Πανεπιστήμιο Πειραιώς

Τμήμα Ψηφιακών Συστημάτων

Π.Μ.Σ. Τεχνοοικονομική Διοίκηση & Ασφάλεια Ψηφιακών Συστημάτων

Μεταπτυχιακή Διατριβή

Μελέτη αποτυπωμάτων μνήμης κρυπτοσυστήματος Triple DES εφαρμογής Android

Βερνάδος Γεώργιος

ΜΤΕ 1103

Επιβλέπων καθηγητής: Ξενάκης Χρήστος

Abstract

Protection of personal user data and privacy are the dominant issues of contemporary age. Mobile devices and in particular the Android ecosystem, which is their most widespread manifestation, are basic pillars on which the security of the above goods is compromised. This subject triggered the implementation and examination of the Android security of an application based on the Triple DES cryptosystem. The purpose of this thesis is to analyze the architecture of Android software, the study of the Triple DES encryption function and finally the appearance, location and analysis of the key and the other cryptographic parameters existing in the Android application memory dump.

Περίληψη

Η προστασία των προσωπικών δεδομένων του χρήστη και της ιδιωτικότητάς του αποτελούν κυρίαρχα ζητήματα της σύχρονης εποχής. Οι φορητές συσκευές και ιδίως το οικοσύστημα του Android, που αποτελεί την πιο διαδεδομένη έκφανση αυτών, αποτελούν βασικούς πυλώνες στους οποίους διακυβεύεται η ασφάλεια των παραπάνω αγαθών. Για το λόγο αυτό υλοποιείται και εξετάζεται στην παρούσια διπλωματική εργασία η ασφάλεια Android εφαρμογής βασισμένης σε κρυπτοσύστημα Triple DES. Σκοπός της εργασίας αυτής είναι η ανάλυση της αρχιτεκτονικής του λογισμικού Android, η μελέτη λειτουργίας κρυπτογράφησης με Triple DES και τέλος η εμφάνιση, εύρεση και ανάλυση του κλειδιού και των υπόλοιπων παραμέτρων κρυπτογράφησης στο αποτύπωμα της μνήμης.

Περιεχόμενα

Πίνακας εικόνων

Ευχαριστίες

Κατ' αρχάς θέλω να ευχαριστήσω την οικογένειά μου για τη συμπαράσταση, υποστήριξη και κατανόηση που μου παρείχαν όλα αυτά τα χρόνια η οποία ήταν για μένα πολύτιμη.

Θα ήθελα επίσης να ευχαριστήσω τον επιβλέποντα της διπλωματικής εργασίας καθηγητή κ. Χρήστο Ξενάκη, τον επιστημονικό συνεργάτη κ. Χριστόφορο Νταντογιάν και τον συνάδελφό μου κ. Ραδάμανθυ Δερεδάκη για την καθοδήγηση, τις γνώσεις τους και τις συμβουλές τους κατά τη συγγραφή της παρούσας εργασίας.

1 Εισαγωγή

Η προστασία των προσωπικών δεδομένων του χρήστη και της ιδιωτικότητάς του στις διαρκώς αυξανόμενες φορητές συσκευές επιτάσσει την ανάγκη ανάπτυξης εφαρμογών που βασίζονται σε χρήση συστημάτων κρυπτογράφησης με βάση το password (Password Based Encryption). Για το λόγο αυτό υλοποιείται και εξετάζεται στην παρούσια διπλωματική εργασία η ασφάλεια Android εφαρμογής βασισμένης σε κρυπτοσύστημα Triple DES.

Στο κεφάλαιο 2 αναλύεται η αρχιτεκτονική δομή και οι διάφορες εκδόσεις του λογισμικού Android, του πιο διαδεδομένου λειτουργικού συστήματος για κινητές συσκευές.

Στο κεφάλαιο 3 πραγματοποιείται η μελέτη λειτουργίας και αναλύεται ο αλγόριθμος κρυπτογράφησης του κρυπτοσυστήματος Triple DES.

Στο κεφάλαιο 4 γίνεται ανάλυση της εφαρμογής Android που υλοποιήθηκε και γίνεται αναζήτηση και ανάλυση του κλειδιού και των υπόλοιπων παραμέτρων κρυπτογράφησης στο αποτύπωμα της μνήμης καθώς και η τοποθεσία αυτών.

Στο κεφάλαιο 5 αναλύονται τα συμπεράσματα που προκύπτουν αναφορικά με την ασφάλεια του μελετώμενου κρυπτοσυστήματος.

2 Android

2.1 Εισαγωγή στο Android

Το Android είναι λειτουργικό σύστημα για συσκευές κινητής τηλεφωνίας το οποίο τρέχει τον Linux πυρήνα 2.6. Αρχικά αναπτύχθηκε από την Google και αργότερα από την Open Handset Alliance. Επιτρέπει στους κατασκευαστές λογισμικού να συνθέτουν κώδικα με την χρήση της γλώσσας προγραμματισμού Java, ελέγχοντας την συσκευή μέσω βιβλιοθηκών λογισμικού αναπτυγμένων από την Google.

Η πρώτη παρουσίαση της πλατφόρμας Android έγινε στις 5 Νοεμβρίου 2007, παράλληλα με την ανακοίνωση της ίδρυσης του οργανισμού Open Handset Alliance, μιας κοινοπραξίας 48 τηλεπικοινωνιακών εταιριών, εταιριών λογισμικού καθώς και κατασκευής hardware, οι οποίες είναι αφιερωμένες στην ανάπτυξη και εξέλιξη ανοιχτών προτύπων στις συσκευές κινητής τηλεφωνίας. Η Google δημοσίευσε το μεγαλύτερο μέρος του κώδικα του Android υπό τους όρους του Apache License της ελεύθερης άδειας λογισμικού.

Η αρχιτεκτονική του λειτουργικού:

Η πλατφόρμα του λειτουργικού Android χωρίζεται στα ακόλουθα επίπεδα, των οποίων η λειτουργία και ιδιότητες πρόκειται στη συνέχεια να επεξηγηθούν :

1. Εφαρμογές (Applications)

2. Πλαίσιο εφαρμογών (Application Framework)

3. Βιβλιοθήκες (Libraries)

4. Βάση του λειτουργικού (Android Runtime)

5. Πυρήνας του λειτουργικού (Linux Kernel)

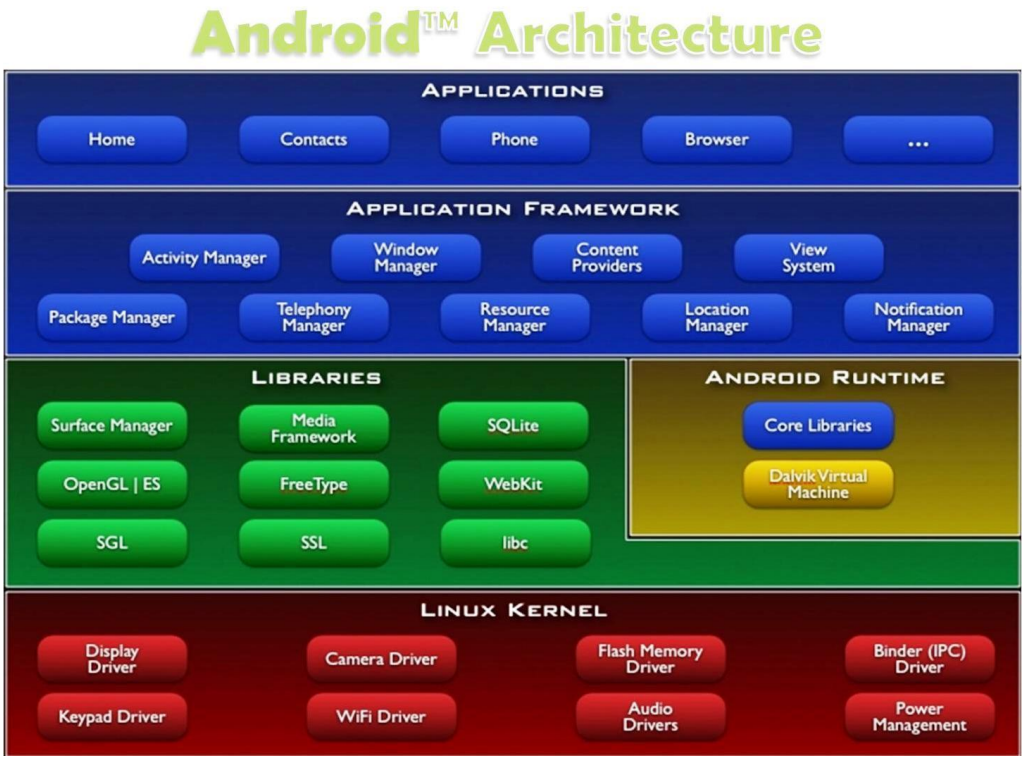

Figure 2-1 *Τα επίπεδα της πλατφόρμας Android*

Οι Εφαρμογές (Applications) είναι μια δέσμη προγραμμάτων, όπως ο διαχειριστής SMS, το ημερολόγιο, το web-browser, η διαχείριση επαφών κ.ά, που ενσωματώνονται ως βασικά προγράμματα στην Android συσκευή.

Το Πλαίσιο εφαρμογών (Application Framework) έχει σχεδιαστεί για να προωθηθεί η επαναχρησιμοποίηση των στοιχείων, έτσι ώστε κάθε εφαρμογή να μπορεί να εξάγει τις διασυνδέσεις της και να αλληλεπιδρά με άλλες εφαρμογές. Οι αλληλεπιδράσεις αυτές μπορεί να είναι δραστηριότητες (Activities), παροχή περιεχομένου, διαχείριση δραστηριότητας κτλ.

Οι Βιβλιοθήκες (Libraries) προορίζονται για τους προγραμματιστές και περιλαμβάνουν ένα σύστημα που βασίζεται στη βιβλιοθήκη BSD derived System-C.

Η Βάση του λειτουργικού (Android Runtime) παρέχει τα χαρακτηριστικά γνωρίσματα προγραμματισμού Java και την εικονική μηχανή.

Το Android χρησιμοποιεί τον **Πυρήνα (Kernel)** Linux 2,6 για τις διαδικασίες χαμηλού επιπέδου του συστήματος, όπως η διαχείριση της μνήμης, των διαδικασιών και της στοίβας του δικτύου.

2.2 Σύστημα αρχείων

Το λειτουργικό Android επιτρέπει την αποθήκευση των δεδομένων τοπικά ως αρχεία. Χρησιμοποιεί επίσης ένα σύστημα αρχείων [2] για την αποθήκευση και για το χειρισμό των ρυθμίσεων της κάθε εφαρμογής (Προτιμήσεις) αλλά και για την βάση δεδομένων SQLite. Για κάθε εφαρμογή, το λειτουργικό Android δημιουργεί έναν κατάλογο στο "data/data/-το όνομα του πακέτου της εφαρμογής-". Τα αρχεία αποθηκεύονται στον φάκελο “files” και οι ρυθμίσεις των εφαρμογών στον φάκελο "shared_prefs" με την μορφή XML αρχείου. Εκεί η κάθε εφαρμογή έχει τον δικό της υποφάκελλο καθώς και δικαιώματα τροποποίησης, ανάγνωσης αλλά και εκχώρησης αυτών των δικαιωμάτων σε 3ες εφαρμογές. Η πρόσβαση στο σύστημα αρχείων γίνεται μέσω του πακέτου της Java: java.io

Το Android επίσης παρέχει βοηθητικές κλάσεις για τη δημιουργία και την πρόσβαση σε νέα αρχεία και καταλόγους. Για παράδειγμα η μέθοδος getDir(String, int) θα δημιουργήσει ή θα παρέχει πρόσβαση, η openFileInput(String s) θα ανοίξει ένα αρχείο για είσοδο και η openFileOutput(String s, int) θα δημιουργήσει ένα αρχείο.

Το όρισμα int καθορίζει τα δικαιώματα : ·

- MODE_PRIVATE – Καμία πρόσβαση από άλλες εφαρμογές
- MODE_WORLD_READABLE – Μονό ανάγνωση από άλλες εφαρμογές
- MODE_WORLD_WRITABLE Μονό εγγραφή από άλλες εφαρμογές
- MODE_WORLD_READABLE | MODE_WORLD_WRITABLE – Ανάγνωση και εγγραφή

2.2.1 Περιορισμοί της σχεδίασης που επιβάλλονται από την πλατφόρμα

Η πλατφόρμα Android δημιουργήθηκε για συσκευές με περιορισμένη επεξεργαστική ισχύ, μνήμη και αποθήκευση. Οι ελάχιστες απαιτήσεις για μια συσκευή Android είναι ανάλογες με την έκδοση του λειτουργικού.

