στις επιθέσεις αυτές γνωρίζουμε μέρος του αρχικού μηνύματος. Εφαρμόζοντας την πράξη XOR μεταξύ του κρυπτοκειμένου και του μηνύματος ανακαλύπτεται μέρος της κλειδοροής. Αν γνωρίζουμε 2*N bit της κλειδοροής (όπου N το μέγεθος του LFSR που παράγει την ακολουθία) μπορούμε να βρούμε έναν πρωταρχικό LFSR που να παράγει ολόκληρη την κλειδοροή (Αλγόριθμος Berlekamp-Massey): αυτό συμβαίνει γιατί οι ακολουθίες που παράγονται από έναν LFSR έχουν χαμηλή γραμμική πολυπλοκότητα (όπως αυτή ορίζεται στη συνέχεια). Γιαυτό ο LFSR συνήθως χρησιμοποιείται ως μέρος πιο σύνθετων δομών.

5.3.2 Γραμμική πολυπλοκότητα (Linear Complexity)

Έστω η ακολουθία a = [a_1, a_2, …] και έστω a^n τα πρώτα n bits της ακολουθίας αυτής. Ως γραμμική πολυπλοκότητα της a^n ονομάζουμε τον ελάχιστο αριθμό στοιχείων, συμβολικά LC(a^n), ενός καταχωρητή ολίσθησης, που απαιτούνται για να παραχθεί η ακολουθία a^n [59]

Για παράδειγμα έστω η ακολουθία 1011100. Η συγκεκριμένη ακολουθία μπορεί να δημιουργηθεί από ένα LFSR με αρχική κατάσταση 101, και ανάδραση στα bit 2,3. Ο συγκεκριμένος LFSR είναι και ο μικρότερος σε μέγεθος που μπορεί να δημιουργήσει την συγκεκριμένη ακολουθία (φυσικά υπάρχουν πολλοί σε αριθμό LFSR μεγαλύτερου μήκους με την ίδια έξοδο). Αφού το μήκος του είναι 3 bits άρα και η ακολουθία έχει γραμμική πολυπλοκότητα 3.

Η γραμμική πολυπλοκότητα ενός LFSR εξαρτάτε μόνο από την συνάρτηση ανάδρασης. Αποτελεί ένα από τα μετρίσιμα στοιχεία που αξιολογούν την ασφάλεια ενός κρυπτογραφικού αλγορίθμου. Φυσικά όσο μεγαλύτερη η γραμμική πολυπλοκότητα τόσο πιο ασφαλής η διαδικασία.

Μια διαδικασία υπολογισμού του μικρότερου σε μήκος LFSR που παράγει μια συγκεκριμένη ακολουθία από bits (άρα και της γραμμικής της πολυπλοκότητας) υλοποιείται με τον αλγόριθμο Berlekamp-Massey.

5.3.3 Αλγόριθμος Berlekamp-Massey

Καθώς αποκαλύπτονται ένα ένα τα bits της ακολουθίας διαμορφώνεται το μέγεθος του LFSR και της συνάρτησης ανάδρασης. Αρχικά το μέγεθος του LFSR είναι 1 και για κάθε νέο bit που προστίθεται στην ακολουθία, ελέγχεται αν είναι απαραίτητη η αύξηση του μήκους του LFSR και η αναπροσαρμογή της ανάδρασης. Με την εισαγωγή και του τελευταίου bit της ακολουθίας ολοκληρώνεται η διαδικασία και ο αλγόριθμος έχει υπολογίζει τον μικρότερο LFSR που παράγει την ακολουθία άρα και την γραμμική πολυπλοκότητα της ακολουθίας. Αναλυτικά ο αλγόριθμος [29] (όπου η συνάρτηση ανάδρασης περιγράφεται ισοδύναμα με το χαρακτηριστικό πολυώνυμο – βλ. π.χ. [29]):

1. Αρχικές τιμές:
   $f(x) \leftarrow 1$, χαρακτηριστικό πολυώνυμο
   $b(x) \leftarrow 1$, προσωρινή μεταβλητή
   $l \leftarrow 0$, μέγεθος καταχωρητή ολίσθησης
   $N \leftarrow 0$, μετρητής
   $m \leftarrow -1$, προσωρινή αποθήκευση μετρητή
2. Αν $N \models n-1$ τότε πήγαινε στο (10).
3. Υπολόγισε τη διαφορά της πρόβλεψης από την ακολουθία:
   $$d = a_N + \sum_{i=0}^{l-1} c_i a_{N+i-l}$$
4. Υπάρχει διαφορά; Αν όχι, ($d = 0$) τότε πήγαινε στο (9)
5. Αν ναι, ($d = 1$) τότε:
   $f'(x) \leftarrow f(x)$ αποθήκευσε το πολυώνυμο
   $f(x) \leftarrow f(x) + b(x)x^{N-m}$ υπολόγισε τη νέα μορφή
6. Το μέγεθος του καταχωρητή είναι μεγαλύτερο του $\frac{N}{2}$;
7. Αν ναι, ($l > \frac{N}{2}$) τότε πήγαινε στο (9).
8. Αν όχι, ($l \le \frac{N}{2}$) τότε:
   $l \leftarrow N+1-l$ αύξησε το μέγεθος του καταχωρητή ανάλογα
   $b(x) \leftarrow f'(x)$ αποθήκευσε το παλιό πολυώνυμο
   $m \leftarrow N$ αποθήκευσε την τρέχουσα τιμή του N.
9. Αύξησε το $N \leftarrow N+1$ και πήγαινε στο (2)
10. Το χαρακτηριστικό πολυώνυμο είναι το $f(x)$. Τέλος!

Εικόνα 5.6 Ψευδοκώδικας Αλγόριθμου Berlekamp-Massay (πηγή: [59])

5.3.4 Ασφάλεια Καταχωρητών Ολίσθησης με Γραμμική Ανάδραση (LFSR)

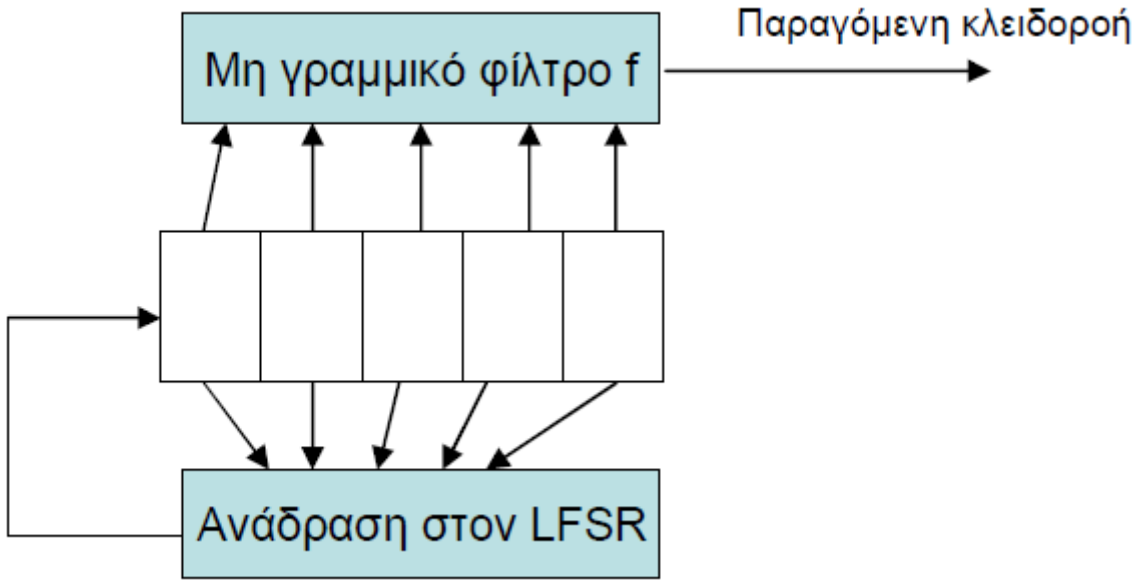
Η Γραμμική πολυπλοκότητα είναι μετρήσιμο στοιχείο ασφάλειας ενός κρυπτογραφικού αλγορίθμου. Σε τι βαθμό όμως την επηρεάζει;

Έστω μια ακολουθία με γραμμική πολυπλοκότητα L. Με τον αλγόριθμο Berlekamp-Massay απαιτούνται 2*L διαδοχικά bits μόνο, για να εντοπιστεί ο ελάχιστος LFSR που την παράγει. Στην περίπτωση που αυτός είναι μοναδικός έχουμε εντοπίσει την γεννήτρια όλης της ακολουθίας. Για παράδειγμα ακολουθία μεγέθους 2^{10}-1 bits, απαιτεί την γνώση 20 (2*10) διαδοχικών bits της κλειδοροής για να σπάσει (με τον αλγόριθμο Berlekamp-Massay) και να αναπαραχθεί ολόκληρη

η κλειδοροή. Γνώση της κλειδοροής και του κρυπτοκειμένου όμως συνεπάγεται και αποκάλυψη του μηνύματος. Ακολουθία με μικρή γραμμική πολυπλοκότητα μεταφράζεται σε «προβλέψιμη» ακολουθία με χαμηλό δείκτη ασφάλειας.

5.3.5 Μη Γραμμικά Φίλτρα

Μια υλοποίηση γεννήτριας κλειδοροής που βασίζεται σε LFSR είναι τα μη γραμμικά φίλτρα. Η διαφορά από έναν απλό LFSR είναι ότι η έξοδος της κλειδοροής δεν προέρχεται από το bit 0 του LFSR, αλλά από την εφαρμογή μιας λογικής συνάρτησης στα bit του LFSR.



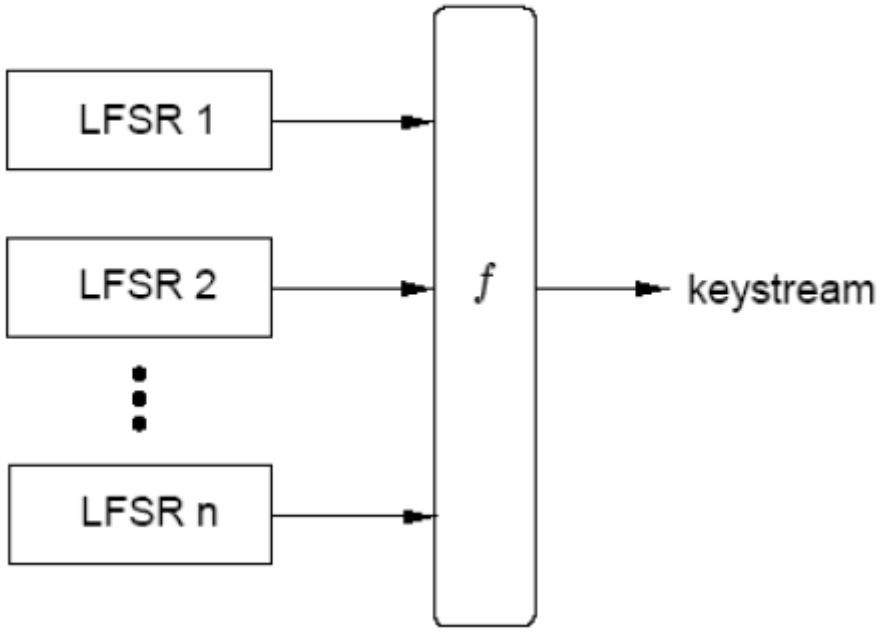
Εικόνα 5.7 Μη γραμμικό φίλτρο.

Αφού η έξοδος δεν είναι από τον LFSR θα πρέπει να προσεχθεί η λογική συνάρτηση να παράγει ακολουθία που να είναι ισοβαρής. Να έχει δηλαδή ισοκατανεμημένο πλήθος από 0 και 1. Γενικά η υλοποίηση της γεννήτριας με την χρήση μη γραμμικού φίλτρου μπορεί να αυξήσει σημαντικά την γραμμική πολυπλοκότητα της παραγόμενης ακολουθίας, βελτιώνοντας τα χαρακτηριστικά ασφαλείας.

Αποδεικνύεται ότι για κατάλληλη επιλογή του μη γραμμικού φίλτρου μπορούν να παραχθούν ακολουθίες εγγυημένα πολύ υψηλής γραμμικής πολυπλοκότητας (βλ. π.χ. Κεφάλαιο 8 στο [06]).

5.3.6 Μη Γραμμικοί Συνδυαστές

Μια διαφορετική υλοποίηση γεννήτριας κλειδοροής που επίσης προσφέρει χαρακτηριστικά μη γραμμικότητας είναι οι μη γραμμικοί συνδυαστές. Εδώ πολλοί διαφορετικοί LFSR τροφοδοτούν τις εισόδους μιας λογικής συνάρτησης. Η κλειδοροή και εδώ είναι η έξοδος της λογικής συνάρτησης. Με κατάλληλη επιλογή της συνάρτησης και των LFSR μπορούμε να διασφαλιστεί μεγάλη περίοδος κλειδοροής αλλά και αυξημένη γραμμική πολυπλοκότητα.



Εικόνα 5.8 Πηγή σχήματος [33] Μη γραμμικός συνδυαστής.

Η ακριβής τιμή της γραμμικής πολυπλοκότητας της παραγόμενης κλειδοροής αποδεικνύεται ότι μπορεί να είναι πολύ υψηλή για κατάλληλη επιλογή των LFSRs και τη συνάρτησης f (βλ. π.χ. Κεφάλαιο 8 στο [06]).

5.3.7 Άλλες τεχνικές παραγωγής κλειδοροής

Υπάρχουν και άλλες τεχνικές για την παραγωγή ακολουθιών υψηλής γραμμικής πολυπλοκότητας, όπως για παράδειγμα οι χρονικά ελεγχόμενοι καταχωρητές ή οι μη γραμμικοί καταχωρητές με ανάδραση (βλ. πχ. Κεφ. 8 στο [06]). Οι τεχνικές αυτές χρησιμοποιούνται σε σύγχρονους αλγορίθμους (όπως π.χ. οι αλγόριθμοι Trivium, Grain που προτάθηκαν στο πλαίσιο

του προγράμματος eSTREAM[2]). Οι γεννήτριες αυτές εμφανίζεται να είναι ανθεκτικές στις γνωστές κρυπταναλυτικές τεχνικές, ωστόσο το θεωρητικό υπόβαθρο που γνωρίζουμε για να αποτιμήσουμε μαθηματικά την ασφάλειά τους δεν είναι τόσο πλούσιο.

5.4 Κρυπταλγόριθμοι Τμήματος

Εκτός από τους αλγόριθμους ροής, μία άλλη σημαντική κατηγορία συμμετρικών αλγορίθμων κρυπτογράφησης είναι οι κρυπταλγόριθμοι τμήματος (block ciphers). Στους κρυπταλγόριθμους τμήματος το μήνυμα χωρίζεται σε τμήματα (block) σταθερού μεγέθους. Το κάθε τμήμα που προκύπτει κρυπτογραφείται ξεχωριστά από τα υπόλοιπα. Αφού η κρυπτογράφηση συντελείται πάνω σε τμήμα από bits και όχι σε μεμονωμένα bits (όπως στους κρυπταλγορίθμους ροής), η πράξη της κρυπτογράφησης μπορεί να είναι πιο σύνθετη από ότι μία πράξη XOR.

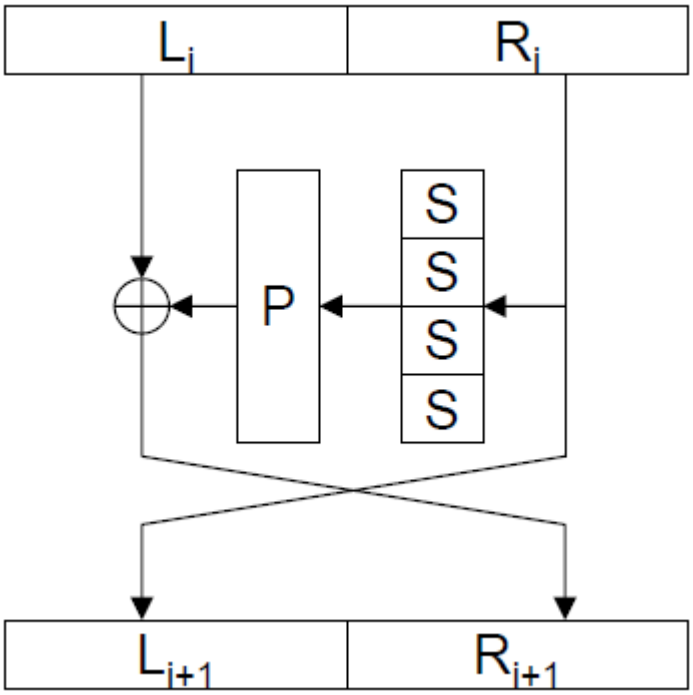
Αν και για τους αλγορίθμους ροής δεν υπήρξε επίσημα καθιερωμένο διεθνές πρότυπο κρυπτογράφησης, αυτό δεν ισχύει για τους κρυπταλγορίθμους τμήματος: επί τρεις σχεδόν δεκαετίες υπήρξε ο πρότυπος αλγόριθμος DES, ο οποίος αντικαταστάθηκε πλέον (από το Νοέμβριο του 2000) από τον αλγόριθμο AES.

5.4.1 Αλγόριθμος DES

Ο αλγόριθμος DES (Data Encryption Standard) ([04],[05],[07],[10],[30],[51]) ορίστηκε σαν πρότυπο κρυπτογράφησης στις 23 Νοεμβρίου 1976.

Δίκτυα Feistel

[2] http://www.ecrypt.eu.org/stream/

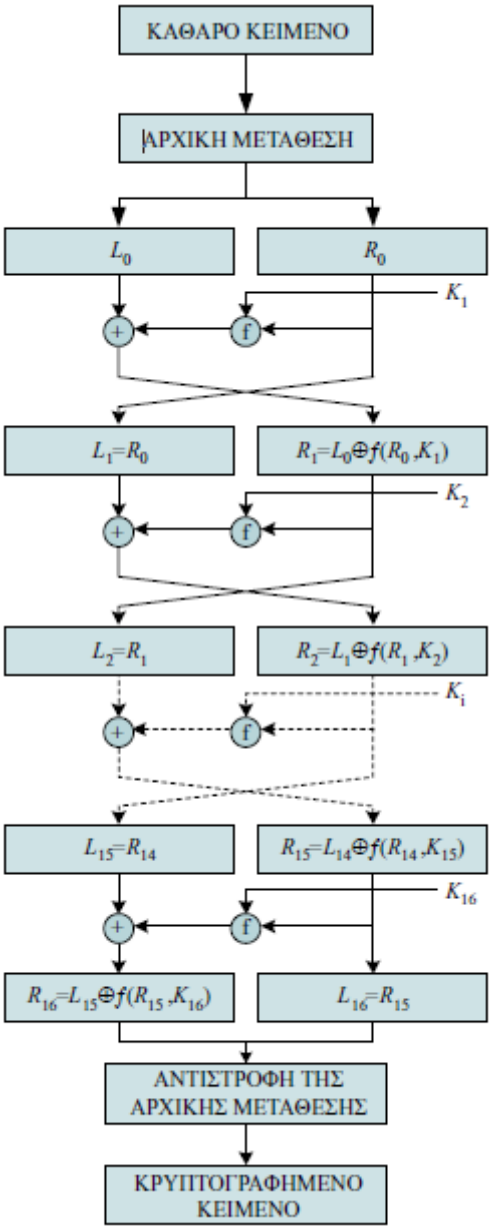


Εικόνα 5.9 Γύρος σε δίκτυο Feistel.

Μια συνηθισμένη πρακτική που υλοποιείται σε πολλούς κρυπταλγόριθμους τμήματος (συμπεριλαμβανομένου του DES) είναι τα δίκτυα Feistel. Στην είσοδο, το block του μηνύματος χωρίζεται σε δύο μέρη (συνήθως ίσου μεγέθους). Το δεξί τμήμα τροφοδοτεί χωρίς τροποποίηση την αριστερή βαθμίδα της εξόδου. Στο δεξί τμήμα της εισόδου εφαρμόζεται κάποια συνάρτηση μετατροπής και στο αποτέλεσμα γίνεται η πράξη XOR με το αριστερό τμήμα της εισόδου. Το νέο αποτέλεσμα τροφοδοτεί το δεξί τμήμα της εξόδου.

Η συνάρτηση μετατροπής υλοποιείται με 2 κυρίως λειτουργίες. Η πρώτη κάνει αντικαταστάσεις στα bit του Block, και η άλλη αντιμεταθέσεις. Τα κυκλώματα των αντικαταστάσεων καλούνται substitution boxes ή s-boxes. Τα κυκλώματα των αντιμεταθέσεων καλούνται permutation boxes ή p-boxes.

Κρυπτογράφηση



Εικόνα 5.10 πηγή:[15] Διαδικασία Κρυπτογράφησης στον DES

Στον αλγόριθμο DES, ο οποίος ακολουθεί τη δομή Feistel. η διαδικασία κρυπτογράφησης περιγράφεται από τα ακόλουθα βήματα.

1ο Βήμα: Το μήνυμα μετατρέπεται σε ακολουθία από bits και χωρίζεται σε τμήματα (blocks) των 64 bits.

2ο Βήμα: Αρχική μετάθεση

IP							
58	50	42	34	26	18	10	2
60	52	44	36	28	20	12	4
62	54	46	38	30	22	14	6
64	56	48	40	32	24	16	8
57	49	41	33	25	17	9	1
59	51	43	35	27	19	11	3
61	53	45	37	29	21	13	5
63	55	47	39	31	23	15	7

Εικόνα 5.11 Πίνακας Αρχικής Αντιμετάθεση (IP) στον DES

Στα bits του τμήματος εφαρμόζεται μια αρχική μετάθεση σύμφωνα με τον πίνακα IP. Στην 1η θέση του block μεταφέρεται το 58ο bit, στην 2η θέση το 50ο bit κ.ο.κ.

3ο Βήμα: Ακολουθούν 16 γύροι δικτύου Feistel. Στην συνάρτηση f υπεισέρχεται το μυστικό κλειδί κάθε γύρου και υλοποιείτε από sbox και pbox.

4ο Βήμα: Αντιστροφή της αρχικής μετάθεσης.

IP^{-1}							
40	8	48	16	56	24	64	32
39	7	47	15	55	23	63	31
38	6	46	14	54	22	62	30
37	5	45	13	53	21	61	29
36	4	44	12	52	20	60	28
35	3	43	11	51	19	59	27
34	2	42	10	50	18	58	26
33	1	41	9	49	17	57	25

Εικόνα 5.12 Πίνακας Αντιστροφής Αρχικής Αντιμετάθεσης (IP^{-1}) στον DES

Στο Block που προέρχεται από το 16ο γύρο εφαρμόζεται αντιστροφή της αρχικής μετάθεσης σύμφωνα με τον πίνακα IP^{-1}.

Το block που προκύπτει είναι το κρυπτογραφημένο block.

Παραγωγή Υποκλειδιών

Στον DES το κλειδί αποτελείτε από 56 bit. Σε αυτό προστίθενται κάποια bit ισοτιμίας που εισέρχονται στις θέσεις 8,16,24,…64. Σε κάθε γύρο από τους 16 γύρους του DES χρησιμοποιείτε ένα διαφορετικό 48bit υποκλειδί που προκύπτει με μια διαδικασία μετασχηματισμών και ολισθήσεων στα bit του αρχικού κλειδιού.

Αποκρυπτογράφηση

Η αποκρυπτογράφηση πραγματοποιείτε με την ίδια ακριβώς διαδικασία με την διαφορά ότι αλλάζει η σειρά των κλειδιών του κάθε γύρου. Το 16ο κλειδί στην διαδικασία κρυπτογράφησης χρησιμοποιείτε στον 1ο γύρο της αποκρυπτογράφησης. Το 15ο στο 2ο κ.ο.κ.

5.4.2 3DES (Triple DES)

Ο αλγόριθμος DES έχει πολύ μικρό μέγεθος κλειδιού, μόλις 56 bits. Έτσι θεωρείται πλέον ανασφαλής αλγόριθμος (και αυτός είναι και ο λόγος για το ότι, ήδη από το 1997, ξεκίνησε η διαδικασία υιοθέτησης νέου προτύπου). Ο 3DES μπορεί να θεωρηθεί μια εξέλιξη που DES που άρει την αδυναμία του μικρού κλειδιού (χρησιμοποιείται ευρέως και σήμερα, αν και δεν αποτελεί πρότυπο κρυπτογράφησης λόγω της σχετικά χαμηλής του απόδοσης). Χρησιμοποιεί τρείς κρυπτογραφήσεις του απλού DES στην σειρά, που ο καθένας έχει το δικό του 56bit κλειδί. Η συνάρτηση κρυπτογράφησης είναι η ακόλουθη:

$$Κρυπτοκείμενο = E_{k3}(D_{k2}(E_{k1}(μήνυμα)))$$ όπου k_1,k_2,k_3 τα κλειδιά των DES

Δηλαδή κρυπτογραφούμε με το k3, έπειτα αποκρυπτογραφούμε με το k2, και τέλος κρυπτογραφούμε με το k1. Ουσιαστικά κρυπτογραφούμε με μέγεθος κλειδιού 3 χ 56 = 168 bits. Κάθε διαδικασία τριπλής κρυπτογράφησης εφαρμόζεται σε Block κειμένου 64 bits. Ο συγκεκριμένος αλγόριθμος παρουσιάζει ένα ενδιαφέρον χαρακτηριστικό. Αν χρησιμοποιηθεί

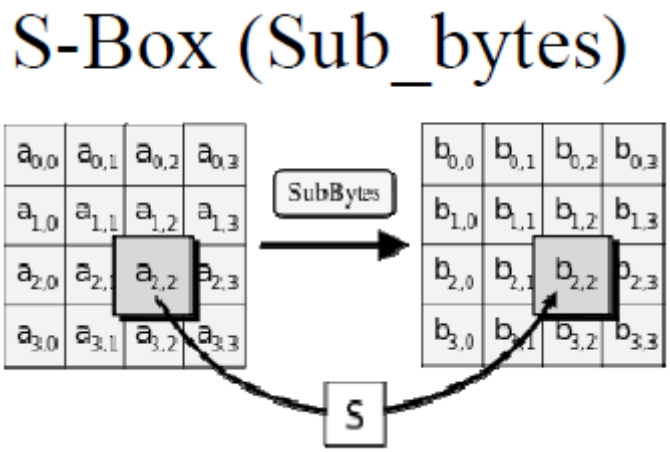
κοινό κλειδί τότε συμπεριφέρεται σαν τον απλό DES. Αυτό συμβαίνει αφού τα 2 πρώτα βήματα με κοινό κλειδί επιστρέφουν το αρχικό μήνυμα και ουσιαστικά εφαρμόζεται μία κρυπτογράφηση στο 3ο βήμα. Έτσι ένα κύκλωμα 3DES μπορεί να χρησιμοποιηθεί και για κρυπτογράφηση & αποκρυπτογράφηση απλού DES.

5.4.3 AES (Advanced Encryption Standard).

Ο AES ([01],[12],[36]) ορίστηκε σαν πρότυπο κρυπτογράφησης τον Νοέμβριο του 2001. Αντικατέστησε τον αλγόριθμο DES και είναι πλέον ο προτεινόμενος αλγόριθμος κρυπτογράφησης. Τα Block που χειρίζεται ο αλγόριθμος είναι μεγέθους 128 bits. Τα μήκη κλειδιού που υποστηρίζει είναι 128, 192 και 256. Ο AES βασίζεται στον αλγόριθμο κρυπτογράφησης Rijndael. Ο αλγόριθμος ορίζει ένα πλήθος από γύρους επεξεργασίας των block. Το πλήθος των γύρων επεξεργασίας εξαρτάτε από το μέγεθος του κλειδιού. Για κλειδί 128 bits απαιτούνται 10 γύροι, για 192 bits 12 γύροι και για 256 Bits κλειδί 14 γύροι. Σε κάθε γύρο πραγματοποιούνται μια σειρά από μετασχηματισμούς (σε επίπεδο byte). Συγκεκριμένα οι τέσσερις μετασχηματισμοί που εφαρμόζονται είναι:

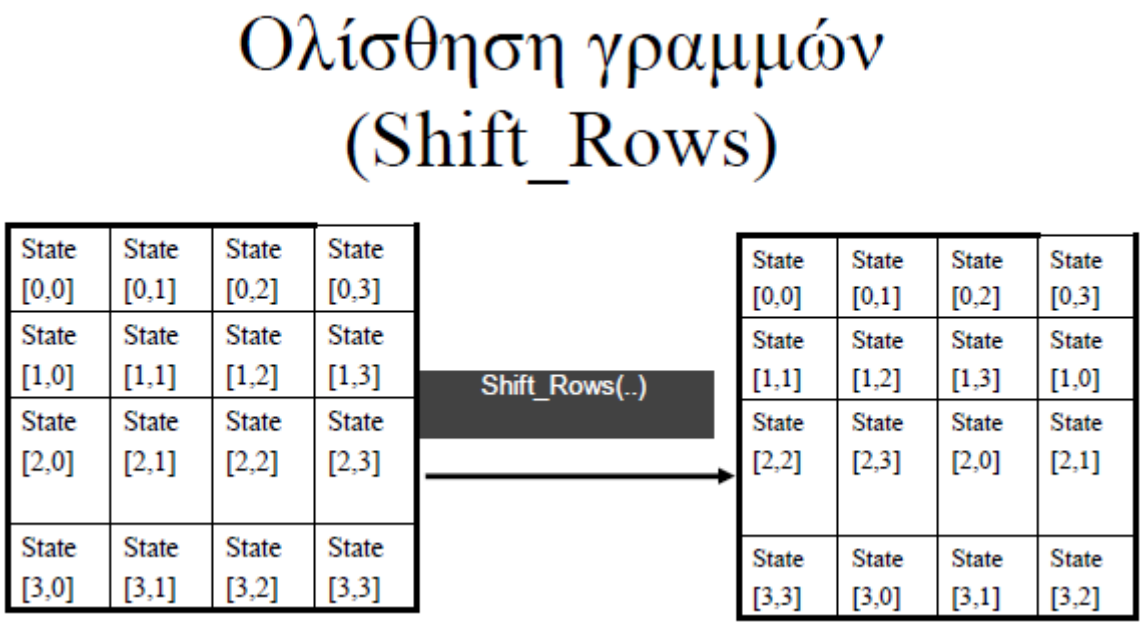
- Sub_Bytes. Μετασχηματισμός αντικατάστασης με χρήση σχετικού πίνακα.
- Shift_Rows. Διαδικασία ολίσθησης των bytes.
- MixColumns. Διαδικασία ανάμειξης των bytes.
- Add_Round_Key. Προσθήκη ενός υποκλειδιού.

Μετασχηματισμοί & λειτουργίες



Εικόνα 5.13 Μετασχηματισμός Sub_Bytes

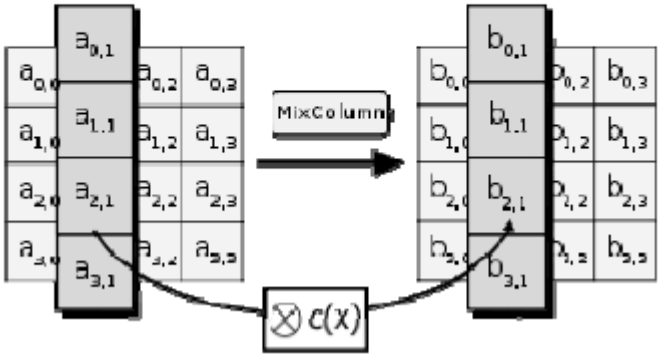
Εδώ κάθε byte a(i,j) μετατρέπεται σε ένα νέο byte b(i,j). Η συνάρτηση μετατροπής είναι ισχυρά μη γραμμική ώστε να προσφέρει ισχυρά χαρακτηριστικά ασφαλείας.



Εικόνα 5.14 Μετασχηματισμός Shift_Rows

Η 1η γραμμή δεν ολισθαίνει καθόλου. Η 2η γραμμή ολισθαίνει κατά 1 θέση αριστερά. Η 3η γραμμή ολισθαίνει κατά 2 θέσεις αριστερά. Η 4η γραμμή ολισθαίνει κατά 3 θέσεις αριστερά.

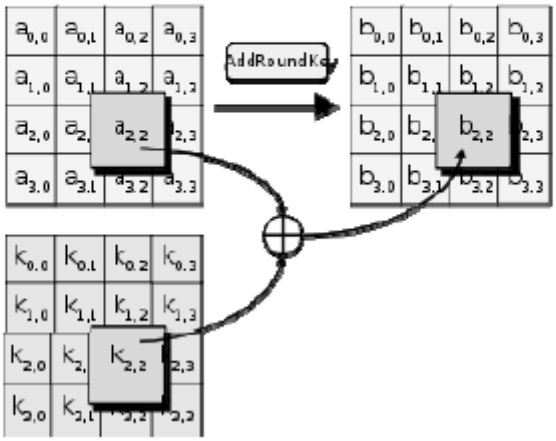
Μείξη στηλών (MixColumn)



Εικόνα 5.15 Μετασχηματισμός Mix_Column

Κάθε στήλη του πίνακα πολλαπλασιάζεται με ένα πίνακα 4 x 4. δημιουργώντας μια νέα τροποποιημένη στήλη.

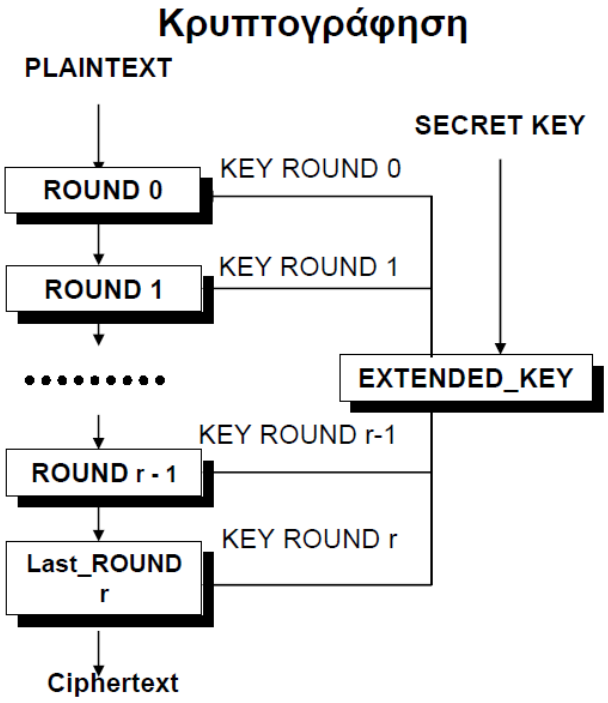
Πρόσθεση υπο-κλειδιού (Add_Round_Key)



Εικόνα 5.16 Μετασχηματισμός Add_Round_Key

Πραγματοποιείτε η πράξη XOR μεταξύ του Block και του υποκλειδιού του γύρου.

Κρυπτογράφηση



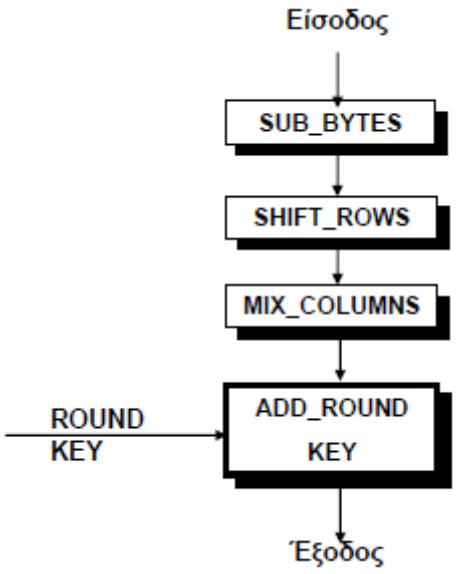
Εικόνα 5.17 Διαδικασία Κρυπτογράφηση στον AES

Στον αλγόριθμο AES η διαδικασία κρυπτογράφησης περιγράφεται από τα ακόλουθα βήματα.

1ο Βήμα: Το μήνυμα μετατρέπεται σε ακολουθία από bits και σπάει σε τμήματα (blocks) των 128 bits (ή σε μορφή πίνακα 4 x 4 Bytes).

2ο Βήμα: Στον 1ο γύρο στο block εφαρμόζεται η πράξη **XOR** με το μυστικό κλειδί.

3ο Βήμα Ακολουθούν 9 γύροι με μετασχηματισμούς.



Εικόνα 5.18 Ένας Τυπικός Γύρος στον AES

Οι μετασχηματισμοί αυτοί είναι οι Sub_Bytes, Shift_Rows, Mix. Επίσης προστίθεται (πράξη XOR) κάθε φορά και ένα διαφορετικό υποκλειδί (Add_Round_key).

4ο Βήμα: Ο τελευταίος γύρος διαφοροποιείτε από τους προηγούμενους γιατί δεν πραγματοποιείτε η λειτουργία Mix_Columns.

Αποκρυπτογράφηση

Πραγματοποιούνται οι αντίστροφοι μετασχηματισμοί κατά σειρά και με την αντίστροφη σειρά (Inv_Mix_Columns, Inv_Shift_Rows, Inv_Sub_Bytes). Η αποκρυπτογράφηση υλοποιείτε πιο αργά από την κρυπτογράφηση. Παρόλα αυτά η ταχύτητα της συνολικής διαδικασίας είναι ικανοποιητική σε σύγκριση με άλλους αλγορίθμους.

5.5 Αλγόριθμοι Δημοσίου Κλειδιού

Οι αλγόριθμοι δημοσίου κλειδιού αναπτύχθηκαν για να δώσουν λύση σε δυο προβλήματα που αντιμετώπιζαν οι συμμετρικοί αλγόριθμοι κρυπτογράφησης.

1. Πώς θα γίνει ασφαλής ανταλλαγή του μυστικού κλειδιού ανάμεσα σε αποστολέα και παραλήπτη (key distribution).

2. Πώς θα αποδειχθεί η γνησιότητα ενός ψηφιακού μηνύματος ή εγγράφου. Η γνησιότητα αναφέρεται στην πιστοποίηση ότι το μήνυμα ανήκει πραγματικά στον αποστολέα που αναφέρεται στο μήνυμα, και στο ότι το μήνυμα δεν αλλοιώθηκε η παραποιήθηκε κατά την μεταφορά του (ψηφιακή υπογραφή).

Οι αλγόριθμοι δημοσίου κλειδιού χρησιμοποιούν διαφορετικό κλειδί κατά την κρυπτογράφηση του μηνύματος και διαφορετικό κατά την αποκρυπτογράφηση.

- Το δημόσιο κλειδί (η public key), είναι γνωστό σε όλους και χρησιμοποιείτε για την κρυπτογράφηση του μηνύματος. Χρησιμοποιείτε επίσης για την επιβεβαίωση της ψηφιακής υπογραφής.

- Το ιδιωτικό κλειδί το γνωρίζει μόνο ο παραλήπτης και το χρησιμοποιεί για να αποκρυπτογραφήσει το μήνυμα. Επίσης χρησιμοποιείται για να υπογράψει ο αποστολέας το μήνυμα.

Προϋποθέτει να είναι υπολογιστικά αδύνατο κάποιος που ξέρει το δημόσιο κλειδί να μπορεί να προσδιορίσει το ιδιωτικό κλειδί.

5.5.1 Αλγόριθμος Diffie Hellman

Ο αλγόριθμος αυτός προτάθηκε από τους Diffie και Hellman το 1976 [16]. Δεν είναι αλγόριθμος κρυπτογράφησης; σκοπός του είναι μόνο η ασφαλής ανταλλαγή κλειδιού μεταξύ αποστολέα και παραλήπτη. Συνήθως το κλειδί που ανταλλάσσεται είναι το κλειδί κάποιου συμμετρικού αλγορίθμου, που αναλαμβάνει στην συνέχεια την κρυπτογράφηση.

Περιγραφή της Διαδικασίας

Οι δύο χρήστες που επιθυμούν να ανταλλάξουν μια μυστική ποσότητα, συμφωνούν χωρίς καμία μυστικότητα (δημόσια), σε δύο αριθμούς. Ο πρώτος είναι ένας μεγάλος πρώτος αριθμός, έστω p. Ο δεύτερος είναι γεννήτορας (mod p) - έστω g. Το ζεύγος των αριθμών (p,g) είναι γνωστό σε όλους. Ο καθένας τους επιλέγει από έναν μυστικό αριθμό. Έστω x ο μυστικός αριθμός του

πρώτου χρήστη και y του δεύτερου χρήστη. Οι χρήστες υπολογίζουν αντίστοιχα τις ποσότητες $x' = g^x \pmod p$ και $y' = g^y \pmod p$ και τις ανταλλάσουν δημόσια. Η διαδικασία ολοκληρώνεται με τον υπολογισμό της ποσότητας $(y')^x$ για τον 1ο χρήστη και της ποσότητας $(x')^y$ για τον 2ο χρήστη. Οι δύο ποσότητες είναι ίδιες και εκφράζουν τον αριθμό που αντάλλαξαν με ασφάλεια.

Απόδειξη:

$$(y')^x = \left(g^y\right)^x = g^{yx} = g^{xy}$$

$$(x')^y = \left(g^x\right)^y = g^{xy}$$

Ανακεφαλαιώνοντας

	1ος Χρήστης	2ος Χρήστης
Δημόσιο κλειδί	(p,g,g^x)	(p,g,g^y)
Ιδιωτικό κλειδί	x	y
Πληροφορία που ανταλλάσσεται	g^{xy}	g^{xy}

Πίνακας 5.3 Πληροφορία που ανταλλάσσεται στον αλγόριθμο Diffie-Hellman

Για μεγάλα p,g η γνώση των δημοσίων κλειδιών δεν μπορεί να μας οδηγήσει σε ανακάλυψη ούτε των ιδιωτικών κλειδιών, ούτε φυσικά της πληροφορίας που ανταλλάσσεται. Το δυσκολία έγκειται στο πρόβλημα υπολογισμού του διακριτού λογαρίθμου (discrete logarithm problem). Όταν δηλαδή γνωρίζουμε το $g^x \pmod p$, g και p, δεν υπάρχει αποδοτικός αλγόριθμος υπολογισμού του x (για αρκούντως μεγάλα p, g, x).

5.5.2 Αλγόριθμος RSA

Ο αλγόριθμος RSA ([38],[39],[52])πήρε το όνομα του από τους Rivest, Shamir & Adleman. Είναι αλγόριθμος δημοσίου κλειδιού. Η ασφάλεια του οφείλεται στο ότι δεν υπάρχει αποδοτικός αλγόριθμος για την παραγοντοποίηση μεγάλων αριθμών. Παραγοντοποίηση καλείται η ανάπτυξη ενός αριθμού σαν γινόμενο πρώτων αριθμών.– δηλαδή, με άλλα λόγια, η εύρεση όλων των πρώτων παραγόντων του αριθμού.

Περιγραφή του αλγορίθμου.

Αρχικά είναι απαραίτητη η διαδικασία δημιουργίας των κλειδιών.

1) Ο χρήστης επιλέγει δύο πολύ μεγάλους πρώτους αριθμούς, έστω τους αριθμούς p και q.

2) Υπολογίζει την τιμή N=p*q.

3) Υπολογίζει την τιμή Φ(N)=(p-1)*(q-1) (συνάρτηση Euler).

4) Επιλέγει τυχαία ένα αριθμό e, πρώτο ως προς το Φ(N). Δηλαδή Μ.Κ.Δ.(e,Φ(N))=1.

5) Υπολογίζει τον αριθμό $d = e^{-1} \pmod{\Phi(N)}$

6) Ανακοινώνει τους αριθμούς (N,e) που αποτελούν το δημόσιο κλειδί του.

7) Κρατάει κρυφό το d που αποτελεί το ιδιωτικό κλειδί του. Επίσης κρατάει κρυφά τα p,q,Φ(N) αφού η δημοσιοποίησή τους θα πρόδιδε το ιδιωτικό του κλειδί.

Η δημιουργία των κλειδιών ολοκληρώθηκε. Πλέον ο χρήστης μπορεί να δέχεται κρυπτογραφημένα μηνύματα και να τα αποκρυπτογραφεί.

Για να στείλει κάποιος το μήνυμα Μ στον χρήστη ακολουθεί την ακόλουθη διαδικασία:

- Λαμβάνει το δημόσιο κλειδί του. Το ζευγάρι (N,e)
- Υπολογίζει την ποσότητα $C=M^e \pmod{N}$
- Μεταδίδει το C

Αν το Μ είναι μεγαλύτερο του Ν τότε το Μ πρέπει να σπάσει σε τμήματα που θα κρυπτογραφηθούν ξεχωριστά.

Ο παραλήπτης που λαμβάνει το C απλά εφαρμόζει την ακόλουθη σχέση, $M = C^d \pmod{N}$ Το Μ αντιστοιχεί στο αρχικό μήνυμα.

Η ασφάλεια του αλγορίθμου βασίζεται στο πρόβλημα της παραγοντοποίησης του N: ο αλγόριθμος θεωρείται ασφαλής για μεγάλες τιμές του N (μήκους 1024 – 2048 bits).

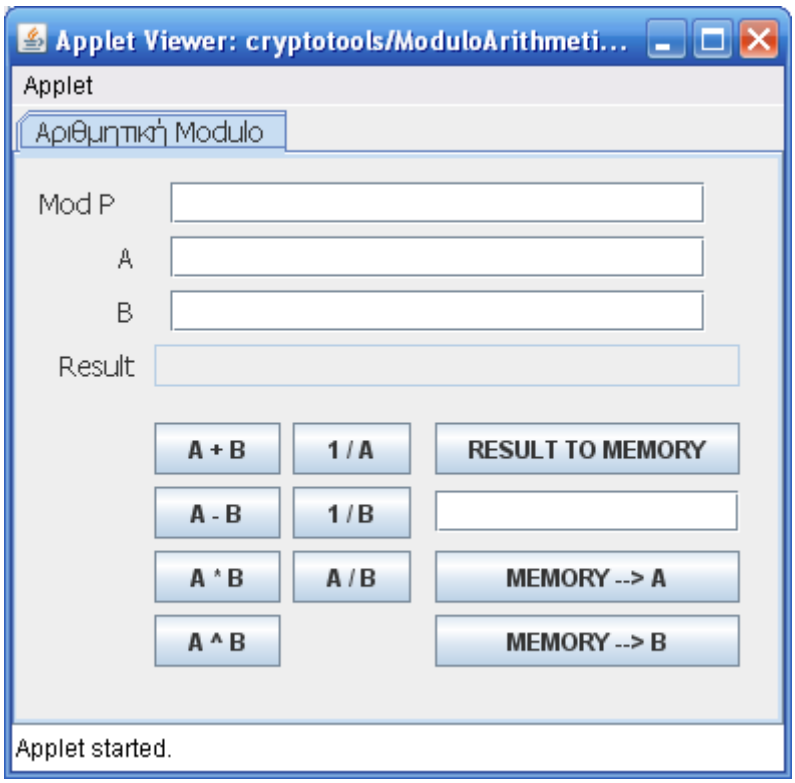
Κεφάλαιο 6
Η Εφαρμογή

Η διαδικασία κατασκευής του λογισμικού κινήθηκε σε 2 άξονες. Ο πρώτος ήταν η κατασκευή του εκπαιδευτικού υλικού που αφορούσε τα θέματα της Θεματικής ενότητας της κρυπτογραφίας. Ο δεύτερος ήταν η κατασκευή της εκπαιδευτικής πλατφόρμας που θα υποδεχόταν το εκπαιδευτικό υλικό. Σχεδιαστικός στόχος ήταν η ανεξαρτητοποίηση των 2 αυτών τμημάτων. Έτσι το εκπαιδευτικό υλικό να μπορεί να χρησιμοποιηθεί και ανεξάρτητα από την εκπαιδευτική πλατφόρμα, ανεβάζοντας το για παράδειγμα σε έναν Web Server. Επίσης η εκπαιδευτική πλατφόρμα να μπορεί να δεχθεί επιπλέον εκπαιδευτικό υλικό, πέρα αυτού που δημιουργήθηκε στα πλαίσια αυτής της μεταπτυχιακής διατριβής.

6.1 Η Κλάση Lookup

Η κλάση αυτή διαχειρίζεται θέματα σχετικά με το αλφάβητο που χρησιμοποιείτε στις διαδικασίες κρυπτογράφησης, αποκρυπτογράφησης και κρυπτανάλυσης. Παρέχει σχετικές μεθόδους για μετατροπή χαρακτήρα σε αριθμό και αντίστροφα κ.λ.π. Καλείται σαν κλάση από άλλους κρυπτογραφικούς αλγορίθμους.

6.2 Η Κλάση ModuloArithmeticApplet



Εικόνα 6.1 Screenshot of ModuloArithmetic Applet.

Η κλάση αυτή υλοποιεί τις βασικές πράξεις της αριθμητικής Modulo. Συγκεκριμένα υπολογίζονται το άθροισμα, ή διαφορά, το γινόμενο, ή διαίρεση 2 αριθμών, καθώς και ο αντίστροφος ενός αριθμού. Η κλάση αυτή λειτουργεί σαν ένα αυτόνομο Applet. Καλείτε όμως και σε διάφορα σημεία της εφαρμογής για να κάνει υπολογισμούς για διάφορους κρυπτογραφικούς αλγορίθμους πχ RSA. Οι σημαντικότεροι μέθοδοι που περιλαμβάνει είναι οι ακόλουθοι:

6.2.1 Συναρτήσεις σχετικές με τον αλγόριθμο του Ευκλείδη

- Ο συνάρτηση ExtendedEuclid εκτελεί τον εκτεταμένο αλγόριθμο του Ευκλείδη για να υπολογίσει τον Μέγιστο Κοινό Διαιρέτη gcd των αριθμών a,b που δίνονται ως παράμετροι. Επιπλέον επιστρέφει τους αριθμούς j,k ώστε να ισχύει η σχέση gcd = j*a + k*b. Πηγή του αλγορίθμου είναι η Διεύθυνση
  http://cgi.csc.liv.ac.uk/~martin/teaching/comp202/Java/GCD.html

```
public static int[] ExtendedEuclid(int a, int b)
{
int[] ans = new int[3];
int q;
```

```
if (b == 0) { /* If b = 0, then we're done... */
 ans[0] = a;
 ans[1] = 1;
 ans[2] = 0;
} else { /* Otherwise, make a recursive function call */
 q = a / b;
 ans = ExtendedEuclid(b, a % b);
 int temp = ans[1] - ans[2] * q;
 ans[1] = ans[2];
 ans[2] = temp;
}
return ans;
}
```

- Η Συνάρτηση gcdProcess επιστρέφει σε μορφή html την διαδικασία Εύρεσης του Μέγιστου Κοινού Διαιρέτη.

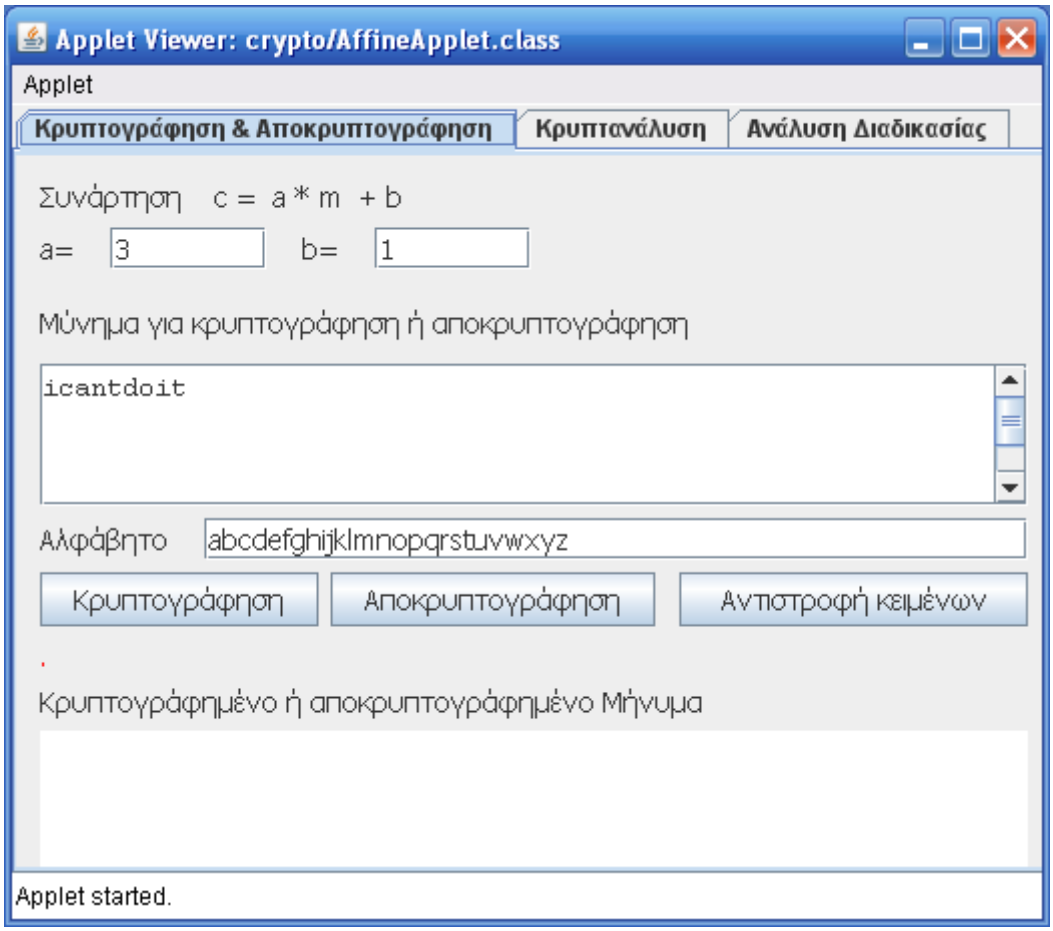
```
 public String gcdProcess(int a, int n) {
 int b = n;
 int c = a;
 int d = b % c;
 String s = "Διαδικασία Έυρεσης Μ.Κ.Δ. των " + a + " , " + n + " με τον εκτεταμένο
Αλγόριθμο του Ευκλείδη<br>";
 s += "<html><body><table>";
 while (d != 0) {
  s += "<tr><td align='right'>" + b + "</td><td>=</td><td align='center'>" + (int) (b / c) +
" * " + c + "</td><td>+</td><td align='center'>" + d + "</td></tr>";
  b = c;
  c = d;
  d = b % c;
 }
 s += "</table>";
 s += "Ο μέγιστος κοινός διαιρέτης είναι:" + c + "<br>";
 /* Check for input of two zeros, and print error if that's that case */
 b = n;
 int sign_a = 1;
 int sign_b = 1;

 if ((a == 0) && (b == 0)) {
  s += "\n Λάθος και οι 2 παράμετροι είναι 0! Δεν υπάρχει ΜΚΔ του 0!\n";
  System.out.println("\n Λάθος και οι 2 παράμετροι είναι 0! Δεν υπάρχει ΜΚΔ του 0!\n");
  System.exit(1);
 }

 /* If a and/or b is negative, then track this information for later output, because
  the extendedEuclid function expects nonnegative input. */
 if (a < 0) {
  sign_a = -1;
  a = Math.abs(a);
```

```
}
if (b < 0) {
 sign_b = -1;
 b = Math.abs(b);
}

int[] ans = ExtendedEuclid(a, b);
if (c == 1) {
 s += "Ο αντίστροφος είναι " + sign_a * ans[1] + "<br>";
 if (sign_a * ans[1] < 0) {
 s += "ή σε μορφή θετικού αριθμού είναι:" + (sign_a * ans[1] + n) + "<br>";

 }
}

s += "" + ans[0] + " = (" + sign_a * ans[1] + ") (" + sign_a * a + ")";
s += " + (" + sign_b * ans[2] + ") (" + sign_b * b + ")\n";

if (c != 1) {
 s += "Δεν Υπάρχει ο αντίστροφος <br>";
}
return (s);
}
```

6.3 Η Κλάση AffineApplet

Η κλάση αυτή υλοποιεί τον γραμμικό αλγόριθμο. Παρουσιάζει την διαδικασία κρυπτογράφησης, αποκρυπτογράφησης και κρυπτανάλυσης. Σημαντικό στοιχείο είναι η καταγραφή των διαδικασιών βήμα προς βήμα μέχρι την ολοκλήρωση της λειτουργίας.

6.3.1 Κρυπτογράφηση – Αποκρυπτογράφηση



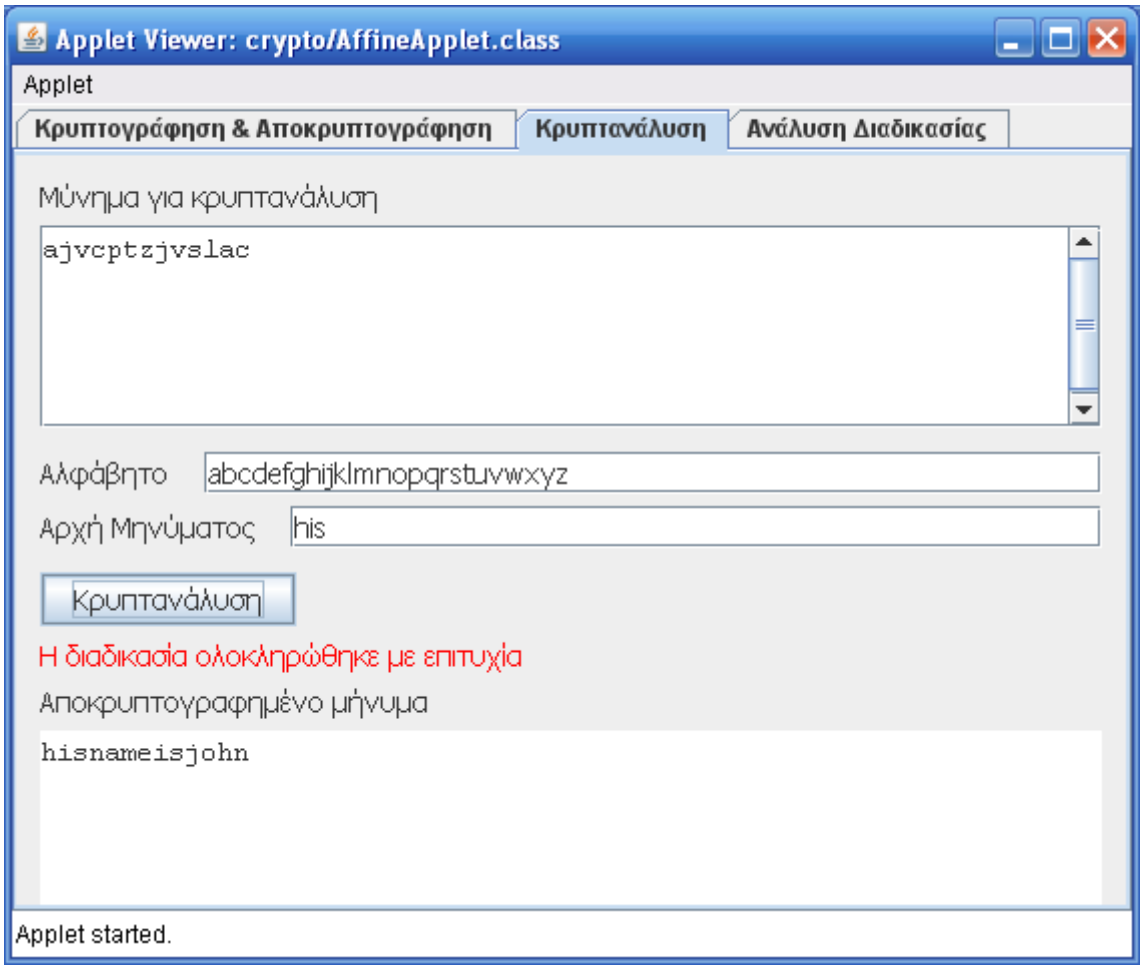
Εικόνα 6.2 Screenshot of AffineApplet (Κρυπτογράφηση & Αποκρυπτογράφηση).

Ακολουθούμε τα εξής βήματα:

- Συμπληρώνουμε τις μεταβλητές a,b που εκφράζουν το μυστικό κλειδί του αλγόριθμου.
- Συμπληρώνουμε (ακριβώς από κάτω) το μήνυμα ή το κρυπτομήνυμα.
- Εφόσον επιθυμούμε άλλο αλφάβητο το πληκτρολογούμε στην αντίστοιχη θέση.
- Επιλέγουμε αναλόγως Κρυπτογράφηση ή Αποκρυπτογράφηση.

Η εφαρμογή μας ενημερώνει για την επιτυχία ή όχι της διαδικασίας, και μας παρουσιάζει το αποτέλεσμα. Εφόσον επιθυμούμε να δούμε αναλυτικά την διαδικασία βήμα- βήμα επιλέγουμε το tab "Ανάλυση Διαδικασίας".

6.3.2 Κρυπτανάλυση



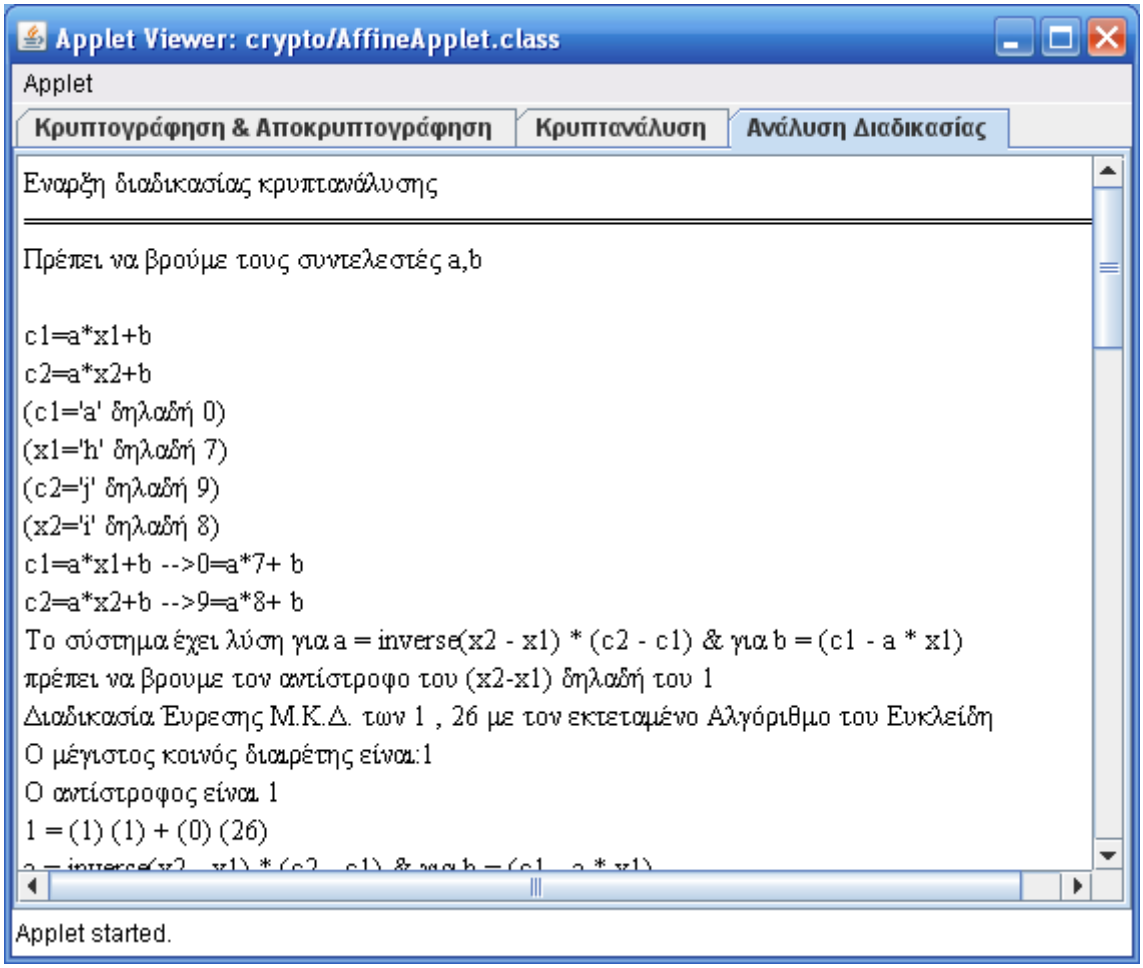
Εικόνα 6.3 Screenshot of AffineApplet (Κρυπτανάλυση).

Ακολουθούμε τα εξής βήματα:

- Συμπληρώνουμε το κρυπτομήνυμα.
- Εφόσον επιθυμούμε άλλο αλφάβητο, το πληκτρολογούμε στην αντίστοιχη θέση.
- Συμπληρώνουμε την αρχή του μηνύματος. (μελετάμε την περίπτωση known plaintext attack)
- Επιλέγουμε κρυπτανάλυση.

Η εφαρμογή μας ενημερώνει για την επιτυχία ή όχι της διαδικασίας, και μας παρουσιάζει το αποτέλεσμα. Εφόσον επιθυμούμε να δούμε αναλυτικά την διαδικασία βήμα- βήμα επιλέγουμε το tab "Ανάλυση Διαδικασίας".

6.3.3 Καταγραφή & Ανάλυση Διαδικασίας

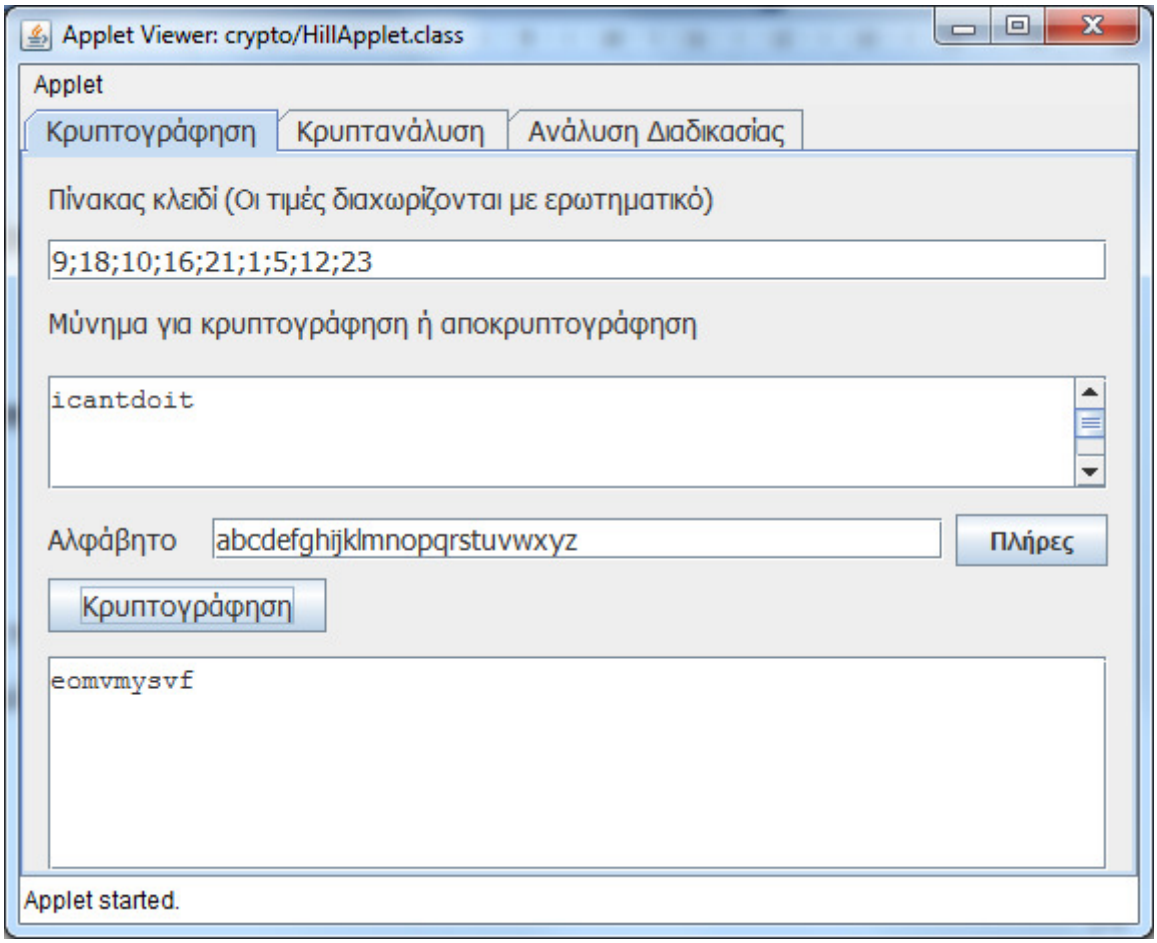


Εικόνα 6.4 Screenshot of AffineApplet (Ανάλυση Διαδικασίας).

Η σημαντικότερη εκπαιδευτικά λειτουργία βρίσκεται σε αυτή την επιλογή. Μετά το πέρας οποιασδήποτε λειτουργίας κρυπτογράφησης, αποκρυπτογράφησης ή κρυπτανάλυσης, επιλέγοντας το συγκεκριμένο tab, μας παρουσιάζεται αναλυτικά η επιλεγμένη λειτουργία βήμα προς βήμα.

6.4 Η Κλάση HillApplet

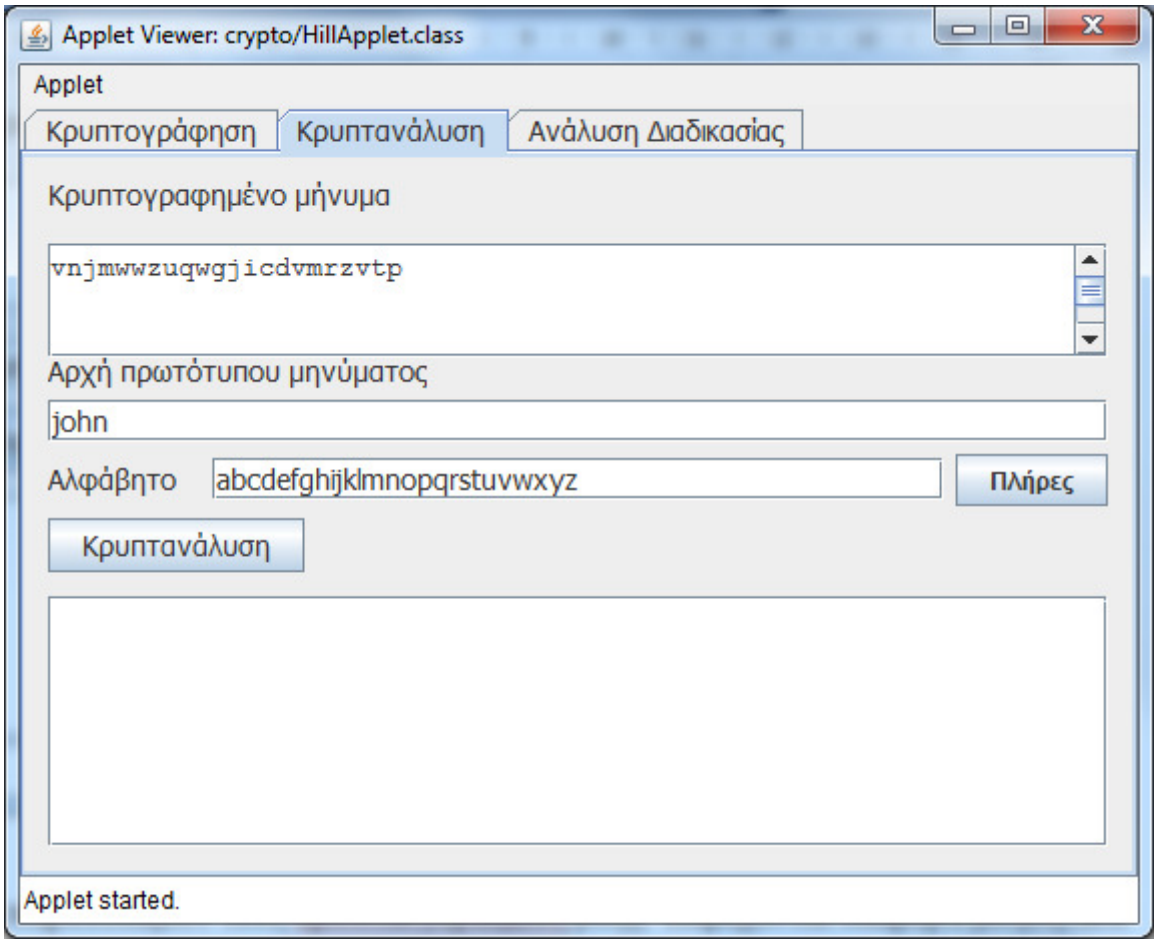
6.4.1 Κρυπτογράφηση - Αποκρυπτογράφηση.



Εικόνα 6.5 Screenshot of HillApplet (Κρυπτογράφηση).

Οι κλάση αυτή παρουσιάζει την διαδικασία κρυπτογράφησης στον αλγόριθμο HILL. Ο χρήστης δίνει τον πίνακα κλειδί με την μορφή αλφαριθμητικού που κάθε στοιχείο διαχωρίζεται με ερωτηματικό. Έπειτα συμπληρώνει το μήνυμα και το αλφάβητο που θα χρησιμοποιήσει. Πατώντας το πλήκτρο «Κρυπτογράφηση» εμφανίζεται το κρυπτογραφημένο κείμενο στο σχετικό πλαίσιο. Εφόσον ο χρήστης το επιθυμεί μπορεί να δει την διαδικασία υπολογισμού του κρυπτοκειμένου βήμα προς βήμα πατώντας το tab «Ανάλυση Διαδικασίας». Δεν παρουσιάζεται ξεχωριστή διαδικασία αποκρυπτογράφησης γιατί ουσιαστικά η αποκρυπτογράφηση είναι κρυπτογράφηση με κλειδί τον αντίστροφο (mod P) του πίνακα κλειδί.

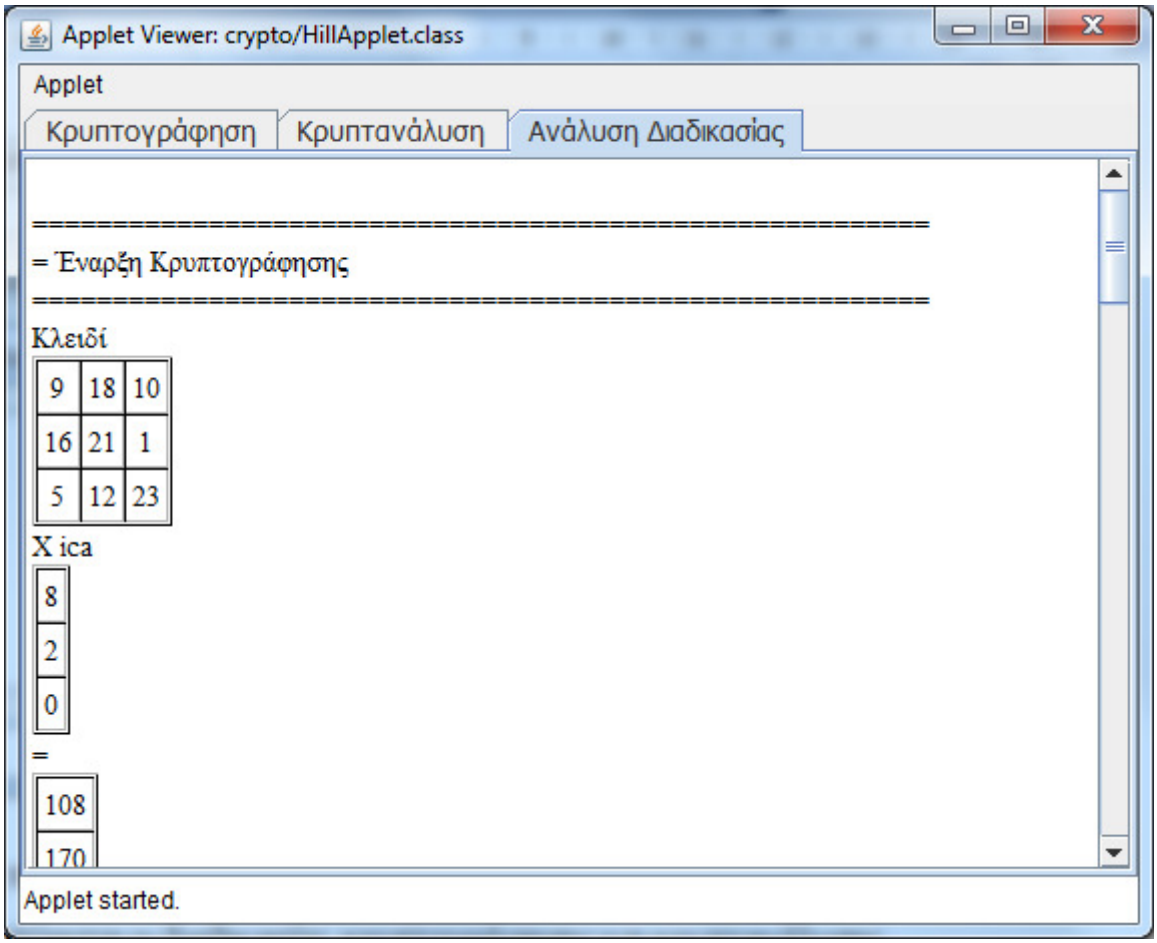
6.4.2 Κρυπτανάλυση.



Εικόνα 6.6 Screenshot of HillApplet (Κρυπτανάλυση).

Εδώ παρουσιάζεται η διαδικασία κρυπτανάλυσης σε επίθεση «Known plaintext». Συμπληρώνουμε το κρυπτομήνυμα, την αρχή του μηνύματος και το αλφάβητο που χρησιμοποιούμε. Με το πλήκτρο «Κρυπτανάλυση» εμφανίζουμε όλο το μήνυμα. Για την βήμα προς βήμα ανάλυση της της διαδικασίας πατάμε το σχετικό tab.

6.4.3 Καταγραφή & Ανάλυση Διαδικασίας.



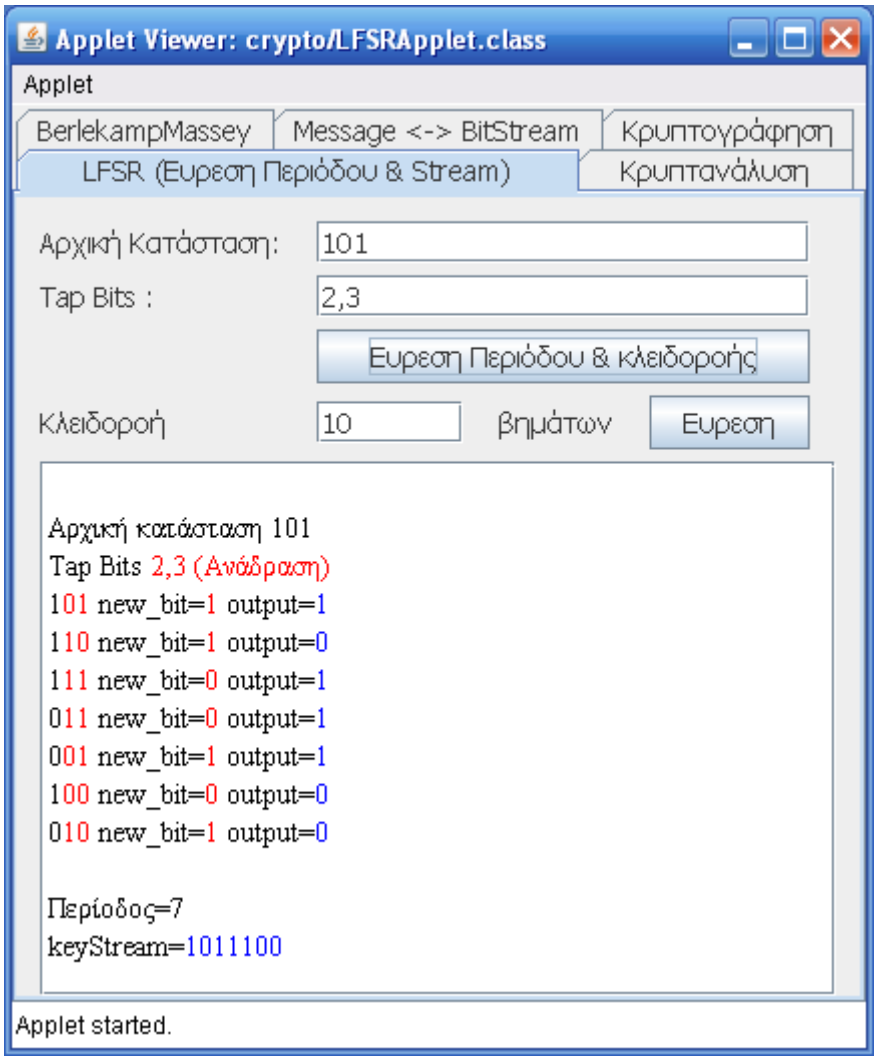
Εικόνα 6.7 Screenshot of HillApplet (Ανάλυση Διαδικασίας).

Εδώ παρουσιάζεται η ανάλυση της τελευταίας επιλεγμένης διαδικασίας (κρυπτογράφησης ή κρυπτανάλυσης).

6.5 Οι Κλάσεις LFSRApplet & LFSR

Οι κλάσεις αυτές παρουσιάζουν τους κρυπταλγόριθμους ροής. Παρέχονται διάφορα βοηθητικά εργαλεία, και αναλύονται οι διαδικασίες κρυπτογράφησης και κρυπτανάλυσης.

6.5.1 Εύρεση περιόδου & κρυπτοροής LFSR.



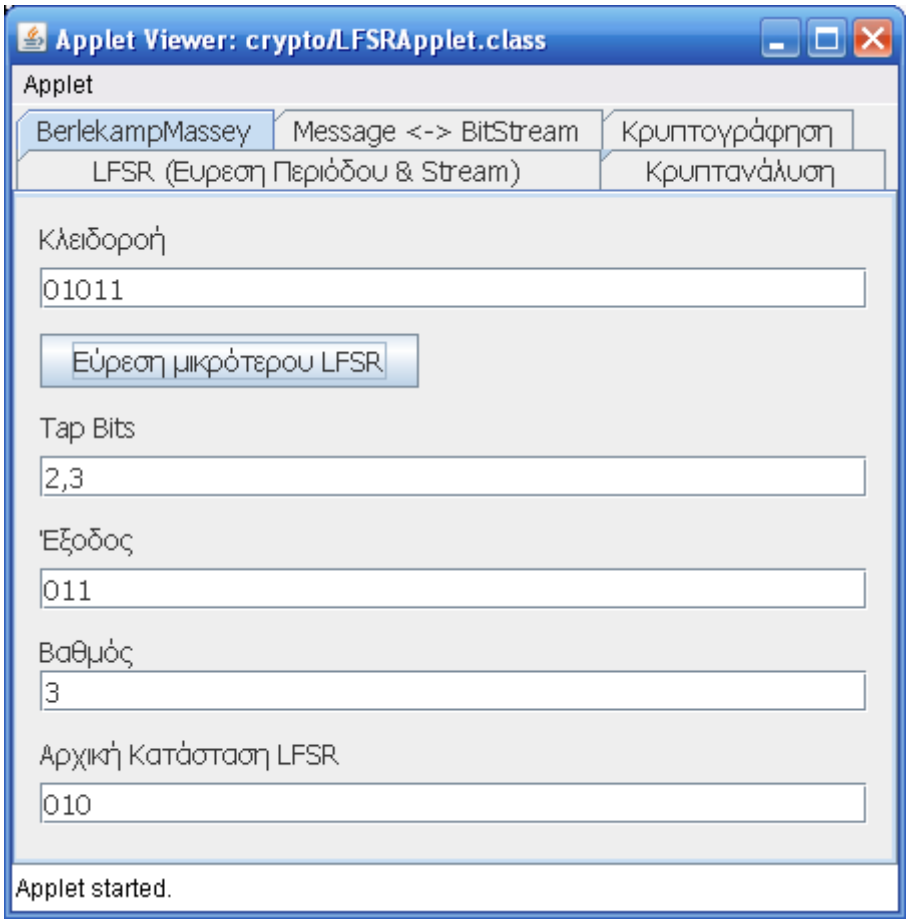
Εικόνα 6.8 Screenshot of LFSRApplet (Εύρεση Περιόδου & Stream).