2.3 Android Phone - μνήμη και αποθηκευτικά μέσα

Μία συσκευή Android μπορεί να έχει διαφορετικούς τύπους μνήμης και διαφορετικά αποθηκευτικά μέσα. Όπως για παράδειγμα: το LG Optimus το οποίο

έχει μνήμη ROM 512MB, μνήμη RAM 512MB και δέχεται εξωτερικές μνήμες micro SDHC slot επεκτάσιμη έως 32GB.

2.3.1 Η μνήμη RAM

Η μνήμη τυχαίας προσπέλασης (Random Access Memory) η οποία βρίσκεται σχεδόν σε όλους τους υπολογιστές και αλλά στα smart phones. Στην μνήμη RAM φορτώνονται και εκτελούνται όλα τα προγράμματα γρήγορα. Μετά τον τερματισμό της συσκευής τα δεδομένα εξασθενούν και ύστερα από κάποιο χρονικό διάστημα σβήνονται.

2.3.2 Η μνήμη ROM

"Η μνήμη μόνο για ανάγνωση" (Read-Only Memory). Τα δυαδικά ψηφία που είναι αποθηκευμένα σε αυτόν τον τύπο μνήμης δεν μπορούν ποτέ να τροποποιηθούν από την στιγμή που φεύγουν από το εργοστάσιο, το νέο είδος ROM είναι το EEPROM, που αντικατέστησε ROM, το οποίο επιτρέπει την αντικατάσταση των δεδομένων όταν εφαρμόζεται υψηλότερη τάση έτσι ώστε να μπορεί να εξυπηρετήσει ενημερώσεις. Το EEPROM αντικαθίστανται σταδιακά από την Flash Memory ως επί το πλείστον, η οποία επιτρέπει την αντικατάσταση εύκολα. Πλέον η μνήμη ROM σε ένα smart phone είναι Flash Memory. Η μνήμη ROM στις τηλεφωνικές συσκευές συχνά χωρίζεται σε πολλά διαμερίσματα (partitions). Στα

Android, το ένα partition είναι για την εγκατάσταση του λειτουργικού συστήματος, το οποίο συνήθως προστατεύεται και δεν επιτρέπεται η εγγραφή σε αυτό. Το Rooting σημαίνει η λήψη όλων των δικαιωμάτων των χρηστών του λειτουργικού συστήματος, συνεπώς με το Rooting επιτρέπεται η ανάγνωση και η εγγραφή στο διαμέρισμα του λειτουργικού συστήματος. Τα παραπάνω επιτρέπουν στον χρήστη, που έχει πάρει τα δικαιώματα αυτά, να εκτελέσει διαχειριστικές διεργασίες όπως να τροποποιήσει το λειτουργικό ή ακόμα και να εγκαταστήσει ένα διαφορετικό στην θέση του. Το άλλο partition είναι για τα δεδομένα των χρηστών, συμπεριλαμβανομένων των ληφθέντων εφαρμογών και των αποθηκευμένων δεδομένων τους. Αυτό το partition δεν χρησιμοποιείται μόνο για για ανάγνωση. Το τμήμα αυτό ονομάζεται επίσης εσωτερική μνήμη του τηλεφώνου. Δηλαδή κάτι ανάλογο με τον C: drive στα Windows. Τέλος, ο φάκελος των Windows είναι αόρατος και στο partition του OS. Για παράδειγμα το LG Optimus, έχει αρχικά διαθέσιμο χώρο 180MB. Ο διαθέσιμος χώρος ελαττώνεται με την εγκατάσταση νέων εφαρμογών. Αυτό φαίνεται στο : **Settings | SD card & phone storage settings | Internal Phone Storage.** Όταν ο χώρος γίνει ελάχιστος δεν επιτρέπεται η περαιτέρω εγκατάσταση νέων εφαρμογών. Πλέον στα σύγχρονα smart phones η εσωτερική μνήμη του τηλεφώνου είναι συνήθως μεγαλύτερη από 1 GB και συνδυάζεται με εξωτερικές κάρτες μνήμης.

2.3.3 Εξωτερικές κάρτες μνήμης Micro SD / SDHC

Η χρήση εξωτερικών καρτών μνήμης αποτελεί τη μόνη δυνατότητα αύξησης του αποθηκευτικού χώρου στη συσκευή. Αυτές μοιάζουν με τον εξωτερικό σκληρό δίσκο ενός υπολογιστή. (Για παράδειγμα το Optimus από κατασκευής έχει μια τοποθετημένη κάρτα SD 2GB η οποία μπορεί να αντικατασταθεί με οποιαδήποτε κάρτα έως 32GB). Η micro SD είναι τοποθετημένη στον φάκελο / mnt / sdcard. Οι ρυθμίσεις της είναι **Settings | SD card & phone storage settings | SD card**.

Σε αυτή την κάρτα μπορούν να αποθηκευθούν δεδομένα και αρχεία ανεξάρτητα όπως πχ. ταινίες, μουσική, φωτογραφίες. Η κάρτα SD μπορεί επίσης να χρησιμοποιηθεί και για μεταφορά από SD κάρτα σε SD κάρτα ή από συσκευή σε συσκευή. Μετά το Android 2.1 παρέχεται η δυνατότητα σε ένα μέρος μίας εγκατεστημένης εφαρμογής να μπορεί να μετακινηθεί από την εσωτερική στην εξωτερική μνήμη, εξοικονομώντας με αυτό τον τρόπο πολύτιμο εσωτερικό χώρο στην εσωτερική μνήμη. Βέβαια δεν είναι δυνατό αυτό για όλες τις εφαρμογές ή τουλάχιστον για κάποια συγκεκριμένα τμήματα εφαρμογών να μπορούν να μετακινηθούν από την εσωτερική μνήμη στην κάρτα SD. Έτσι, η προσθήκη μιας μεγαλύτερης κάρτας SD δεν είναι απαραίτητο ότι θα βοηθήσει πολύ αν εσωτερική μνήμη είναι γεμάτη. Επίσης υπάρχουν εφαρμογές που παρέχουν πολλές δυνατότητες επεξεργασίας και ενημέρωσης σχετικά με τις εξωτερικές κάρτες.

2.4 Η εικονική μηχανή Dalvik

Δεδομένου ότι η βάση του λειτουργικού Android (application runtime) πρέπει να υποστηρίζει ένα ευρύ σύνολο συσκευών σε συνδυασμό με το ότι οι εφαρμογές πρέπει να είναι απομονωμένες (sandboxed) για λόγους ασφάλειας, επιδόσεων και αξιοπιστίας μια εικονική μηχανή φαίνεται σαν μια προφανής επιλογή. Ωστόσο, ένα λειτουργικό που βασίζεται σε μια εικονική μηχανή δεν είναι απαραίτητο ότι θα μπορέσει να ισορροπήσει τις απαιτήσεις αυτές με περιορισμένη ταχύτητα επεξεργαστή και μνήμη RAM τις οποίες έχουν οι περισσότερες φορητές συσκευές.

Για την αντιμετώπιση όλων αυτών των κάπως αντικρουόμενων απαιτήσεων η Google δημιούργησε την εικονική μηχανή Dalvik. Συνοπτικά το παραπάνω εγχείρημα στοχεύει στην υλοποίηση ενός περιβάλλοντος εκτέλεσης εφαρμογών με τον περιορισμό ότι κάθε εφαρμογή Android τρέχει σαν αυτόνομη διαδικασία, με το δικό της τμήμα της εικονικής μηχανής Dalvik. Το Dalvik έχει γραφτεί έτσι ώστε μια συσκευή να έχει την δυνατότητα εκτέλεσης πολλαπλών Vms(Virtual machine). Το Dalvik VM εκτελεί εκτελέσιμα αρχεία Dalvik (.DEX) μορφής, τα οποία έχουν βελτιστοποιηθεί για ελάχιστο ίχνος μνήμης. Το VM είναι βασισμένο στα συστήματα καταχωρητών και τρέχει προγράμματα γραμμένα σε Java τα οποία έχουν μετατραπεί σε μορφή .dex. Το Dalvik VM βασίζεται στον πυρήνα Linux για την υποκείμενη λειτουργικότητα, όπως threading και χαμηλού επιπέδου διαχείρισης μνήμης. Δεδομένου ότι κάθε εφαρμογή τρέχει στη δική της διαδικασία μέσα στην

ίδια εικονική μηχανή της, όχι μόνο θα πρέπει η λειτουργία των πολλαπλών VMs να είναι αποτελεσματική αλλά και δημιουργία νέων VMs πρέπει να είναι γρήγορη.

2.5 Οι διαφορετικές εκδόσεις του Android

Στη συνέχεια παρατίθενται όλες οι εκδόσεις του Android που έχουν κυκλοφορήσει έως σήμερα δίδοντας κάποια βασικά χαρακτηριστικά για την κάθε μία ξεχωριστά

2.5.1 Android 5.0 Lollipop

Η Lollipop είναι ένα επανασχεδιασμένο περιβάλλον εργασίας χρήστη χτισμένο γύρω από μία διαδραστική σχεδιαστική γλώσσα που αποκαλείται ως «υλικό σχεδιασμού». Επιπλέον βελτιώσεις του συστήματος είναι ότι το notification system επιτρέπει κοινοποιήσεις που μπορούν να προσπελαστούν από τη lockscreen κι εμφανίζονται μαζί με εφαρμογές ως banner πάνω στην κορυφή της οθόνης. Εσωτερικές αλλαγές που έγιναν επίσης στην πλατφόρμα, πιό συγκεκριμένα, το Android Runtime (ART) αντικατέστησε το Dalvik με μία βελτιωμένη έκδοση, γνωστή ως Project Volta, η οποία παρέχει καλύτερη απόδοση των εφαρμογών, πράγμα το οποίο σημαίνει ότι υπάρχουν και αλλαγές που αποσκοπούν στη βελτίωση και βελτιστοποίηση της χρήσης της μπαταρίας.

2.5.2 Android 4.4 KitKat

Πρόκειται για την πιο πρόσφατη έκδοση του Android. Εμφανίστηκε το Σεπτέμβριο του 2013 και έχει πολλές βελτιώσεις σε σχέση με τους προκατόχους του. Η διεπαφή του ΛΣ είναι ανανεωμένη και η επίδοση των συσκευών με χαμηλότερες επιδόσεις μπορούν να λειτουργήσουν ικανοποιητικά. Μπορεί να συνδεθεί ασύρματα με εκτυπωτή και αναβαθμίστηκαν το NFC και το Google Chrome . Το λογισμικό της κάμερας επιτρέπει στο χρήστη να ανεβάσει απευθείας στο Google και φωτογραφίες.

Βελτιώσεις έγιναν και στις λειτουργίες του ήχου και παράλληλα είναι δυνατή η αποθήκευση δεδομένων από άλλες συσκευές. Το μενού των ρυθμίσεων επανασχεδιάστηκε και στην ενότητα «Γρήγορες Ρυθμίσεις», τοποθετήθηκαν επιπλέον λειτουργίες. Τέλος, βελτιώσεις ενσωματώθηκαν στο ΛΣ σχετικά με την ασφάλειά του.

2.5.3 Android 4.1 - 4.3 Jelly Bean

Η έκδοση Jelly Bean, ανακοινώθηκε τον Ιούνιο του 2012 και προσθέτει μια σειρά από σημαντικά χαρακτηριστικά για το Android. Παραθέτουμε τα χαρακτηριστικά του Android 4.1.

- Google Now: ένα εργαλείο βοηθός που εμφανίζει τις σχετικές πληροφορίες με βάση το ιστορικό αναζήτησής και τα δεδομένα θέσης.
- Υψηλός ρυθμός περιήγησης μέσα στα μενού και τα home screens

- Προβολή φωτογραφιών γρήγορα περνώντας από την κάμερα σε προβολή αυτών ως filmstrips.
- Τα Widgets και τις εφαρμογές μπορεί ο χρήστης να τα μετακινήσει καθώς προσθέτει νέα.
- Οι ειδοποιήσεις τώρα περιλαμβάνουν περισσότερες πληροφορίες, όπως φωτογραφίες ή το θέμα στα μηνύματα ηλεκτρονικού ταχυδρομείου.
- Τα αποτελέσματα αναζήτησης μπορεί τώρα να εμφανίζουν απαντήσεις σε ερωτήματα, και όχι απλώς μια λίστα με Google συνδέσμους στο διαδίκτυο.
- Ένας νέος τρόπος κινήσεων για τη βελτίωση της προσβασιμότητας για τυφλούς χρήστες, επιτρέποντάς τους να περιηγηθούν στο UI χρησιμοποιώντας touch χειρονομίες, σε συνδυασμό με την παραγωγή ομιλίας.

2.5.4 Android 4.0 Ice Cream Sandwich

Η έκδοση Ice Cream Sandwich (ICS) ανακοινώθηκε στο Google I / O συνέδριο τον Μάιο 2011. Η έκδοση αυτή σχεδιάστηκε για να συγχωνεύσει την έκδοση Gingerbread για κινητά τηλέφωνα με την έκδοση Honeycomb, η οποία είχε σχεδιαστεί για τα table. Πλεονεκτήματα της έκδοσης Ice Cream Sandwich σε σχέση με την έκδοση Gingerbread:

- Ταχύτερο και πιο ομαλό πρόγραμμα περιήγησης.

- Η παρακολούθηση της κίνησης δεδομένων βοηθάει τον χρήστη να μην υπερβεί το όριο χρήσης δεδομένων που επιβάλλεται από τις εταιρίες κινητής τηλεφωνίας.
- Περισσότερος χώρος αποθήκευσης για τις εφαρμογές του χρήστη.
- Ένα νέο φιλικό προς το χρήστη action bar που αντικαθιστά το κουμπί του Μενού
- Αναγνώριση προσώπου για το ξεκλείδωμα του τηλεφώνου του χρήστη.
- Η ικανότητα να απορρίπτει ο χρήστης κλήσεις με προ-επιλεγμένα μηνύματα κειμένου

Ένα μειονέκτημα είναι το γεγονός ότι η έκδοση ICS δεν υποστηρίζει το Adobe Flash, αλλά δεν αποτελεί πλέον σημαντική έλλειψη καθώς η εταιρεία έχει ήδη επιβεβαιώσει ότι πρόκειται να το υποστηρίξει .

2.5.5 Android 3.0 και 3.1 Honeycomb

Η έκδοση Honeycomb του Android δημιουργήθηκε για να έχει εφαρμογή στις μεγάλες οθόνες των υπολογιστών tablet. Αυτή η έκδοση του Android είναι ένα ξεχωριστός κλάδος που απευθύνεται μόνο σε tablet, και δεν θα έχει εφαρμογή σε κινητά τηλέφωνα.

Το Android 3.1 ανακοινώθηκε το Μάιο του 2011, και προσθέτει σημαντικές βελτιώσεις για τον χρήστη της έκδοσης Honeycomb. Το Google αναφέρει ότι η

έκδοση Honeycomb θα κάνει «τα στοιχεία UI να είναι πιο εύκολο να τα δούμε, να τα καταλάβουμε και τα χρησιμοποιήσουμε». Τα Widgets θα αποκτήσουν τη δυνατότητα μεγαλώνουν ή να μικραίνουν, για να ταιριάζουν στην οθόνη. Το Android 3.1 υποστηρίζει τους USB flash drives στα tablet για να μεταφέρει ο χρήστης αρχεία χωρίς σύνδεση σε υπολογιστή, καθώς και τα USB πληκτρολόγια, ποντίκια και χειριστήρια.

Χαρακτηριστικά:

- Ένα μπλε σχεδιασμός wireframe δίνει στην έκδοση Honeycomb μια εμπνευσμένη εμφάνιση.
- Η αρχική οθόνη φαίνεται να περιστρέφεται γύρω από ένα 3D καρουσέλ.
- Τα widgets είναι μεγαλύτερα και πιο τολμηρά ώστε να ταιριάζουν με το μέγεθος της οθόνης του tablet.
- Τα κουμπιά – στην αρχική οθόνη και πίσω - έχουν μεταφερθεί επί της οθόνης, ως εικονικά πλήκτρα που κινούνται ταυτόχρονα καθώς περιστρέφετε το tablet.
- Το μενού των εφαρμογών επανατοποθετείται στην άνω δεξιά γωνία. Υπάρχει επίσης ένα νέο κουμπί που εμφανίζει μια λίστα με τις τρέχουσες εφαρμογές, ορατές ως μικρογραφίες.

- Οι βασικές εφαρμογές, όπως το Gmail και το YouTube, σε μεγάλο βαθμό έχουν επανασχεδιαστεί ώστε να επωφεληθούν οι χρήστες του διαθέσιμου χώρου.
- Το πρόγραμμα περιήγησης στο διαδίκτυο εισάγει περιήγηση με καρτέλες, ένα χαρακτηριστικό γνωστό από τα desktop προγράμματα περιήγησης, όπως το Chrome. Υπάρχει επίσης η δυνατότητα ανώνυμης περιήγησης για να περιηγηθεί ο χρήστης ήσυχα.
- Τέλος, ένα μεγαλύτερο multi-touch πληκτρολόγιο επιτρέπει στον χρήστη να κρατήσει πατημένα πολλαπλά κλειδιά με προσωρινή εναλλαγή για παράδειγμα μεταξύ γραμμάτων και αριθμών.

2.5.6 Android 2.3 Gingerbread

Η έκδοση Gingerbread λανσαρίστηκε το Δεκέμβριο του 2010. Το NFC για πληρωμές και το SIP για κλήσεις μέσω διαδικτύου και τα δύο θέτουν τα θεμέλια για τις μελλοντικές εξελίξεις αν και δεν είναι πολύ διασκεδαστικά.

Το Android 2.3.3 όταν έφτασε στα τηλέφωνα τον Απρίλιο του 2011, πρόσθεσε μόνο ένα νέο χαρακτηριστικό - τη δυνατότητα για τηλέφωνα με single-core επεξεργαστές να τρέχουν εφαρμογές που έχουν σχεδιαστεί για dual-core επεξεργαστές. Το Android 2.3.4 πρόσθεσε ακόμα περισσότερες διορθώσεις σφαλμάτων. Παραθέτουμε τα χαρακτηριστικά του Android 2.3.:

- Τα στοιχεία του περιβάλλοντος εργασίας του χρήστη, όπως η γραμμή ειδοποιήσεων, μετατρέπονται από γκρι σε μαύρο χρώμα, σε μια προσπάθεια να αποφευχθεί το burn -in της οθόνης να και να αυξηθεί η διάρκεια ζωής της μπαταρίας.
- Οι συντομεύσεις του πληκτρολογίου στην οθόνη του κινητού τηλεφώνου αυξάνονται και ένας δείκτης βοηθά να επιλέξει ο χρήστης και να αντιγράψει κείμενο.
- Υποστήριξη για μια μπροστινή κάμερα για κλήσεις βίντεο και emo πορτρέτα.
- Χρήση download manager ώστε να μπορεί ο χρήστης να παρακολουθεί ότι έχει κατεβάσει.

2.5.7 Android 2.2 Froyo

Φτάνοντας στο Μάιο του 2010, η έκδοση Froyo εισήγαγε το Flash, το οποίο έχει γίνει μια από τις καθοριστικές διαφορές μεταξύ Android και του κύριου ανταγωνιστή της, το iPhone. Πλεονεκτήματα:

- Το Flash Player 10.1 ήρθε στο Android. Βίντεο, slideshow φωτογραφιών και audio streaming ξαφνικά έγιναν ορατά στο κινητό τηλέφωνο του χρήστη.
- Οι ρυθμίσεις του κινητού τηλεφώνου συνδέθηκαν με τις επαφές και το e-mail για την δημιουργία αντιγράφων ασφαλείας σε διακομιστές της Google και τα

οποία αποκαθίσταται αυτόματα αν ο χρήστης επιλέξει ένα νέο Android τηλέφωνο.

- Παρέχει περισσότερες δυνατότητες για τη σύνδεση με το λογαριασμό Microsoft Exchange, συμπεριλαμβανομένου και της πρόσβασης στο Outlook στο βιβλίο διευθύνσεων. Επίσης, παρέχει την δυνατότητα στο τμήμα μηχανογράφησης να «ξεσκονίσει» από μακριά το τηλέφωνό.
- Στα σημεία πρόσβασης Wi-Fi hotspot επιτρέπετε ο χρήστης να μοιραστεί την 3G σύνδεση στο διαδίκτυο του τηλεφώνου του με άλλες συσκευές, μέσω Wi-Fi.
- Ταχύτερη περιήγηση στο διαδίκτυο, χάρη στις αλλαγές στο πρόγραμμα περιήγησης.
- Καλύτερη συμβατότητα Bluetooth στα ηχεία αυτοκινήτου, καθώς και η προσθήκη της κλήσης φωνής μέσω Bluetooth.

2.5.8 Android 2.0 και 2.1 Eclair

Η έκδοση Android 2.0 έφτασε, μόλις έναν μήνα μετά την έκδοση Donut, τον Νοέμβριο του 2009. Η έκδοση Eclair έφτασε και υποστηρίζει τον Microsoft Exchange server, τον οποίο οι περισσότερες επιχειρήσεις χρησιμοποιούν για το ηλεκτρονικό ταχυδρομείο τους. Η έκδοση Android 2.1 Eclair έφτασε τον Ιανουάριο του 2010. Η έκδοση αυτή διόρθωσε κάποια σφάλματα και πρόσφερε στους προγραμματιστές

εφαρμογές με περισσότερες δυνατότητες, αλλά δεν πρόσθεσε νέα χαρακτηριστικά στους χρήστες. Παραθέτουμε τα χαρακτηριστικά του Android 2.1:

- Υποστήριξη ανταλλαγής, ώστε ο χρήστης να λαμβάνει τα Outlook e-mail του. Υπάρχει επίσης ένας ενιαίος φάκελος εισερχομένων μηνυμάτων ηλεκτρονικού ταχυδρομείου. Ωστόσο, ακόμη διατηρείται με POP και IMAP e-mail σε μια ξεχωριστή εφαρμογή στο Gmail.
- Η υποστήριξη πολλαπλών λογαριασμών Google παρέχει την δυνατότητα να φυλάσσονται όλα τα Gmail του χρήστη.
- Ρυθμίσεις της φωτογραφικής μηχανής συμπεριλαμβανομένης της υποστήριξης για flash, ψηφιακό zoom, ισορροπία λευκού και χρωματικά εφέ.
- Παρέχει την δυνατότητα αναζήτησης μέσα στα μηνύματα κειμένου και τα μηνύματα MMS.
- Η Multi-touch υποστήριξη στο πληκτρολόγιο της οθόνης βοηθά να εντοπίσει ο χρήστης το λάθος αμέσως. Το λεξικό ενσωματώνει τις επαφές, έτσι ώστε ο χρήστης να επιλέγει τα ονόματα των επαφών.
- Το πρόγραμμα περιήγησης στον διαδίκτυο ανανεώνεται με νέα γραμμή διευθύνσεων και μικρογραφίες για επιλογή στα bookmarks.

2.5.9 Android 1.6 Donut

Τον Οκτώβριο του 2009, εμφανίστηκε η έκδοση Donut. Προσέφερε λιγότερο σημαντικές βελτιώσεις, αλλά έφερε στα Android νέο πλήθος χρηστών, χάρη στην προσθήκη της υποστήριξης για CDMA - τεχνολογία που χρησιμοποιείται από ορισμένα αμερικανικά δίκτυα κινητής τηλεφωνίας. Παραθέτουμε τα χαρακτηριστικά του Android 1.6:

- Η λειτουργία αναζήτησης βοήθησε τους χρήστες να εντοπίσουν τις εφαρμογές και τις επαφές στο κινητό τους τηλέφωνο καθώς και να μεταβούν στην αναζήτηση στο διαδίκτυο.
- Υποστήριξη για μεγαλύτερης ανάλυσης οθόνη για τα Android τηλέφωνα διαφόρων μεγεθών.
- Στην πλοήγηση Google Maps προστίθεται δωρεάν το turn-by-turn sat-nav.