Ακολουθούμε τα εξής βήματα:

- Συμπληρώνουμε την αρχική κατάσταση του LFSR.
- Συμπληρώνουμε ποια bits του LFSR αποτελούν την ανάδραση. Οι αριθμοί που εκφράζουν τα bits της ανάδρασης πρέπει να χωρίζονται με κόμμα.
- Για να βρούμε την περίοδο και την αντίστοιχη κλειδορή επιλέγουμε το αντίστοιχο πλήκτρο.
- Εναλλακτικά επιλέγουμε πλήθος βημάτων και «εύρεση».

Εμφανίζονται τα αποτελέσματα της επιλογής μας στο σχετικό πλαίσιο κειμένου.

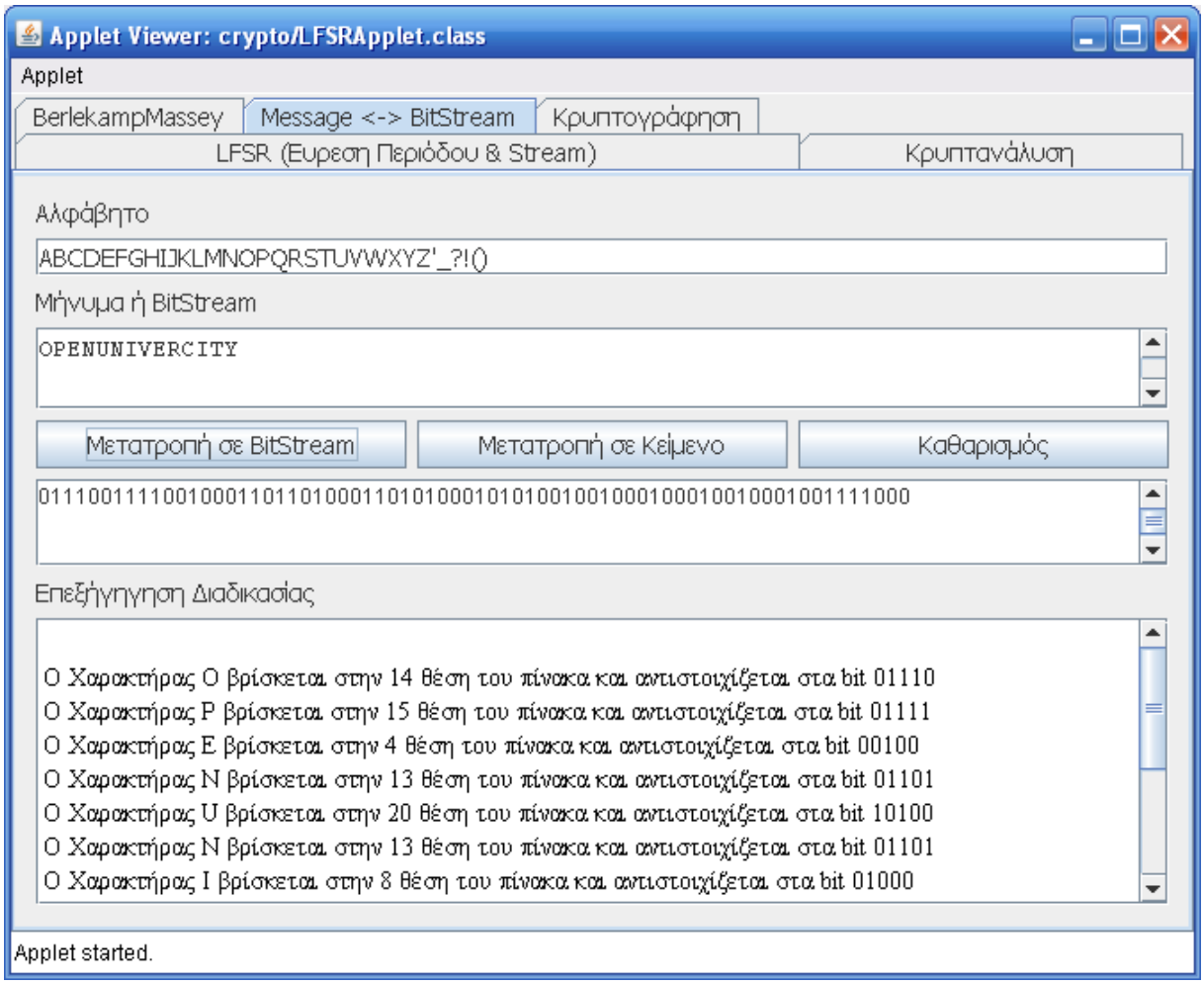
6.5.2 Ο Αλγόριθμος Berlekamp Massey



Εικόνα 6.9 Screenshot of LFSRApplet (BerlekampMassey).

Ο αλγόριθμος αυτός, δοθείσης κλειδορρής, υπολογίζει τον μικρότερο LFSR που την παράγει. Απλά πληκτρολογούμε την κλειδορρή στο αντίστοιχο πεδίο και πατάμε του πλήκτρο «Εύρεση μικρότερου LFSR». Η κλάση υπολογίζει τα στοιχεία που περιγράφουν τον LFSR (βαθμός, bits ανάδρασης, έξοδος και αρχική κατάσταση) και ενημερώνει τα αντίστοιχα πεδία.

6.5.3 Message ←→ BitStream



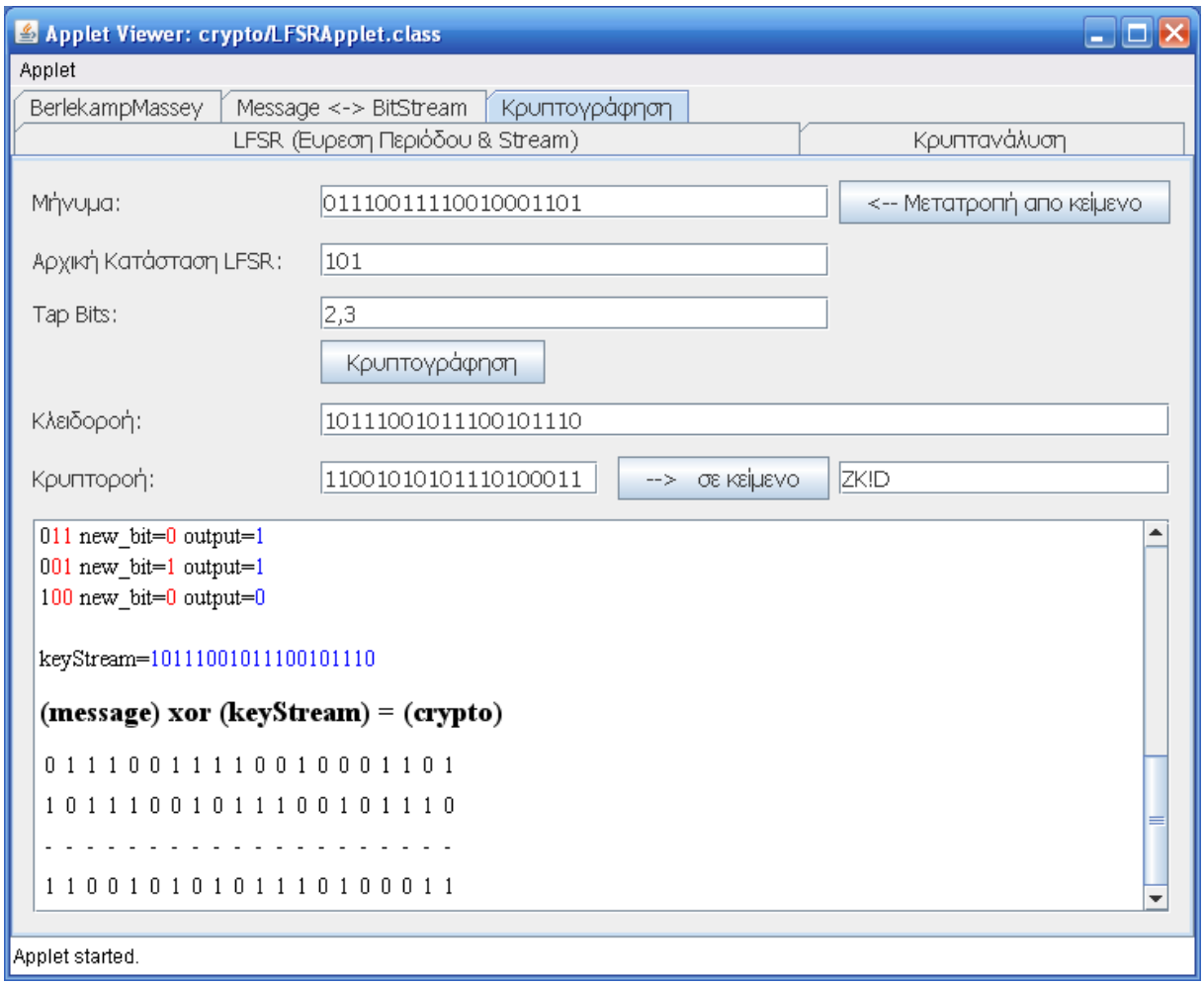
Εικόνα 6.10 Screenshot of LFSRApplet (Message ← → BitStream).

Εδώ γίνεται μετατροπή κειμένου σε ακολουθία από bits (BitStream) και αντίστροφα. Ακολουθούμε τα εξής βήματα:

- Καταχωρούμε το αλφάβητο που θα χρησιμοποιήσουμε (ελληνικό, λατινικό κ.λ.π.).
- Συμπληρώνουμε το μήνυμα ή το BitStream που θέλουμε να μετατρέψουμε.
- Επιλέγουμε το πλήκτρο με την αντίστοιχη λειτουργία.

Στα δυο πλαίσια κειμένου στο κάτω μέρος, παρουσιάζονται τα αποτελέσματα της επιλεγμένης λειτουργίας και αναλυτικά βήμα - βήμα η διαδικασία.

6.5.4 Κρυπτογράφηση



Εικόνα 6.11 Screenshot of LFSRApplet (Κρυπτογράφηση).

Εδώ παρουσιάζεται η διαδικασία κρυπτογράφησης. Ακολουθούμε τα εξής βήματα:

- Συμπληρώνουμε το μήνυμα σε μορφή BitStream ή πατάμε το πλήκτρο «Μετατροπή από κείμενο» ώστε να το μετατρέψει η εφαρμογή με την αντίστοιχη λειτουργία που περιγράψαμε προηγουμένως.

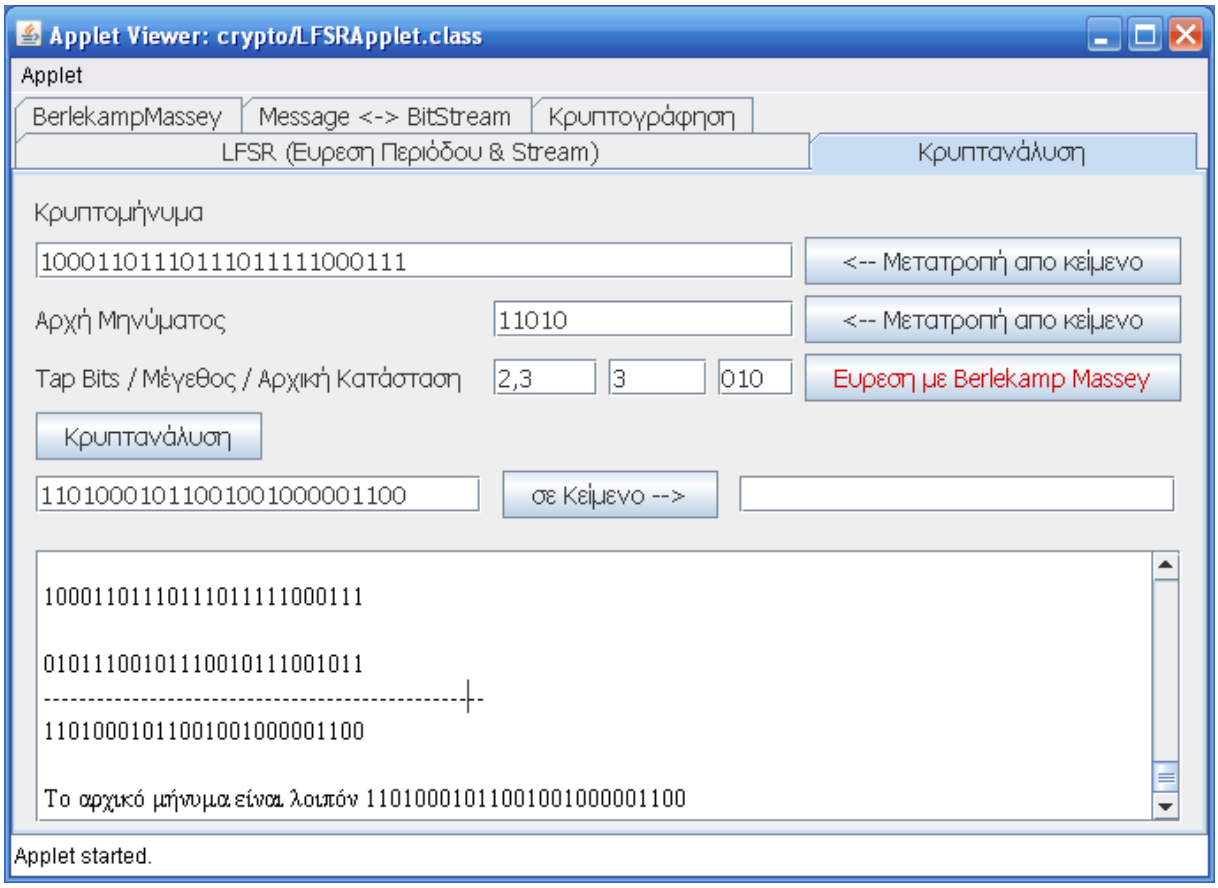
- Συμπληρώνουμε την αρχική κατάσταση του LFSR (μυστικό κλειδί) και τα bits της ανάδρασης.

- Πατάμε το πλήκτρο «κρυπτογράφηση».

- Η εφαρμογή υπολογίζει την κλειδορροή και την κρυπτορροή. Εφόσον θέλουμε μπορούμε να μετατρέψουμε την κρυπτορροή σε χαρακτήρες κειμένου επιλέγοντας το αντίστοιχο πλήκτρο.

Στο πλαίσιο κειμένου στο κάτω μέρος παρουσιάζεται αναλυτικά η διαδικασία της κρυπτογράφησης.

6.5.5 Κρυπτανάλυση



Εικόνα 6.12 Screenshot of LFSRApplet (Κρυπτανάλυση).

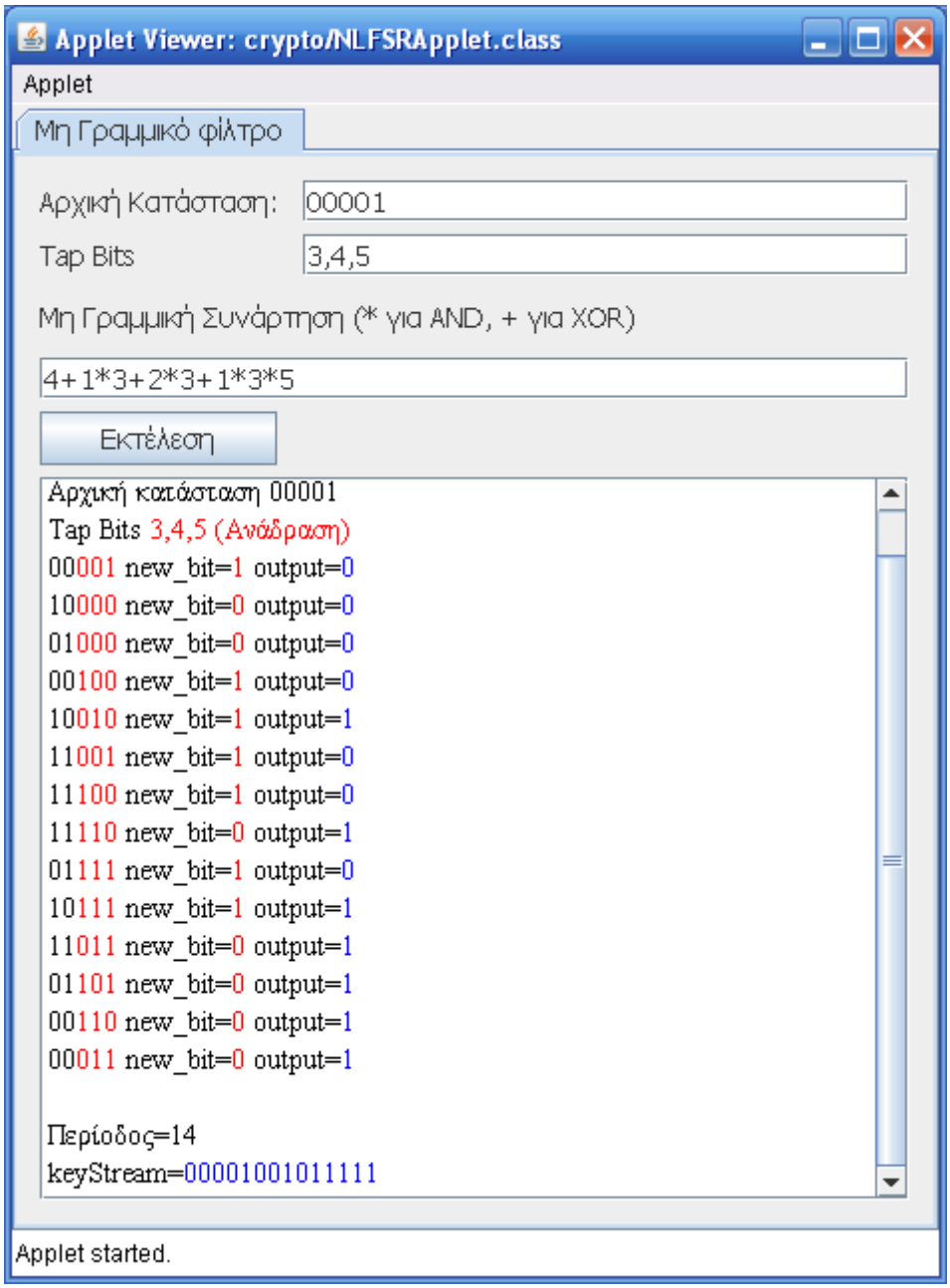
Εδώ μελετάμε τη διαδικασία κρυπτανάλυσης σε επίθεση «known plaintext». Ακολουθούμε τα εξής βήματα:

- Συμπληρώνουμε το κρυπτομήνυμα σε μορφή BitStream ή πατάμε το πλήκτρο «Μετατροπή από κείμενο» ώστε να το μετατρέψει η εφαρμογή με την αντίστοιχη λειτουργία.
- Συμπληρώνουμε τα αρχικά bits του μηνύματος.
- Πατώντας το πλήκτρο «Εύρεση με Berlekamp Massey» η εφαρμογή υπολογίζει τα στοιχεία του LFSR, χρησιμοποιώντας τον σχετικό αλγόριθμο.

- Πατάμε το πλήκτρο «κρυπτανάλυση».
- Η εφαρμογή υπολογίζει ολόκληρο το μήνυμα. Εφόσον θέλουμε μπορούμε να το μετατρέψουμε σε χαρακτήρες κειμένου επιλέγοντας το αντίστοιχο πλήκτρο.

Στο πλαίσιο κειμένου στο κάτω μέρος παρουσιάζεται αναλυτικά η διαδικασία της κρυπτανάλυσης.

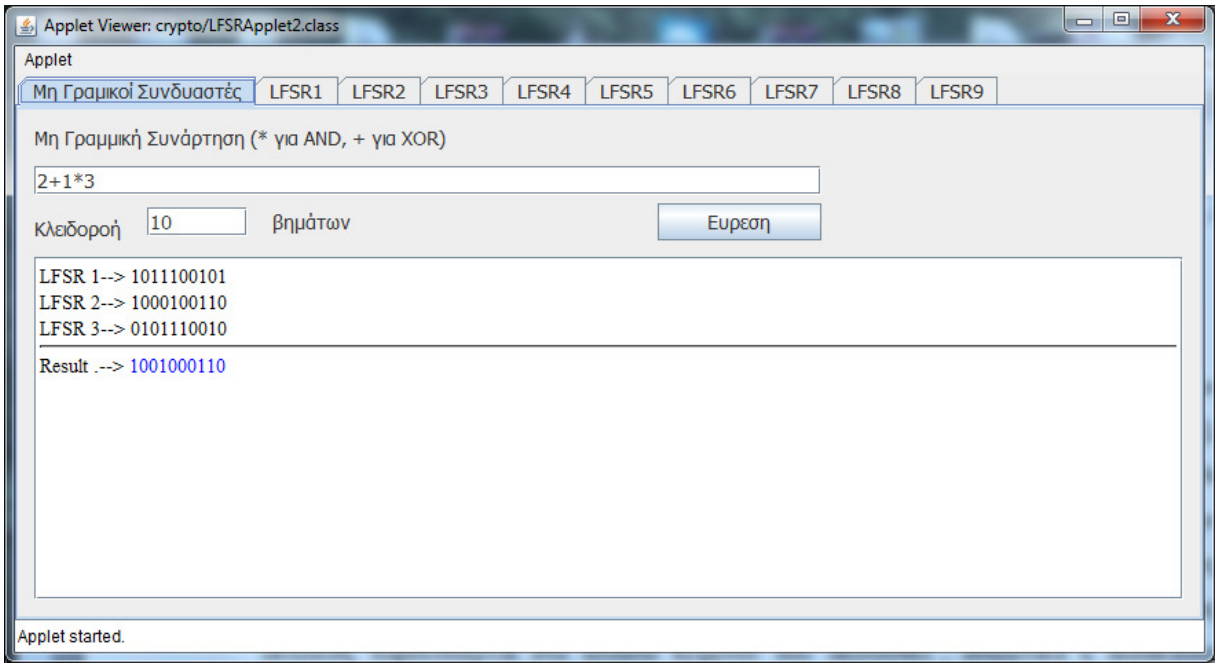
6.6 Κλάση NLFSRApplet



Εικόνα 6.13 Screenshot of NLFSRApplet (Μη Γραμμικό Φίλτρο).

Εδώ παρουσιάζεται η διαδικασία εύρεσης κλειδοροής στις περιπτώσεις χρήσης μη γραμμικών φίλτρων. Αρχικά πληκτρολογούμε τα στοιχεία του LFSR (αρχική κατάσταση και bits ανάδρασης). Έπειτα καθορίζουμε τη μη γραμμική συνάρτηση που εφαρμόζεται στα bits του LFSR. Οι επιτρεπόμενοι τελεστές είναι ο '*' για να εκφράσει την πράξη AND και ο '+' για να εκφράσει την πράξη XOR μεταξύ των bits. Τα bits εκφράζονται με τον αριθμό που αντιστοιχεί στην θέση τους στον LFSR. Έτσι η πράξη bit1 XOR (bit2 AND bit3) πρέπει να γραφτεί 1+2*3. Πατώντας «εκτέλεση», παρουσιάζεται στο πλαίσιο κειμένου που ακολουθεί, αναλυτικά η διαδικασία υπολογισμού της κλειδοροής.

6.7 Κλάση NLFSRApplet2

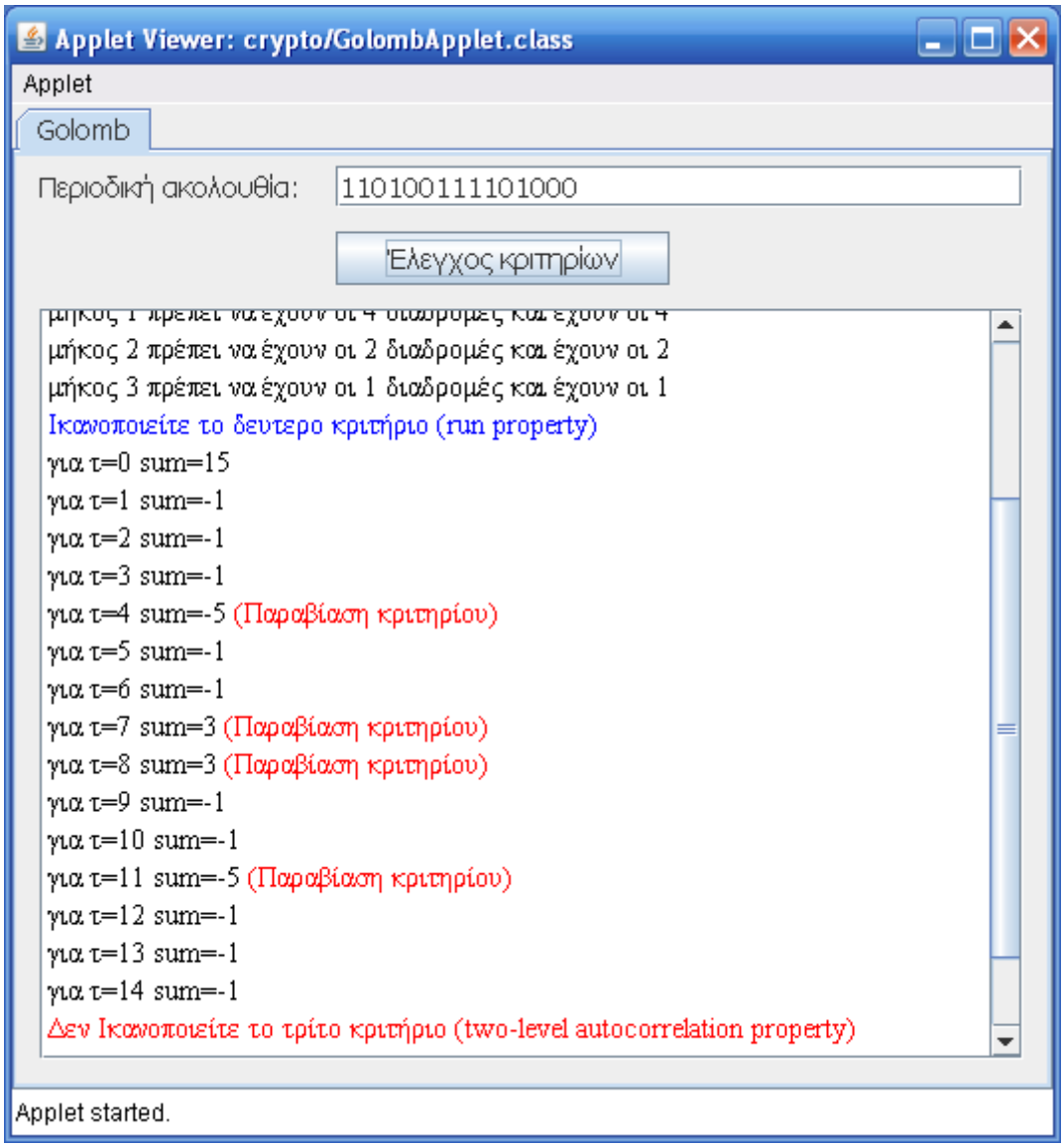


Εικόνα 6.14 Screenshot of NLFSRApplet2 (Μη Γραμμικοί Συνδυαστές).

Εδώ παρουσιάζεται η διαδικασία εύρεσης κλειδοροής στις περιπτώσεις χρήσης μη γραμμικών συνδυαστών. Αρχικά καθορίζουμε τη μη γραμμική συνάρτηση που εφαρμόζεται στις εξόδους των LFSRs. Οι επιτρεπόμενοι τελεστές είναι ο '*' για να εκφράσει την πράξη AND και ο '+' για να εκφράσει την πράξη XOR μεταξύ των εξόδων. Κάθε LFSR εκφράζεται με κάποιο αριθμό από το 1 μέχρι και το 9 (Το Applet υποστηρίζει την χρήση το πολύ μέχρι 9 LFSRs). Έτσι η πράξη LFSR_1 XOR (LFSR_2 AND LFSR_3) πρέπει να γραφτεί 1+2*3. Έπειτα για κάθε LFSR που συμμετέχει στην συνάρτηση, δηλώνουμε μέσω της αντίστοιχης καρτέλας τα στοιχεία που τον περιγράφουν (Αρχική Κατάσταση και bits Ανάδρασης). Επιλέγοντας το πλήθος των βημάτων και πατώντας εύρεση, υπολογίζονται οι κλειδοροές όλων των σχετικών LFSR καθώς και το αποτέλεσμα της συνάρτησης.

6.8 Κλάση Golomb & GolombApplet

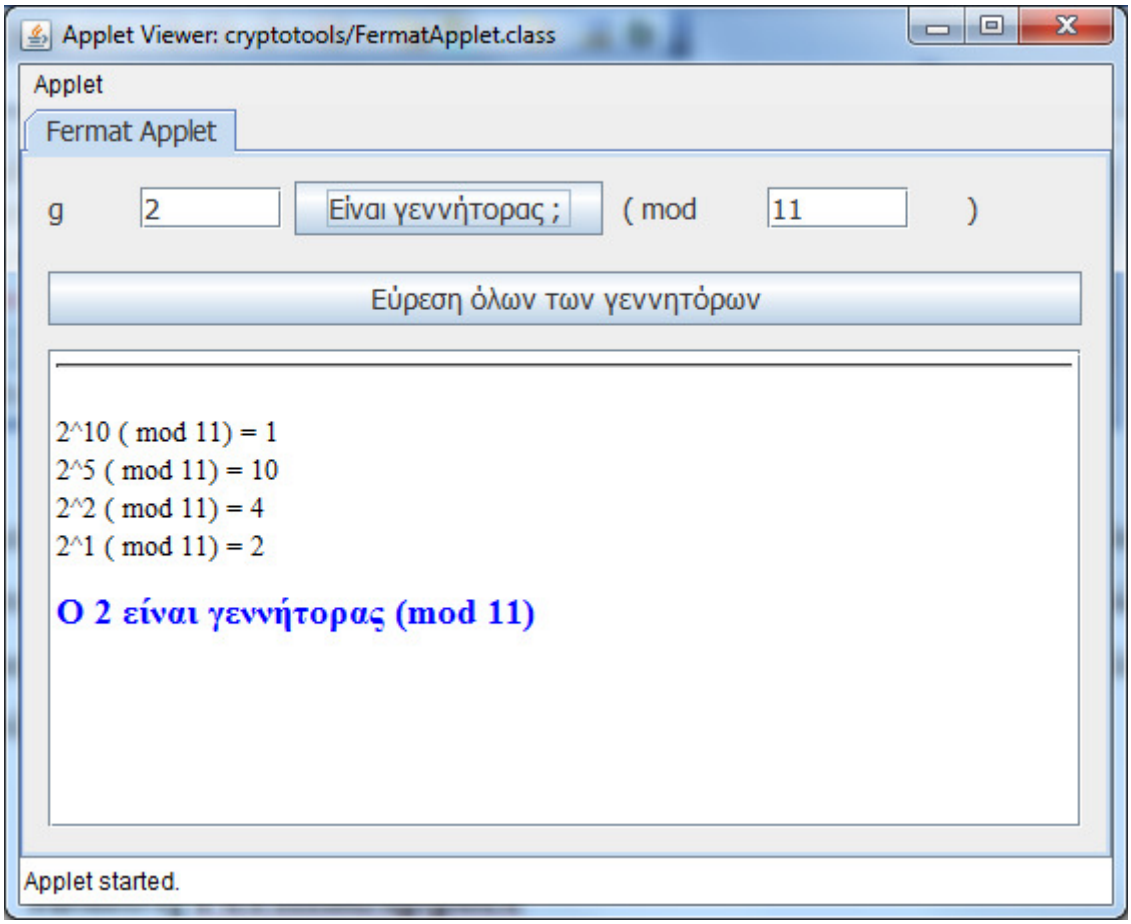
6.8.1 Έλεγχος κριτηρίων τυχαιότητας κατά Golomb.



Εικόνα 6.15 Screenshot of GolombApplet (Έλεγχος Κριτηρίων τυχαιότητας).

Εδώ μελετάμε αν πληρούνται τα κριτήρια τυχαιότητας κατά Golomb. Πληκτρολογούμε την ακολουθία που θέλουμε να ελέγξουμε και πατάμε το πλήκτρο «Έλεγχος κριτηρίων». Στο πλαίσιο κειμένου στο κάτω μέρος παρουσιάζεται αναλυτικά η διαδικασία ελέγχου, και εμφανίζονται μηνύματα για τα κριτήρια που παραβιάζονται.

6.9 Κλάση FermatApplet



Εικόνα 6.16 Screenshot of FermatApplet (Εύρεση Γεννητόρων).

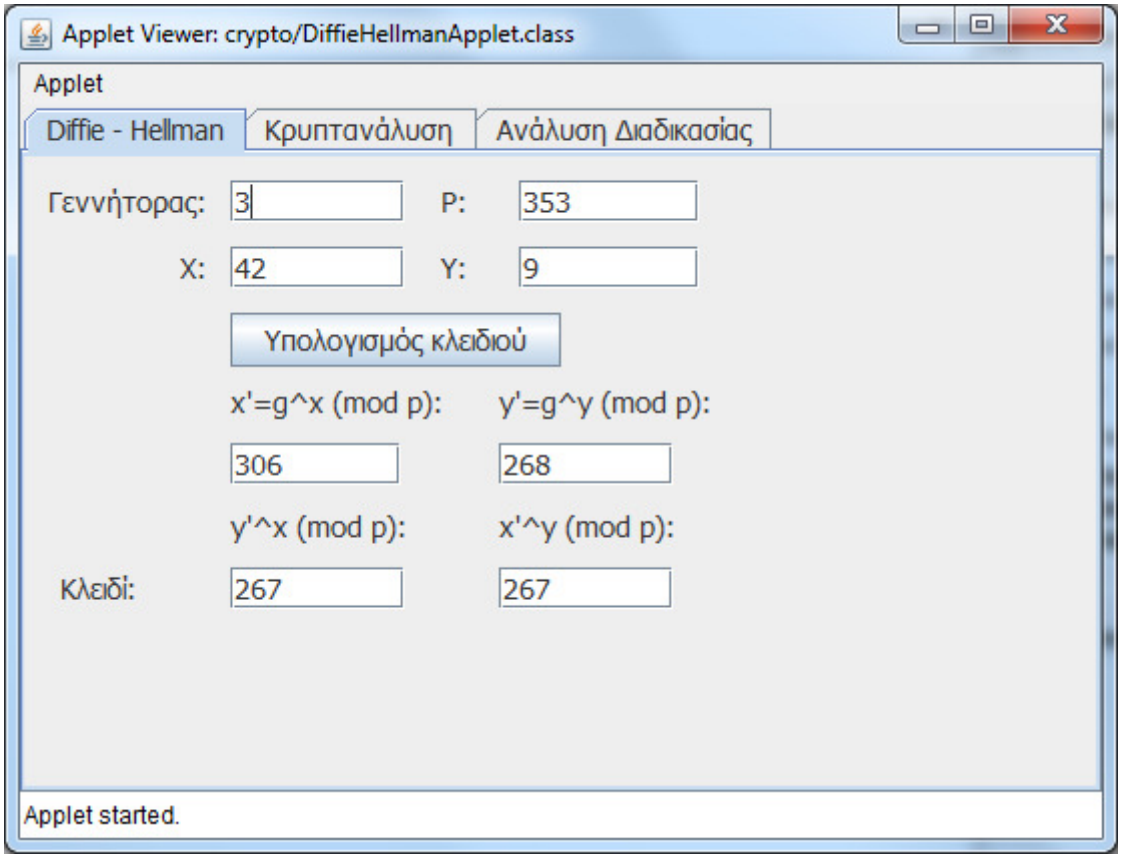
Εδώ παρουσιάζονται δύο λειτουργίες.

- Η πρώτη ελέγχει αν ένας αριθμός είναι γεννήτορας mod p. Ο Αλγόριθμος βασίζεται στο θεώρημα του Fermat και στις ιδιότητες των γεννητόρων. Ελέγχονται αν όλοι οι διαιρέτες του p-1 είναι διαφορετικοί του 1. Εφόσον ισχύει αυτό εμφανίζεται το μήνυμα ότι το επιλεγμένο g είναι γεννήτορας mod p.

- Η δεύτερη λειτουργία ελέγχει όλους του αριθμούς από 1 έως και p-1 για το αν είναι γεννήτορες mod p. Ουσιαστικά εφαρμόζεται επαναληπτικά η 1η λειτουργία για όλους αυτούς τους αριθμούς. Στο σχετικό πλαίσιο κειμένου εμφανίζονται όλοι οι αριθμοί και το αποτέλεσμα του ελέγχου.

6.10 Κλάση DiffieHellmanApplet

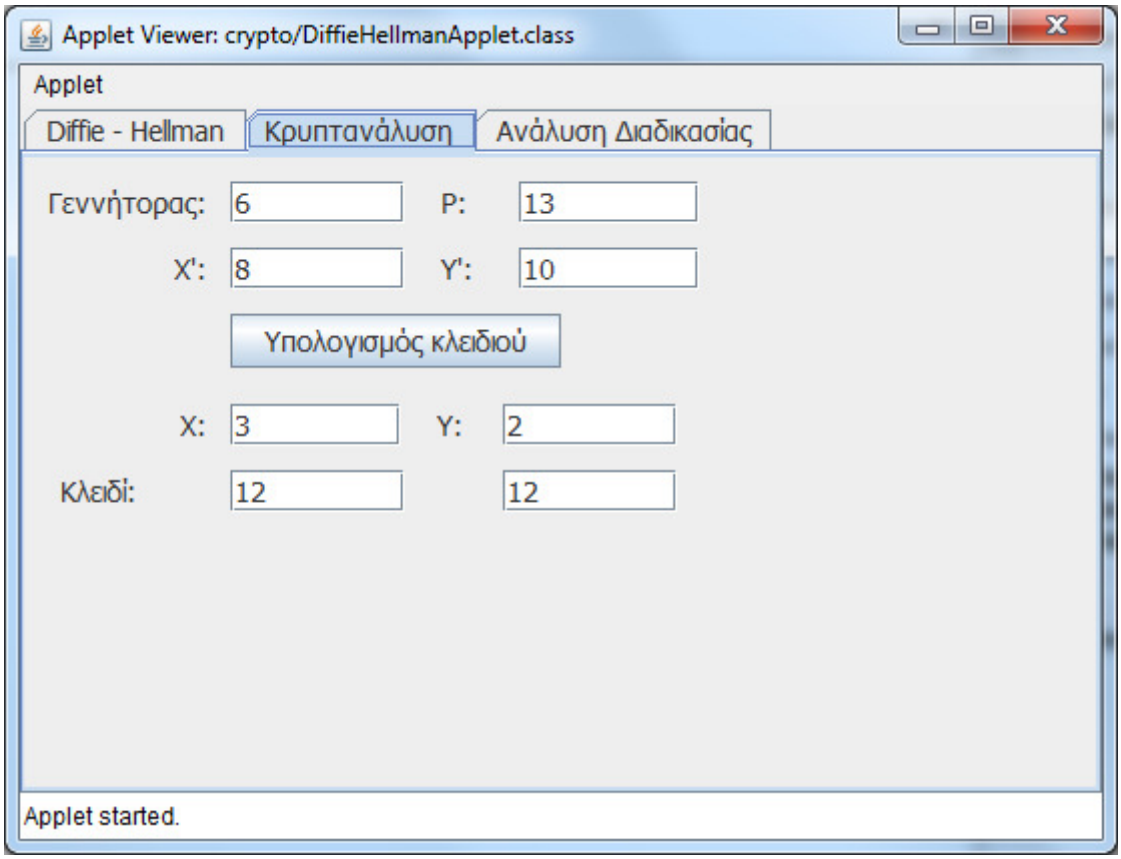
6.10.1 Διαδικασία παραγωγής μυστικού κλειδιού.



Εικόνα 6.17 Screenshot of DiffieHellmanApplet (Diffie – Hellman).

Εδώ παρουσιάζεται η διαδικασία ανταλλαγής μυστικού κλειδιού με τον αλγόριθμο Diffie-Hellman. Οι μεταβλητές p,g (γεννήτορας mod p), x (μυστικό κλειδί 1ου χρήστη), y (μυστικό κλειδί 2ου χρήστη) είναι οι τιμές που συμπληρώνουμε για είσοδο στον αλγόριθμο. Πατώντας το πλήκτρο «Υπολογισμός κλειδιού» υπολογίζονται τα x',y' καθώς και το μυστικό κλειδί που ανταλλάσσεται. Η πλήρη επεξήγηση της διαδικασίας είναι διαθέσιμη μέσω του tab «Ανάλυση Διαδικασίας».