2.5.10 Android 1.5 Cupcake

Η χρήση ονομάτων γλυκών ξεκίνησε με το Cupcake, η πρώτη σημαντική αναβάθμιση για το Android, το οποίο έκανε την εμφάνιση του τον Μάιο του 2009. Η έκδοση Cupcake ήταν γεμάτη με νέα χαρακτηριστικά, αλλά ίσως το πιο σημαντικό ήταν το εικονικό πληκτρολόγιο, το οποίο άνοιξε το δρόμο για πλήκτρα, όπως το HTC Magic. Βασικά χαρακτηριστικά:

- Συντομεύσεις και widgets στην αρχική οθόνη σημαίνει ότι τα κινητά τηλέφωνα τώρα μπορούν να είναι προσαρμοσμένα στις ανάγκες του κάθε χρήστη.
- Ένα εικονικό πληκτρολόγιο επί της οθόνης θα μπορούσε να αντικαταστήσει το πληκτρολόγιο με αποτέλεσμα τα κινητά τηλέφωνα να είναι ελαφρύτερα και πιο λιτά.
- Προστέθηκε η εγγραφή βίντεο με κάμερα, καθώς και η δυνατότητα να ανεβάζονται τα βίντεο απευθείας στο YouTube.
- Το Stereo Bluetooth επιτρέπει στον χρήστη να ακούσει μουσική χωρίς καλώδια.
- Το πρόγραμμα περιήγησης στο διαδίκτυο παίρνει μεγάλη ώθηση με τη λειτουργία αντιγραφής και επικόλλησης.

2.5.11 Android 1.0 και 1.1

Το Android γεννήθηκε το 2008, εφαρμόστηκε στο T-Mobile G1. Το T-Mobile G1 κατασκευάστηκε από την HTC. Αυτή η πρώιμη έκδοση του Anroid είχε πολλές δυνατότητες, αλλά ταίριαζε καλύτερα σε gadgets. Παρά το γεγονός ότι το G1 δεν μπορούσε να νικήσει την εκκολαπτόμενη iPhone της Apple στην βιομηχανία του στυλ, προσέφερε τα περισσότερα από τα κύρια

χαρακτηριστικά του Android που γνωρίζουν και αγαπούν οι χρήστες. Χαρακτηριστικά:

- Το Android Market προσφέρει εφαρμογές χωρίς τους αυστηρούς κανόνες εισόδου του App Store της Apple, και παρέχει μια ποικιλία από εφαρμογές που κυμαίνονται από την υψηλή προς την πιο γελοία.
- Το πρόγραμμα περιήγησης της Android κάνει πιο ευχάριστη την περιήγηση στο διαδίκτυο μέσω του κινητού τηλέφωνου του χρήστη, χάρη στην ικανότητα να αποδώσει τις ιστοσελίδες γρήγορα και με ακρίβεια.
- Η Google Maps χρησιμοποιεί το GPS του κινητού τηλεφώνου και το Wi-Fi για να εντοπίσει τη θέση του χρήστη στον χάρτη, με αποτέλεσμα ο χρήστης ποτέ ξανά δεν θα χαθεί.
- Ο συγχρονισμός με τις επαφές του χρήστη, το e-mail και το ημερολόγιο του χρήστη σε απευθείας σύνδεση με την Google αρχικά έκανε τον χρήστη δύσπιστο όσον αφορά την ανταλλαγή όλων των δεδομένων με την Google, αλλά οι ανησυχίες για την προστασία της ιδιωτικής ζωής του χρήστη σύντομα νικήθηκαν από την ευκολία της πρόσβασης οπουδήποτε και από οπουδήποτε.

3 Ο αλγόριθμος DES (Data Encryption Standard)

Ο αλγόριθμος Data Encryption Standard (DES), που συναντάται στη βιβλιογραφία και ως Data Encryption Algorithm (DEA) αποτελεί ένα διεθνές πρότυπο κρυπτογράφησης που χρησιμοποιείται για δεκαετίες με πολύ ικανοποιητικά αποτελέσματα και χαρακτηριστικά ασφάλειας απέναντι σε διαφόρων ειδών επιθέσεις κρυπτανάλυσης. Η παρουσίασή του έγινε από την IBM έπειτα από απαίτηση της κυβέρνησης των Ηνωμένων Πολιτειών για μεγαλύτερη ασφάλεια στην κρυπτογράφηση των πληροφοριών από κάποιο σύστημα το οποίο θα είναι οικονομικό, ευρύτατα διαθέσιμο και ιδιαίτερα ασφαλές. Αρχικά χρησιμοποιούσε για την κρυπτογράφηση κλειδί μήκους 128 bit αλλά στη συνέχεια το μέγεθος του κλειδιού ήταν λέξεις των 56 bit. Η πρώτη προσέγγιση του συστήματος αυτού έγινε το 1974 με την παρουσίαση του αλγορίθμου Lucifer που πληρούσε σε ικανοποιητικό βαθμό τις παραπάνω απαιτήσεις του NIST (National Institute of Standards and Technology). Στη συνέχεια και μετά από διάφορες βελτιωτικές αλλαγές και τροποποιήσεις το 1977 κατοχυρώθηκε και υιοθετήθηκε με τη σημερινή του μορφή ως αλγόριθμος DES.

Η κρυπτογράφηση με βάση τον αλγόριθμο αυτό γίνεται σε τμήματα μεγέθους 64 bits του αρχικού κειμένου, ενώ και το αποτέλεσμα στην έξοδο της διαδικασίας είναι ένα κρυπτογραφημένο τμήμα των 64-bit. Λόγω της συμμετρικής

φύσης του αλγορίθμου, κατά τη λειτουργία του χρησιμοποιούνται τόσο για την κρυπτογράφηση όσο και για την αποκρυπτογράφηση ο ίδιος αλγόριθμος και τα ίδια κλειδιά κρυπτογράφησης. Το μήκος του κλειδιού κρυπτογράφησης είναι 56-bits καθώς από τα 64-bit κάθε όγδοο bit χρησιμοποιείται για έλεγχο ισοτιμίας και δεν λαμβάνεται υπόψη. Οποιοσδήποτε αριθμός των 56-bit μπορεί να αποτελέσει το κλειδί κρυπτογράφησης αλλά και να μεταβληθεί αν αυτό κριθεί αναγκαίο. Επειδή όπως γίνεται κατανοητό το σημαντικό στοιχείο ασφάλειας του αλγορίθμου είναι η ύπαρξη ισχυρών κλειδιών κάποια κλειδιά που θεωρούνται αδύναμα και ευάλωτα σε υποκλοπές μπορεί να αποφευχθούν και να επιλεγούν στη θέση τους άλλα.

Ο αλγόριθμος ικανοποιεί σε μέγιστο βαθμό τις κύριες και θεμελιώδεις ιδιότητες της κρυπτογράφησης, την διάχυση και την σύγχυση. Έτσι το πιο ισχυρό και ουσιώδες τμήμα του αλγορίθμου αποτελείται από μια αντικατάσταση των διαφόρων bit και ακολούθως από μια μετάθεση, ενέργειες που βασίζονται στο κλειδί κρυπτογράφησης. Η διαδικασία αυτή που αποκαλείται κύκλος (round) επαναλαμβάνεται στο αρχικό κείμενο από τον DES 16 φορές έως ότου επιτευχθεί η επιθυμητή κρυπτογράφηση.

Στην εικόνα 3.1 φαίνεται συνοπτικά ο τρόπος κρυπτογράφησης με τον αλγόριθμο DES. Το αρχικό κείμενο των 64 bit κρυπτογραφείται σε ένα κρυπτογράφημα του ιδίου μεγέθους. Στην πρώτη φάση λειτουργίας του αλγορίθμου πραγματοποιείται μια μετάθεση στο αρχικό κείμενο με βάση έναν δεδομένο πίνακα

αντικατάστασης και στην οποία δεν συμμετέχει το κλειδί κρυπτογράφησης. Στη συνέχεια με βάση τις συναρτήσεις των κλειδιών ο αλγόριθμος εκτελεί τους 16 κύκλους του και παράγει τα 64 bit του κρυπτογραφημένου μηνύματος. Στην προτελευταία φάση του DES το κρυπτογράφημα διαιρείται σε δυο τμήματα και γίνεται μια αντιμετάθεση των 32 πιο αριστερών bit με τα 32 πιο δεξιά. Στην τελευταία φάση γίνεται η αντίθετη διαδικασία που ακολουθήθηκε στο πρώτο βήμα με τον πίνακα αντικατάστασης.

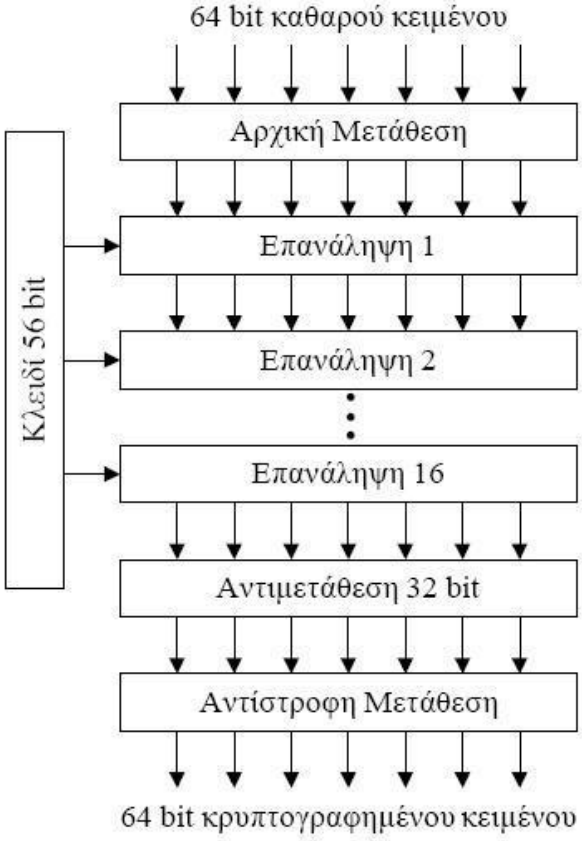

Figure 3-1 *Στάδια κρυπτογράφησης DES*

Λόγω του ιδιαίτερου σχεδιασμού του αλγορίθμου DES, η αποκρυπτογράφηση μπορεί να γίνει χρησιμοποιώντας το ίδιο κλειδί που χρησιμοποιήθηκε κατά τη διαδικασία της κρυπτογράφησης. Απλώς όπως είναι προφανές θα πρέπει τα βήματα του αλγορίθμου να εκτελεστούν με την αντίστροφη σειρά.

Κατά τη λειτουργία των 16 ενδιάμεσων φάσεων πραγματοποιούνται ακριβώς οι ίδιες ενέργειες και το μόνο που αλλάζει είναι η συνάρτηση του κλειδιού σε κάθε γύρο. Η λειτουργία ενός ενδιάμεσου κύκλου κρυπτογράφησης του DES φαίνεται στην εικόνα 3.2. Σε κάθε τέτοιο κύκλο χρησιμοποιούνται τα κουτιά αντικατάστασης S-box τα οποία αναπαριστώνται ως πίνακες δυο διαστάσεων. Την είσοδο σε κάθε κύκλο αποτελούν δυο τμήματα των 32 bit και μετά από την εφαρμογή των μετασχηματισμών λαμβάνονται στην έξοδο επίσης δυο τμήματα των 32 bit. Το δεξιό τμήμα Ri προκύπτει από την αποκλειστική διάζευξη XOR της αριστερής εισόδου και της συνάρτησης f που ορίζεται από την δεξιά είσοδο και το κλειδί Ki της συγκεκριμένης φάσης. Το αριστερό τμήμα της εξόδου είναι ταυτόσημο με την δεξιά είσοδο.

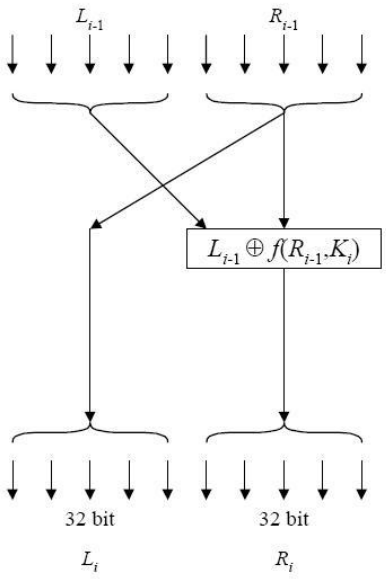

Figure 3-2 *Ενδιάμεση φάση λειτουργίας DES*

Το κύριο συνθετικό κάθε ενδιάμεσου κύκλου και στο οποίο βασίζεται η ασφάλειά του αποτελεί η συνάρτηση του κλειδιού. Το κλειδί κάθε κύκλου προφανώς και είναι διαφορετικό. Το αρχικό κλειδί των 56 bit υπόκειται σε μια διαδικασία μετάθεσης και πριν κάθε κύκλο διαιρείται σε δυο τμήματα των 28 bit. Σε κάθε τέτοιο τμήμα εφαρμόζεται αριστερή ολίσθηση τόσων bit όσων ορίζει ο αριθμός κύκλου και έπειτα από μια νέα μετάθεση προκύπτει το υποκλειδί Ki. Κατά τη διαδικασία της αποκρυπτογράφησης η μοναδική διαφορά στη δημιουργία των κλειδιών είναι ότι δεν πραγματοποιείται αριστερή αλλά δεξιά ολίσθηση.

Κατά την εφαρμογή της συνάρτησης του κλειδιού κάθε κύκλου επεκτείνεται κάθε δεξί τμήμα Ri-1 βάσει δεδομένων πινάκων, κατασκευάζοντας ένα νέο τμήμα

των 48 bit που συμβολίζεται με Ei. Έπειτα ακολουθεί η πράξη της αποκλειστικής διάζευξης του Ei και του αντίστοιχου Ki του συγκεκριμένου κύκλου. Το τμήμα των 48 bit διαιρείται σε τμήματα των 6 bit με κάθε τμήμα να αποτελεί την είσοδο στα οκτώ κουτιά αντικατάστασης από τα οποία προκύπτουν ως έξοδοι τμήματα των 4 bit, δηλαδή ένα νέο τμήμα των 32 bit. Το τμήμα αυτό τελικά χρησιμοποιείται για μετάθεση από ένα κουτί P.

Υπάρχουν τρεις διαφορετικές παραλλαγές του τρόπου λειτουργίας του αλγορίθμου DES οι οποίες δεν θα αναπτυχθούν στην ενότητα αυτή. Πρόκειται για τους Electronic Code Book (ECB), Chain Block Coding (CBC) και ο Cipher Feedback (CFB). Η μείωση του μεγέθους του κλειδιού καθιστά πιο εύκολη την πιθανή επίθεση κρυπτανάλυσης στον αλγόριθμο DES και το μόνο που παραμένει αποθαρρυντικό είναι το μεγάλο κόστος παραβίασης. Μια συνήθης πρακτική για την αποτροπή επιθέσεων και την καλύτερη ασφάλεια είναι η διπλή εφαρμογή του αλγορίθμου κατά την διαδικασία της κρυπτογράφησης, χωρίς αυτό να σημαίνει ότι απαλείφεται εντελώς ο κίνδυνος κρυπτανάλυσης. Η σημαντικότερη δικλείδα ασφαλείας του αλγορίθμου είναι η χρήση κλειδιού κρυπτογράφησης μεγάλου μεγέθους ενώ στη σύγχρονη κρυπτογραφία έχει υιοθετηθεί και η τεχνική Triple DES, η λειτουργία της οποίας παρουσιάζεται παρακάτω εν συντομία.

3.1 Triple DES

Ο αλγόριθμος Triple DES αποτελεί μια μικρή διαφοροποίηση του αρχικού αλγορίθμου DES. Αναφορικά με την ταχύτητα εκτέλεσης είναι τρεις φορές πιο αργός από τον DES αλλά η κατάλληλη χρήση του μπορεί να προσδώσει μέγιστη ασφάλεια στην διαδικασία της κρυπτογράφησης. Παρότι επιστημονικά καμία επιλογή αλγορίθμου και τεχνική κρυπτογράφησης δεν είναι άτρωτη σε επιθέσεις, το μεγάλου μήκους κλειδί του Triple DES είτε αντιμετωπίζει αποτελεσματικά τις όποιες προσπάθειες κρυπτανάλυσης είτε αυξάνει δραματικά το χρόνο για την παραβίαση του αλγορίθμου. Κατά τη λειτουργία του γίνεται χρήση δυο ή τριών κλειδιών και εναλλαγή καταστάσεων κρυπτογράφησης – αποκρυπτογράφησης. Υπάρχουν τέσσερις τέτοιοι διαφορετικοί τρόποι λειτουργίας με γνώμονα την επίτευξη της διαδοχικής κρυπτογράφησης και αποκρυπτογράφησης με διαφορετικά κλειδιά και την ενίσχυση του βασικού αλγορίθμου. Σε κάθε διαφορετική λειτουργία τα επιπλέον κλειδιά δημιουργούνται χρησιμοποιώντας κατάλληλους αλγορίθμους σε συνδυασμό με το ιδιωτικό κλειδί. Ως πιο ασφαλής τρόπος λειτουργίας είναι βάσει επιστημονικών μετρήσεων ο DES-EEE3, που χρησιμοποιεί τρεις διαδοχικές κρυπτογραφήσεις τρία διαφορετικά κλειδιά.

- Εκτέλεση τριών κρυπτογραφήσεων με τρία διαφορετικά κλειδιά **(DES-EEE3)**
- Εκτέλεση διαδοχικά κρυπτογράφησης **-** αποκρυπτογράφησης **-** κρυπτογράφησης με τρία διαφορετικά κλειδιά **(DES-EDE3)**

- Εκτέλεση τριών κρυπτογραφήσεων με δύο διαφορετικά κλειδιά **(DES-EEE2)**
- Εκτέλεση διαδοχικά κρυπτογράφησης **-** αποκρυπτογράφησης **-** κρυπτογράφησης με δύο διαφορετικά κλειδιά **(DES-EDE2)**

Στην περίπτωση των τριών κλειδιών ο Triple DES χρησιμοποιεί τρία κλειδιά των 64 bit δημιουργώντας συνολικό μήκος κλειδιού 192 bits. Όπως και στον αλγόριθμο DES από το αρχικό κλειδί των 64 bit λαμβάνουμε κλειδί των 56 bit αγνοώντας τα bit ισοτιμίας έτσι και στον triple DES από τα 192 bits του αρχικού κλειδιού λαμβάνουμε τελικά κλειδί συνολικού μήκους 168 bit αγνοώντας 8 bit ισοτιμίας για κάθε ένα από τα τρία διαφορετικά κλειδιά κρυπτογράφησης.

Η διαδικασία κρυπτογράφησης, επαναλαμβανόμενη τρεις φορές (triple) είναι πανομοιότυπη με αυτή του κλασικού αλγορίθμου DES. Έτσι το αρχικό κείμενο υπόκειται σε κρυπτογράφηση με το πρώτο κλειδί, στη συνέχεια οδηγείται σε αποκρυπτογράφηση με το δεύτερο κλειδί και τελικά υπόκειται σε εκ νέου κρυπτογράφηση με το τρίτο κλειδί.

4 ΥΛΟΠΟΙΗΣΗ & ΑΝΑΛΥΣΗ ΕΦΑΡΜΟΓΗΣ 3DES_168

Στο κεφάλαιο αυτό αναλύεται η υλοποίηση της εφαρμογής TRIPLE DES 168. Γίνεται ανάλυση και σχολιασμός του τρόπου δημιουργίας της, ο τρόπος λειτουργίας της καθώς και τα ευρήματα που προκύπτουν από την εξέταση των αποτυπωμάτων μνήμης.

Η εφαρμογή αυτή δημιουργήθηκε ώστε να προσομοιάσει (σε όσο το δυνατόν μεγαλύτερο βαθμό) παρόμοιες Android εφαρμογές οι οποίες χρησιμοποιούν κρυπτογράφηση Triple DES με βάση τη χρήση κωδικού για την κρυπτογράφηση ενός κειμένου του χρήστη.

4.1 TRIPLE DES 168: Αρχικό Στάδιο Δημιουργίας Εφαρμογής

Το πρόγραμμα Eclipse Luna το οποίο είχε ενσωματωμένα τα εργαλεία για την ανάπτυξη εφαρμογών Android (Android Development Tools-ADT) χρησιμοποιήθηκε για τη δημιουργία της συγκεκριμένης εφαρμογής.

Παράλληλα με το παραπάνω πρόγραμμα χρησιμοποιήθηκε το Android Software Development Kit (SDK) το οποίο αποτελεί μια ολοκληρωμένη πλατφόρμα εργαλείων τα οποία χρειάζονται για την ανάπτυξη μιας εφαρμογής Android.

Τα πιο σημαντικά από αυτά τα εργαλεία είναι ο προσομοιωτής (emulator), το πρόγραμμα εντοπισμού σφαλμάτων (debugger), και οι απαραίτητες βιβλιοθήκες έτσι ώστε να μπορέσει να εκτελεστεί το Android στον προσομοιωτή.

Δημιουργήθηκε μια εικονική συσκευή Android (Android Virtual Device – AVD) με τη βοήθεια του προσομοιωτή για την λειτουργία και τον έλεγχο σφαλμάτων της εφαρμογής μας. Η ονομασία της εικονικής αυτής συσκευή είναι: "TRIPLE_DES_CRYPT".

Όπως φαίνεται και από την εικόνα 4.1 η συσκευή η οποία επιλέχτηκε είναι η Nexus 4, η οποία λειτουργεί με την έκδοση Jelly Bean (API level 17) του λογισμικού Android.

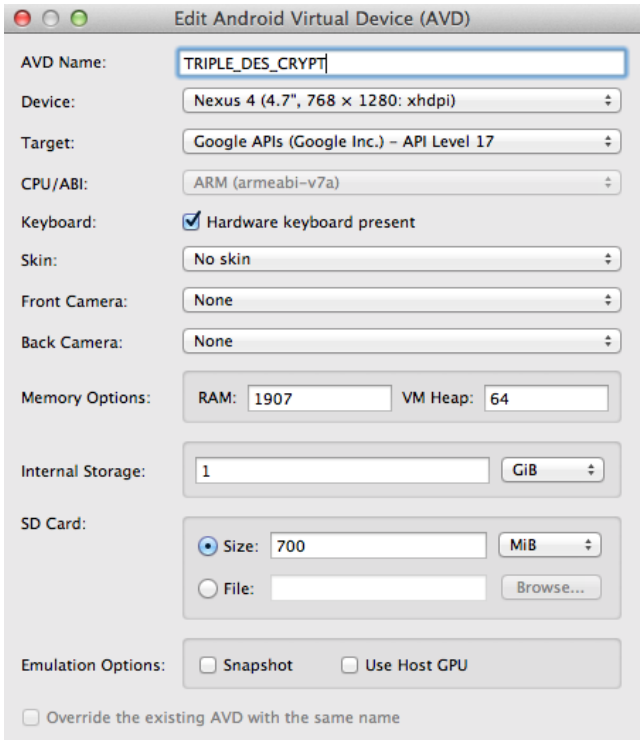

Figure 4-1 *Χαρακτηριστικά Εικονικής Συσκευής Εφαρμογής*

Για την CPU επιλέχθηκε η αρχιτεκτονική ARM η οποία είναι και η πιο διαδομένη αρχιτεκτονική στα κινητά τηλέφωνα, εσωτερική μνήμη 1GB, μνήμη RAM 1907MB και SD Card 700MB.

Figure 4-2 Αρχική Οθόνη Εξομοιωτή

Figure 4-3 Οθόνη Εφαρμογών Εξομοιωτή

Η εφαρμογή αποτελείται από τη βασική οθόνη με την οποία μπορεί να αλληλεπιδράσει ο χρήστης. Η βασική κλάση της Java, η οποία περιέχει την υλοποίηση του αλγόριθμου Triple DES είναι η This_Is_Main.java στην οποία γίνεται

η κρυπτογράφηση και αποκρυπτογράφηση του κειμένου το οποίο δίνει ο χρήστης σε συνδυασμό με κάποιο μυστικό κωδικό.