6.10.2 Κρυπτανάλυση.

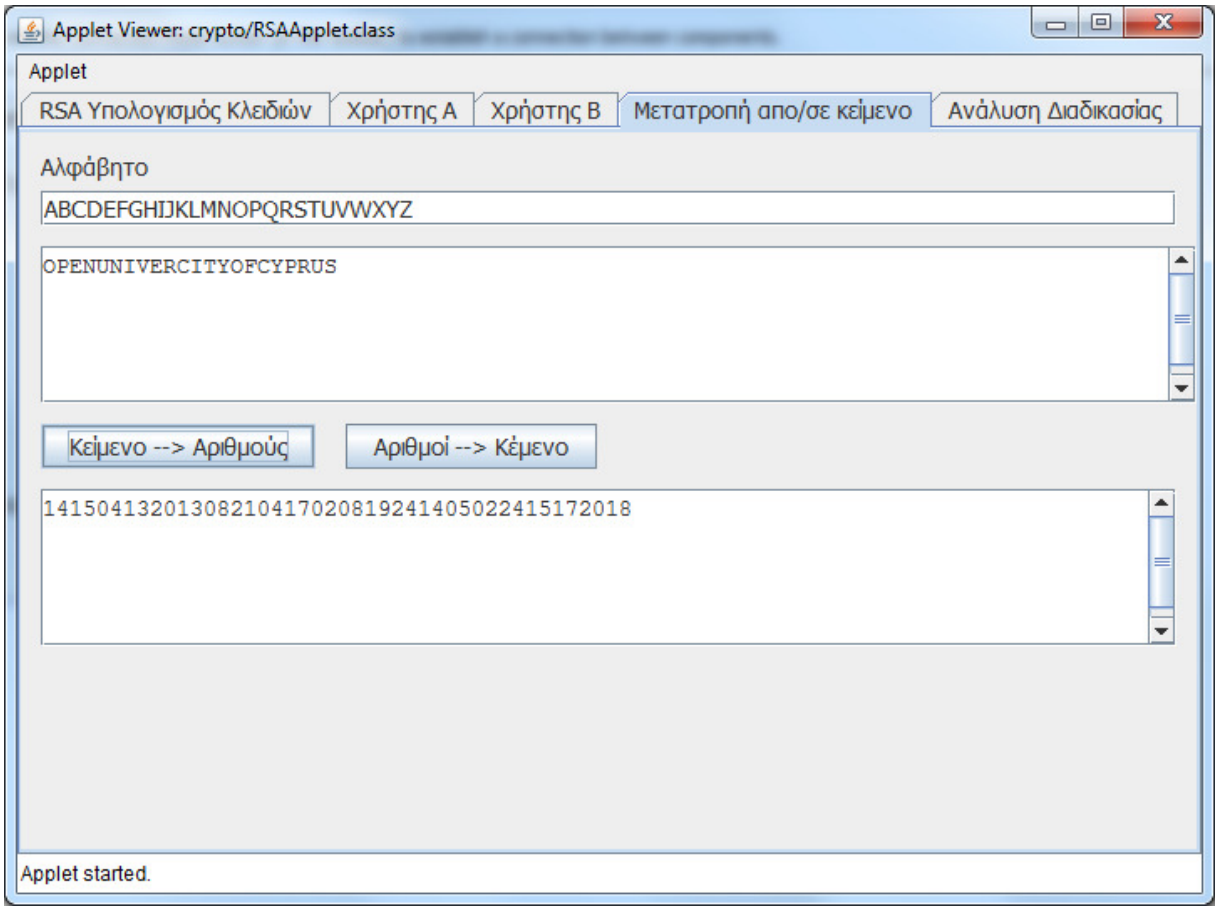


Εικόνα 6.18 Screenshot of DiffieHellmanApplet (Κρυπτανάλυση).

Εδώ παρουσιάζεται η προσπάθεια εύρεσης του μυστικού κλειδιού που ανταλλάσσεται με τον αλγόριθμο Diffie – Hellman. Η τεχνική που ακολουθείτε είναι τύπου «Brute Force» (δοκιμή όλων των πιθανών κλειδιών). Σαν είσοδο βάζουμε τα δημόσια κλειδιά στα οποία ο επιτιθέμενος έχει πρόσβαση, δηλαδή το g,p,x',y'. Δοκιμάζονται όλα τα πιθανά ιδιωτικά κλειδιά x,y ώστε να προκύψουν τα δημόσια κλειδιά x',y'. Φυσικά η μέθοδος αυτή μπορεί να δώσει αποτέλεσμα μόνο για μικρές τιμές των p,g. Για μεγάλες τιμές η διαδικασία είναι υπολογιστικά αδύνατη. Η πλήρη επεξήγηση της διαδικασίας είναι διαθέσιμη μέσω του tab «Ανάλυση Διαδικασίας».

6.11 Κλάση RSAApplet

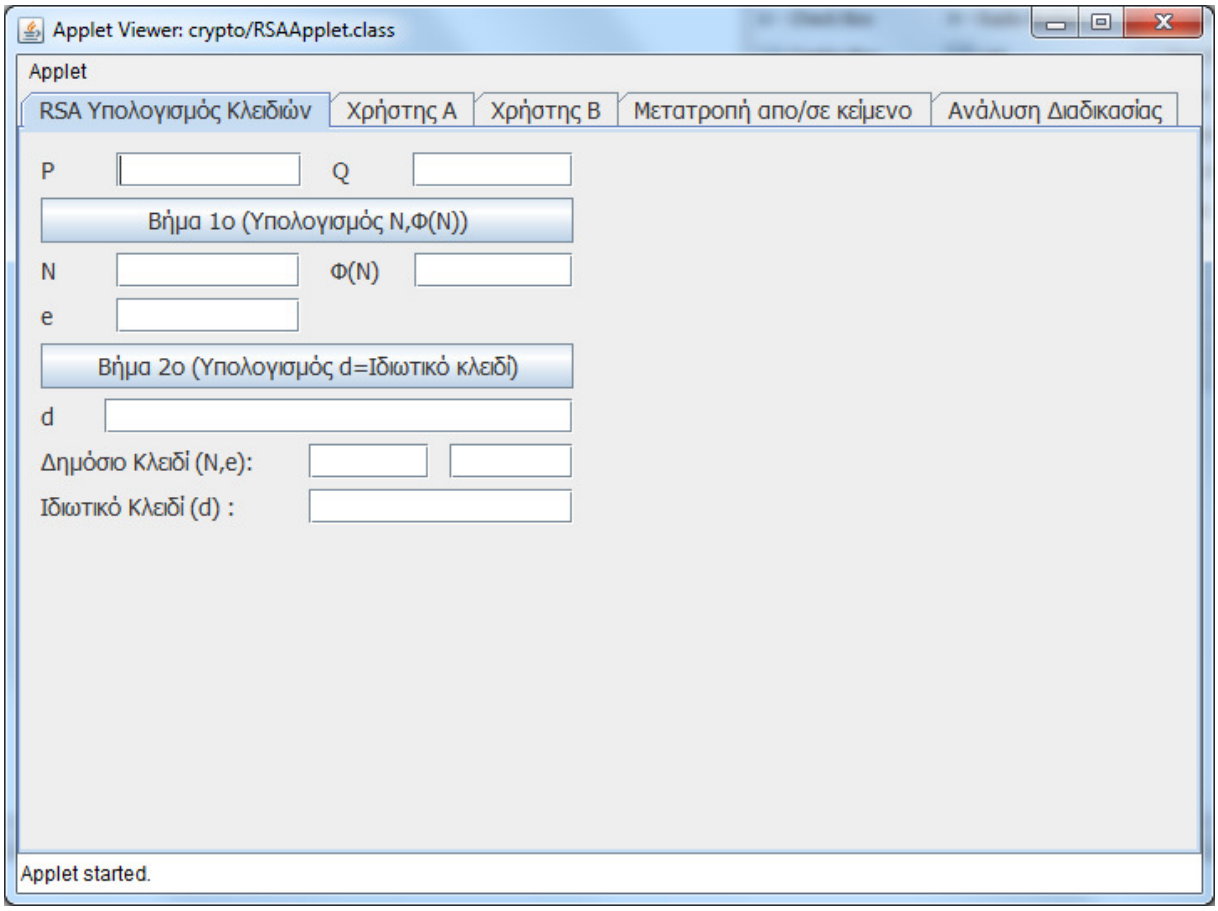
6.11.1 Μετατροπή από/σε κείμενο.



Εικόνα 6.19 Screenshot of RSAApplet (Μετατροπή από/σε κείμενο).

Η συγκεκριμένη βοηθητική λειτουργία έχει στόχο την μετατροπή ενός αλφαριθμητικού μηνύματος σε μια ακολουθία αριθμών και αντίστροφα. Αρχικά εισάγουμε το αλφάβητο που θα χρησιμοποιηθεί. Έπειτα το μήνυμα ή την αριθμητική ακολουθία για την μετατροπή. Τέλος επιλέγουμε την λειτουργία που μας ενδιαφέρει. Στο πλαίσιο κειμένου στο κάτω μέρος εμφανίζεται το αποτέλεσμα της επιλεγμένης ενέργειας.

6.11.2 Υπολογισμός κλειδιού.



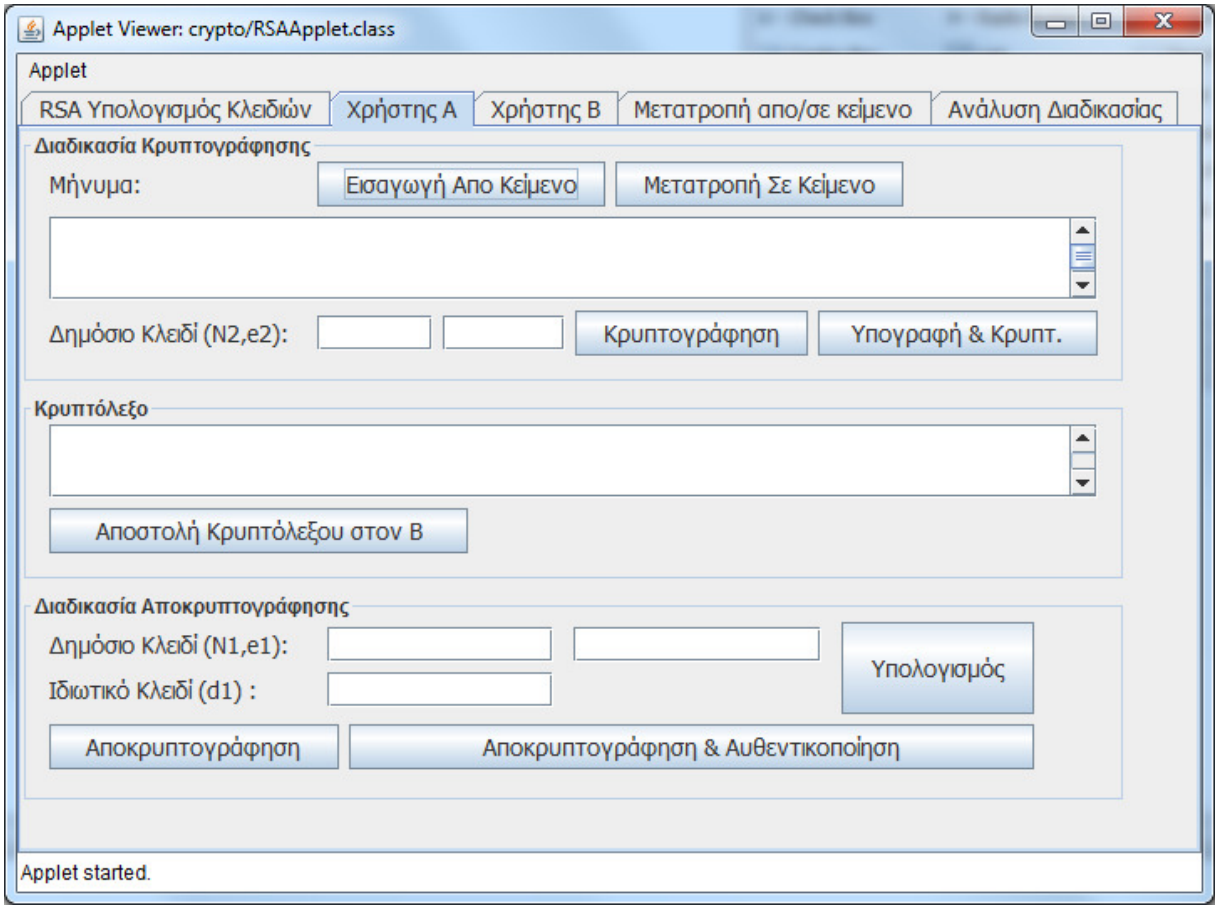
Εικόνα 6.20 Screenshot of RSAApplet (Υπολογισμός Κλειδιών).

Η συγκεκριμένη λειτουργία δημιουργεί το δημόσιο και το ιδιωτικό κλειδί του χρήστη. Τα βήματα είναι τα ακόλουθα:

- Εισαγωγή 2 πρώτων αριθμών P,Q.
- Πατάμε το πλήκτρο «Βήμα 1ο (υπολογισμός N,Φ(N))» και η εφαρμογή υπολογίζει τις δύο αυτές τιμές.
- Επιλέγουμε ένα e πρώτο ως προς το Φ(N) (ώστε να υπάρχει ο αντίστροφος mod Φ(N)).
- Πατάμε το πλήκτρο «Βήμα 2ο (υπολογισμός d= Ιδιωτικό κλειδί)».
- Η εφαρμογή υπολογίζει το ιδιωτικό κλειδί d, παρουσιάζει το ζευγάρι των κλειδιών του χρήστη (δημόσιο- Ιδιωτικό).

Η πλήρη ανάλυση της διαδικασίας εμφανίζεται στο tab «Ανάλυση Διαδικασίας»

6.11.3 Διαδικασίες Χρήστη Α.



Εικόνα 6.21 Screenshot of RSAApplet (Χρήστης Α).

Το σχετικό tab είναι χωρισμένο σε δύο panels, παρουσιάζοντας το πρώτο (επάνω) την διαδικασία της κρυπτογράφησης, και το δεύτερο (κάτω) την διαδικασία της αποκρυπτογράφησης. Αναλυτικά οι δύο διαδικασίες έχουν ως εξής:

- Διαδικασία Κρυπτογράφησης:
    - Ο χρήστης πληκτρολογεί το μήνυμα και το δημόσιο κλειδί του παραλήπτη.
    - Έπειτα πατάει το πλήκτρο κρυπτογράφηση για να το κρυπτογραφήσει. Εφόσον επιθυμεί να υπογράψει και να κρυπτογραφήσει το μήνυμα πατάει το αντίστοιχο πλήκτρο. Η διαδικασία της υπογραφής βέβαια προϋποθέτει την προηγούμενη δημιουργία κλειδιών για τον Αποστολέα.
    - Τέλος πατώντας το πλήκτρο «Αποστολή Κρυπτόλεξου στον Β» η εφαρμογή τοποθετεί το κρυπτόλεξο στο αντίστοιχο πεδίο της φόρμας στο tab του χρήστη Β.

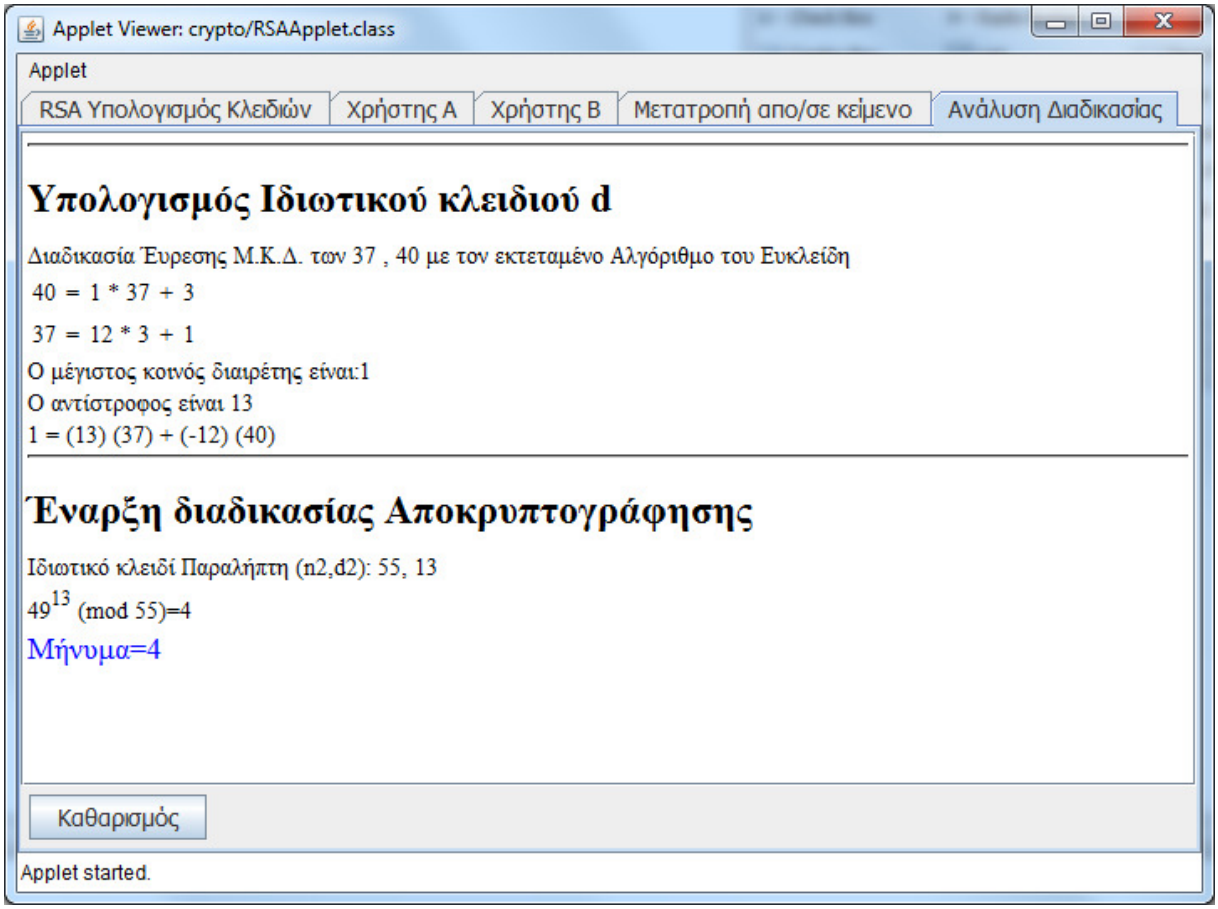
- Διαδικασία αποκρυπτογράφησης:

    - Ο χρήστης γράφει στην θέση «Κρυπτόλεξο» το κρυπτογραφημένο μήνυμα που λαμβάνει

    - Έπειτα συμπληρώνει το Δημόσιο και το Ιδιωτικό κλειδί του στις αντίστοιχες θέσεις στην φόρμα. Εφόσον επιθυμεί να δημιουργήσει νέο ζευγάρι κλειδιών, πατάει το πλήκτρο Υπολογισμός (η εφαρμογή τον οδηγεί στο tab «RSA υπολογισμός κλειδιών» για την δημιουργία των κλειδιών).

    - Πατάει το πλήκτρο «Αποκρυπτογράφηση» για να αποκρυπτογραφήσει το μήνυμα. Εφόσον το μήνυμα είναι υπογεγραμμένο αντί του πλήκτρου «αποκρυπτογράφηση» πατάμε το πλήκτρο «Αποκρυπτογράφηση & Αυθεντικοποίηση». Στην δεύτερη περίπτωση απαιτείται να έχουμε συμπληρώσει το Δημόσιο κλειδί του Αποστολέα στο αντίστοιχο πεδίο της φόρμας.

6.11.4 Ανάλυση Διαδικασίας



Εικόνα 6.22 Screenshot of RSAApplet (Ανάλυση Διαδικασίας).

Το σχετικό tab καταγράφει κάθε δραστηριότητα που εκτελούμε στο Applet, αναλύοντας βήμα προς βήμα τις διαδικασίες που εκτελούνται. Κάθε νέα δραστηριότητα δεν διαγράφει την ανάλυση της προηγούμενης. Απλά προστίθεται στο τέλος. Εφόσον θέλουμε να καθαρίσουμε και να ξαναρχίσουμε την καταγραφή πατάμε το πλήκτρο «Καθαρισμός».

6.12 Η Εφαρμογή της εκπαιδευτικής πλατφόρμας.

6.12.1 Η Βάση Δεδομένων.

Για την αποθήκευση της οργάνωσης, της δομής αλλά και μέρους του εκπαιδευτικού υλικού χρησιμοποιήθηκε η βάση δεδομένων SQLite. Από την εφαρμογή παρακολουθούνται δυο διαφορετικές βάσεις δεδομένων.

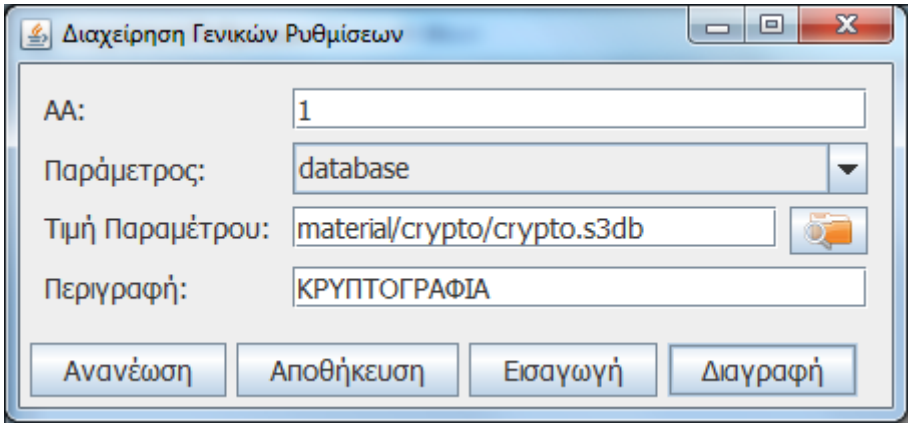
Η Β.Δ. των Ρυθμίσεων (Config.s3db).

Σε αυτήν καταγράφονται ρυθμίσεις της εφαρμογής. Τοποθετείται απαραίτητα στον ίδιο φάκελο με το εκτελέσιμο αρχείο της εφαρμογής. Περιέχει έναν μόνο πίνακα με όνομα config. Η δομή του πίνακα είναι η ακόλουθη:

TABLE [config] (
[aa] INTEGER PRIMARY KEY NOT NULL,
[code] VARCHAR(80) NULL,
[value] VARCHAR(120) NULL,
[description] VARCHAR(120) NULL)

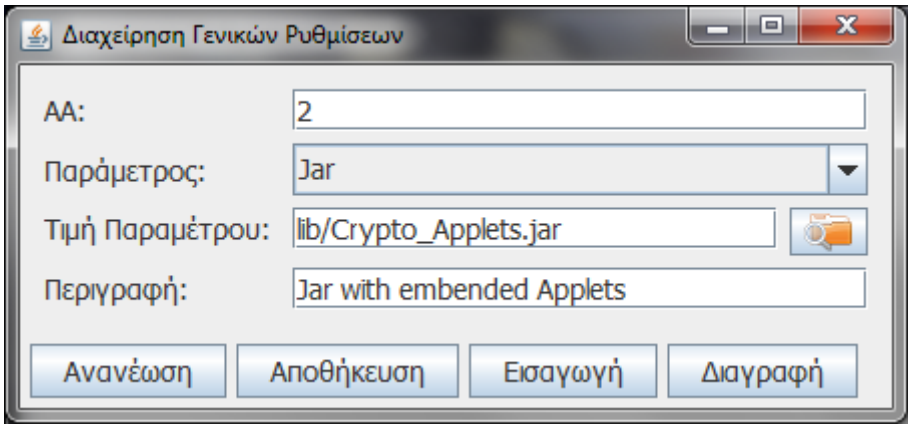
Η σημαντικότερη χρήση του πίνακα είναι να καταχωρεί στην εφαρμογή τις βάσεις δεδομένων (μία ή περισσότερες) που περιέχουν το εκπαιδευτικό υλικό. Μπορούμε να καταχωρήσουμε πρόσθετη βάση δεδομένων με εκπαιδευτικό υλικό, απλά εισάγοντας εγγραφή στον πίνακα config, θέτοντας στην παράμετρο (code) «database» και σαν τιμή παραμέτρου το σχετικό path

στο αρχείο της DATABASE. Η πρόσβαση στον συγκεκριμένο πίνακα μέσω της εφαρμογής γίνεται μέσω της ροής: Αρχική Οθόνη Εφαρμογής → Ρυθμίσεις → Γενικές → Επεξεργασία.



Εικόνα 6.23 Διαχείριση Γενικών Ρυθμίσεων (Προσθήκη Database με Εκπαιδευτικό Υλικό).

Στο παράδειγμα της εικόνας 6.23, έχει δηλωθεί ότι η εφαρμογή θα χρησιμοποιήσει την βάση δεδομένων crypto.s3db που βρίσκεται στο υποφάκελο material/crypto/. Στην περίπτωση που το αρχείο δεν υπάρχει, η εφαρμογή δημιουργεί νέα βάση δεδομένων με την κατάλληλη δομή.



Εικόνα 6.24 Διαχείριση Γενικών Ρυθμίσεων (Προσθήκη Αρχείου .Jar)

Η δεύτερη λειτουργία αφορά την επεκτασιμότητα των δυνατοτήτων της εφαρμογής. Η εφαρμογή φορτώνει δυναμικά τα αρχεία jar που δηλώνονται εδώ. Έπειτα οι κλάσεις που εμπεριέχονται είναι διαθέσιμες στην εφαρμογή. Μπορούμε λοιπόν να καταχωρήσουμε βιβλιοθήκες γραμμένες σε java, απλά εισάγοντας εγγραφή στον πίνακα config θέτοντας στην παράμετρο (code) «jar» και σαν τιμή παραμέτρου το σχετικό path.

Η Β.Δ. με το περιεχόμενο του Εκπαιδευτικού Υλικού (Crypto.s3db).

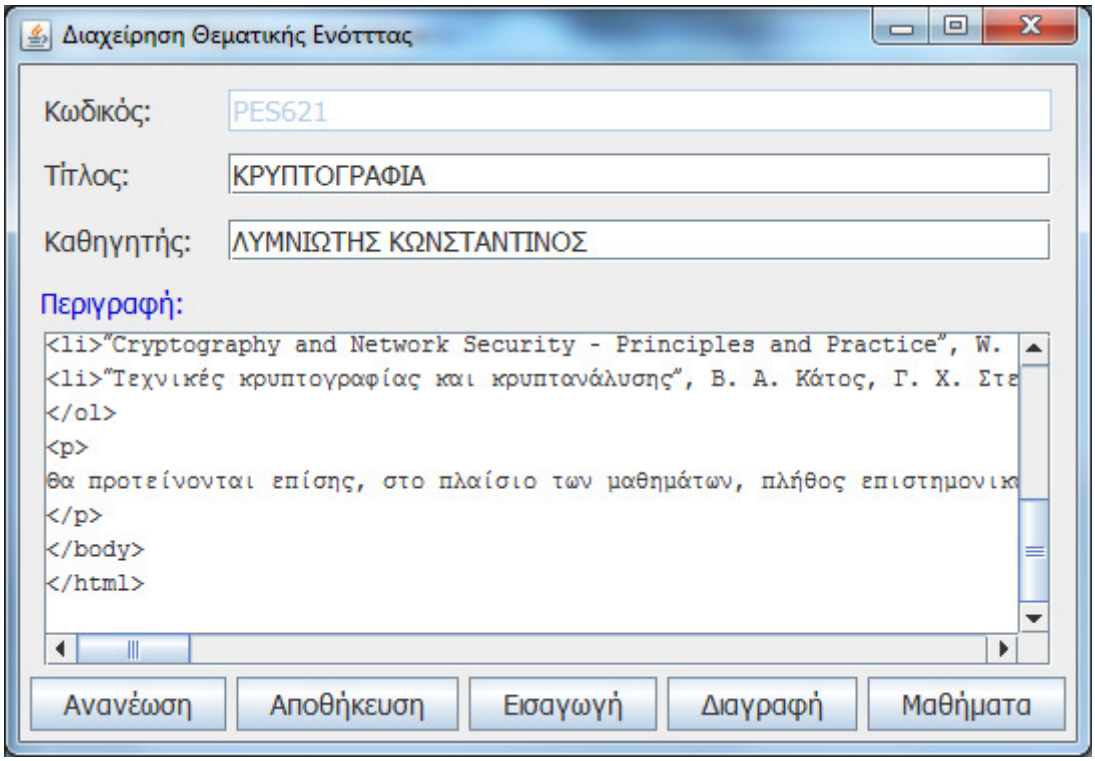
Η οργάνωση του εκπαιδευτικού υλικού είναι σε τρία επίπεδα ως ακολούθως:

- Επίπεδο Θεματικών Ενοτήτων. Παρακολουθείτε από τον πίνακα theme.
- Επίπεδο Μαθημάτων. Παρακολουθείτε από τον πίνακα lesson.
- Επίπεδο Εκπαιδευτικού υλικού. Παρακολουθείτε από τον πίνακα material.

Η δομή του πίνακα theme είναι η ακόλουθη:

TABLE [theme] (
[theme] VARCHAR(20) PRIMARY KEY NULL,
[title] VARCHAR(70) NOT NULL,
[description] TEXT NULL,
[teacher] VARCHAR(60) NULL
)

Η πρόσβαση στον συγκεκριμένο πίνακα μέσω της εφαρμογής γίνεται μέσω της ροής: Αρχική Οθόνη Εφαρμογής → Ρυθμίσεις → Κρυπτογραφία → Θεματικές Ενότητες



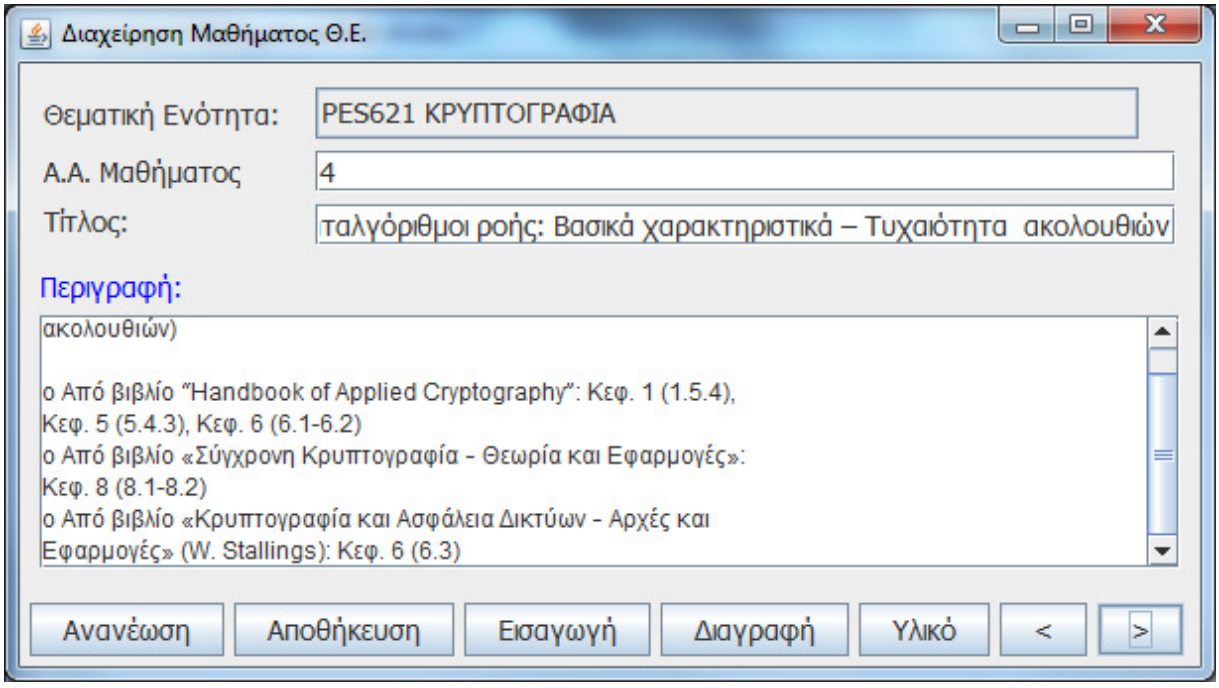
Εικόνα 6.25 Διαχείριση Θεματικής Ενότητας.

Εδώ καταχωρούμε έναν κωδικό για την θεματική ενότητα, έναν τίτλο, το ονοματεπώνυμο του εκπαιδευτή, και μια περιγραφή. Μέσω της συγκεκριμένης φόρμας μπορούμε να κάνουμε εισαγωγή, μεταβολή και διαγραφή στις εγγραφές του πίνακα. Επίσης μπορούμε να προβάλουμε τα μαθήματα που έχουν δημιουργηθεί κάτω από την συγκεκριμένη Θ.Ε.

Η δομή του πίνακα Lesson είναι η ακόλουθη:

TABLE [lesson] (
[lesson] INTEGER PRIMARY KEY AUTOINCREMENT NOT NULL,
[theme] VARCHAR(20) NOT NULL,
[aa] INTEGER NULL,
[title] VARCHAR(70) NOT NULL,
[description] TEXT NULL,
[stitle] VARCHAR(30) NULL
)

Η πρόσβαση στον συγκεκριμένο πίνακα μέσω της εφαρμογής γίνεται μέσω της ροής: Αρχική Οθόνη Εφαρμογής → Ρυθμίσεις → Κρυπτογραφία → Μαθήματα



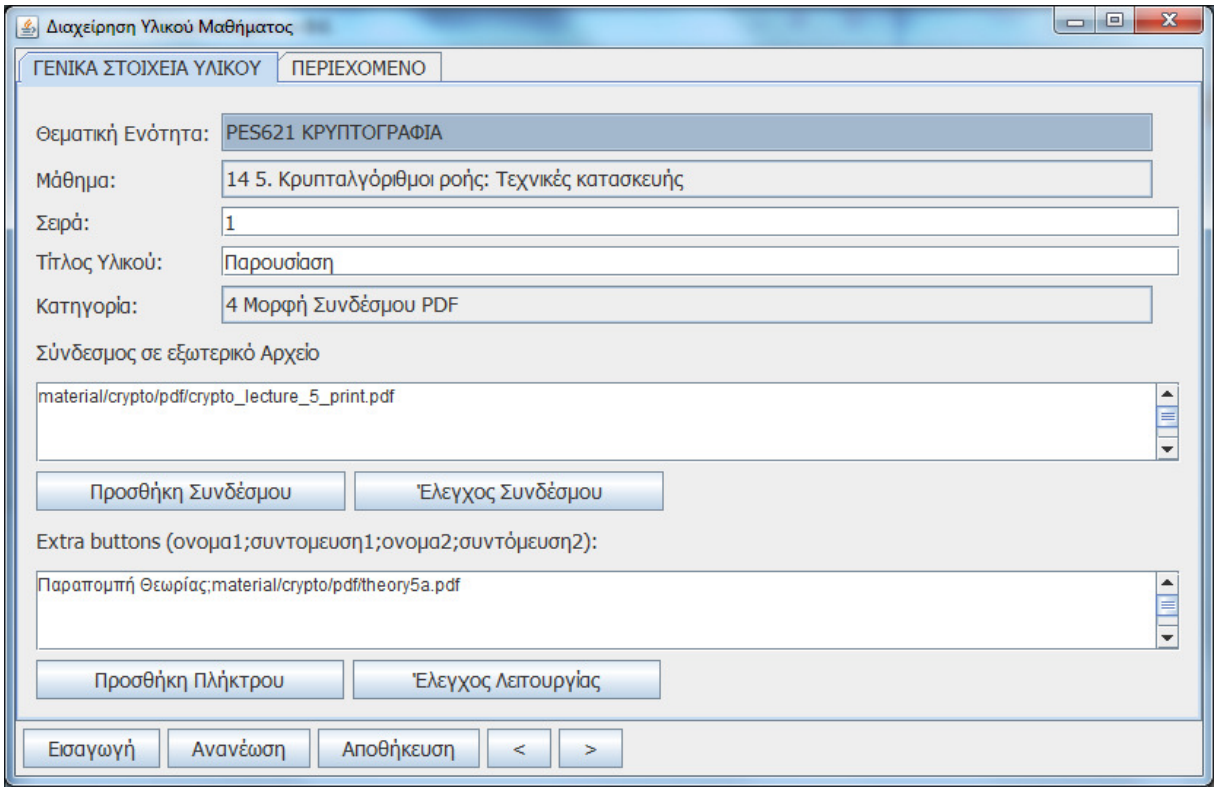
Εικόνα 6.26 Διαχείριση Μαθήματος Θ. Ε.

Εδώ καταχωρούμε την Θ.Ε. που ανήκει το συγκεκριμένο μάθημα, έναν αύξοντα αριθμό (για ταξινόμηση του μαθήματος εντός της Θ.Ε.), τον τίτλο του μαθήματος και μια περιγραφή. Επίσης μπορούμε να προβάλουμε το υλικό που έχει αντιστοιχιστεί με το συγκεκριμένο μάθημα.

Η δομή του πίνακα Material είναι η ακόλουθη:

```
TABLE [material] (
[material] INTEGER PRIMARY KEY AUTOINCREMENT NOT NULL,
[lesson] INTEGER NULL,
[title] VARCHAR(80) NULL,
[category] INTEGER NULL,
[type] INTEGER NULL,
[link] TEXT NULL,
[shortcut] TEXT NULL,
[description] TEXT NULL,
[aa] INTEGER NULL
)
```

Η πρόσβαση στον συγκεκριμένο πίνακα μέσω της εφαρμογής γίνεται μέσω της ροής: Αρχική Οθόνη Εφαρμογής → Ρυθμίσεις → Κρυπτογραφία → Υλικό.



Εικόνα 6.27 Διαχείριση Υλικού Μαθήματος (Γενικά Στοιχεία).

Μέσω αυτής της φόρμας μπορούμε να προσθέσουμε υλικό στην εφαρμογή μας. Αρχικά καταχωρούμε την Θ.Ε. και το μάθημα στο οποίο αντιστοιχεί. Έπειτα έναν αριθμό για σειρά παρουσίασης του υλικού μέσα στο μάθημα στο οποίο εντάσσεται. Στο πεδίο κατηγορία καταχωρούμε τον τύπο του υλικού. Οι τύποι του υλικού που υποστηρίζονται είναι οι ακόλουθοι:

1. Μορφή Απλού Κειμένου. Η πιο απλή μορφή υλικού που μπορούμε να προσθέσουμε. Το κείμενο το γράφουμε στο πλαίσιο κειμένου που υπάρχει στο tab «ΠΕΡΙΕΧΟΜΕΝΟ».

2. Μορφή HTML Το κείμενο σε μορφή HTML έχει πολύ περισσότερες δυνατότητες διαμόρφωσης. Ο συγκεκριμένος τύπος Υλικού υποστηρίζει HTML έκδοση 3. Όπως προηγουμένως το περιεχόμενο το γράφουμε στο πλαίσιο κειμένου που υπάρχει στο tab «ΠΕΡΙΕΧΟΜΕΝΟ».

3. Μορφή Συνδέσμου HTML. Εδώ δεν γράφουμε κείμενο σε μορφή HTML αλλά καταχωρούμε έναν σύνδεσμο που παραπέμπει σε εξωτερικό αρχείο HTML. Το μονοπάτι (τη σχετική διαδρομή) προς το αρχείο το καταχωρούμε στο πεδίο «Σύνδεσμος σε εξωτερικό αρχείο». Πατώντας το πλήκτρο «Προσθήκη συνδέσμου» διαλέγουμε το αρχείο και η εφαρμογή καταγράφει την σχετική διαδρομή του συνδέσμου. Τέλος με το

πλήκτρο «Έλεγχος Συνδέσμου» μπορούμε να ελέγξουμε προβλήματα σχετικά με τον σύνδεσμο αλλά και την εμφάνιση του περιεχομένου του. Όπως προηγουμένως υποστηρίζεται μορφή αρχείου HTML έκδοσης 3. Στο πλαίσιο κειμένου που υπάρχει στο tab «ΠΕΡΙΕΧΟΜΕΝΟ» μπορούμε προαιρετικά να καταχωρήσουμε μια περιγραφή της Ιστοσελίδας. Ο ρόλος της περιγραφής αυτής στην συγκεκριμένη περίπτωση είναι μόνο για την λειτουργία της αναζήτησης.

4. Μορφή Συνδέσμου PDF. Και σε αυτήν την περίπτωση καταχωρούμε σύνδεσμο σε αρχείο. Αυτή την φορά βέβαια ο προορισμός είναι αρχείο PDF. Το μονοπάτι (την σχετική διαδρομή) προς το αρχείο το καταχωρούμε στο πεδίο «Σύνδεσμος σε εξωτερικό αρχείο». Στο πλαίσιο κειμένου που υπάρχει στο tab «ΠΕΡΙΕΧΟΜΕΝΟ» μπορούμε προαιρετικά να καταχωρήσουμε μια περιγραφή του περιεχομένου του PDF. Ο ρόλος της περιγραφής αυτής είναι μόνο για την λειτουργία της αναζήτησης.

5. Μορφή HTML4. Εδώ έχουμε πλήρη υποστήριξη HTML4 (css, javascript κ.λ.π.). Το περιεχόμενο το γράφουμε στο πλαίσιο κειμένου που υπάρχει στο tab «ΠΕΡΙΕΧΟΜΕΝΟ».