Οι παράμετροι που χρησιμοποιήθηκαν για τη δημιουργία της κλάσης αυτής φαίνονται παρακάτω:

Παράμετροι Κρυπτογράφησης	**Τιμή**
Αλγόριθμος Κρυπτογράφησης	Triple DES
Τρόπος λειτουργίας	CBC
Συνάρτηση Δημιουργίας Κλειδιού	PBKDF2
Μήκος Κλειδιού	168
Κωδικοποίηση κρυπτογράμματος	Base-64
Επαναλήψεις	100
Διάνυσμα Αρχικοποίησης -IV	12345678
Αλάτι-Salt	The salt is only 32 bytes long

Figure 4-4 ***Παράμετροι αλγόριθμου 3DES για το πρόγραμμα TRIPLE_DES_168***

Βασικά σημεία του κώδικα της κλάσης This_Is_Main.java είναι τα παρακάτω:

```
package com.GV.TRIPLE_DES_168;
import javax.crypto.BadPaddingException;
import javax.crypto.Cipher;
import javax.crypto.SecretKey;
import javax.crypto.SecretKeyFactory;
import javax.crypto.spec.IvParameterSpec;
import javax.crypto.spec.DESedeKeySpec;
import javax.crypto.spec.PBEKeySpec;
import javax.crypto.spec.SecretKeySpec;

import Android.os.Build;
import Android.util.Base64;
import Android.annotation.SuppressLint;
import Android.annotation.TargetApi;
import Android.app.Activity;
import Android.app.AlertDialog;
import Android.app.Dialog;
import Android.app.DialogFragment;
import Android.content.ClipData;
import Android.content.ClipDescription;
import Android.content.ClipboardManager;
import Android.content.Context;
import Android.content.DialogInterface;
import Android.util.Base64;
import Android.view.Menu;
import Android.view.MenuItem;
import Android.view.View;
import Android.widget.*;

……..
```

```
        // E N C R Y P T I O N ! ! !
                public static String encrypt(String plaintext) {
                    try {
                        byte[] saltBytes = salt.getBytes("UTF-8");

                        IvParameterSpec ivspec= new IvParameterSpec(iv.getBytes());
                        SecretKeyFactory                    factory                    =
SecretKeyFactory.getInstance("PBKDF2WithHmacSHA1");
        // Καταχώρηση των παραμέτρων για κρυπτογράφηση με χρήση μυστικού κωδικού.
(password based encryption)
                        PBEKeySpec spec = new PBEKeySpec(
                                password.toCharArray(),
                                saltBytes,
                                pswdIterations,
                                keyselect
                                );

                       SecretKey secretKey = factory.generateSecret(spec);
                       String  stringKey  =  Base64.encodeToString(secretKey.getEncoded(),
0);

                       boolean on = ((ToggleButton) toggle).isChecked();
                       if (on)
                       {outputkey.setText(stringKey);}
                       else
                       {outputkey.setText("");}

                        Cipher cipher = Cipher.getInstance("DESede/CBC/PKCS5Padding");
                        cipher.init(Cipher.ENCRYPT_MODE, secretKey, ivspec);
                        AlgorithmParameters params = cipher.getParameters();
                        byte[]                    encryptedTextBytes                    =
cipher.doFinal(plaintext.getBytes("UTF-8"));
```

```
                    return Base64.encodeToString(encryptedTextBytes,Base64.DEFAULT);

                } catch (Exception ex) {
                    ex.printStackTrace();
                }
                return null;
            }

    //  D E C R Y P T I O N ! ! !
            public static String decrypt(String encryptedText) {
                try {
    // Αρχικοποίηση Διανύσματος Αρχικοποίησης και «Αλατιού»
                    byte[] saltBytes = salt.getBytes("UTF-8");
                    byte[]    encryptedTextBytes    =       Base64.decode(encryptedText,
Base64.DEFAULT);

                    IvParameterSpec ivspec= new IvParameterSpec(iv.getBytes());

                    // Derive the Key
                    SecretKeyFactory                    factory                    =
SecretKeyFactory.getInstance("PBKDF2WithHmacSHA1");
    //  Καταχώρηση  των  παραμέτρων  για  κρυπτογράφηση  με  χρήση  μυστικού  κωδικού.
(password based encryption)
                    PBEKeySpec spec = new PBEKeySpec(
                            password.toCharArray(),
                            saltBytes,
                            pswdIterations,
                            keyselect
                            );

                    SecretKey secretKey = factory.generateSecret(spec);
                    stringKeydec = Base64.encodeToString(secretKey.getEncoded(), 0);
```

```
    // Decrypt the message

        Cipher cipher = Cipher.getInstance("DESede/CBC/PKCS5Padding");
        cipher.init(Cipher.DECRYPT_MODE, secretKey, ivspec);
        byte[] decryptedTextBytes = cipher.doFinal(encryptedTextBytes);


       String go = new String(decryptedTextBytes);
        return go;

    } catch (Exception ex) {
        ex.printStackTrace();

    }


   return null;
}
```

4.2 Λειτουργία της Εφαρμογής 3DES_168

Σε αυτή την ενότητα παρουσιάζεται συνοπτικά η λειτουργία της εφαρμογής, για τη λειτουργία κρυπτογράφησης και για τη λειτουργία αποκρυπτογράφησης. Κατά την εκκίνηση της εφαρμογής εμφανίζεται στο χρήστη η κύρια οθόνη η οποία φαίνεται στην παρακάτω εικόνα:

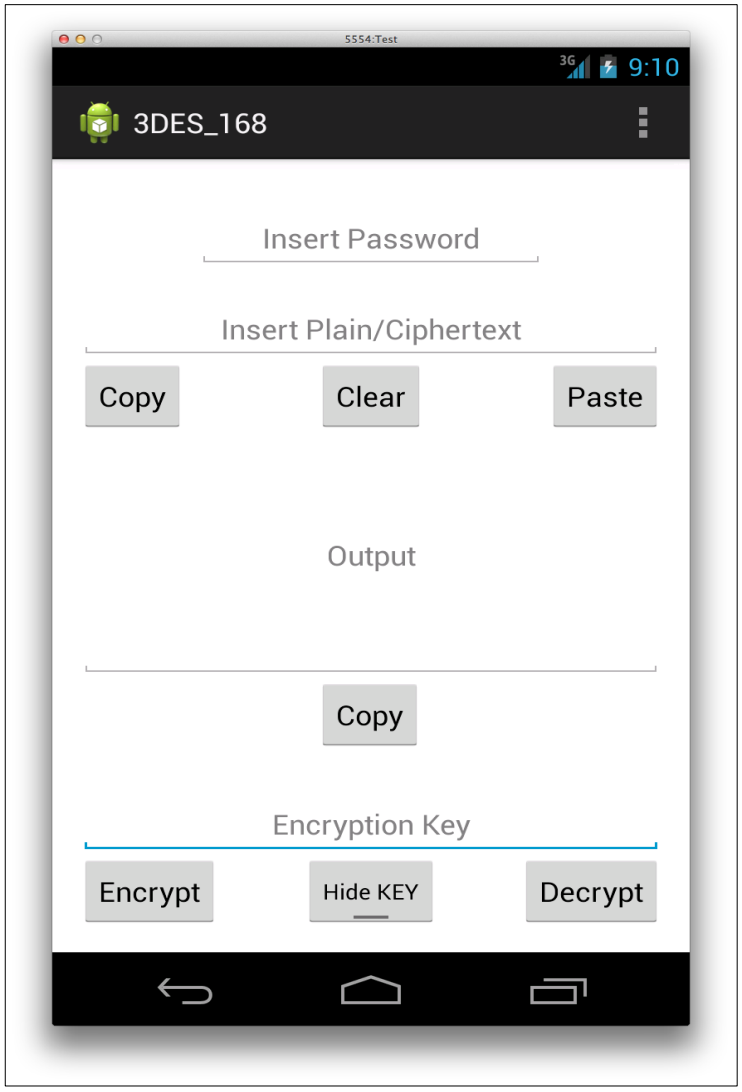

Figure 4-5 *Αρχική οθόνη της εφαρμογής 3DES_168*

Στην οθόνη αυτή υπάρχουν δύο πεδία τα οποία προτρέπουν το χρήστη να δώσει τον κωδικό (Insert Password) και το κείμενο που επιθυμεί να κρυπτογραφήσει/αποκρυπτογραφήσει (Insert Plain/Ciphertext).

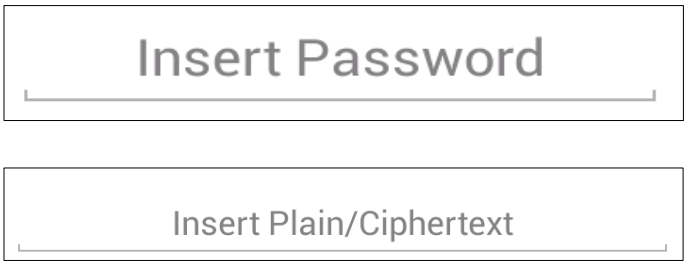

Figure 4-6 *Εισαγωγή κωδικού και απλού Κειμένου ή Κρυπτογράμματος*

Δίπλα σε κάθε πεδίο υπάρχει ένα κουμπί το οποίο άμα επιλεγεί εμφανίζει στο χρήση επιπλέον επιλογές για την επεξεργασία κειμένου.

Οι επιλογές που προσφέρονται στο χρήστη είναι η αντιγραφή (Copy), επικόλληση (Paste), και διαγραφή (Clear) του κειμένου το οποίο επιθυμεί.

Figure 4-7 *Επιλογές για επεξεργασία κειμένου*

Όσον αφορά την αποκρυπτογράφηση, για να εκτελεστεί σωστά πρέπει να πληρούνται οι παρακάτω προϋποθέσεις:

1. Το κείμενο που θα δοθεί να είναι σε μορφή Base-64 η οποία χρησιμοποιεί για την αναπαράσταση κειμένου τους χαρακτήρες A-Z, a-z, 0-9, +, -.

Επίσης για την κωδικοποίηση του κάθε χαρακτήρα αντίθετα με το UTF-8 το οποίο χρησιμοποιεί 8 bits για κάθε χαρακτήρα, η Base-64 χρησιμοποιεί 6 bits/χαρακτήρα. Οπότε μια ακολουθία χαρακτήρων θα έχει μεγαλύτερο μήκος κωδικοποιημένη σε Base-64 από ότι σε UTF-8.

Επειδή σε ορισμένες περιπτώσεις όταν η αρχική ακολουθία δεν είναι ακριβές πολλαπλάσιο του 6, ο τελευταίος χαρακτήρας της Base-64 ακολουθίας δεν θα έχει ακριβώς 6 bits, αλλά θα έχει είτε 2 είτε 4.

Οπότε για να συμπληρωθεί ο αριθμός των 6 bits που απαιτούνται και να μπορέσει να κωδικοποιηθεί σωστά, στην πρώτη περίπτωση προστίθενται 4 bits και 2 bits στην δεύτερη.

Αυτή η προσθήκη των bits φαίνεται σε μια Base-64 ακολουθία με το σύμβολο '==' στο τέλος μιας ακολουθίας στην οποία έχουν προστεθεί 4 bits στον τελευταίο χαρακτήρα, και με το σύμβολο '=' όταν έχουν προστεθεί 2 bits.

Ο χαρακτήρας '=' δεν συμβολίζει κάποιον χαρακτήρα της Base-64 κωδικοποίησης, βρίσκεται πάντα στο τέλος μιας ακολουθίας και ο ρόλος τους είναι να δείχνει πόσα bit έχουν προστεθεί στην ακολουθία.

2. Το κείμενο πέραν της μορφής Base-64, πρέπει να έχει το σωστό μήκος το οποίο να αντιπροσωπεύει ένα κρυπτόγραμμα.

Η κρυπτογράφηση εκτελείται πατώντας το κουμπί "Encrypt" και η αποκρυπτογράφηση αντίστοιχα με το κουμπί "Decrypt".

Το κουμπί εναλλαγής Show/Hide Key δίνει στο χρήστη τη δυνατότητα να εμφανίζει ή όχι το κλειδί της κρυπτογράφησης.

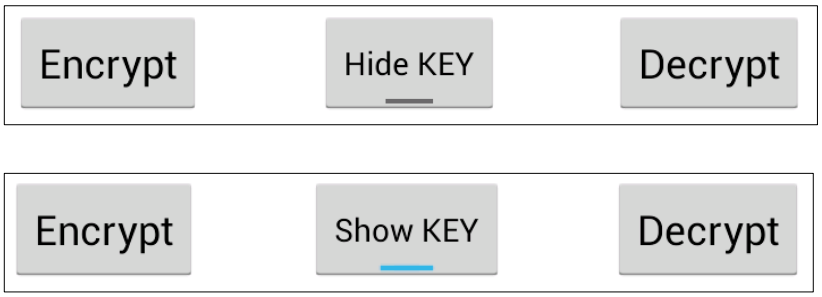

Figure 4-8 *Εναλλαγή εμφανισιμότητας κλειδιού Κρυπτογράφησης*

Επίσης στην αρχική οθόνη υπάρχει μενού για την ενεργοποίηση/ απενεργοποίηση Garbage Function.