6. Μορφή Συνδέσμου HTML4. Όπως και στην επιλογή 3 με την διαφορά ότι υποστηρίζεται η έκδοση 4 της HTML.

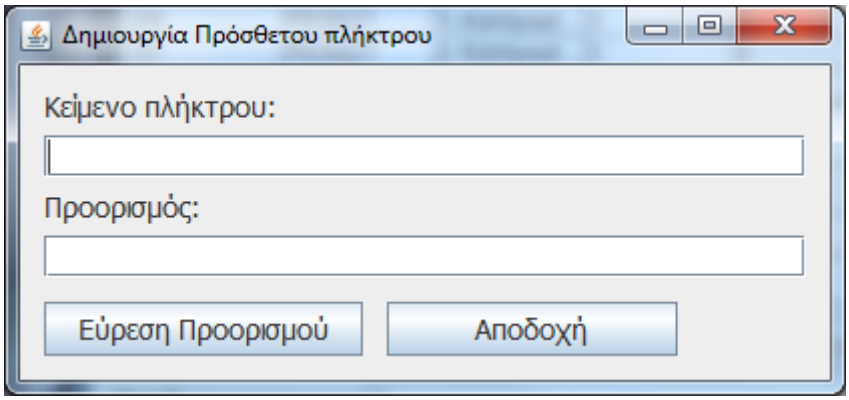
7. Flash Animation. Σε αυτή την επιλογή καταχωρούμε σύνδεσμο σε αρχείο flash. Το μονοπάτι (την σχετική διαδρομή) προς το αρχείο το καταχωρούμε στο πεδίο «Σύνδεσμος σε εξωτερικό αρχείο». Στο πλαίσιο κειμένου που υπάρχει στο tab «ΠΕΡΙΕΧΟΜΕΝΟ» μπορούμε προαιρετικά να καταχωρήσουμε μια περιγραφή του περιεχομένου του αρχείου flash. Ο ρόλος της περιγραφής αυτής είναι μόνο για την λειτουργία της αναζήτησης.

8. Video File. Σε αυτή την επιλογή καταχωρούμε σύνδεσμο σε αρχείο video. Το μονοπάτι (τη σχετική διαδρομή) προς το αρχείο το καταχωρούμε στο πεδίο «Σύνδεσμος σε εξωτερικό αρχείο». Στο πλαίσιο κειμένου που υπάρχει στο tab «ΠΕΡΙΕΧΟΜΕΝΟ» μπορούμε προαιρετικά να καταχωρήσουμε μια περιγραφή του περιεχομένου του αρχείου. Ο ρόλος της περιγραφής αυτής είναι μόνο για την λειτουργία της αναζήτησης.

9. Java Class. Αυτή την επιλογή την χρησιμοποιούμε για τα Applet και για άλλες κλάσεις, που βρίσκονται σε java βιβλιοθήκες που έχουν δηλωθεί στην Β.Δ. των ρυθμίσεων (config.s3db). Στο πεδίο «Σύνδεσμος σε εξωτερικό αρχείο» τοποθετούμε το όνομα της κλάσης του Applet, στην μορφή package.class_name (πχ crypto.LFSRApplet). Οι τύποι

των κλάσεων που υποστηρίζονται είναι όλες οι κλάσεις εξειδίκευσης των κλάσεων Applet, JApplet, jPanel, jFrame, και JComponent. Στο πλαίσιο κειμένου που υπάρχει στο tab «ΠΕΡΙΕΧΟΜΕΝΟ» μπορούμε προαιρετικά να καταχωρήσουμε μια περιγραφή του περιεχομένου του Applet για την λειτουργία της αναζήτησης.

Υπάρχει η δυνατότητα προσθήκης με την μορφή πλήκτρων συνδέσμων σε αρχεία του Η/Υ. Όταν πατηθούν αυτά τα πλήκτρα η εφαρμογή προωθεί την απαίτηση στο λειτουργικό σύστημα που με την σειρά του εντοπίζει την κατάλληλη εφαρμογή για το άνοιγμα του αρχείου. Αυτό δηλώνεται στο πεδίο «Extra Buttons». Ο ενδεδειγμένος τρόπος προσθήκης ενός τέτοιου πλήκτρου είναι η χρήση του «Προσθήκη πλήκτρου». Αυτό ενεργοποιεί την ακόλουθη φόρμα:

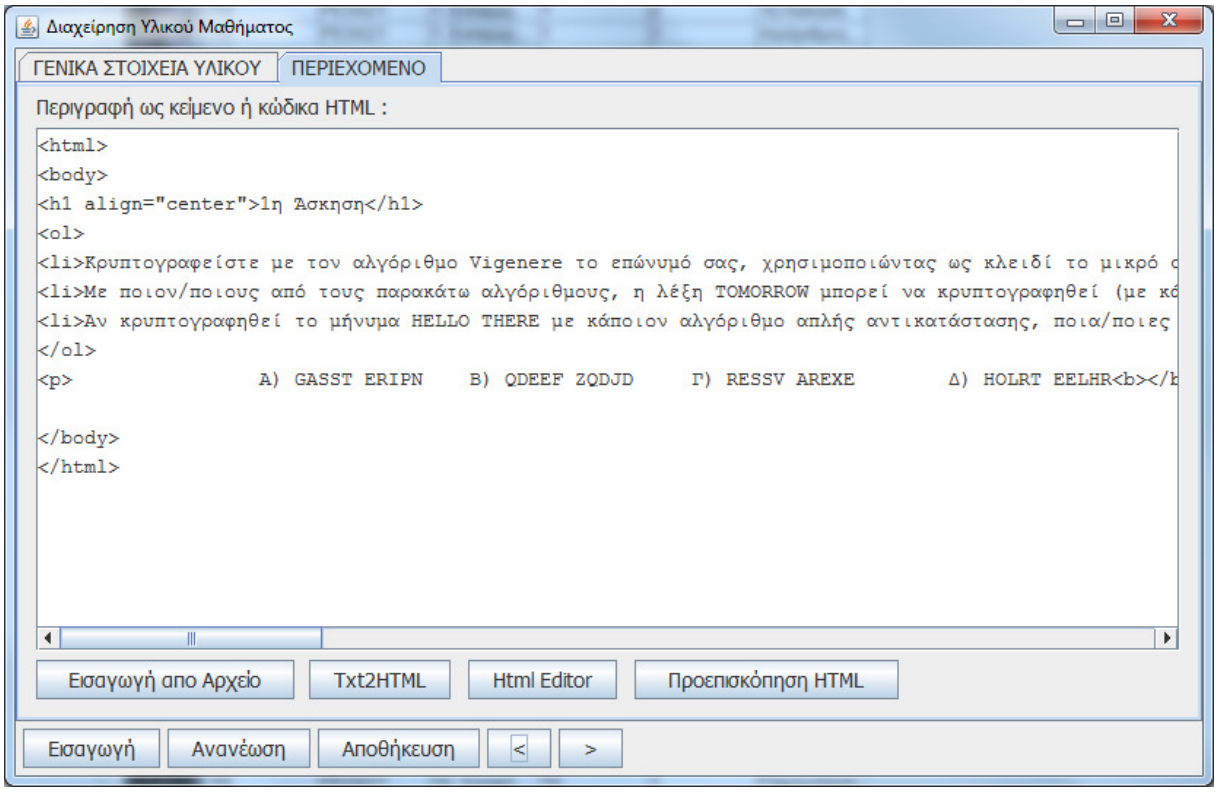


Εικόνα 6.27 Δημιουργία Πρόσθετου πλήκτρου.

Αρχικά δίνουμε το όνομα που επιθυμούμε για το πλήκτρο. Έπειτα πατώντας το πλήκτρο «Εύρεση Προορισμού» καθορίζουμε την σχετική διαδρομή του αρχείου. Τέλος πατώντας «Αποδοχή» αποδεχόμαστε την προσθήκη του πλήκτρου.

Μπορούμε να επαναλάβουμε την διαδικασία και να προσθέσουμε και άλλα πλήκτρα. Επίσης μπορούμε πατώντας στο «Έλεγχος Λειτουργίας» να ελέγξουμε την συμπεριφορά των πλήκτρων που δηλώσαμε.

Στην καρτέλα ΠΕΡΙΕΧΟΜΕΝΟ καταγράφουμε το περιεχόμενο του κειμένου (κατηγορία υλικού 1), το HTML περιεχόμενο (κατηγορία υλικού 2 & 5) ή την περιγραφή του πολυμεσικού υλικού (κατηγορίες υλικού 3,4,6,7 και 8).



Εικόνα 6.28 Διαχείριση Υλικού Μαθήματος (Περιεχόμενο).

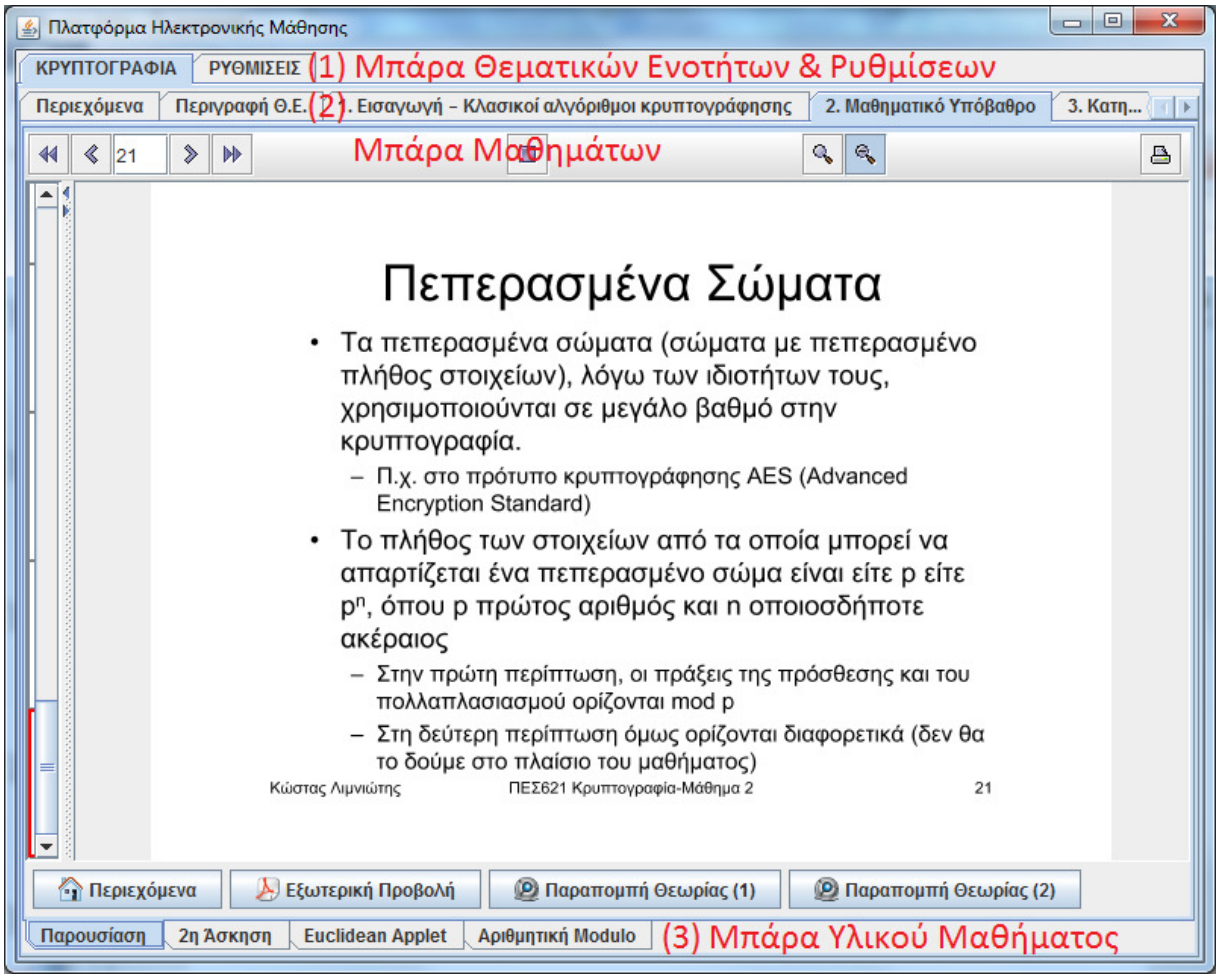
Η Καρτέλα «Περιεχόμενο» μας παρέχει διάφορες βοηθητικές λειτουργίες ως ακολούθως:

- «Εισαγωγή από Αρχείο». Εισάγουμε στο πλαίσιο το περιεχόμενο ενός αρχείου.
- «Txt2HTML». Μπορούμε να γράψουμε απλό κείμενο στο πλαίσιο και πατώντας το συγκεκριμένο πλήκτρο να διαμορφωθεί σαν κείμενο HTML.
- «Html Editor». Μας εμφανίζει έναν Editor που μπορούμε να δημιουργήσουμε μια HTML σελίδα (είναι βασισμένο στο http://examples.oreilly.com/jswing2/code/ch23/).
- «Προεπισκόπηση HTML» Μας εμφανίζει ένα παράθυρο που μας δείχνει πως θα εμφανίζεται το έγγραφο HTML που δημιουργήσαμε.

6.12.2 Το Περιβάλλον της Εφαρμογής.

Ξεκινώντας η εφαρμογή ανοίγει την τοπική βάση (config.s3db) με τις ρυθμίσεις. Αρχικά φορτώνει δυναμικά όλα τα αρχεία jar που έχουν δηλωθεί στον πίνακα config. Έπειτα δημιουργεί δυναμικά όλα της τα μενού. Ελέγχει στον πίνακα config για όλες τις εγγραφές Βάσεων

Δεδομένων με εκπαιδευτικό υλικό. Έπειτα ανοίγει κάθε εγγεγραμμένη Β.Δ. και αναζητεί τις Θεματικές ενότητες, τα μαθήματα και το εκπαιδευτικό υλικό.



Εικόνα 6.29 Η Βασική Οθόνη τηςΕφαρμογής.

Η Οθόνη της εφαρμογής αποτελείτε από 4 περιοχές.

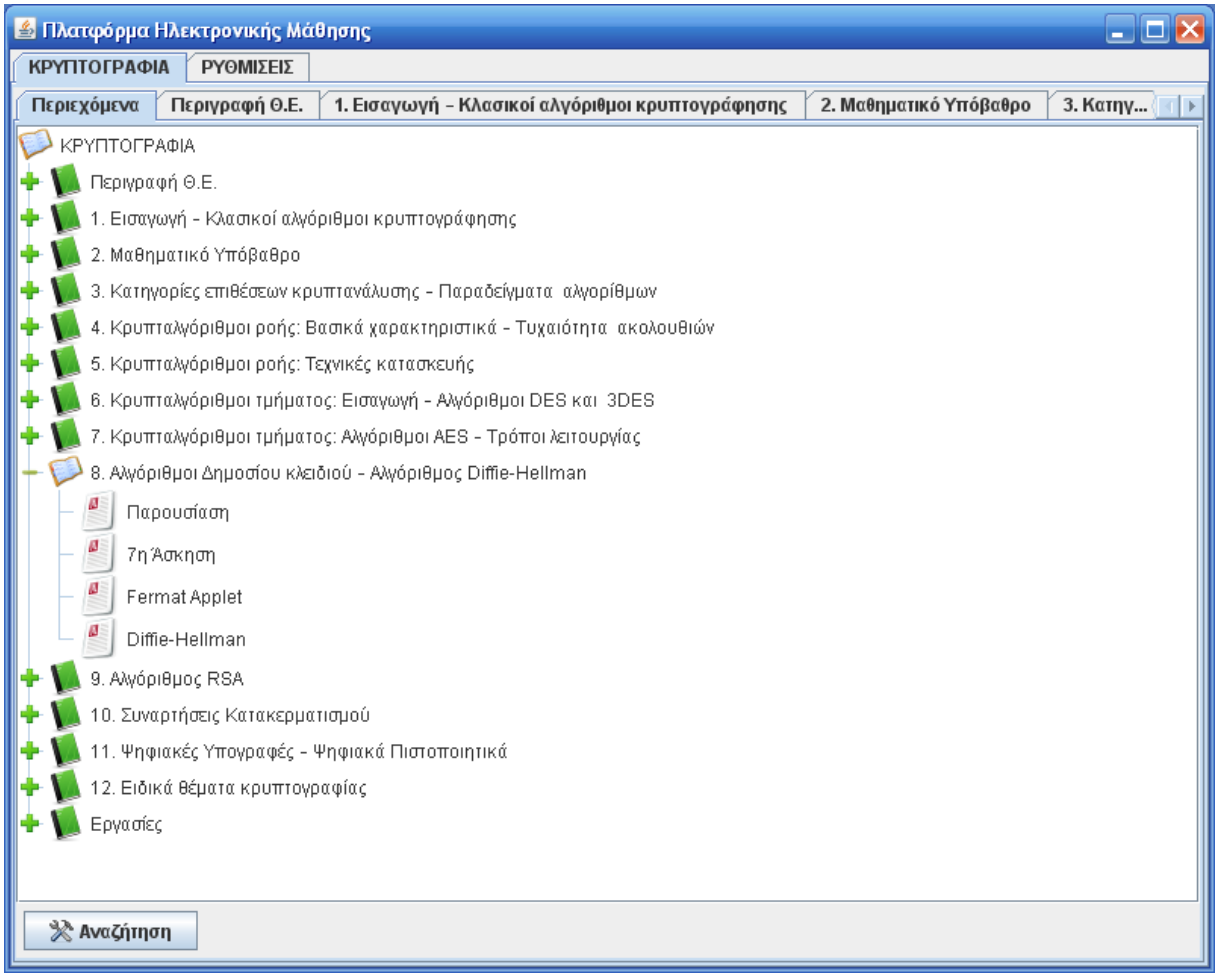
1. ***Μπάρα Θεματικών ενοτήτων και Ρυθμίσεων.*** Σε αυτήν εμφανίζονται σε καρτέλες, οι τίτλοι των Θ.Ε. που υπάρχουν στον πίνακα theme της (ή των) Β.Δ. του Εκπαιδευτικού Υλικού. Η Τελευταία καρτέλα «ΡΥΘΜΙΣΕΙΣ» μας δίνει πρόσβαση στην διαχείριση των πινάκων της εφαρμογής.

2. ***Μπάρα Μαθημάτων.*** Για κάθε Επιλεγμένη Θ.Ε. από την 1η Μπάρα παρουσιάζονται τα μαθήματα που της αντιστοιχούν. Ο τίτλος κάθε μαθήματος εμφανίζεται σε διαφορετική καρτέλα. Οι πληροφορίες προέρχονται από τον πίνακα lesson της Β.Δ..

3. ***Μπάρα Υλικού Μαθήματος***. Για κάθε μάθημα που επιλέγουμε στην 2η μπάρα εμφανίζεται το αντίστοιχο υλικό μαθήματος που έχουμε προσθέσει. Οι πληροφορίες εδώ προέρχονται από τον πίνακα material της Β.Δ. Κάθε καρτέλα είναι και μια εγγραφή στον πίνακα material.

4. ***Περιοχή Περιεχομένου***. Όλη η περιοχή ανάμεσα στην 2η και την 3η μπάρα είναι η διαθέσιμη περιοχή για την απεικόνιση του περιεχομένου του εκπαιδευτικού υλικού. Πώς θα διαμορφωθεί αυτή η περιοχή εξαρτάτε από την κατηγορία περιεχομένου που έχει δηλωθεί ότι χρησιμοποιούμε σε κάθε περίπτωση. Μπορεί να εμφανίζεται κείμενο, περιεχόμενο html, αρχείο PDF, αρχείο FLASH, αρχείο VIDEO. Εφόσον στην εγγραφή του υλικού έχουν δηλωθεί επιπλέον πλήκτρα (extra buttons) για συντομεύσεις σε αρχεία, αυτά εμφανίζονται στην τελευταία γραμμή, ακριβώς πάνω από την μπάρα υλικού.

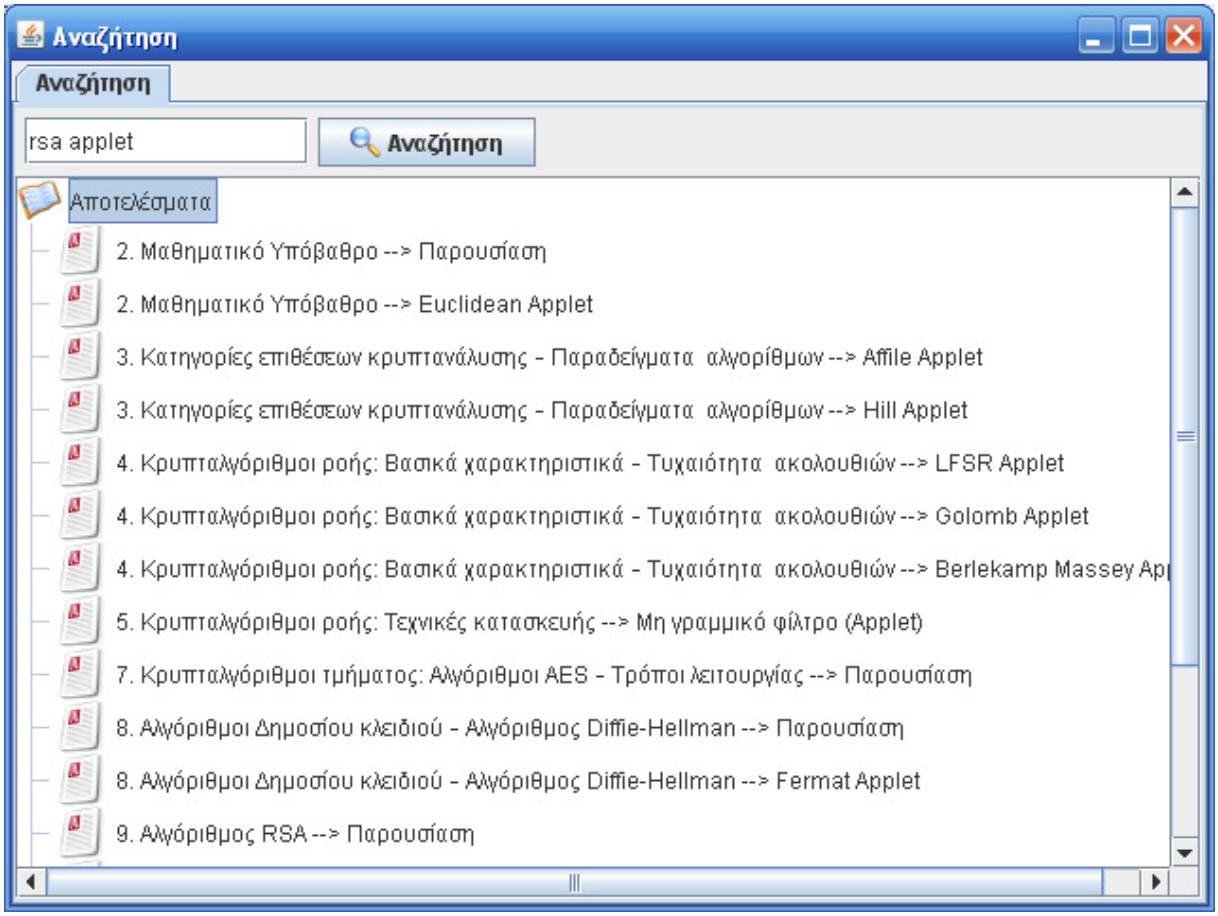
6.12.3 Ο Πίνακας Περιεχομένων.



Εικόνα 6.30 Ο πίνακας Περιεχομένων της Εφαρμογής.

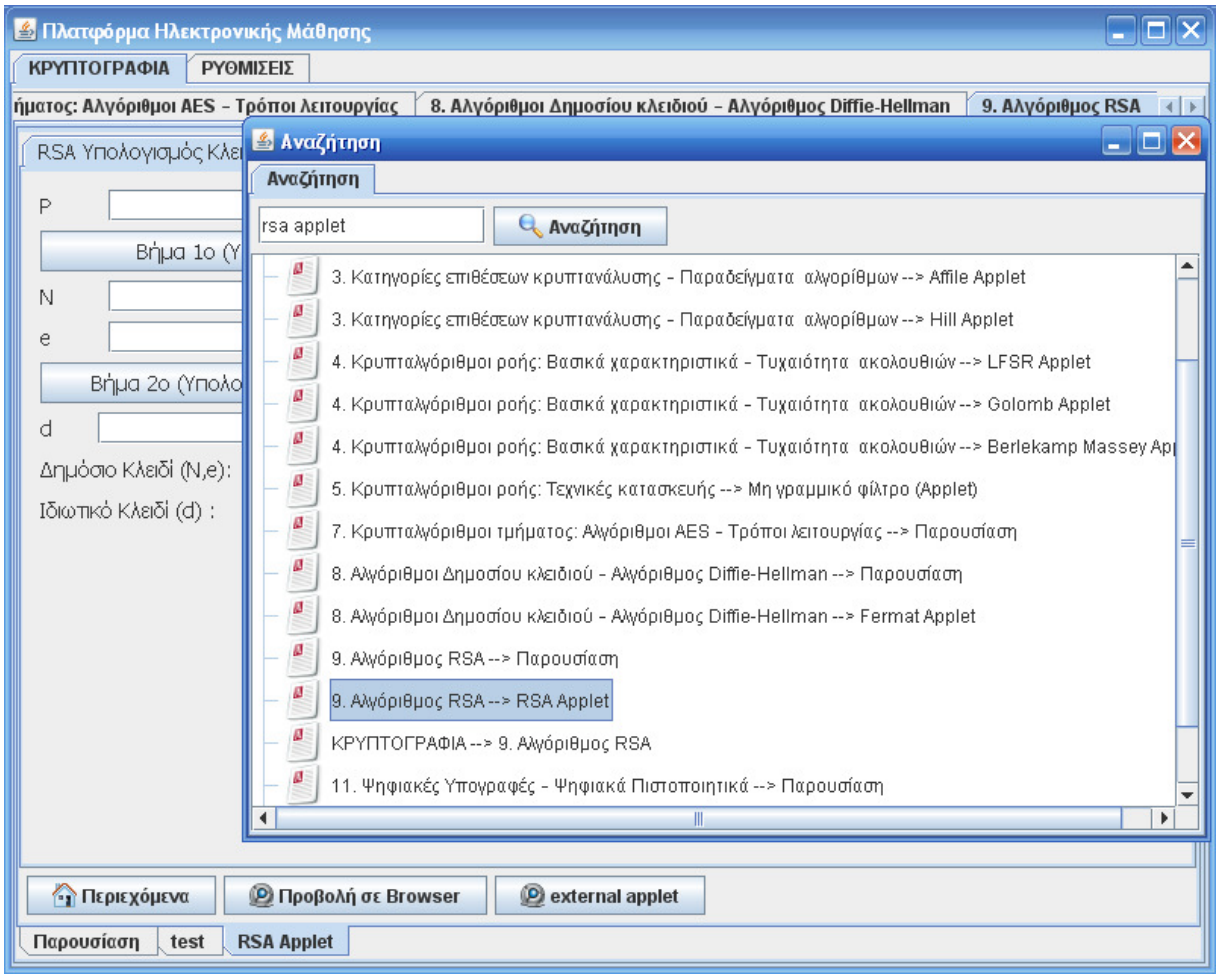
Σε κάθε Θ.Ε. η 1η καρτέλα στην μπάρα μαθημάτων δεν προέρχεται από το πίνακα lesson. Είναι ο πίνακας περιεχομένων της Θ.Ε.. Δημιουργείται αυτόματα από την εφαρμογή και παρουσιάζει σε δομή δέντρου όλη την οργάνωση του υλικού της Θ.Ε. Επιλέγοντας κάποιο «φύλλο» του δέντρου μεταφερόμαστε αυτόματα στο αντίστοιχο περιεχόμενο.

6.12.4 Η Αναζήτηση.



Εικόνα 6.31 Ο οθόνη της Αναζήτησης.

Από την οθόνη των περιεχομένων μπορούμε να μεταβούμε στην λειτουργία της αναζήτησης. Υποστηρίζεται αναζήτηση με πολλαπλές λέξεις, απλά πρέπει να είναι χωρισμένες με τον κενό χαρακτήρα. Η πράξη που υλοποιείται όταν χρησιμοποιούνται πολλαπλές λέξεις είναι η πράξη OR. Όποια από τις λέξεις εντοπιστεί θα επιστραφεί η αντίστοιχη εγγραφή του υλικού σαν αποτέλεσμα. Τα πεδία της βάσης δεδομένων που χρησιμοποιούνται για να εντοπιστούν οι εγγραφές είναι οι τίτλοι και οι περιγραφές των εγγραφών.



Εικόνα 6.32 Οθόνη Αναζήτησης και μετάβαση σε περιεχόμενο.

Όταν επιλέξουμε κάποιο από τα αποτελέσματα που επιστρέφει η αναζήτηση, τότε αυτόματα η βασική οθόνη της εφαρμογής (βρίσκεται πίσω από την οθόνη της αναζήτησης) μεταφέρεται στο συγκεκριμένο περιεχόμενο.

Κεφάλαιο 7
Αποτίμηση Εκπαιδευτικού Εργαλείου

Στο τελευταίο μέρος της τρέχουσας έρευνας θα προσπαθήσουμε να αξιολογήσουμε το εκπαιδευτικό εργαλείο. Η αξιολόγηση δεν έρχεται μόνο να μετρήσει το αποτέλεσμα, αλλά αποτελεί μέρος της διαδικασίας της μάθησης που προσπαθεί να το κατανοήσει και να συμβάλει στη βελτίωση της εφαρμογής.

7.1 Στόχοι της εφαρμογής

Ο σκοπός της τρέχουσας διατριβής ήταν η δημιουργία μιας σειράς μαθημάτων ως υποστηρικτικό εργαλείο, με αντικείμενο την θεματική ενότητα «Κρυπτογραφία». Το σύνολο αυτών των ηλεκτρονικών μαθημάτων απευθύνεται πρώτιστα σε σπουδαστές που φοιτούν σε τμήματα εξ' αποστάσεως εκπαίδευσης.

Επιπρόσθετα χαρακτηριστικά που τέθηκαν στο σχεδιαστικό στάδιο είναι τα ακόλουθα:

- Η εκπαιδευτική πλατφόρμα πρέπει να είναι ανοικτή ώστε να είναι εύκολη η προσθήκη ή μεταβολή του υλικού που περιέχει. Να μπορεί να εφαρμοστεί σε οποιαδήποτε Θεματική Ενότητα.
- Να υποστηρίζεται κάθε είδους πολυμεσικό υλικό.
- Να είναι σε portable μορφή ώστε να μην χρειάζεται εγκατάσταση και να εκτελείται ακόμα και σε Η/Υ με περιορισμένα επίπεδα πρόσβασης.
- Να παρουσιάζει χαρακτηριστικά ανεξαρτησίας από το λειτουργικό σύστημα.

7.2 Υλοποίηση

Για να ανταποκριθούμε στους στόχους και στα χαρακτηριστικά που απαιτούσαμε έγιναν οι ακόλουθες επιλογές.

- Χρησιμοποιήσαμε Β.Δ. για να καταχωρούμε το εκπαιδευτικό υλικό. Διασφαλίσαμε έτσι το ανοικτό της εφαρμογής αφού η προσθήκη, μεταβολή εκπαιδευτικού υλικού ανάγεται σε προσθήκη, μεταβολή εγγραφών στην Β.Δ.
- Χρησιμοποιήσαμε σαν Β.Δ. την SQLite. Δεν χρειάζεται εγκατάσταση και εξασφαλίσαμε το portable της εφαρμογής.
- Επιλέχθηκε η γλώσσα προγραμματισμού Java ώστε να επιτυγχάνεται η ανεξαρτησία από το λειτουργικό σύστημα.

- Οι προσομοιώσεις υλοποιήθηκαν με Java Applets ώστε να μπορούν να χρησιμοποιηθούν και ανεξάρτητα από την εκπαιδευτική πλατφόρμα (πχ ενσωμάτωσή τους σε ιστοσελίδες).

7.3 Αξιολόγηση

Η αξιολόγηση της εφαρμογής ουσιαστικά στηρίχθηκε στην διανομή και συμπλήρωση ενός ερωτηματολογίου. Οι περιορισμοί (κυρίως γεωγραφικοί) που επιβάλει το μοντέλο της εξ' αποστάσεως εκπαίδευσης έκαναν αδύνατη την εφαρμογή άλλης μεθόδου αξιολόγησης. Η εφαρμογή διανεμήθηκε στους σπουδαστές περίπου ένα μήνα πριν την ολοκλήρωση της Θεματικής Ενότητας. Οι σπουδαστές χρησιμοποίησαν την εφαρμογή κυρίως για στην προετοιμασία τους για τις εξετάσεις. Στο διάστημα αυτό, παρατηρήσεις και αντιδράσεις εκ μέρους των σπουδαστών οδήγησαν σε αλλαγές, προσθήκες και βελτιώσεις στην εφαρμογή. Μετά το πέρας των εξετάσεων και την ολοκλήρωση των υποχρεώσεων τους για την Θ.Ε. συμπλήρωσαν το ερωτηματολόγιο αξιολόγησης. Τα συμπεράσματα από την ανάλυση των απαντήσεων του ερωτηματολογίου, οδήγησαν στις τελικές επεμβάσεις στην εφαρμογή και το περιεχόμενο της.

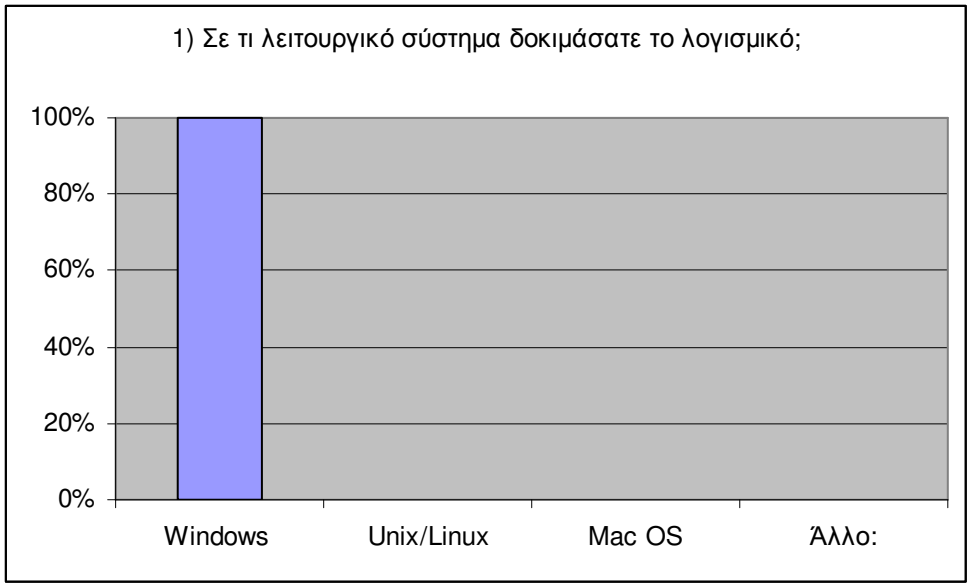
7.3.1 Ερωτηματολόγιο.

Το ερωτηματολόγιο αξιολόγησης περιλαμβάνει ερωτήσεις των ακόλουθων κατηγοριών [56].

- Αξιολόγησης απαιτήσεων Υλικού και Λογισμικού
- Σχεδίασης
- Διδακτικών Στόχων
- Εκπαιδευτικού Περιεχόμενου
- Περιβάλλοντος της εφαρμογής
- Προσαρμογής στις απαιτήσεις της εξ αποστάσεως εκπαίδευσης.

Αναρτήθηκε στην ακόλουθη διεύθυνση:
https://docs.google.com/spreadsheet/viewform?formkey=dEEzcVJkZG93bVVNSjFnMDM4UU8taHc6MQ#gid=0.

7.3.2 Ερωτήσεις



Εικόνα 7.1 Ερωτηματολόγιο – Ερώτηση 1η.

Αριθμός Ερώτησης: 1.

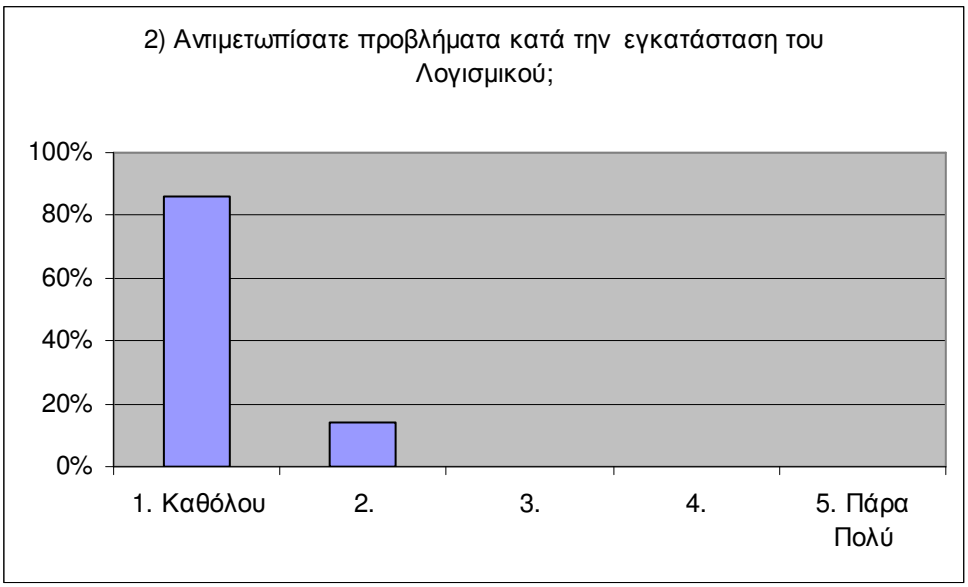
Κατηγορία Ερώτησης: Αξιολόγηση απαιτήσεων Υλικού – Λογισμικού.

Ερώτηση: Σε τι λειτουργικό σύστημα δοκιμάσατε το λογισμικό;

Σκοπός της Ερώτησης: Να διερευνηθεί το λειτουργικό σύστημα που χρησιμοποιηθούν οι σπουδαστές. Η υποστήριξη πολλαπλών λειτουργικών συστημάτων θέτει περιορισμούς σε θέματα σχεδίασης του λογισμικού καθώς και συμβιβασμούς σε θέματα απόδοσης, παρουσίασης κ.λ.π.

Συμπεράσματα: Το σύνολο των σπουδαστών της έρευνας χρησιμοποιεί τα windows.

Σχόλια: Δεν φαίνεται να υπάρχει ανάγκη να υποστηρίζονται πολλαπλά λειτουργικά συστήματα.



Εικόνα 7.2 Ερωτηματολόγιο – Ερώτηση 2η.

Αριθμός Ερώτησης: 2.

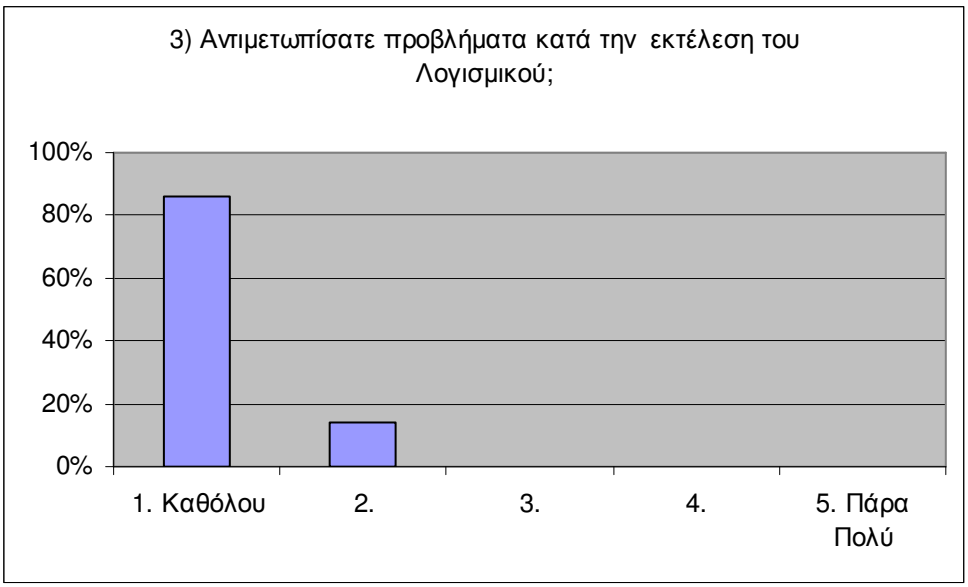
Κατηγορία Ερώτησης: Αξιολόγηση σχεδίασης.

Ερώτηση: Αντιμετωπίσατε προβλήματα κατά την εγκατάσταση του λογισμικού;

Σκοπός της Ερώτησης: Να διερευνηθεί η δυσκολία που αντιμετώπισαν οι σπουδαστές για να εγκαταστήσουν την εφαρμογή στον Η/Υ τους. Στις πρακτικές καλής σχεδίασης του Λογισμικού είναι η δυνατότητα χρήσης του από μη έμπειρους χρήστες.

Συμπεράσματα: Σε γενικές γραμμές δεν παρουσιάστηκαν προβλήματα.

Σχόλια: Το λογισμικό δεν απαιτεί κάποια ειδική λειτουργία εγκατάστασης. Είναι portable εφαρμογή και ουσιαστικά διανέμουμε ένα συμπιεσμένο αρχείο, που περιέχει έναν φάκελο με την εφαρμογή και το απαραίτητο υλικό. Κατά την περίοδο της δοκιμαστικής λειτουργίας της εφαρμογής το αρχείο ήταν σε μορφή winrar. Η επιλογή αυτή έγινε κυρίως λόγω των αυξημένων επιδόσεων σε συμπίεση που μας παρέχει το συγκεκριμένο format. Σε κανονική λειτουργία θα μπορεί να είναι σε μορφή zip (υπάρχει ενσωματωμένη υποστήριξη του συγκεκριμένου format σε όλα τα λειτουργικά συστήματα.), ή σε μορφή αυτό-εξαγόμενου αρχείου (self-extracted), ώστε να μην απαιτείται η εγκατάσταση προγράμματος διαχείρισης συμπιεσμένων αρχείων.



Εικόνα 7.3 Ερωτηματολόγιο – Ερώτηση 3η.

Αριθμός Ερώτησης: 3.

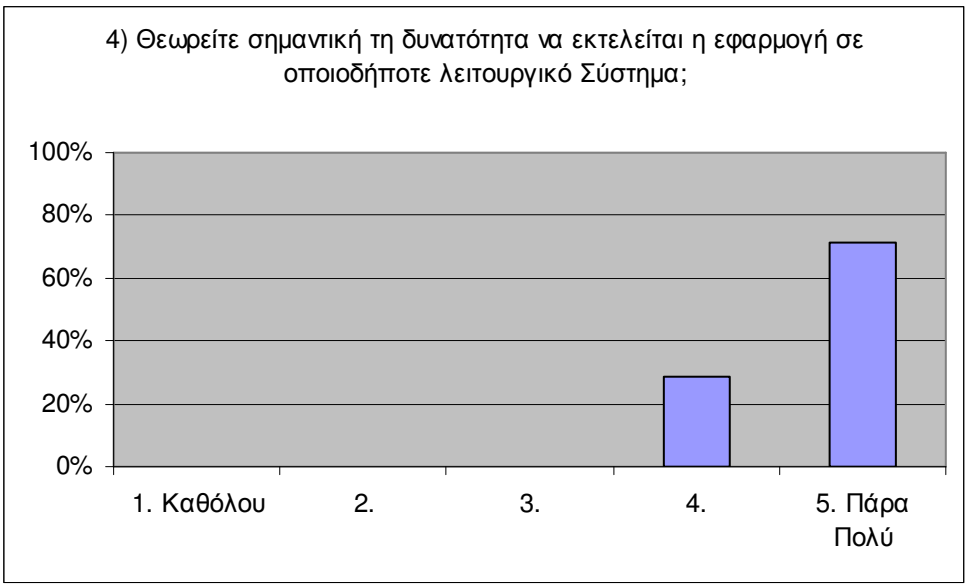
Κατηγορία Ερώτησης: Αξιολόγηση σχεδίασης

Ερώτηση: Αντιμετωπίσατε προβλήματα κατά την εκτέλεση του Λογισμικού;

Σκοπός της Ερώτησης: Να διερευνηθούν οι δυσκολίες που αντιμετώπισαν οι σπουδαστές κατά την εκτέλεση της εφαρμογής.

Συμπεράσματα: Σε γενικές γραμμές δεν παρουσιάστηκαν προβλήματα.

Σχόλια: Η εφαρμογή απαιτεί το runtime της JAVA για να εκτελεστεί. Ένα πιθανό πρόβλημα είναι ο Η/Υ να μην το διαθέτει και να πρέπει να γίνει download από το site της Oracle. Λόγω του αντικειμένου ενασχόλησης των σπουδαστών δεν προβλέφτηκε κάποια διαδικασία αυτοματισμού της συγκεκριμένης λειτουργίας. Μια δεύτερη δυσλειτουργία που παρουσιάστηκε (σε μικρή έκταση) ήταν κάποια bugs που εντοπίστηκαν στην εφαρμογή, τα οποία όμως αντιμετωπίστηκαν και διορθώθηκαν άμεσα.



Εικόνα 7.4 Ερωτηματολόγιο – Ερώτηση 4η.

Αριθμός Ερώτησης: 4.

Κατηγορία Ερώτησης: Αξιολόγηση Υλικού και λογισμικού.

Ερώτηση: Θεωρείτε σημαντική τη δυνατότητα να εκτελείται η εφαρμογή σε οποιοδήποτε λειτουργικό σύστημα;

Σκοπός της Ερώτησης: Να διερευνηθεί αν η υποστήριξη πολλαπλών λειτουργικών συστημάτων από μια εφαρμογή, αποτελεί σημαντικό πλεονέκτημα κατά την γνώμη των ερωτηθέντων.

Συμπεράσματα: Σε συνδυασμό με την 1η ερώτηση, διαπιστώνουμε ότι παρότι το κύριο λειτουργικό σύστημα που έρχονται σε επαφή είναι τα windows, η δυνατότητα της υποστήριξης πολλαπλών λειτουργικών δίνει πρόσθετη αξία στην εφαρμογή.

Σχόλια: Δεν έχει διερευνηθεί σε βάθος το επίπεδο ανεξαρτησίας από το Λ.Σ. Οι επιλογές σε εργαλεία λογισμικού που χρησιμοποιήθηκαν ήταν με γνώμονα αυτή την δυνατότητα. Οι περισσότερες δοκιμές έγιναν σε περιβάλλον Windows. Δοκιμές έγιναν και σε Linux Kubuntu. Σε κάθε περίπτωση η εφαρμογή λειτουργούσε, απλά δεν εμφανιζόταν υλικό που απαιτούσε συγκεκριμένο εγκατεστημένο λογισμικό. Για παράδειγμα, για την παρουσίαση αρχείων βίντεο στο LINUX, πρέπει να είναι εγκατεστημένος ο VLC Player. Περισσότερες πληροφορίες αναφέρονται στο παράρτημα Α.

Εικόνα 7.5 Ερωτηματολόγιο – Ερώτηση 5η.

Αριθμός Ερώτησης: 5.

Κατηγορία Ερώτησης: Αξιολόγηση Υλικού και λογισμικού.

Ερώτηση: Με τι βαθμό θα αξιολογούσατε τη σημασία της φορητότητας (portability) της εφαρμογής ;

Σκοπός της Ερώτησης: Η διαδικασία εγκατάστασης μιας εφαρμογής (ειδικά από μη έμπειρους χρήστες) πολλές φορές αποτελεί τροχοπέδη στην επιτυχημένη χρήση της. Ειδικά σε περιβάλλοντα που υπάρχει περιορισμός δικαιωμάτων στον λογαριασμό του χρήστη, η δυνατότητα χρήσης λογισμικού που απαιτεί εγκατάσταση είναι αδύνατη. Η ερώτηση διερευνά την γνώμη των σπουδαστών σε αυτό το θέμα.

Συμπεράσματα: Είναι επιθυμητό η εφαρμογή να είναι portable.

Σχόλια: Η αξιοποίηση του λογισμικού σε κάθε Η/Υ, με η χωρίς δικαιώματα διαχειριστή, δίνει στην χρηστικότητα του λογισμικού πρόσθετη αξία. Έχοντας την εφαρμογή μέσα σε ένα usb stick μπορεί να χρησιμοποιηθεί άμεσα σε οποιονδήποτε Η/Υ. (οικία, εργασία, εκπαιδευτικό ίδρυμα, internet caffe).

Εικόνα 7.6 Ερωτηματολόγιο – Ερώτηση 6η.

Αριθμός Ερώτησης: 6.

Κατηγορία Ερώτησης: Αξιολόγηση σχεδίασης.

Ερώτηση: Επιτρέπετε στους εκπαιδευόμενους να πλοηγούνται ελεύθερα μέσα στο λογισμικό κάνοντας προσωπικές επιλογές;

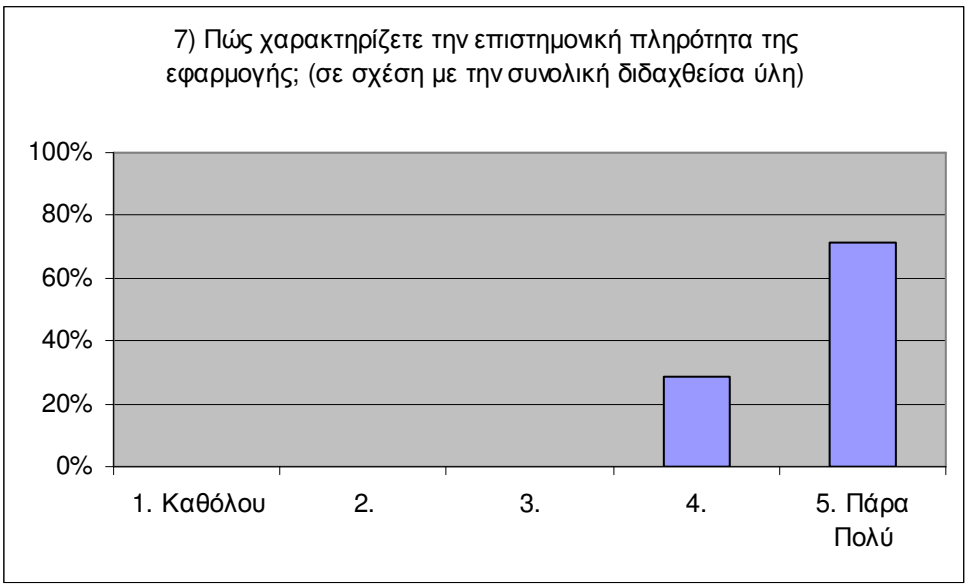
Σκοπός της Ερώτησης: Χαρακτηριστικό καλής σχεδίασης Εκπαιδευτικού Λογισμικού είναι να επιτρέπει μη γραμμική μετάδοση της πληροφορίας. Διερευνάτε εδώ σε ποιο βαθμό αυτό επιτυγχάνεται.

Συμπεράσματα: Η μη γραμμική μετάδοση της πληροφορίας ικανοποιείτε σε ικανοποιητικό βαθμό.

Σχόλια: Η οργάνωση του υλικού στην έκδοση του λογισμικού που αξιολογήθηκε από τους σπουδαστές, ήταν με την μορφή καρτελών (tabs) για την επιλογή των Θ.Ε., των μαθημάτων και του εκπαιδευτικού υλικού. Στην συνέχεια και μετά την επεξεργασία των στοιχείων των ερωτηματολογίων, προστέθηκαν δύο ακόμα μέθοδοι για την πρόσβαση στην πληροφορία.

1ος) Ο πίνακας περιεχομένων του εκπαιδευτικού υλικού που το οργανώνει σε μορφή δενδρικής δομής. Επιτυγχάνεται έτσι πιο γρήγορη μετάβαση.

2ος) Η λειτουργία αναζήτησης που εντοπίζει το εκπαιδευτικό υλικό με χρήση λέξεων κλειδιών.



Εικόνα 7.7 Ερωτηματολόγιο – Ερώτηση 7η.

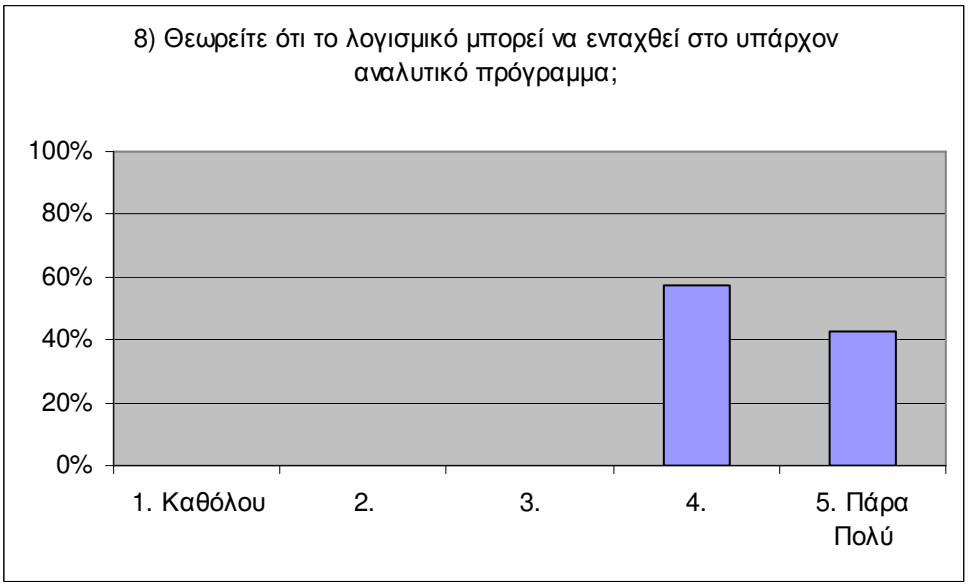
Αριθμός Ερώτησης: 7.

Κατηγορία Ερώτησης: Αξιολόγηση του Εκπαιδευτικού περιεχομένου.

Ερώτηση: Πώς χαρακτηρίζετε την επιστημονική πληρότητα της εφαρμογής (σε σχέση με την συνολική διδαχθείσα ύλη);

Συμπεράσματα: Κυμαίνεται σε υψηλό επίπεδο.

Σχόλια: Η εφαρμογή είναι ανοιχτή σε μεταβολές του περιεχομένου της. Με κατάλληλη αναπροσαρμογή του, μπορεί να επιτευχθούν καλύτερες επιδόσεις στον συγκεκριμένο τομέα.



Εικόνα 7.8 Ερωτηματολόγιο – Ερώτηση 8η.

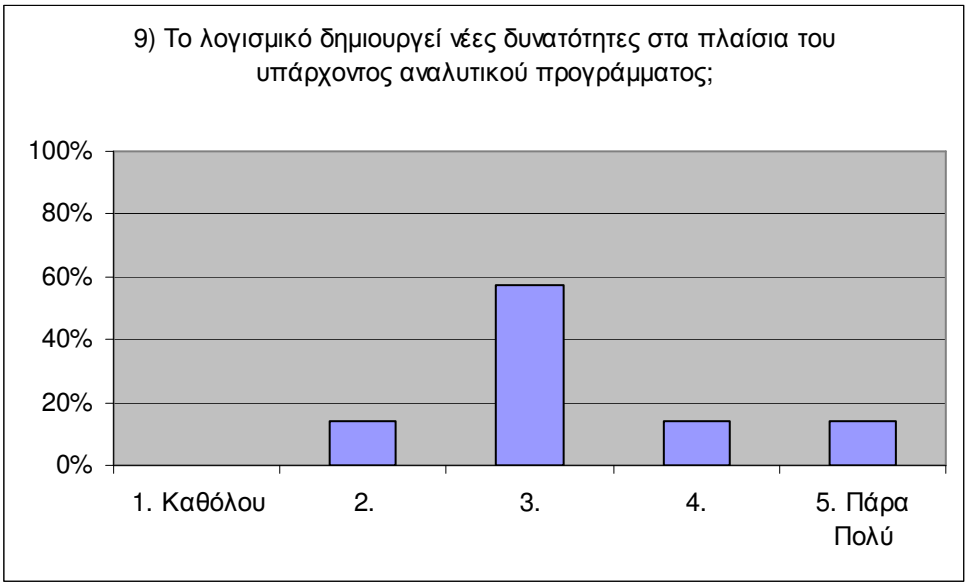
Αριθμός Ερώτησης: 8.

Κατηγορία Ερώτησης: Αξιολόγηση των Διδακτικών στόχων.

Ερώτηση: Θεωρείτε ότι το λογισμικό μπορεί να ενταχθεί στο υπάρχον αναλυτικό πρόγραμμα;

Συμπεράσματα: Οι απόψεις των ερωτηθέντων είναι θετικές.

Σχόλια: Η εφαρμογή είναι ανοιχτή σε μεταβολές του περιεχομένου της. Με κατάλληλη αναπροσαρμογή του, μπορεί να επιτευχθούν καλύτερες επιδόσεις στον συγκεκριμένο τομέα.



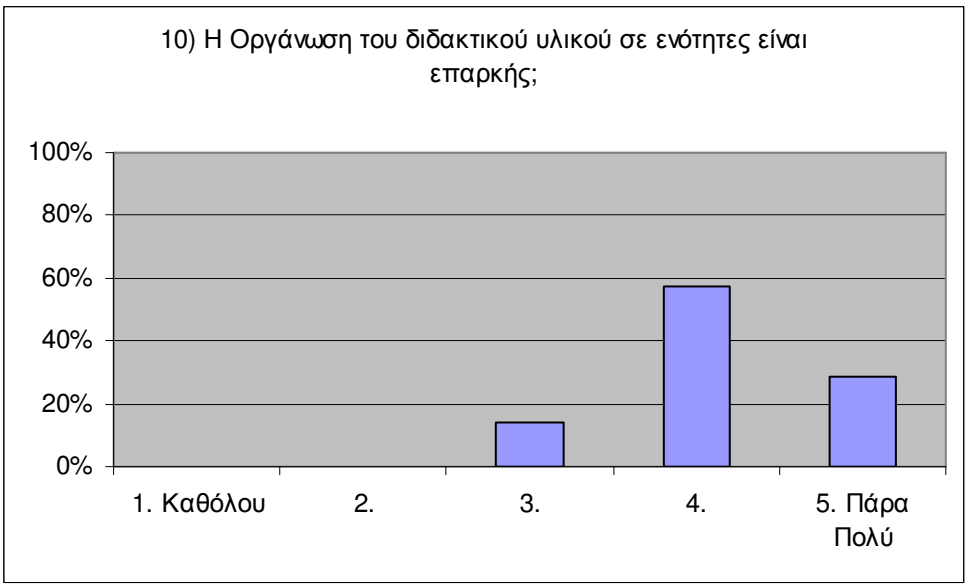
Εικόνα 7.9 Ερωτηματολόγιο – Ερώτηση 9η.

Αριθμός Ερώτησης: 9.

Κατηγορία Ερώτησης: Αξιολόγηση των Διδακτικών στόχων.

Ερώτηση: Το λογισμικό δημιουργεί νέες δυνατότητες στα πλαίσια του υπάρχοντος αναλυτικού προγράμματος;

Σκοπός της Ερώτησης: Η απόψεις κινούνται στο μέσο όρο της κλίμακας αξιολόγησης.



Εικόνα 7.10 Ερωτηματολόγιο – Ερώτηση 10η.

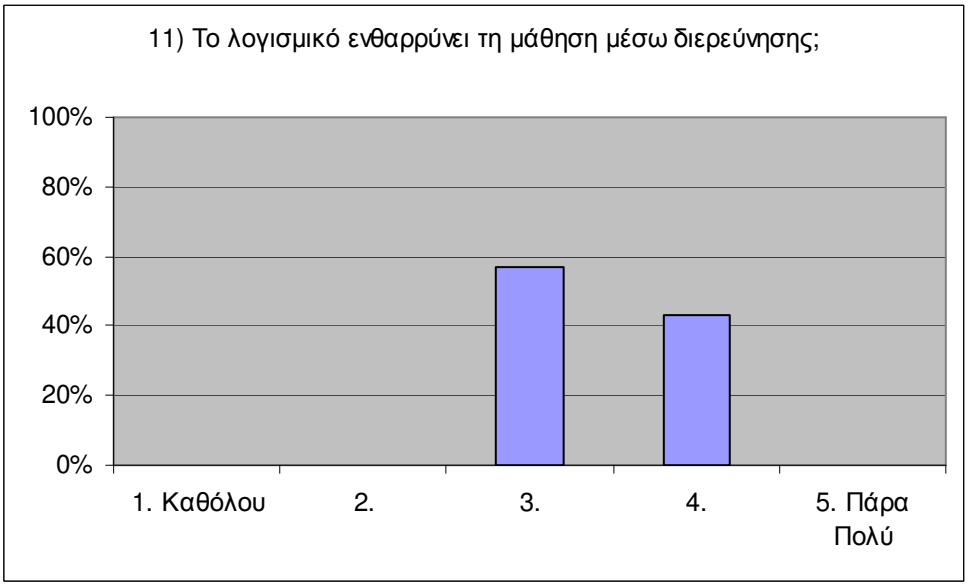
Αριθμός Ερώτησης: 10.

Κατηγορία Ερώτησης: Αξιολόγηση του Εκπαιδευτικού Περιεχομένου.

Ερώτηση: Η οργάνωση του διδακτικού υλικού σε ενότητες είναι επαρκής;

Συμπεράσματα: Είναι επαρκής σε ικανοποιητικό βαθμό.

Σχόλια: Η εφαρμογή είναι ανοιχτή σε μεταβολές του περιεχομένου της. Με κατάλληλη αναπροσαρμογή του, μπορεί να επιτευχθούν καλύτερες επιδόσεις στον συγκεκριμένο τομέα.



Εικόνα 7.11 Ερωτηματολόγιο – Ερώτηση 11η.

Αριθμός Ερώτησης: 11.

Κατηγορία Ερώτησης: Αξιολόγηση των Διδακτικών στόχων.

Ερώτηση: Το λογισμικό ενθαρρύνει τη μάθηση μέσω διερεύνησης;

Συμπεράσματα: Η επίδοση στον συγκεκριμένο τομέα κινείται σε ικανοποιητικό επίπεδο.

Σχόλια: Το υλικό που προσθέτει τέτοια χαρακτηριστικά στην εφαρμογή είναι τα Java Applets που εξομοιώνουν τους διάφορους αλγόριθμους κρυπτογράφησης.

Εικόνα 7.12 Ερωτηματολόγιο – Ερώτηση 12η.

Αριθμός Ερώτησης: 12.

Κατηγορία Ερώτησης: Αξιολόγηση του Εκπαιδευτικού Περιεχομένου.

Ερώτηση: Σε ποιο βαθμό το λογισμικό δίνει έμφαση σε κεντρικές έννοιες και αρχές του γνωστικού αντικειμένου;

Συμπεράσματα: Η επίδοση στον συγκεκριμένο τομέα κινείται σε ικανοποιητικό επίπεδο.

Σχόλια: Η εφαρμογή είναι ανοιχτή σε μεταβολές του περιεχομένου της. Με κατάλληλη αναπροσαρμογή του, μπορεί να επιτευχθούν καλύτερες επιδόσεις στον συγκεκριμένο τομέα.

Εικόνα 7.13 Ερωτηματολόγιο – Ερώτηση 13η.

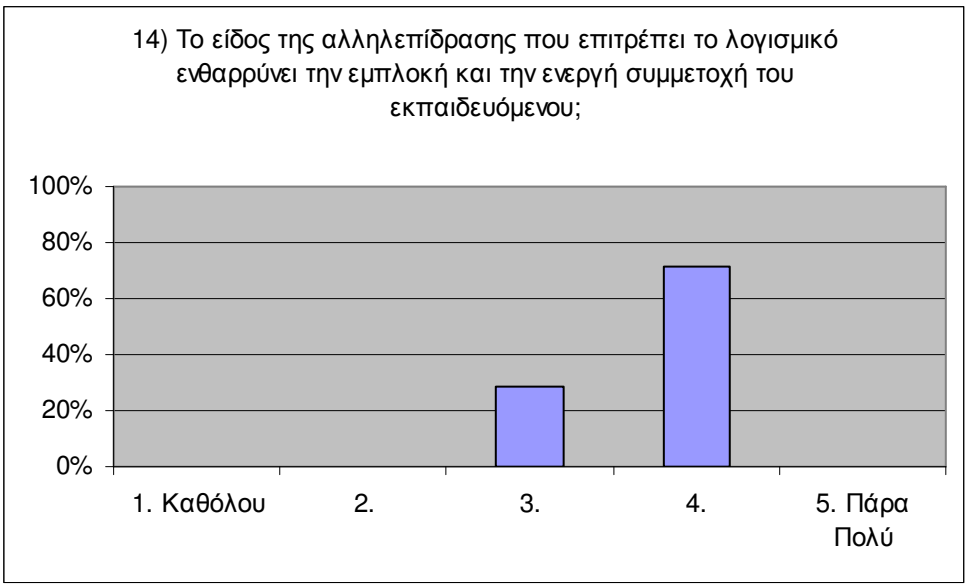
Αριθμός Ερώτησης: 13.

Κατηγορία Ερώτησης: Αξιολόγηση του Εκπαιδευτικού Περιεχομένου.

Ερώτηση: Το λογισμικό χρησιμοποιεί μεθόδους επίλυσης προβλημάτων για να βοηθήσει του εκπαιδευόμενους να οικοδομήσουν την κατανόηση τους στην Θεματική Ενότητα;

Συμπεράσματα: Η επίδοση στον συγκεκριμένο τομέα κινείται σε ικανοποιητικό επίπεδο.

Σχόλια: Η εφαρμογή είναι ανοιχτή σε μεταβολές του περιεχομένου της. Με κατάλληλη αναπροσαρμογή του, μπορεί να επιτευχθούν καλύτερες επιδόσεις στον συγκεκριμένο τομέα.



Εικόνα 7.14 Ερωτηματολόγιο – Ερώτηση 14η.

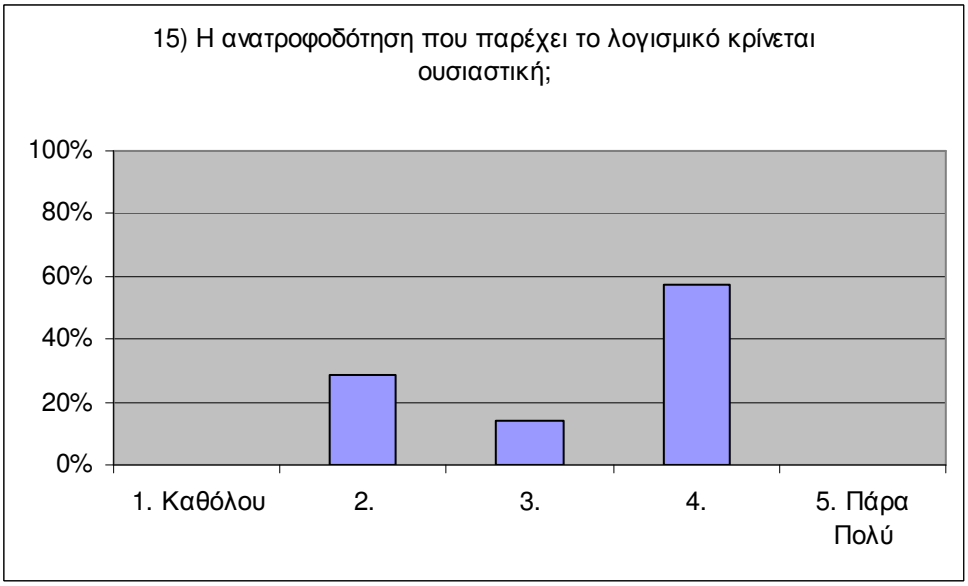
Αριθμός Ερώτησης: 14.

Κατηγορία Ερώτησης: Αξιολόγηση του Εκπαιδευτικού Περιεχομένου.

Ερώτηση: Το είδος της αλληλεπίδρασης που επιτρέπει το λογισμικό, ενθαρρύνει την εμπλοκή και την ενεργή συμμετοχή του εκπαιδευόμενου;

Συμπεράσματα: Η επίδοση στον συγκεκριμένο τομέα κινείται σε ικανοποιητικό επίπεδο.

Σχόλια: Η εφαρμογή είναι ανοιχτή σε μεταβολές του περιεχομένου της. Με κατάλληλη αναπροσαρμογή του, μπορεί να επιτευχθούν καλύτερες επιδόσεις στον συγκεκριμένο τομέα.



Εικόνα 7.15 Ερωτηματολόγιο – Ερώτηση 15η.

Αριθμός Ερώτησης: 15.

Κατηγορία Ερώτησης: Αξιολόγηση του Εκπαιδευτικού Περιεχομένου.

Ερώτηση: Η ανατροφοδότηση που παρέχει το λογισμικό κρίνεται ουσιαστική;

Συμπεράσματα: Η ανατροφοδότηση που παρουσιάζει η εφαρμογή δεν είναι σε ικανοποιητικό επίπεδο.

Σχόλια: Κατά την δοκιμαστική περίοδο της εφαρμογής δεν ήταν ενσωματωμένες δραστηριότητες με υψηλά χαρακτηριστικά διαδραστικότητας. Η ενσωμάτωση υλικού που δημιουργούμε με το Hot Potatoes μπορεί να βελτιώσει αισθητά την απόδοση σε αυτό το τομέα.

Εικόνα 7.16 Ερωτηματολόγιο – Ερώτηση 16η.

Αριθμός Ερώτησης: 16.

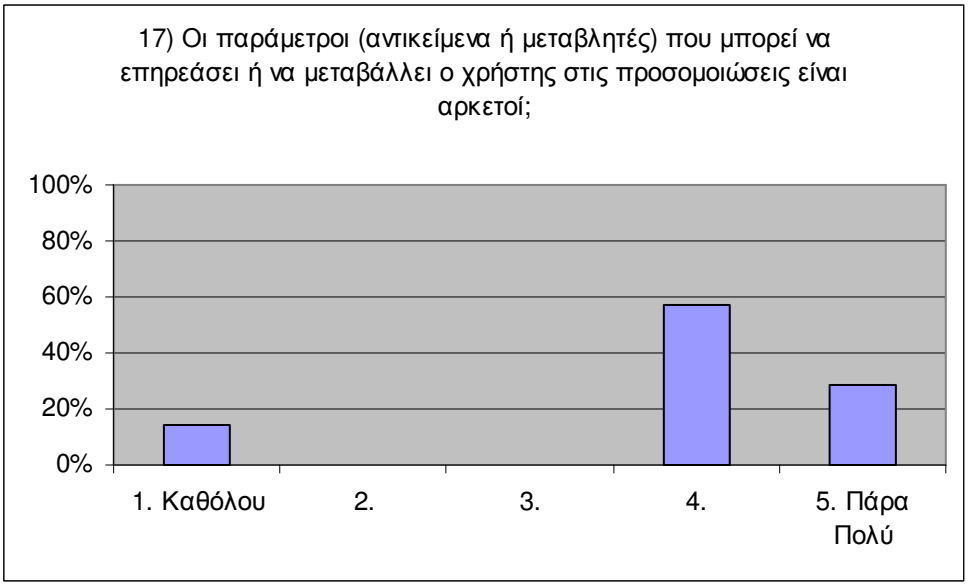
Κατηγορία Ερώτησης: Αξιολόγηση του Εκπαιδευτικού Περιεχομένου.

Ερώτηση: Σε τι βαθμό κρίνετε αναγκαία την εμφάνιση προσομοιώσεων των διαφόρων εννοιών (π.χ. αλγορίθμων) μέσω της εφαρμογής;

Σκοπός της Ερώτησης: Διερευνάμε αν για την καλύτερη εμπέδωση της ύλης απαιτείται λογισμικό προσομοίωσης.

Συμπεράσματα: Είναι απαραίτητη η χρήση λογισμικού προσομοίωσης.

Σχόλια: Τα Java Applets που εξομοιώνουν τους διάφορους αλγόριθμους κρυπτογράφησης αποτελούν σημαντικό κομμάτι του εκπαιδευτικού υλικού που ενσωματώνεται στο λογισμικό.



Εικόνα 7.17 Ερωτηματολόγιο – Ερώτηση 17η.

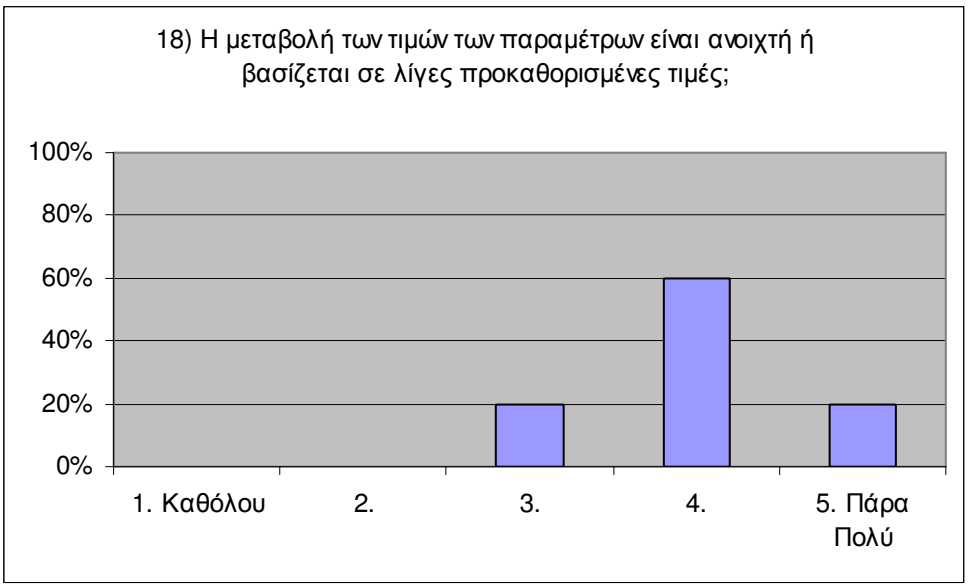
Αριθμός Ερώτησης: 17.

Κατηγορία Ερώτησης: Αξιολόγηση του Εκπαιδευτικού Περιεχομένου.

Ερώτηση: Οι παράμετροι (αντικείμενα ή μεταβλητές) που μπορεί να επηρεάσει ή να μεταβάλλει ο χρήστης στις προσομοιώσεις είναι αρκετοί;

Συμπεράσματα: Η επίδοση στον συγκεκριμένο τομέα κινείται σε υψηλό επίπεδο.

Σχόλια: Οι εξομοιώσεις δεν παρουσιάζουν απλά την διαδικασία, αλλά δίνεται και η δυνατότητα στον χρήστη να τις εκτελέσει με τις δικές του παραμέτρους.



Εικόνα 7.18 Ερωτηματολόγιο – Ερώτηση 18η.

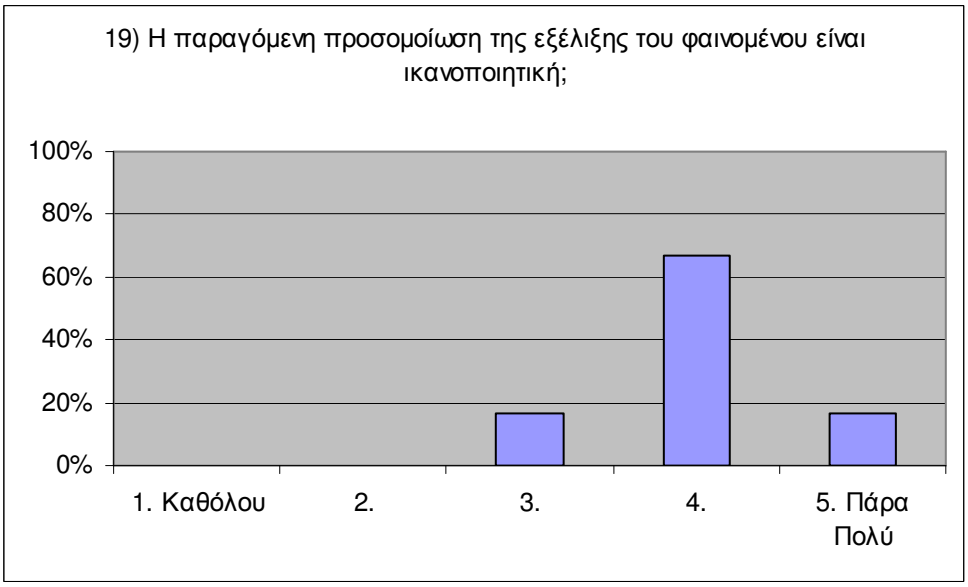
Αριθμός Ερώτησης: 18.

Κατηγορία Ερώτησης: Αξιολόγηση του Εκπαιδευτικού Περιεχομένου.

Ερώτηση: Η μεταβολή των τιμών των παραμέτρων είναι ανοιχτή ή βασίζεται σε λίγες προκαθορισμένες τιμές;

Συμπεράσματα: Η επίδοση στον συγκεκριμένο τομέα κινείται σε υψηλό επίπεδο.

Σχόλια: Οι εξομοιώσεις δεν παρουσιάζουν απλά την διαδικασία, αλλά δίνεται και η δυνατότητα στον χρήστη να τις εκτελέσει με τις δικές του παραμέτρους.



Εικόνα 7.19 Ερωτηματολόγιο – Ερώτηση 19η.

Αριθμός Ερώτησης: 19.

Κατηγορία Ερώτησης: Αξιολόγηση του Εκπαιδευτικού Περιεχομένου.

Ερώτηση: Η παραγόμενη προσομοίωση της εξέλιξης του φαινομένου είναι ικανοποιητική;

Σκοπός της Ερώτησης: Ανταποκρίνεται ικανοποιητικά για χρήση ως Λογισμικό Προσομοίωσης;

Συμπεράσματα: Η επίδοση στον συγκεκριμένο τομέα κινείται σε υψηλό επίπεδο.

Σχόλια: Δεν προσομοιώνεται απλά το φαινόμενο, αλλά καταγράφεται και η πλήρης εξέλιξη του.

Εικόνα 7.20 Ερωτηματολόγιο – Ερώτηση 20η.

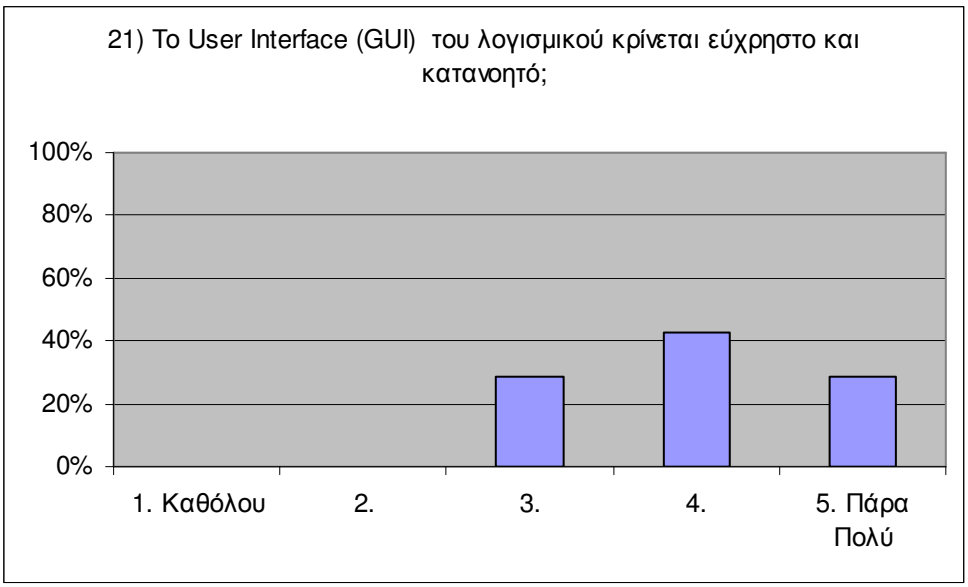
Αριθμός Ερώτησης: 20.

Κατηγορία Ερώτησης: Αξιολόγηση του Εκπαιδευτικού Περιεχομένου.

Ερώτηση: Η βασική ποιότητα του περιεχομένου είναι ικανοποιητική;

Συμπεράσματα: Η επίδοση στον συγκεκριμένο τομέα κινείτε σε υψηλό επίπεδο.

Σχόλια: Η εφαρμογή είναι ανοιχτή σε μεταβολές του περιεχομένου της. Με κατάλληλη αναπροσαρμογή του, μπορεί να επιτευχθούν καλύτερες επιδόσεις στον συγκεκριμένο τομέα.



Εικόνα 7.21 Ερωτηματολόγιο – Ερώτηση 21η.

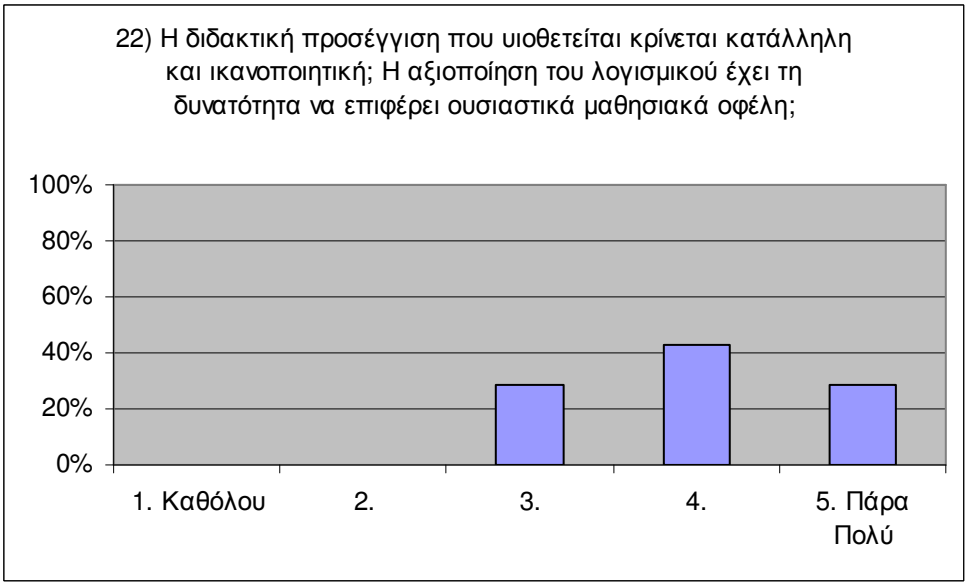
Αριθμός Ερώτησης: 21.

Κατηγορία Ερώτησης: Αξιολόγηση του Περιβάλλοντος της εφαρμογής.

Ερώτηση: Το User Interface (GUI) του λογισμικού κρίνεται εύχρηστο και κατανοητό;

Συμπεράσματα: Η επίδοση στον συγκεκριμένο τομέα κινείται σε υψηλό επίπεδο.

Σχόλια: Το interface χαρακτηρίζεται από απλότητα. Όλο το υλικό της εφαρμογής παρουσιάζεται με την μορφή καρτελών (tabs) δομημένο σε 3 επίπεδα. (Θ.Ε., Μαθήματα, Εκπ. Υλικό) Για κάθε επίπεδο χρησιμοποιείται και μια γραμμή με καρτέλες.



Εικόνα 7.22 Ερωτηματολόγιο – Ερώτηση 22η.

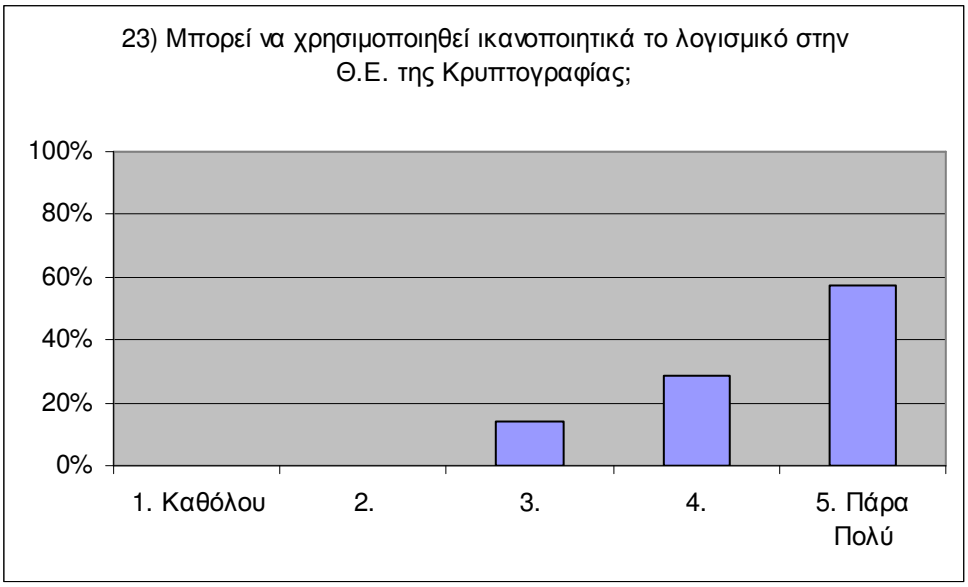
Αριθμός Ερώτησης: 22.

Κατηγορία Ερώτησης: Αξιολόγηση των Διδακτικών στόχων.

Ερώτηση: Η διδακτική προσέγγιση που υιοθετείται κρίνεται κατάλληλη και ικανοποιητική; Η αξιοποίηση του λογισμικού έχει την δυνατότητα να επιφέρει ουσιαστικά μαθησιακά οφέλη;

Συμπεράσματα: Η επίδοση στον συγκεκριμένο τομέα κινείται σε ικανοποιητικό επίπεδο.

Σχόλια: Η σημαντικότερη δυνατότητα που προσφέρει η εφαρμογή είναι η καταγραφή της διαδικασίας εξέλιξης των φαινομένων. Αυτή προσφέρει επιπρόσθετα μαθησιακά οφέλη στην διαδικασία της μάθησης.



Εικόνα 7.23 Ερωτηματολόγιο – Ερώτηση 23η.

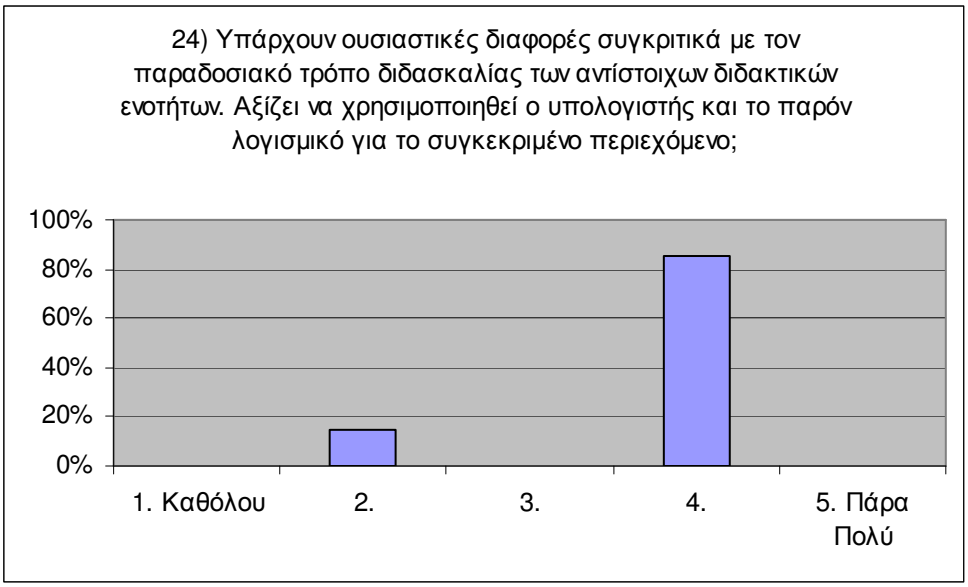
Αριθμός Ερώτησης: 23.

Κατηγορία Ερώτησης: Αξιολόγηση των Διδακτικών στόχων.

Ερώτηση: Μπορεί να χρησιμοποιηθεί ικανοποιητικά το λογισμικό στην Θ.Ε. της Κρυπτογραφίας;

Συμπεράσματα: Η επίδοση στον συγκεκριμένο τομέα κινείτε σε υψηλό επίπεδο.

Σχόλια: Η γενική άποψη για την χρησιμότητα της εφαρμογής στην θ.Ε. της Κρυπτογραφίας είναι θετική.



Εικόνα 7.24 Ερωτηματολόγιο – Ερώτηση 24η.

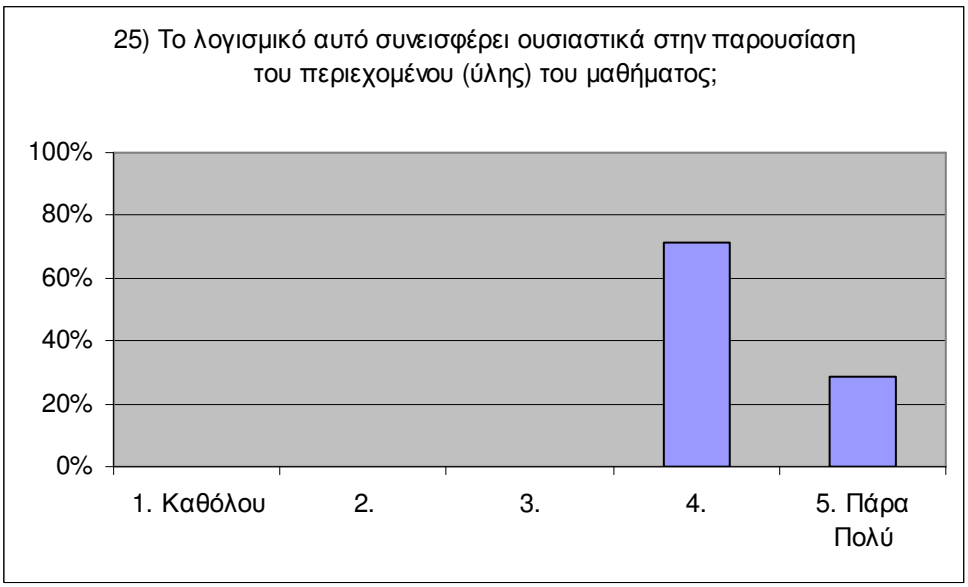
Αριθμός Ερώτησης: 24.

Κατηγορία Ερώτησης: Αξιολόγηση των Διδακτικών στόχων.

Ερώτηση: Υπάρχουν ουσιαστικές διαφορές συγκριτικά με τον παραδοσιακό τρόπο διδασκαλίας των αντίστοιχων διδακτικών ενοτήτων. Αξίζει να χρησιμοποιηθεί ο υπολογιστής και το παρόν λογισμικό για το συγκεκριμένο περιεχόμενο;

Συμπεράσματα: Η επίδοση στον συγκεκριμένο τομέα κινείται σε ικανοποιητικό επίπεδο.

Σχόλια: Η γενική άποψη για την χρησιμότητα της εφαρμογής είναι θετική.



Εικόνα 7.25 Ερωτηματολόγιο – Ερώτηση 25η.

Αριθμός Ερώτησης: 25.

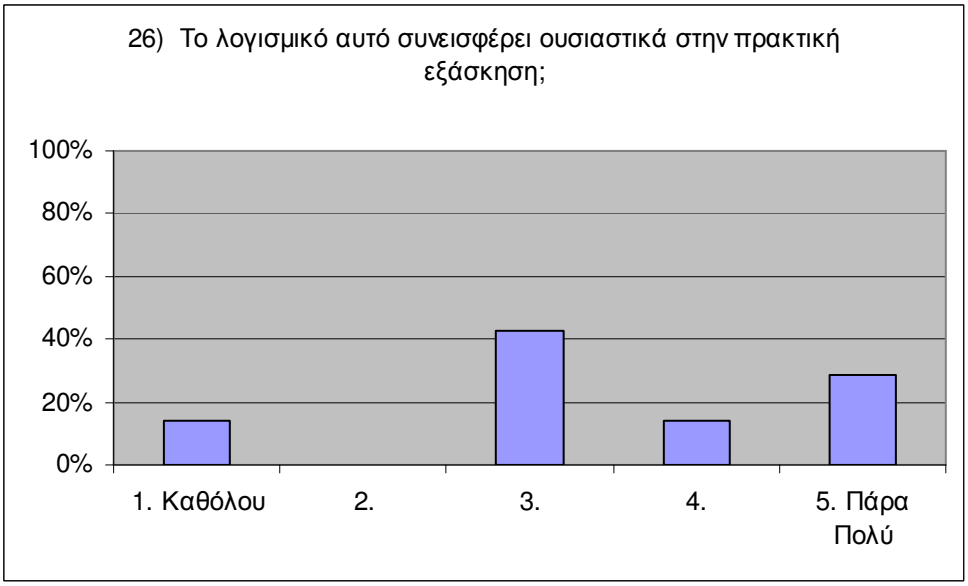
Κατηγορία Ερώτησης: Αξιολόγηση του Εκπαιδευτικού Περιεχομένου.

Ερώτηση: Το λογισμικό αυτό συνεισφέρει ουσιαστικά στην παρουσίαση του περιεχομένου (ύλης) του μαθήματος;

Σκοπός της Ερώτησης: Ανταποκρίνεται ικανοποιητικά για χρήση ως Λογισμικό Παρουσίασης;

Συμπεράσματα: Η επίδοση στον συγκεκριμένο τομέα κινείται σε υψηλό επίπεδο.

Σχόλια: Η εφαρμογή μπορεί να χρησιμοποιηθεί ικανοποιητικά σαν λογισμικό παρουσίασης.



Εικόνα 7.26 Ερωτηματολόγιο – Ερώτηση 26η.

Αριθμός Ερώτησης: 26.

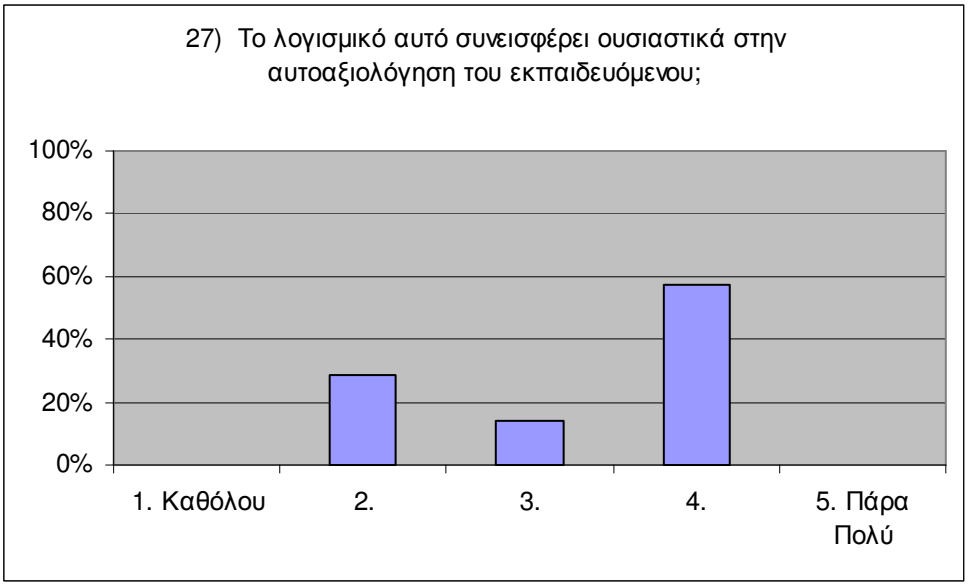
Κατηγορία Ερώτησης: Αξιολόγηση του Εκπαιδευτικού Περιεχομένου.

Ερώτηση: Το λογισμικό αυτό συνεισφέρει ουσιαστικά στην πρακτική εξάσκηση;

Σκοπός της Ερώτησης: Ανταποκρίνεται ικανοποιητικά για χρήση ως Λογισμικό Εξάσκησης και Εμπέδωσης;

Συμπεράσματα: Η επίδοση στον συγκεκριμένο τομέα κινείται σε ικανοποιητικό επίπεδο.

Σχόλια: Η εφαρμογή μπορεί να χρησιμοποιηθεί σαν λογισμικό εξάσκησης και εμπέδωσης.



Εικόνα 7.27 Ερωτηματολόγιο – Ερώτηση 27η.

Αριθμός Ερώτησης: 27.

Κατηγορία Ερώτησης: Αξιολόγηση του Εκπαιδευτικού Περιεχομένου.

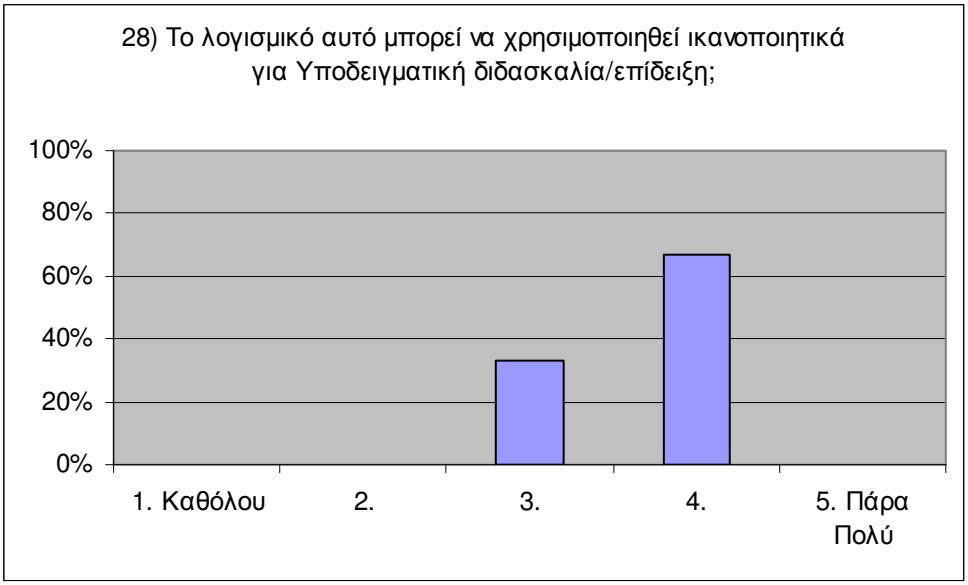
Ερώτηση: Το λογισμικό αυτό συνεισφέρει ουσιαστικά στην αυτοαξιολόγηση του εκπαιδευόμενου;

Σκοπός της Ερώτησης: Υποστηρίζει ικανοποιητικά ιδιαιτερότητες τις εξ αποστάσεως εκπαίδευσης;

Συμπεράσματα: Η επίδοση στον συγκεκριμένο τομέα κινείτε σε μέτριο επίπεδο.

Σχόλια: Κατά την δοκιμαστική περίοδο της εφαρμογής δεν ήταν ενσωματωμένες δραστηριότητες με δυνατότητες αυτό αξιολόγησης.

Η ενσωμάτωση υλικού που δημιουργούμε με το Hot Potatoes μπορεί να βελτιώσει αισθητά την απόδοση σε αυτό το τομέα.



Εικόνα 7.28 Ερωτηματολόγιο – Ερώτηση 28η.

Αριθμός Ερώτησης: 28.

Κατηγορία Ερώτησης: Αξιολόγηση του Εκπαιδευτικού Περιεχομένου.

Ερώτηση: Το λογισμικό αυτό μπορεί να χρησιμοποιηθεί ικανοποιητικά για υποδειγματική διδασκαλία / επίδειξη;

Συμπεράσματα: Η επίδοση στον συγκεκριμένο τομέα κινείται σε ικανοποιητικό επίπεδο.

Σχόλια: Η εφαρμογή είναι ανοιχτή σε μεταβολές του περιεχομένου της. Με κατάλληλη αναπροσαρμογή του, μπορεί να επιτευχθούν καλύτερες επιδόσεις στον συγκεκριμένο τομέα.

Εικόνα 7.29 Ερωτηματολόγιο – Ερώτηση 29η.

Αριθμός Ερώτησης: 29.

Κατηγορία Ερώτησης: Αξιολόγηση του Εκπαιδευτικού Περιεχομένου.

Ερώτηση: Το λογισμικό αυτό μπορεί να χρησιμοποιηθεί ικανοποιητικά για διερεύνηση προσομοιώσεων φαινομένων;

Σκοπός της Ερώτησης: Ανταποκρίνεται ικανοποιητικά για χρήση ως Λογισμικό Προσομοίωσης;

Συμπεράσματα: Η επίδοση στον συγκεκριμένο τομέα κινείτε σε ικανοποιητικό επίπεδο.

Σχόλια: Τα Java Applets που παρουσιάζουν τους διάφορους κρυπτογραφικούς αλγορίθμους είναι ο κύριος λόγος της θετικής αξιολόγησης.

Εικόνα 7.30 Ερωτηματολόγιο – Ερώτηση 30η.

Αριθμός Ερώτησης: 30.

Κατηγορία Ερώτησης: Αξιολόγηση του Εκπαιδευτικού Περιεχομένου.

Ερώτηση: Το λογισμικό αυτό μπορεί να χρησιμοποιηθεί ικανοποιητικά για εμβάθυνση, εμπλουτισμό.

Σκοπός της Ερώτησης: Υποστηρίζει ικανοποιητικά ιδιαιτερότητες τις εξ αποστάσεως εκπαίδευσης.

Συμπεράσματα: Η επίδοση στον συγκεκριμένο τομέα κινείται σε ικανοποιητικό επίπεδο.

Σχόλια: Η εφαρμογή είναι ανοιχτή σε μεταβολές του περιεχομένου της. Με κατάλληλη αναπροσαρμογή του, μπορεί να επιτευχθούν καλύτερες επιδόσεις στον συγκεκριμένο τομέα.

Εικόνα 7.31 Ερωτηματολόγιο – Ερώτηση 31η.

Αριθμός Ερώτησης: 31.

Κατηγορία Ερώτησης: Αξιολόγηση του Εκπαιδευτικού Περιεχομένου.

Ερώτηση: Το λογισμικό αυτό μπορεί να χρησιμοποιηθεί ικανοποιητικά για αναζήτηση πληροφοριών;

Συμπεράσματα: Το λογισμικό δεν παρουσιάζει εξαιρετικές επιδόσεις σε αυτό τον τομέα.

Σχόλια: Μετά την διάγνωση της συγκεκριμένης αδυναμίας, προστέθηκε στην εφαρμογή η δυνατότητα αναζήτησης. Πλέον υπάρχει η δυνατότητα άμεσου εντοπισμού περιεχομένου.

Εικόνα 7.32 Ερωτηματολόγιο – Ερώτηση 32η.

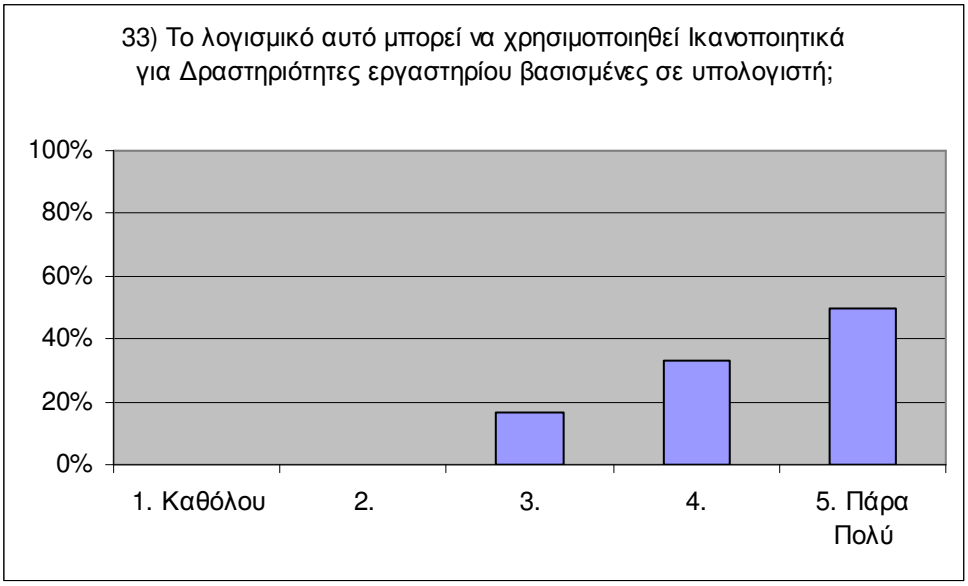
Αριθμός Ερώτησης: 32.

Κατηγορία Ερώτησης: Αξιολόγηση των Διδακτικών στόχων.

Ερώτηση: Το λογισμικό αυτό μπορεί να χρησιμοποιηθεί ικανοποιητικά για συνεργατικές εργασίες;

Συμπεράσματα: Χαμηλές επιδόσεις στον συγκεκριμένο τομέα.

Σχόλια: Το συγκεκριμένο λογισμικό είναι πρωτίστως προσανατολισμένο σε εξατομικευμένη μάθηση, καλύπτοντας τις απαιτήσεις της εξ' αποστάσεως εκπαίδευσης.



Εικόνα 7.33 Ερωτηματολόγιο – Ερώτηση 33η.

Αριθμός Ερώτησης: 33.

Κατηγορία Ερώτησης: Αξιολόγηση του Εκπαιδευτικού Περιεχομένου.

Ερώτηση: Το λογισμικό αυτό μπορεί να χρησιμοποιηθεί ικανοποιητικά για δραστηριότητες εργαστηρίου βασισμένες σε υπολογιστή;

Συμπεράσματα: Η επίδοση στον συγκεκριμένο τομέα κινείτε σε υψηλό επίπεδο.

Σχόλια: Η εφαρμογή είναι ανοιχτή σε μεταβολές του περιεχομένου της. Με κατάλληλη αναπροσαρμογή του, μπορεί να επιτευχθούν καλύτερες επιδόσεις στον συγκεκριμένο τομέα.

Εικόνα 7.34 Ερωτηματολόγιο – Ερώτηση 34η.

Αριθμός Ερώτησης: 34.

Κατηγορία Ερώτησης: Αξιολόγηση των Διδακτικών στόχων.

Ερώτηση: Το λογισμικό αυτό μπορεί να χρησιμοποιηθεί ικανοποιητικά για συμπλήρωση, βελτίωση πληροφοριών και δεδομένων;

Συμπεράσματα: Η επίδοση στον συγκεκριμένο τομέα κινείτε σε υψηλό επίπεδο.

Σχόλια: Η εφαρμογή είναι ανοιχτή σε μεταβολές του περιεχομένου της. Με κατάλληλη αναπροσαρμογή του μπορεί να επιτευχθούν καλύτερες επιδόσεις στον συγκεκριμένο τομέα.

Εικόνα 7.35 Ερωτηματολόγιο – Ερώτηση 35η.

Αριθμός Ερώτησης: 35.

Κατηγορία Ερώτησης: Αξιολόγηση του Εκπαιδευτικού Περιεχομένου.

Ερώτηση: Το λογισμικό αυτό μπορεί να χρησιμοποιηθεί ικανοποιητικά για επίλυση προβλημάτων;

Σκοπός της Ερώτησης: Ανταποκρίνεται ικανοποιητικά για χρήση ως Λογισμικό Επίλυσης Προβλήματος;

Συμπεράσματα: Η επίδοση στον συγκεκριμένο τομέα κινείτε σε υψηλό επίπεδο.

Σχόλια: Οι προσομοιώσεις των διάφορων κρυπτογραφικών αλγορίθμων και οι δυνατότητες παραμετροποίησης τους, προσφέρουν την δυνατότητα να επιλυθούν προβλήματα με σχετικό περιεχόμενο.

Εικόνα 7.36 Ερωτηματολόγιο – Ερώτηση 36η.

Αριθμός Ερώτησης: 36.

Κατηγορία Ερώτησης: Αξιολόγηση του Εκπαιδευτικού Περιεχομένου.

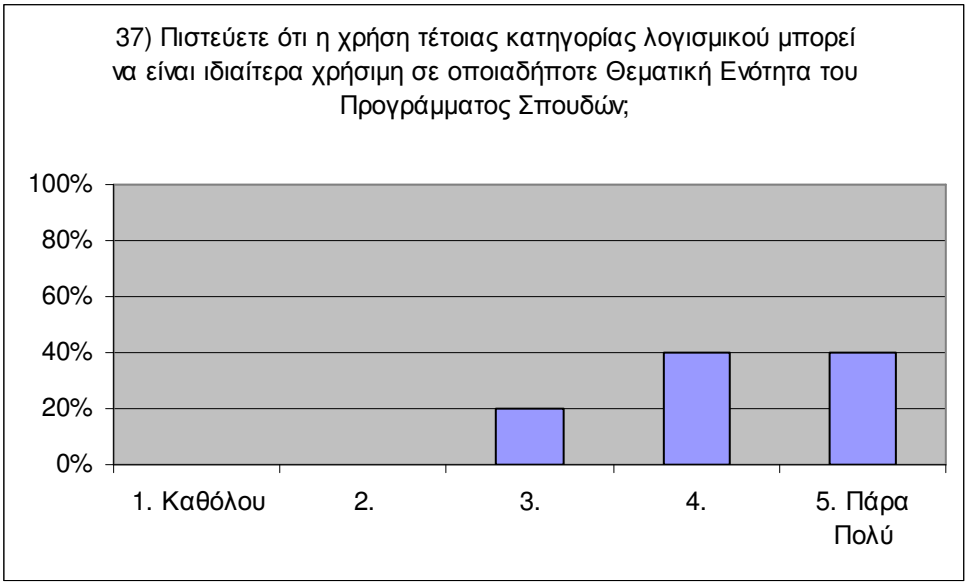
Ερώτηση: Το λογισμικό αυτό μπορεί να χρησιμοποιηθεί ικανοποιητικά για επανάληψη, υποστηρικτική διδασκαλία;

Σκοπός της Ερώτησης: Ανταποκρίνεται ικανοποιητικά για χρήση ως Λογισμικό Εξάσκησης και εμπέδωσης;

Συμπεράσματα: Η επίδοση στον συγκεκριμένο τομέα κινείται σε υψηλό επίπεδο.

Σχόλια: Η εφαρμογή χρησιμοποιήθηκε από τους σπουδαστές το διάστημα πριν τις εξετάσεις. Η θετική αξιολόγηση σημαίνει ότι τους βοήθησε

κατά την επανάληψη της ύλης και την προετοιμασία τους για τις εξετάσεις.



Εικόνα 7.37 Ερωτηματολόγιο – Ερώτηση 37η.

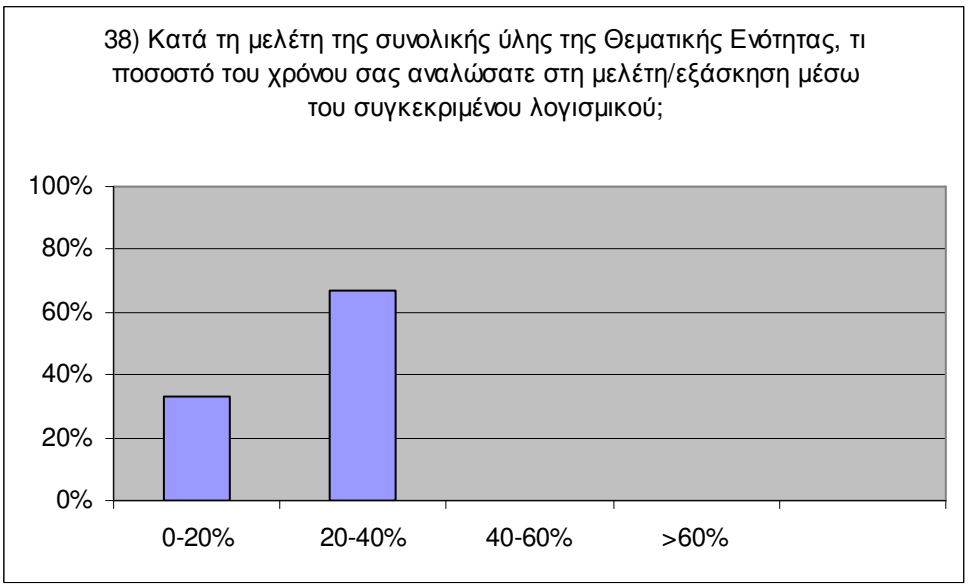
Αριθμός Ερώτησης: 37.

Κατηγορία Ερώτησης: Αξιολόγηση των Διδακτικών στόχων.

Ερώτηση: Πιστεύετε ότι η χρήση τέτοιας κατηγορίας λογισμικού μπορεί να είναι ιδιαίτερα χρήσιμη σε οποιαδήποτε Θεματική Ενότητα του προγράμματος σπουδών;

Συμπεράσματα: Η επίδοση στον συγκεκριμένο τομέα κινείται σε ικανοποιητικό επίπεδο.

Σχόλια: Η εφαρμογή είναι ανοιχτή σε μεταβολές του περιεχομένου της. Με κατάλληλη αναπροσαρμογή του, μπορεί να προσαρμοστεί στις απαιτήσεις οποιασδήποτε Θεματικής Ενότητας.



Εικόνα 7.38 Ερωτηματολόγιο – Ερώτηση 38η.

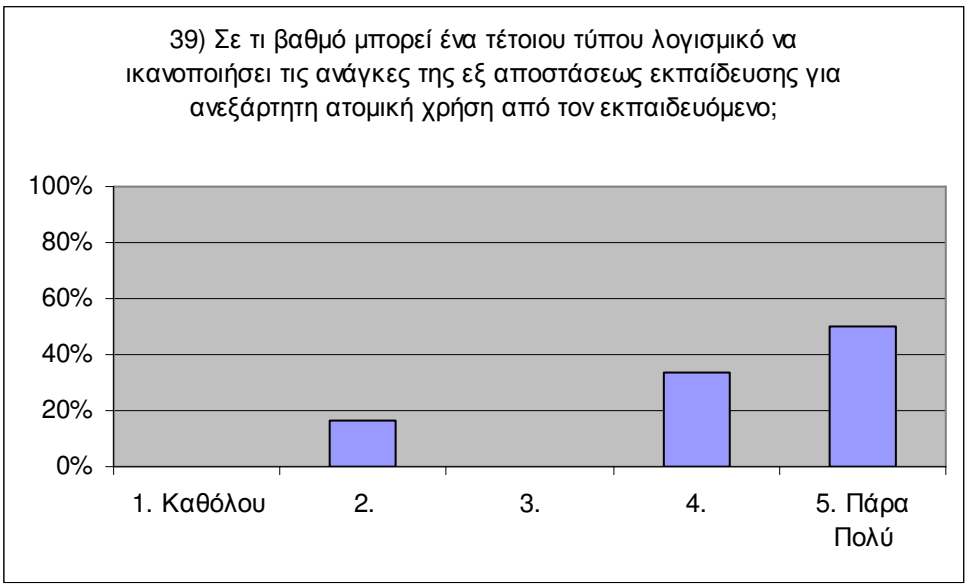
Αριθμός Ερώτησης: 38.

Κατηγορία Ερώτησης: Αξιολόγηση του Εκπαιδευτικού Περιεχομένου.

Ερώτηση: Κατά την μελέτη της συνολικής ύλης της Θεματικής Ενότητας, τι ποσοστό του χρόνου σας αναλώσατε στη μελέτη/εξάσκηση μέσω του συγκεκριμένου λογισμικού;

Συμπεράσματα: Η επίδοση στον συγκεκριμένο τομέα κινείται σε ικανοποιητικό επίπεδο.

Σχόλια: Με ένα Μέσο Όρο λίγο πάνω από 20% - και δεδομένου ότι τέθηκε στη διάθεση των φοιτητών τη χρονική περίοδο πριν τις εξετάσεις και όχι από την αρχή του ακαδημαϊκού εξαμήνου - διαπιστώνεται ότι συνέβαλε αποτελεσματικά στην διαδικασία μάθησης.



Εικόνα 7.39 Ερωτηματολόγιο – Ερώτηση 39η.

Αριθμός Ερώτησης: 39.

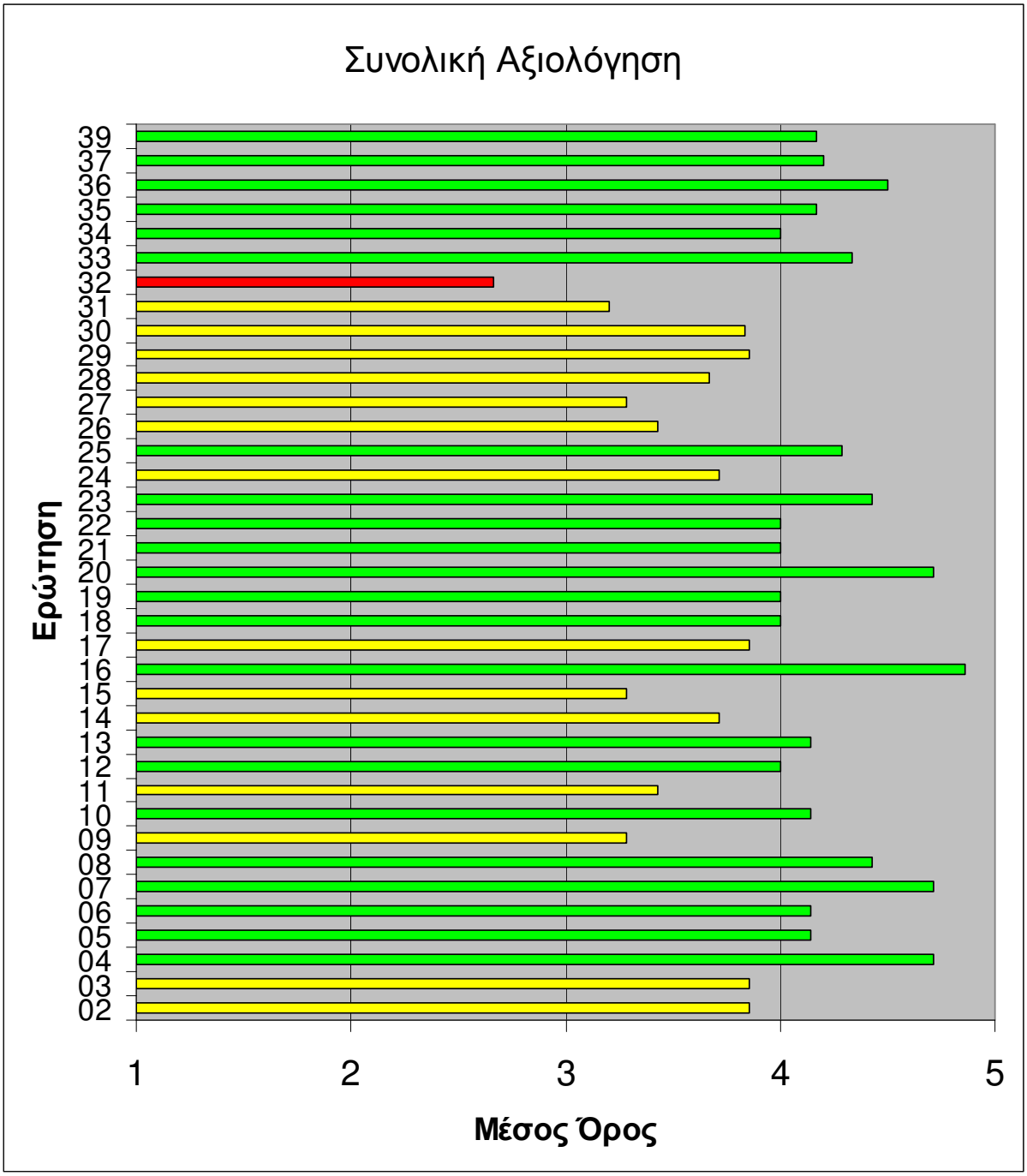
Κατηγορία Ερώτησης: Ιδιαιτερότητες της εξ' αποστάσεως εκπαίδευσης.

Ερώτηση: Σε τι βαθμό μπορεί ένα τέτοιου τύπου λογισμικό να ικανοποιήσει τις ανάγκες της εξ' αποστάσεως εκπαίδευσης για ανεξάρτητη ατομική χρήση από τον εκπαιδευόμενο;

Σκοπός της Ερώτησης: Ανταποκρίνεται στις ιδιαιτερότητες της εξ' αποστάσεως εκπαίδευσης;

Συμπεράσματα: Ανταποκρίνεται σε υψηλό βαθμό.

Σχόλια: Ο σχεδιασμός της εφαρμογής είναι για εξατομικευμένη εκπαίδευση (κύριο χαρακτηριστικό της εξ αποστάσεως εκπαίδευσης) και ο στόχος σύμφωνα με τους σπουδαστές επιτυγχάνεται.



Εικόνα 7.40 Μέσοι Όροι Αξιολόγησης ανά Ερώτηση.

Το γράφημα στην εικόνα 7.40 παρουσιάζει το μέσο όρο αξιολόγησης κάθε ερώτησης στην κλίμακα 1 έως 5. Προκύπτουν τρείς ζώνες ανάλογα με την επίδοση.

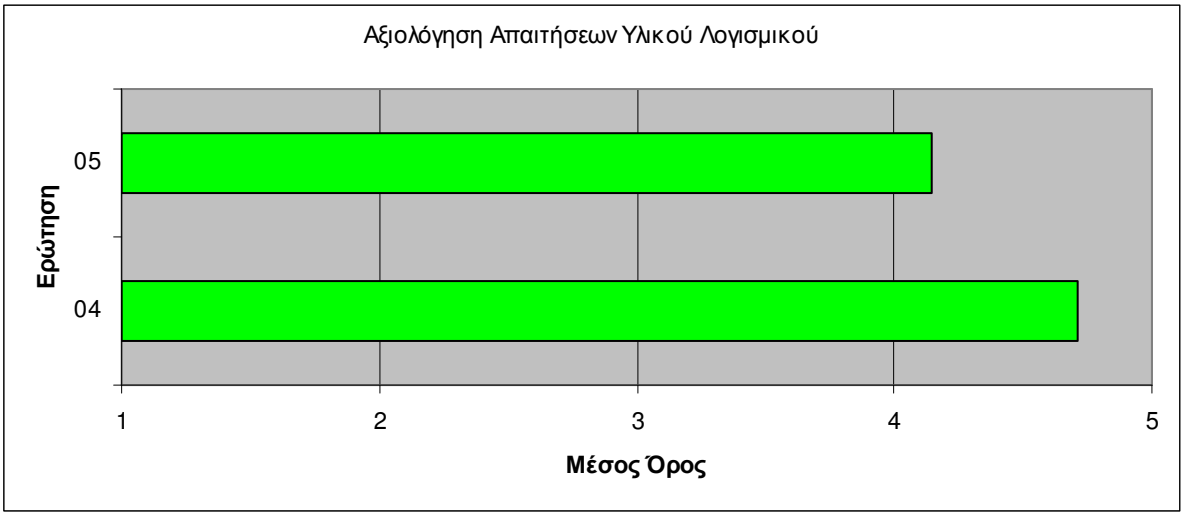
- Ερωτήσεις με Μ.Ο. αξιολόγησης από 4 έως 5 (πολύ έως πάρα πολύ). Σε αυτή την ζώνη έχουμε 22 ερωτήσεις (παρουσιάζονται στην εικόνα 7.40 με πράσινο χρώμα). Εδώ δεν απαιτείται καμία παρέμβαση στην εφαρμογή, στην σχεδίαση ή στο εκπαιδευτικό υλικό.
- Ερωτήσεις με Μ.Ο. αξιολόγησης από 3 έως 4 (μέτρια έως πολύ). Σε αυτή την ζώνη έχουμε 14 ερωτήσεις (παρουσιάζονται με κίτρινο χρώμα). Είναι τα σημεία που απαιτείτε

παρέμβαση ώστε να βελτιωθεί το εκπαιδευτικό λογισμικό. Σε αρκετές περιπτώσεις έγιναν βελτιώσεις όπως αναφέρθηκε πιο πριν στα σχόλια των ερωτήσεων.

- Ερωτήσεις με Μ.Ο. αξιολόγησης από 2 έως 3 (λίγο έως μέτρια). Σε αυτή την ζώνη έχουμε μόνο 1 ερώτηση, την ερώτηση 32 (παρουσιάζεται με κόκκινο χρώμα). Όπως αναφέρθηκε και στα σχόλια της συγκεκριμένης ερώτησης, οι συνεργατικές εργασίες δεν είναι πρωταρχικός διδακτικός στόχος για την εφαρμογή, που είναι προσανατολισμένη στην εξ' αποστάσεως εκπαίδευση.

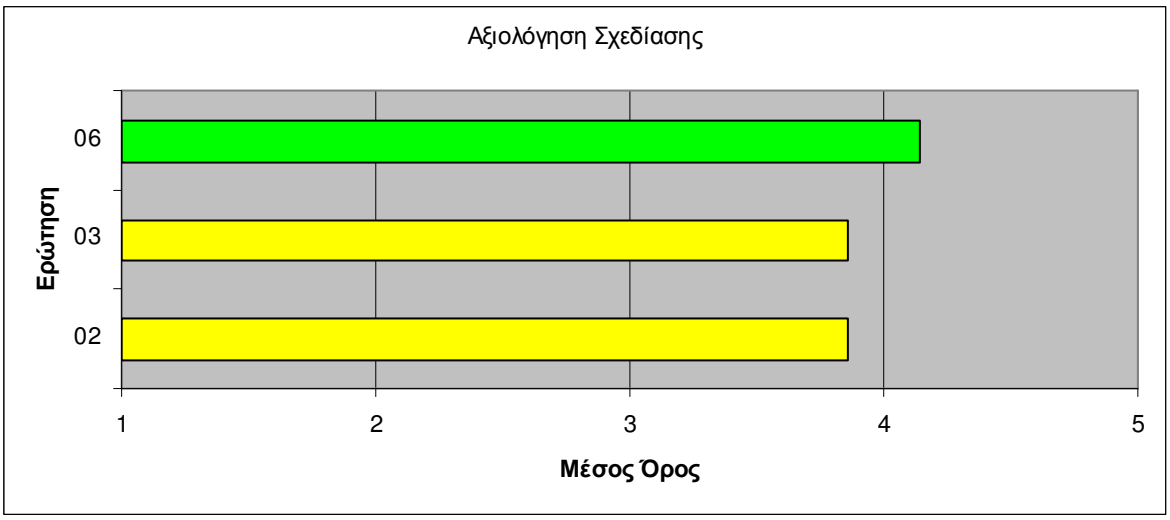
* Για την αξιολόγηση στις ερωτήσεις 2 & 3, η κλίμακα αντιστράφηκε αφού η καλύτερη αξιολόγηση είναι «καθόλου προβλήματα».

7.3.3 Αξιολόγηση ανά κατηγορία Ερωτήσεων



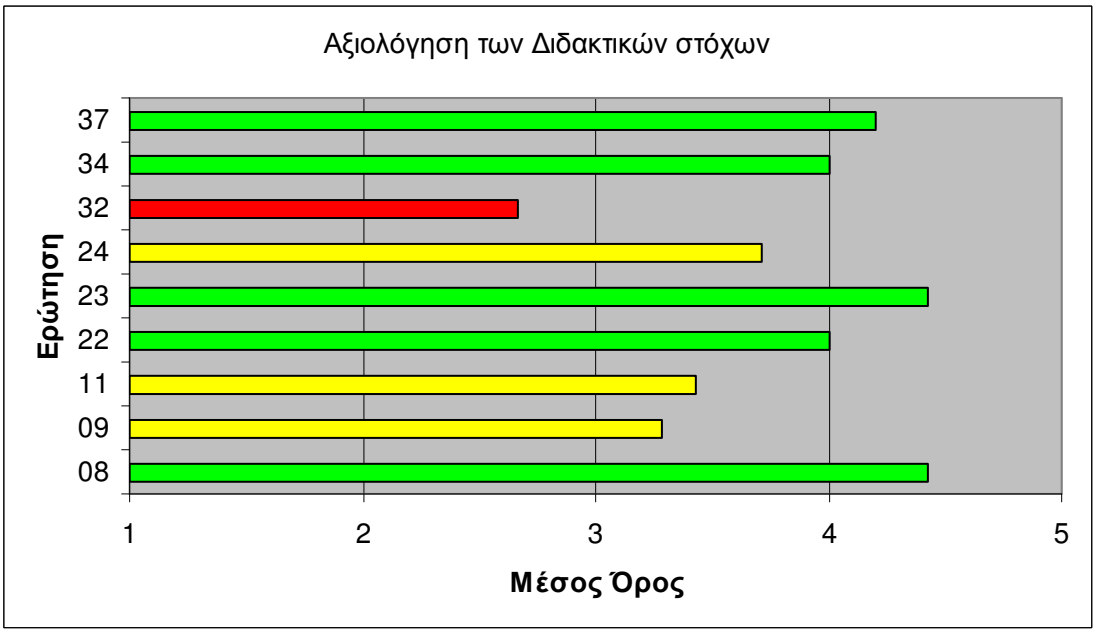
Εικόνα 7.41 Αξιολόγηση Απαιτήσεων Υλικού Λογισμικού.

Στην κατηγορία ερωτήσεων που αφορούν τις απαιτήσεις Υλικού Λογισμικού, έχουμε μέγιστες επιδόσεις, που μεταφράζεται σε επιτυχία στην κάλυψη των αντίστοιχων αρχικών σχεδιαστικών στόχων.



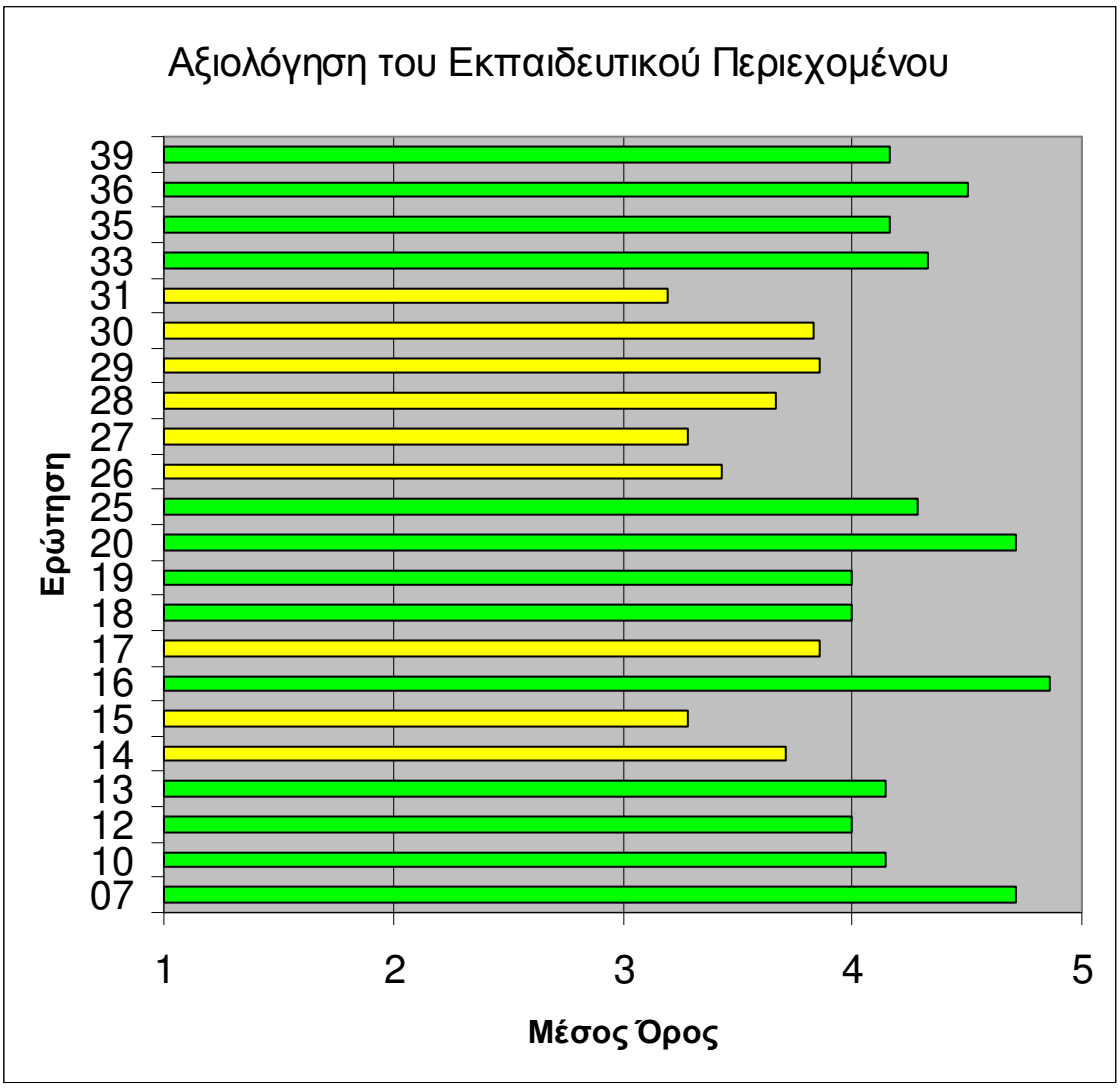
Εικόνα 7.42 Αξιολόγηση Σχεδίασης.

Στην κατηγορία ερωτήσεων που αφορούν την αξιολόγηση σχεδίασης, έχουμε επιδόσεις κοντά στο 4 (καλά) της κλίμακας.



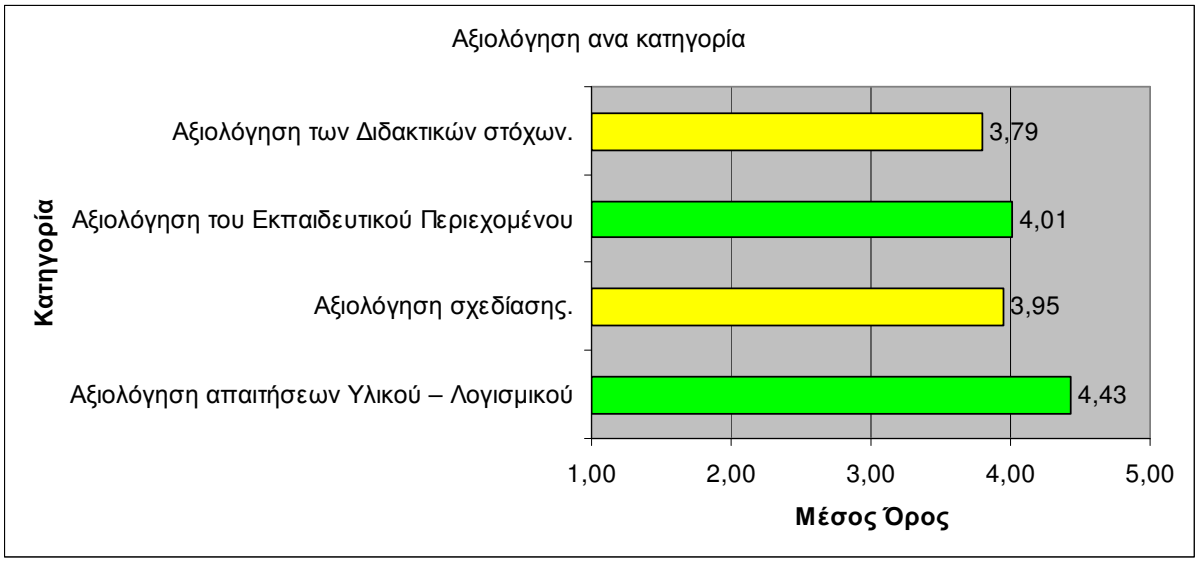
Εικόνα 7.43 Αξιολόγηση Διδακτικών Στόχων.

Στην κατηγορία ερωτήσεων που αφορούν την αξιολόγηση διδακτικών στόχων, έχουμε πέντε περιπτώσεις αξιολόγησης από καλά έως πολύ καλά (4 έως 5), τρείς περιπτώσεις μέτρια έως καλά (3 έως 4), και μία περίπτωση λίγο έως μέτρια (2 έως 3).



Εικόνα 7.44 Αξιολόγηση του Εκπαιδευτικού Περιεχομένου.

Στην κατηγορία ερωτήσεων που αφορούν την αξιολόγηση σχεδίασης, έχουμε δεκατρείς περιπτώσεις αξιολόγησης από καλά έως πολύ καλά (4 έως 5), εννέα περιπτώσεις μέτρια έως καλά (3 έως 4).



Εικόνα 7.45 Αξιολόγηση ανά Κατηγορία Ερωτήσεων.

Το διάγραμμα της εικόνας 7.45 παρουσιάζει τις επιδόσεις του λογισμικού ανά κατηγορία ερωτήσεων. Διαπιστώνουμε ότι η καλύτερη επίδοση είναι στην αξιολόγηση απαιτήσεων Υλικού Λογισμικού. Ακολουθεί το εκπαιδευτικό περιεχόμενο, η σχεδίαση και τέλος οι διδακτικοί στόχοι.

Κεφάλαιο 8
Επίλογος

Με την παρούσα μεταπτυχιακή διατριβή ολοκληρώνεται ο κύκλος των σπουδών μου στο μεταπτυχιακό πρόγραμμα εξειδίκευσης «Πληροφοριακά Συστήματα» του Ανοικτού Πανεπιστημίου Κύπρου. Το αντικείμενο της διατριβής μου έδωσε την ευκαιρία να ασχοληθώ με το λογισμικό στην εκπαιδευτική διαδικασία, κάτι που θα με βοηθήσει στην σταδιοδρομία μου ως εκπαιδευτικό. Από την συνολική διαδικασία και κυρίως την ανατροφοδότηση από τη χρήση του λογισμικού, αποκόμισα πρόσθετα οφέλη και έβγαλα χρήσιμα συμπεράσματα που θα συμβάλουν στην μελλοντική μου εξέλιξη.

Η παρούσα μεταπτυχιακή διατριβή αποτελεί για μέρα το έναυσμα για μια προσπάθεια με σκοπό την παροχή ποιοτικότερης εκπαίδευσης με την χρήση εκπαιδευτικού λογισμικού.

Βιβλιογραφία

[01] AES Security Report, ECRYPT D.STVL.2, ECRYPT Deliverable, 2006.

[02] AES, http://www.cs.bc.edu/~straubin/cs381-05/blockciphers/rijndael_ingles2004.swf

[03] T. Beth and F. C. Piper, The stop-and-go generator, Proceedings of Eurocrypt '84, pp. 88-92, 1985.

[04] E. Biham and A. Shamir, Differential cryptanalysis of DES-like cryptosystems, Crypto '90, Springer, pp. 2-27, 1991.

[05] E. Biham and A. Shamir, Differential cryptanalysis of the full 16-round DES, Crypto '92, Springer, pp. 487-496, 1993.

[06] M. Burmester, Σ. Γκρίτζαλης, Σ. Κάτσικας, Β. Χρυσικόπουλος, Παπασωτηρίου, "Σύγχρονη Κρυπτογραφία - Θεωρία και Εφαρμογές", 2011

[07] K. Cambell and M. J. Wiener, DES is not a group, Crypto '92, Springer, pp. 512-520, 1993.

[08] F. Chabaud and S. Vaudenay, Links between differential and linear cryptanalysis, Eurocrypt '94, Spinger, pp.356-365, 1995.

[09] D. Coppersmith - Krawczys - Mansour, The shrinking generator, Advances in Cryptology - Crypto '93, Springer, pp. 22-94, 1994.

[10] D. Coppersmith, The Data Encryption Standard and its strength against attacks, IBM Journal of Research and Development, 1994.

[11] N. Courtois and W. Meier, "Algebraic attacks on stream ciphers with linear feedback", Advances in Cryptology - Eurocrypt '03, Springer, pp. 345-359, 2003.

[12] J. Daemen and V. Rijmen,AES Submission Document on Rijndael,, Sept. 1999.

[13] H. Deitel, P. Deitel, "Java προγραμματισμός : Έκτη έκδοση", Αθήνα : Γκιούρδας Μ., 2005.

[14] DES, http://kathrynneugent.com/animation.htm

[15] DES, http://www.eap-pli.com/index.php/2012-07-12-17-58-35/25-2012-07-12-17-57-42/195-des

[16] W. Diffie and M. Hellman, New directions in cryptography, IEEE Trans. on Inf. Theory, vol. 22, pp. 644-654, 1976.

[17] C. Ding, G. Xiao and W. Shan, "The stability theory of stream ciphers", Lecture Notes in Computer Science, Springer, vol. 561, 1991.

[18] R. Gagne, "Conditions of Learning", http://www.instructionaldesign.org/theories/conditions-learning.html.

[19] R. Gagne, "Conditions of Learning", http://lrc.binus.ac.id/downloads/TE/Gagne.pdf.

[20] R. Gagne, "The Conditions of Learning: And Theory of Instruction (4th ed.)" New York: Holt, Rinehart & Winston, 1985.

[21] H. Gilbert, H. Handschuh, "Security analysis of SHA-256 and sisters", Crypto 2003, Springer

[22] S. Golomb, "Shift Register Synthesis", Holden-Day, San Francisco, 1969

[23] Greektuts, Java, http://www.greektuts.net/category/programming/java/

[24] Hot Potatoes, http://hotpot.uvic.ca/

[25] P. Keegan, L. Champenois, G. Crawlwy, C. Hunt, C. Webster, "NetBeans IDE, Field Guide", Prentice Hall, 2005.

[26] E. Key, An analysis of the structure and complexity of nonlinear binary key generators, IEEE Trans. Information Theory, vol. 22, pp.732-736, 1976.

[27] K. Kurosawa, T. Iwata and T. Yoshiwara, "New covering-radius of Reed-Muller codes for t-resilient functions", IEEE Trans. Information Theory, vol. 50, pp. 468- 475, 2000.

[28] R. Lidl and H. Niederreiter, "Finite Fields", vol. 20 of Encyclopedia of Mathematics and its Applications, Cambridge University Press, 1996.

[29] J. Massey, "Shift Register Sequences and BCH Decoding", IEEE Trans. on Information Theory, vol. IT-15, pp. 122-127, Jan. 1969 (ο αλγόριθμος Berlekamp-Massey)

[30] M. Matsui, Linear cryptanalysis method for DES cipher, Eurocrypt '93, Springer, pp. 386-397, 1994.

[31] W. Meier and O. Staffelbach, "Fast correlation attacks on stream ciphers", Advances in Cryptology - Eurocrypt '88, Springer, pp. 301-314, 1989.

[32] W. Meier, E. Pasalic and C. Carlet, "Algebraic attacks and decomposition of Boolean functions", Advances in Cryptology - Eurocrypt '04, Springer, pp. 474-491, 2004.

[33] A. Menezes, P. Van Oorschot και S. Vanstone, "Handbook of Applied Cryptography", CRC Press, 1996.

[34] R. Merkle, "One-way hash functions and DES", Crypto '89, Springer

[35] NetBeans, http://netbeans.org/features/index.html

[36] K. Paterson and A. K. L. Yau, Cryptography and theory in practice: The case of encryption in IPSec, Eurocrypt 2006, Springer, pp. 12-29, 2006.

[37] W. Paterson, J. Strickland, Garbage In / Garbage Out: Evaluating Computer Software, The English Record, 2nd quarter, σελ 11-15, 1986.

[38] D. Pointcheval, How to encrypt properly with RSA, RSA Laboratories CryptoBytes, Winter/Spring 2002

[39] R. Rivest, A, Shamir, L. Adleman, A method for obtaining digital signatures and public key cryptosystems, Communcations of the ACM, February 1978.

[40] RSA, Περιγραφή του προτύπου RSA σήμερα: ftp://ftp.rsasecurity.com/pub/pkcs/pkcs-1/pkcs-1v2-1.pdf

[41] R. Rueppel, "Analysis and design of stream ciphers", Series in Communication and Control Engineering. Springer, 1986.

[42] R. Rueppel, "Analysis and design of stream ciphers", Springer, 1986.

[43] B. Schneier, "Applied Cryptography: protocols, algorithms and source code in C (second edition)", Wiley, 1996.

[44] T. Siegenthaler, "Correlation immunity of nonlinear combining functions for cryptographic applications", IEEE Trans. Information Theory, vol. 30, pp. 776-780, 1984.

[45] T. Siegenthaler, "Cryptanalysts representation of nonlinearly filterered m-sequences", Advances in Cryptology - Eurocrypt '85, pp. 103-110, 1986.

[46] S. Smith and J. Marchesini, Addison-Wesley, "The Craft of System Security", 2007.

[47] SQLite, http://www.sqlite.org/about.html

[48] W. Stallings, "Cryptography and Network Security - Principles and Practice", Prentice Hall, 2006.

[49] W3schools,HTML Reference, http://www.w3schools.com/tags/

[50] X. Wang, Y. Yin, H. Yu, "Finding collisions in the full SHA-1", Crypto 2005, Springer

[51] A. Webster and S. E. Tavares, On the design of S-boxes, Crypto '85, Springer, pp. 156-170, 1986.

[52] M. Wiener, Cryptanalysis of short RSA exponents, IEEE Trans. on Inf. Theory, vol. 36, 1990.

[53] WikiPedia,Java, http://el.wikipedia.org/wiki/Java

[54] Γ. Αγγελής, Α. Βλάσση, Χ. Κουτσογιάννης, Σ. Κριλής, Μ. Λαγουδιανάκη, Γ. Μηλάκης, Δ. Μόσχος, Μ. Ξένος, Χ. Παπαγεωργίου, Α. Παπαδόπουλος, Π. Παυλάκης. "Μεθοδολογία Αξιολόγησης του Εκπαιδευτικού Λογισμικού και Προοπτικές Εφαρμογής στο

Εκπαιδευτικό Υλικό του ΕΑΠ", Technical Report HOU-CS-TR-2006-07-GR, Hellenic Open University, 2006.

[55] Θ. Γεωργίου, Ι. Κάππος, Α. Λαδιάς, Α. Μικρόπουλος, Α. Τζιμόγιαννης, Κ. Χαλκιά, "Πολυμέσα Δίκτυα" (βιβλίο Γ' Λυκείου) Αθήνα: Οργανισμός Εκδόσεων Διδακτικών Βιβλίων.

[56] Μ. Γρηγοριάδου Μαρία, Σχεδίαση Εκπαιδευτικού Λογισμικού, eclass.uoa.gr/modules/document/file.php/D58/Εκπαιδευτικό υλικό/Μάθημα 1ο/Σχεδίαση_Εκπαιδευτικού_Λογισμικού.htm, UOA.

[57] ΙΤΥ, "Εκπαιδευτικό Λογισμικό. Πρώτη γνωριμία με Διαθέσιμο Εκπαιδευτικό Λογισμικό" http://www.cti.gr/epimorfosi/files_for_downl/el/20pages.pdf, σελ. 3-20. Πάτρα 2002.

[58] ΙΤΥ, "Περί Εκπαιδευτικού Λογισμικού", http://ekfe-chalandr.att.sch.gr/Advisors/-georgiadou/Subjects/16_ekpaid_logismiko.pdf, Πάτρα 2003.

[59] Β. Κάτος, Γ. Στεφανίδης,, "Τεχνικές κρυπτογραφίας και κρυπτανάλυσης", Ζυγός, 2003.

[60] Ε. Κοτσιφάκος "Παιδαγωγική Αξιοποίηση των Τεχνολογιών της Πληροφορίας και Επικοινωνιών", http://repository.edulll.gr/edulll/retrieve/4739/1341.pdf, σελ. 22-26, Αθήνα, 2008

[61] Τ. Μικρόπουλος, Εκπαιδευτικό Λογισμικό Πολυμέσων / Υπερμέσων, http://www.etpe.gr/files/proceedings/uploads/e6.pdf, σελ. 1.

[62] Τ. Μικρόπουλος, Εκπαιδευτικό Λογισμικό. Θέματα σχεδίασης και αξιολόγησης λογισμικού υπερμέσων", Αθήνα: Κλειδάριθμος, 2000.

[63] ΤΕΙ Σερρών, "Βάσεις Δεδομένων ΙΙ", http://anamorfosi.teiser.gr/ekp_yliko/e-notes/Data/database/main.htm

Παράρτημα Α
Λογισμικό Τρίτων

Η εφαρμογή υποστηρίζει ενσωμάτωση και παρουσίαση των ακόλουθων μορφών εκπαιδευτικού υλικού:

1. Μορφή Απλού Κειμένου.
2. Μορφή HTML
3. Μορφή Συνδέσμου HTML
4. Μορφή Συνδέσμου PDF.
5. Μορφή HTML4.
6. Μορφή Συνδέσμου HTML4
7. Flash Animation.
8. Video File.
9. Java Class.

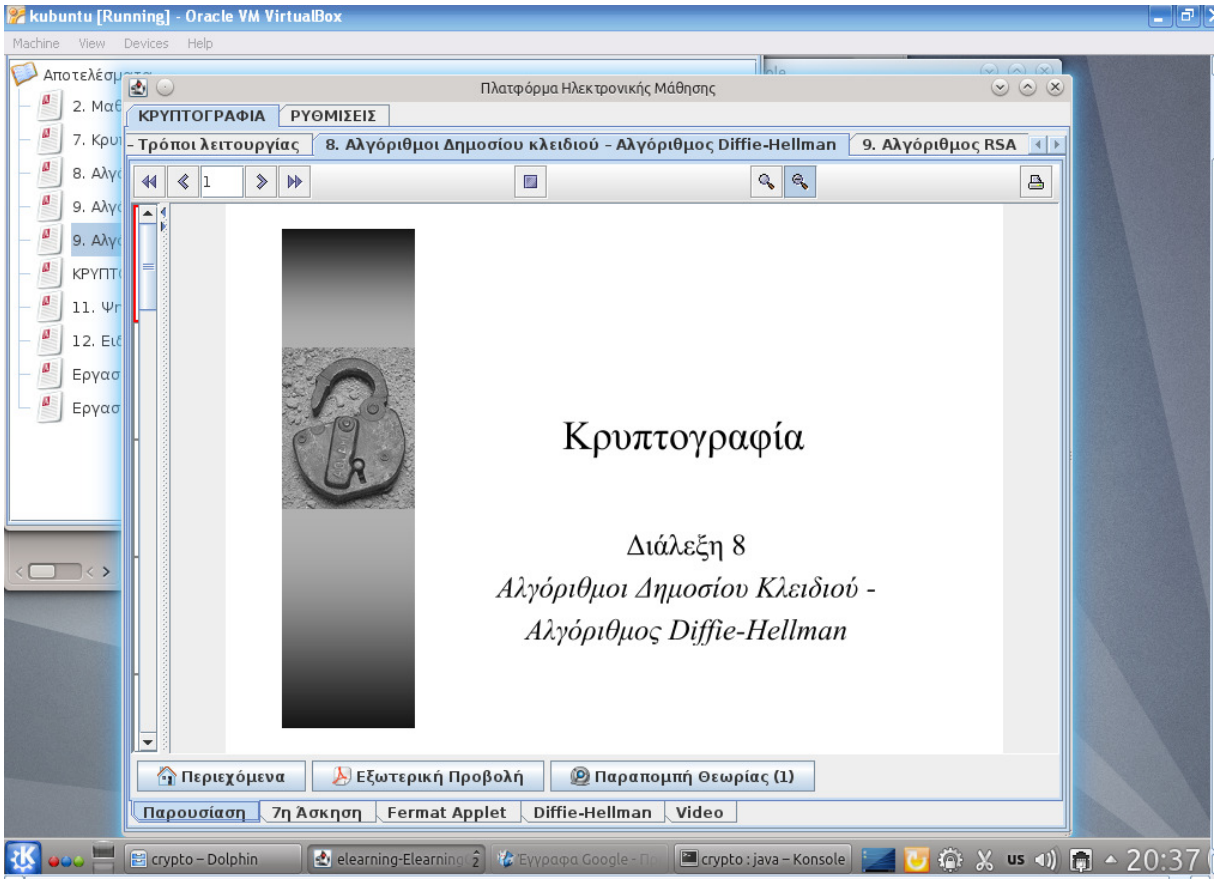
Από αυτές, οι μορφές 1,2,3,9 υποστηρίζονται άμεσα από τις βιβλιοθήκες των αντικειμένων της JAVA. Για τις υπόλοιπες δεν υπάρχει ενσωματωμένη υποστήριξη. Προκειμένου να αρθεί αυτός ο περιορισμός χρησιμοποιήθηκαν βιβλιοθήκες τρίτων κατασκευαστών που δίνουν την δυνατότητα να παρουσιάζεται τέτοιου τύπου υλικό μέσω των GUI αντικειμένων της JAVA. Η

άδεια χρήσης αυτών των βιβλιοθηκών, (LGPL-2.1) επιτρέπει την χρήση και την αναδιανομή τους εφόσον η διάθεση τους στον τελικό χρήστη γίνεται χωρίς χρέωση (περισσότερα στο Α3 του παρόντος).

Επίσης για κάποιους τύπους εκπαιδευτικού υλικού μπορεί να απαιτηθεί η εγκατάσταση συγκεκριμένου λογισμικού. Για παράδειγμα για την προβολή αρχείων PDF (μόνο για την εξωτερική προβολή, η ενσωματωμένη προβολή δεν έχει τέτοια απαίτηση) απαιτείτε η εγκατάσταση του Adobe Reader. Για την προβολή αρχείων HTML4 μπορεί να απαιτηθεί κάποιος συμβατός με την εφαρμογή browser. Ο FireFox συνεργάζεται σίγουρα με την εφαρμογή χωρίς να αποκλείεται η συμβατότητα και με άλλους Browsers. Για την προβολή των Flash Animation απαιτείτε να είναι εγκατεστημένος ο Flash Player. Τέλος για την παρουσίαση ήχου και βίντεο μπορεί να απαιτηθεί η εγκατάσταση του vlc media player (στα Windows χρησιμοποιείτε ο ενσωματωμένος Media Player). Όλα αυτά τα λογισμικά διατίθενται για όλες τις δημοφιλείς πλατφόρμες (windows, Linux, Mac OS).

Ειδικά για περιβάλλον Linux Ubuntu (εικόνα Α.1) που δοκιμάστηκε η εφαρμογή εκτός από τα Windows, παραθέτουμε της ακόλουθες εντολές εγκατάστασης ανά τύπο εκπαιδευτικού υλικού.

Υποστήριξη Υλικού	Εντολή τερματικού για την εγκατάσταση απαραίτητου Λογισμικού
HTML4	Sudo apt-get install libwebkitgtk-1.0-0 Sudo apt-get install firefox
Ήχου – Βίντεο	Sudo apt-get install vlc Mozilla-plugin-vlc
Αρχεία Flash	Sudo apt-get install flashplugin-installer



Εικόνα Α.1 Screenshot της οθόνης της εφαρμογής σε Kubuntu Linux.

Α.1 PDF Renderer

Η βιβλιοθήκη pdf-renderer υποστηρίζει την παρουσίαση υλικού μορφής PDF μέσω των GUI αντικειμένων της JAVA. Η συγκεκριμένη μορφή αρχείου είναι η πλέον διαδεδομένη μορφή ψηφιακών εγγράφων στο Internet. Την βιβλιοθήκη και την σχετική τεκμηρίωση μπορούμε να την κατεβάσουμε από την ηλεκτρονική διεύθυνση http://java.net/projects/pdf-renderer. Η βιβλιοθήκη είναι γραμμένη σε καθαρή JAVA, που σημαίνει ότι παρουσιάζει ανεξαρτησία από υλικό και λογισμικό. Τα αρχεία PDF διαβάζονται μέσω της βιβλιοθήκης ακόμα και όταν δεν είναι εγκατεστημένο το Adobe Reader.

Α.2 The DJ Project

Η GUI βιβλιοθήκη της Java (Swing) υποστηρίζει την παρουσίαση υλικού σε HTML 3.2. Η συγκεκριμένη έκδοση της HTML δεν υποστηρίζει τεχνολογίες CCS και Java Scripts. "Οταν λοιπόν το υλικό που θέλουμε να ενσωματώσουμε απαιτεί την υποστήριξη αυτών των τεχνολογιών (πχ

σελίδες που δημιουργούμε με το Hot Potatoes) τότε επιβάλλεται η δημιουργία ή χρησιμοποίηση επιπρόσθετων βιβλιοθηκών. Στην εφαρμογή χρησιμοποιήθηκε Web Browser από βιβλιοθήκη τρίτου κατασκευαστή. Η ηλεκτρονική διεύθυνση που περιέχει την βιβλιοθήκη και την σχετική τεκμηρίωση είναι http://djproject.sourceforge.net/ns/. Η συγκεκριμένη βιβλιοθήκη παρέχει επίσης ένα flash player (για εκτέλεση εφαρμογών σε ADOBE FLASH), και Multimedia Player για αναπαραγωγή αρχείων ήχου και βίντεο.

A.3 The GNU Lesser General Public License, version 2.1 (LGPL-2.1)

Οι περισσότερες άδειες χρήσης λογισμικού είναι σχεδιασμένες να αφαιρούν την ελευθερία διανομής και τροποποίησης. Αντίθετα, οι Γενικές 'Αδειες Δημόσιας Χρήσης GNU έχουν σκοπό να εγγυηθούν την ελευθερία διανομής και τροποποίησης του ελεύθερου λογισμικού, να διασφαλίσουν, ότι το λογισμικό είναι ελεύθερο για όλους τους χρήστες του.

Το πλήρες κείμενο της άδειας μπορείτε να το βρείτε στην ηλεκτρονική διεύθυνση http://www.gnu.org/licenses/lgpl-2.1.html.

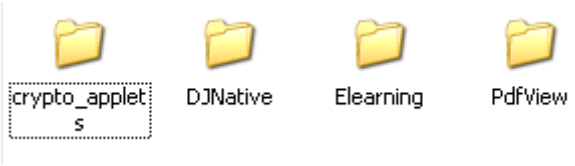
Παράρτημα Β
Τα περιεχόμενα του συνοδευτικού C.D.

Μαζί με το κείμενο της διατριβής παραδόθηκε και ένα CD με το συνοδευτικό υλικό.

Εικόνα Β.1 Τα στοιχεία του ριζικού καταλόγου του CD.

Στην εικόνα Β.1 βλέπουμε τα στοιχεία του ριζικού καταλόγου. Εδώ υπάρχει το κείμενο της διατριβής σε δύο μορφές. Σε μορφή αρχείου Microsoft Word 2003, και σε Kindle format. Επίσης υπάρχουν ο φάκελος Elearning και ο φάκελος Projects.

Β.1 Φάκελος \Projects.



Εικόνα Β.2 Τα στοιχεία του καταλόγου Projects.

Στον φάκελο αυτό υπάρχουν τα projects του Netbeans με τον πηγαίο κώδικα σε Java (εικόνα Β.2).

Β.2.1 Φάκελος \Projects\Crypto_applets.

Ο φάκελος Crypto_applets περιέχει όλες τις κλάσεις με τα applets του εκπαιδευτικού υλικού που εξομοιώνουν τους κρυπτογραφικούς αλγορίθμους. Δημιουργεί την βιβλιοθήκη Crypto_Applets.jar.

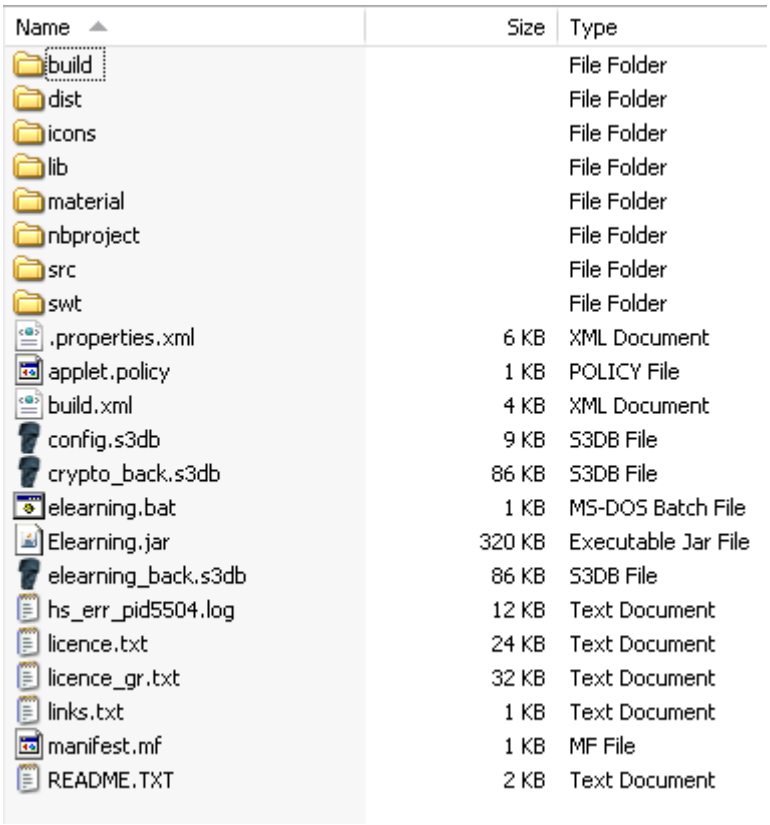
Β.2.2 Φάκελος \Projects\DJNative.

Ο φάκελος DJNative περιέχει το project με τις κλάσεις για την υποστήριξη υλικού HTML4, Flash, Video. Το συγκεκριμένο project εμπεριέχει βιβλιοθήκες με λογισμικό τρίτου κατασκευαστή (βλέπε παράρτημα Α). τα αρχεία που σχετίζονται με αυτό το project είναι DJNative.jar, DJNativeSwing.jar, DJNativeSwing-SWT.jar, Jna-3.2.4.jar, Jna-WindowUtils.jar.

Β.2.3 Φάκελος \Projects\PdfView.

Ο φάκελος PdfView περιέχει το project για την ενσωματωμένη υποστήριξη αρχείων Pdf. Και αυτό το project ενσωματώνει βιβλιοθήκες τρίτου κατασκευαστή (βλέπε παράρτημα Α). Το project δημιουργεί την βιβλιοθήκη PdfView.jar.

Β.2.4 Φάκελος \Projects\Elearning.



Name	Size	Type
build		File Folder
dist		File Folder
icons		File Folder
lib		File Folder
material		File Folder
nbproject		File Folder
src		File Folder
swt		File Folder
.properties.xml	6 KB	XML Document
applet.policy	1 KB	POLICY File
build.xml	4 KB	XML Document
config.s3db	9 KB	S3DB File
crypto_back.s3db	86 KB	S3DB File
elearning.bat	1 KB	MS-DOS Batch File
Elearning.jar	320 KB	Executable Jar File
elearning_back.s3db	86 KB	S3DB File
hs_err_pid5504.log	12 KB	Text Document
licence.txt	24 KB	Text Document
licence_gr.txt	32 KB	Text Document
links.txt	1 KB	Text Document
manifest.mf	1 KB	MF File
README.TXT	2 KB	Text Document

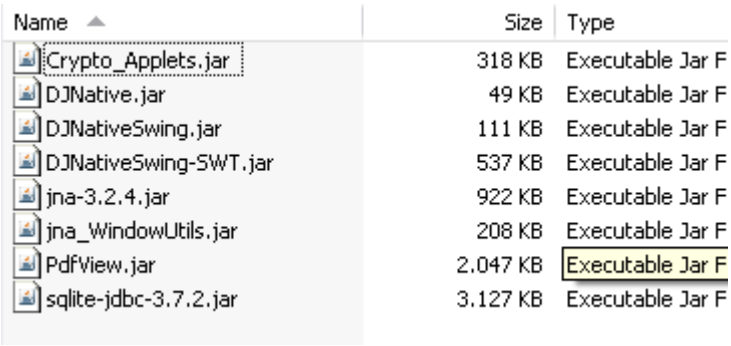
Εικόνα Β.3 Τα στοιχεία του καταλόγου Elearning.

Ο φάκελος Elearning περιέχει το βασικό project της εφαρμογής. Αποτελείτε από τους ακόλουθους φακέλους και αρχεία (εικόνα Β.3):

- Ο φάκελος icons περιέχει εικονίδια της εφαρμογής.
- Οι φάκελοι lib & swt περιέχουν τις απαραίτητες βιβλιοθήκες της εφαρμογής. (βλέπε εικόνα Β.4). Η σημαντικότερη βιβλιοθήκη είναι το αρχείο «sqlite-jdbc-3.7.2.jar» που είναι για την επικοινωνία με την Β.Δ. Οι υπόλοιπες βιβλιοθήκες προέρχονται από τα υπόλοιπα project που αναφέρθηκαν προηγουμένως.
- Ο φάκελος material περιέχει όλο το εκπαιδευτικό υλικό και την αντίστοιχη Β.Δ..
- Ο φάκελος src με τον πηγαίο κώδικα της εφαρμογής.
- Το αρχείο config.s3db είναι η Β.Δ. των ρυθμίσεων.
- Το αρχείο Elearning.jar είναι το εκτελέσιμο αρχείο jar.

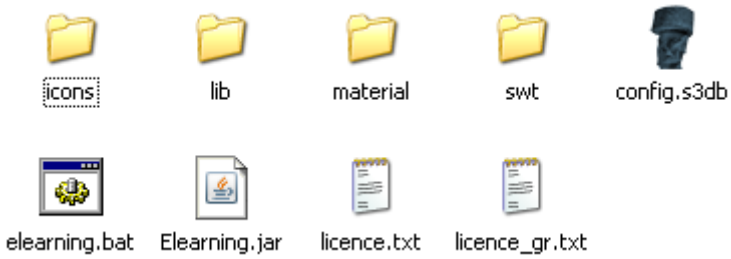
- Το Elearning.bat είναι αρχείο εκκίνησης της εφαρμογής για περιβάλλον Windows.

- Τα αρχεία licence.txt & licence_gr.txt, η άδεια χρήσης στην αγγλική και την ελληνική γλώσσα αντίστοιχα.



Εικόνα Β.4 Τα στοιχεία του καταλόγου Elearning/lib.

Β.2 Φάκελος \Elearning



Εικόνα Β.5 Τα στοιχεία του φακέλου /Elearning.

Στον φάκελο αυτό υπάρχει η έκδοση της εφαρμογής με την μορφή που διατίθεται στους εκπαιδευόμενους. Σε αυτόν τον φάκελο δεν εμπεριέχεται ο πηγαίος κώδικας.