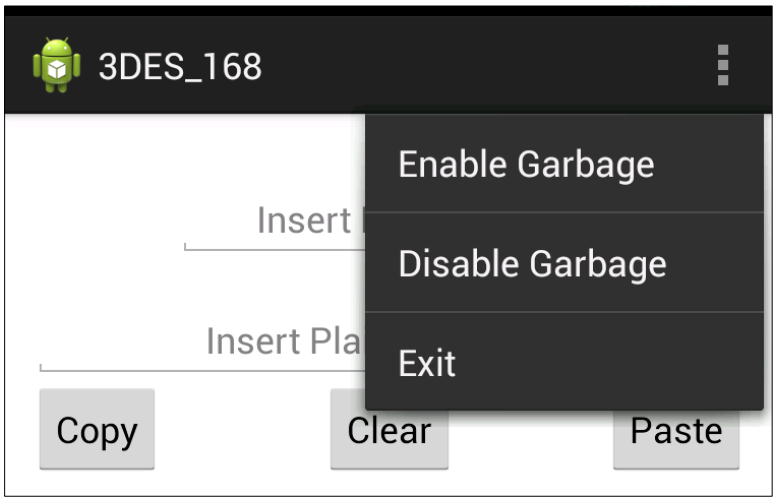

Figure 4-9 *Μενού Κύριας Οθόνης*

Η λειτουργία αυτή κάθε φορά που γίνεται κρυπτογράφηση ή αποκρυπτογράφηση, δημιουργεί ένα τυχαίο διάνυσμα αρχικοποίησης, και το αποθηκεύει στη μεταβλητή garbage_string.

Η μόνη επίπτωση στην εφαρμογή είναι ότι προσθέτει στην εκτέλεση του κώδικα επιπλέον εντολές. Ο λόγος που προστέθηκε αυτή η λειτουργία είναι για να εξεταστεί η επίπτωση που έχουν οι επιπλέον αυτές εντολές που εκτελούνται, στα αποτυπώματα μνήμης της εφαρμογής.

4.2.1 Κρυπτογράφηση Κειμένου

Εξετάζεται και παρουσιάζεται το αποτέλεσμα της κρυπτογράφησης όταν ο χρήστης δώσει σαν είσοδο κωδικό με τιμή "vernadunipi", απλό κείμενο για κρυπτογράφηση με τιμή "Android Memorandum" και μήκος κλειδιού 168 bit.

Στην εφαρμογή έχουμε την παρακάτω εικόνα.

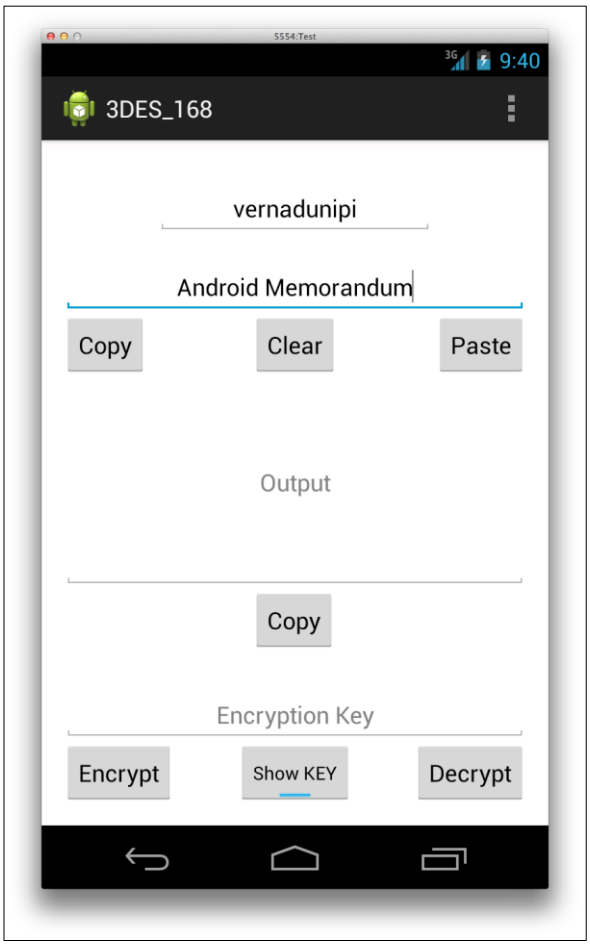

Figure 4-10 *Τιμές Κρυπτογράφησης*

Με αυτές τις τιμές όταν ο χρήστης πατήσει το κουμπί "Encrypt" θα εμφανιστεί στο πεδίο Output, το ciphertext (κρυπτόγραμμα), και στο Encryption Key, το κλειδί κρυπτογράφησης.

Στην επόμενη εικόνα φαίνεται το αποτέλεσμα της κρυπτογράφησης με τις τιμές που επιλέχθηκαν και ορατό το κλειδί κρυπτογράφησης.

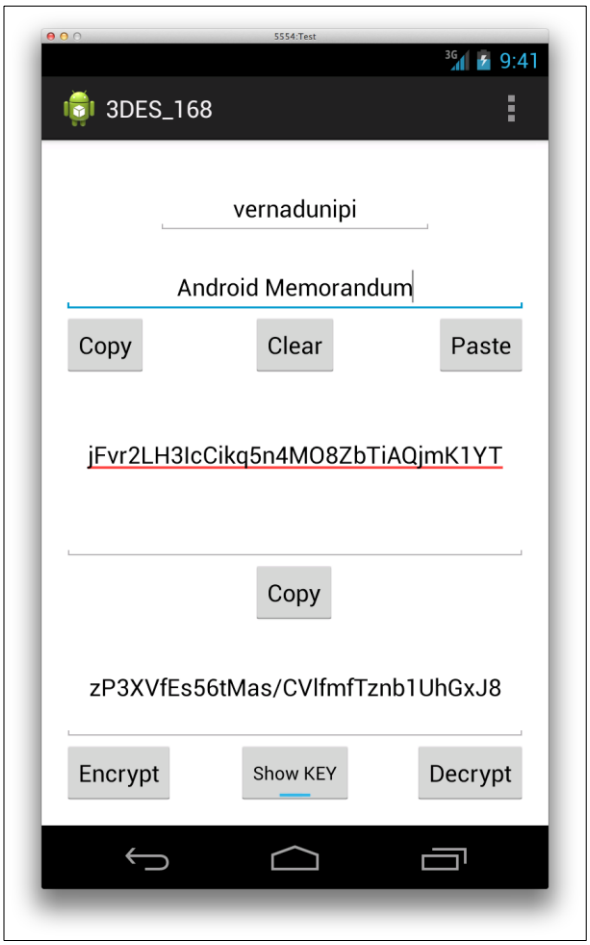

Figure 4-11 *Οθόνη Κρυπτογράφησης*

4.2.2 Αποκρυπτογράφηση Κρυπτογράμματος

Εξετάζεται και παρουσιάζεται το αποτέλεσμα της αποκρυπτογράφησης όταν ο χρήστης δώσει σαν είσοδο κωδικό "vernadunipi", κρυπτόγραμμα για αποκρυπτογράφηση "jFvr2LH3IcCikq5n4MO8ZbTiAQjmK1YT" και μήκος κλειδιού 168 bit.

Πατώντας το δεύτερο ”Copy” μπορούμε να πάρουμε την ήδη εξαγμένη τιμή για το Ciphertext. Με το κουμπί ”Paste” στο πεδίο Inser Plain/Ciphertext κάνουμε επικόλληση της τιμής προς αποκρυπτογράφηση. Με αυτές τις τιμές όταν ο χρήστης πατήσει το κουμπί “Decrypt” θα εμφανιστεί στο πεδίο Output, το απλό κείμενο (plaintext) και στο Encryption Key το κλειδί κρυπτογράφησης.

Η διαδικασία αποκρυπτογράφησης παρουσιάζεται στις παρακάτω εικόνες:

Figure 4-12 *Διαδικασία Αποκρυπτογράφησης*

4.3 Δημιουργία και Ανάλυση Αποτυπωμάτων Μνήμης

Για τη δημιουργία των αποτυπωμάτων μνήμης της εφαρμογής από τον προσομοιωτή χρησιμοποιήθηκε το εργαλείο Dalvik Debug Monitor Server-DDMS, το οποίο είναι διαθέσιμο στο Eclipse μέσω του Android Development Tool-ADT.

Μια από τις επιλογές που παρέχονται από το συγκεκριμένο εργαλείο είναι η δημιουργία αποτυπωμάτων μνήμης μέσω της επιλογής "Dump Hprof File". Η επιλογή αυτή φαίνεται στην παρακάτω εικόνα:

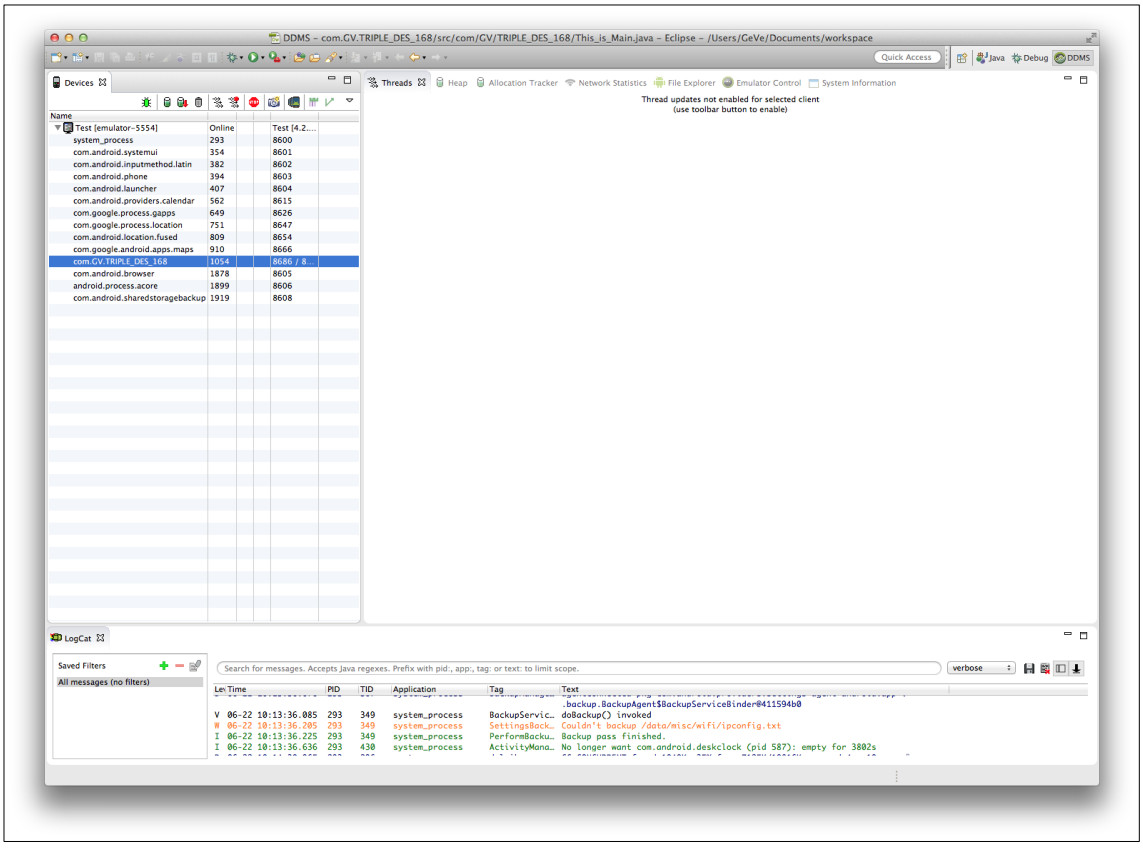

Figure 4-13 *Δημιουργίας αποτυπώματος μνήμης DDMS*

Το πρόγραμμα που χρησιμοποιήθηκε για την ανάγνωση και ανάλυση των αποτυπωμάτων αυτών ήταν το iHex το οποίο δείχνει τόσο το κείμενο σε δεκαεξαδική μορφή (hex) όσο και σε UTF-8 κωδικοποίηση, όπως φαίνεται στην παρακάτω εικόνα:

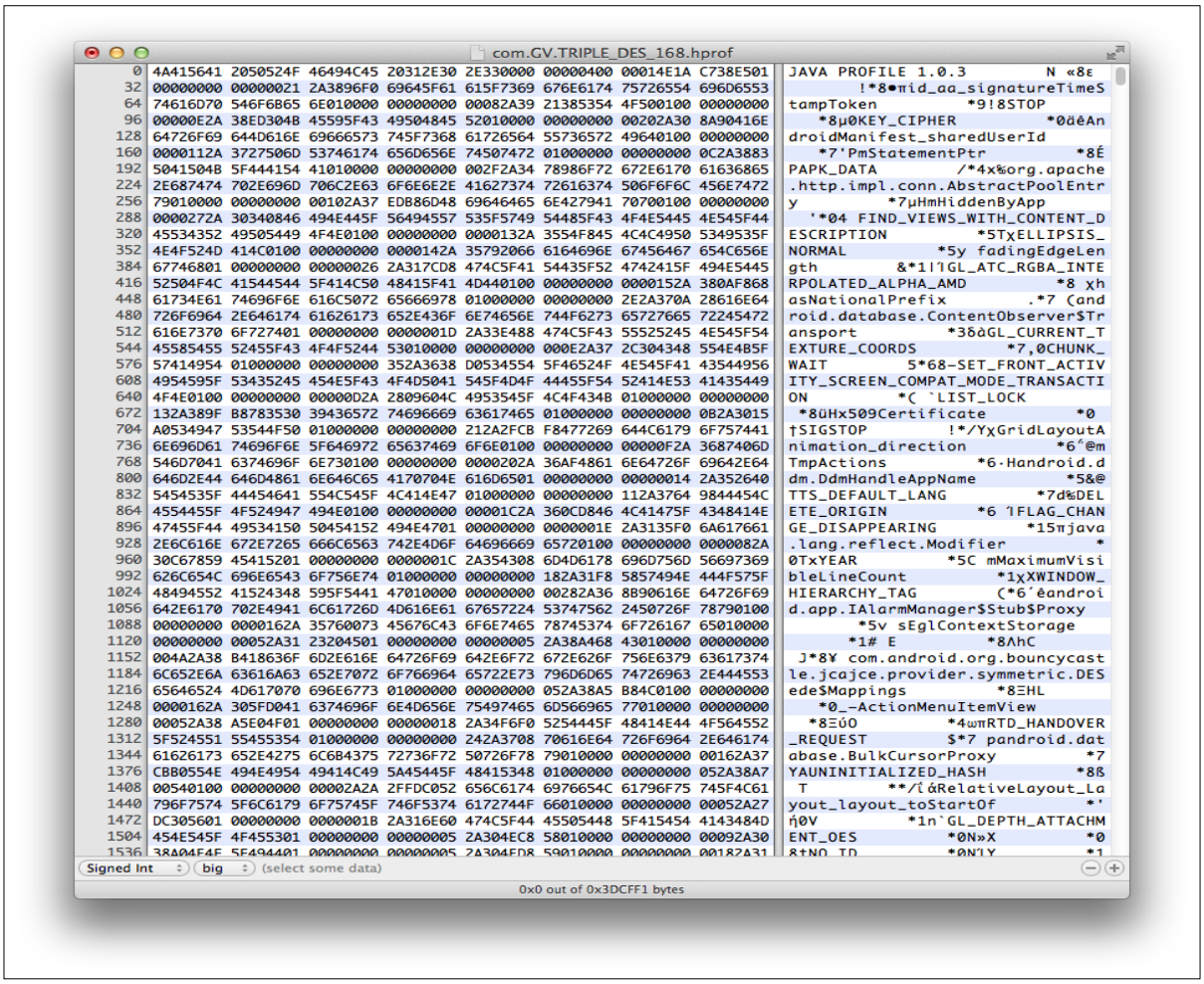

Figure 4-14 *Περιβάλλον προγράμματος iHex*

Δημιουργήθηκαν διάφορα αποτυπώματα μνήμης, με χρήση διαφορετικών κωδικών, διαφορετικών κειμένων, υπό διαφορετικές συνθήκες μέχρι να εξαχθούν ασφαλή συμπεράσματα.

Το αποτύπωμα μνήμης που εξετάστηκε δημιουργήθηκε από την εφαρμογή 3DES_168 με την εκτέλεση των παρακάτω βημάτων:

1. Επιλογή μήκους κλειδιού 168 bits
2. Insert Password
3. Insert Plaintext
4. Encrypt
5. Δημιουργία αποτυπώματος μνήμης μέσω Dump Hprof File από τον DDMS.

Οι τιμές που χρησιμοποιήθηκαν είναι οι εξής:

Παράμετροι	**Τιμές**
Κωδικός	vernadunipi
Κείμενο προς κρυπτογράφηση	Android Memorandum
Κρυπτόγραμμα (Base-64)	jFvr2LH3IcCikq5n4MO8ZbTiAQjmK1YT
Κρυπτόγραμμα (hex)	8C 5B EB D8 B1 F7 21 C0 A2 92 AE 67 E0 C3 BC 65 B4 E2 01 08 E6 2B 56 13
Κρυπτόγραμμα (Windows-1253)	¨[κΙ±ς!άΔ£°gύΟΦe¥βφ+V
Κλειδί κρυπτογράφησης 168 bit (Base-64)	zP3XVfEs56tMas/CVlfmfTznb1UhGxJ8
Κλειδί κρυπτογράφησης 168 bit (hex)	CC FD D7 55 F1 2C E7 AB 4C 6A CF C2 56 57 E6 7D 3C E7 6F 55 21 1B 12 7C
Κλειδί κρυπτογράφησης 168 bit (Windows-1253)	Xΐ'HUώ,γΪLjœ¬VWφ}<γοU!|

Figure 4-15 *Παράμετροι αποτυπώματος μνήμης*

Έπειτα από μια αναζήτηση με τη βοήθεια του προγράμματος iHex προέκυψαν τα εξής ευρήματα:

Ο κωδικός, εμφανίζεται δύο φορές.

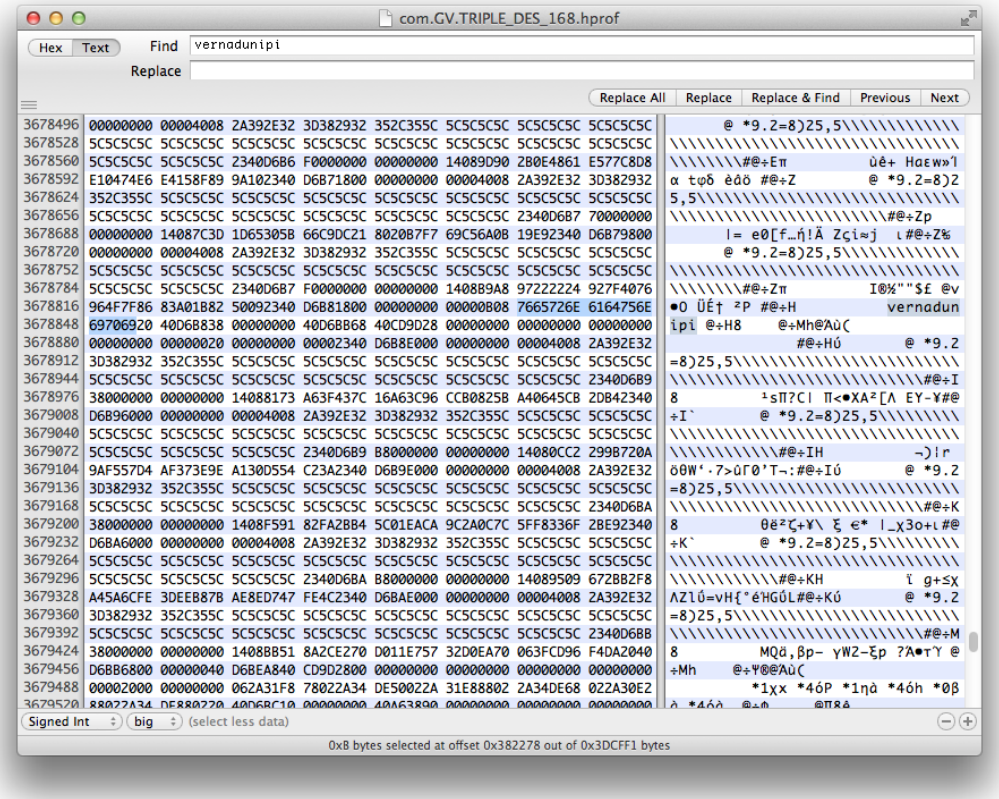

Figure 4-16 *Πρώτη Εμφάνιση Password*

Τη δεύτερη κοντά στο *salt*.

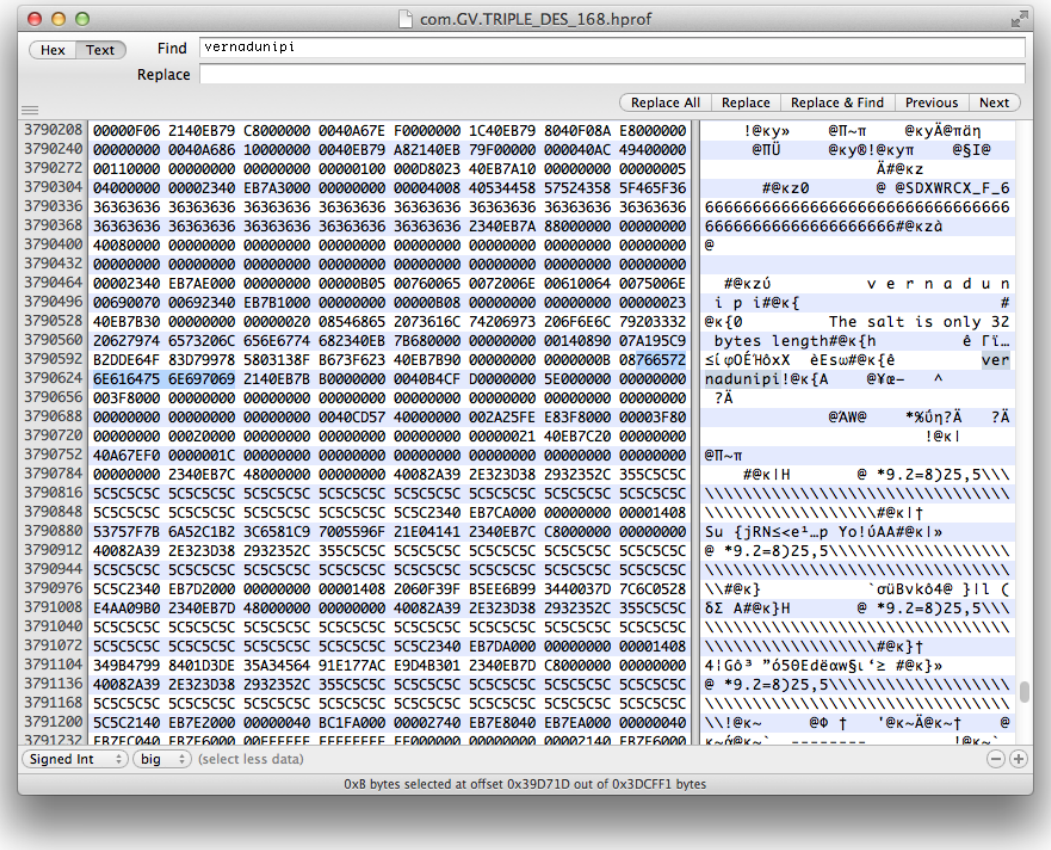

Figure 4-17 *Δεύτερη Εμφάνιση Password*

Άξιο αναφοράς είναι ότι το απλό κείμενο προς κρυπτογράφηση, το κρυπτόγραμμα σε Base-64 και το κρυπτόγραμμα σε hex (που αποκωδικοποιείται σε Windows-1253 από το iHex) εμφανίζονται σε κοντινά offset και τα τρία όπως φαίνεται από την παρακάτω εικόνα

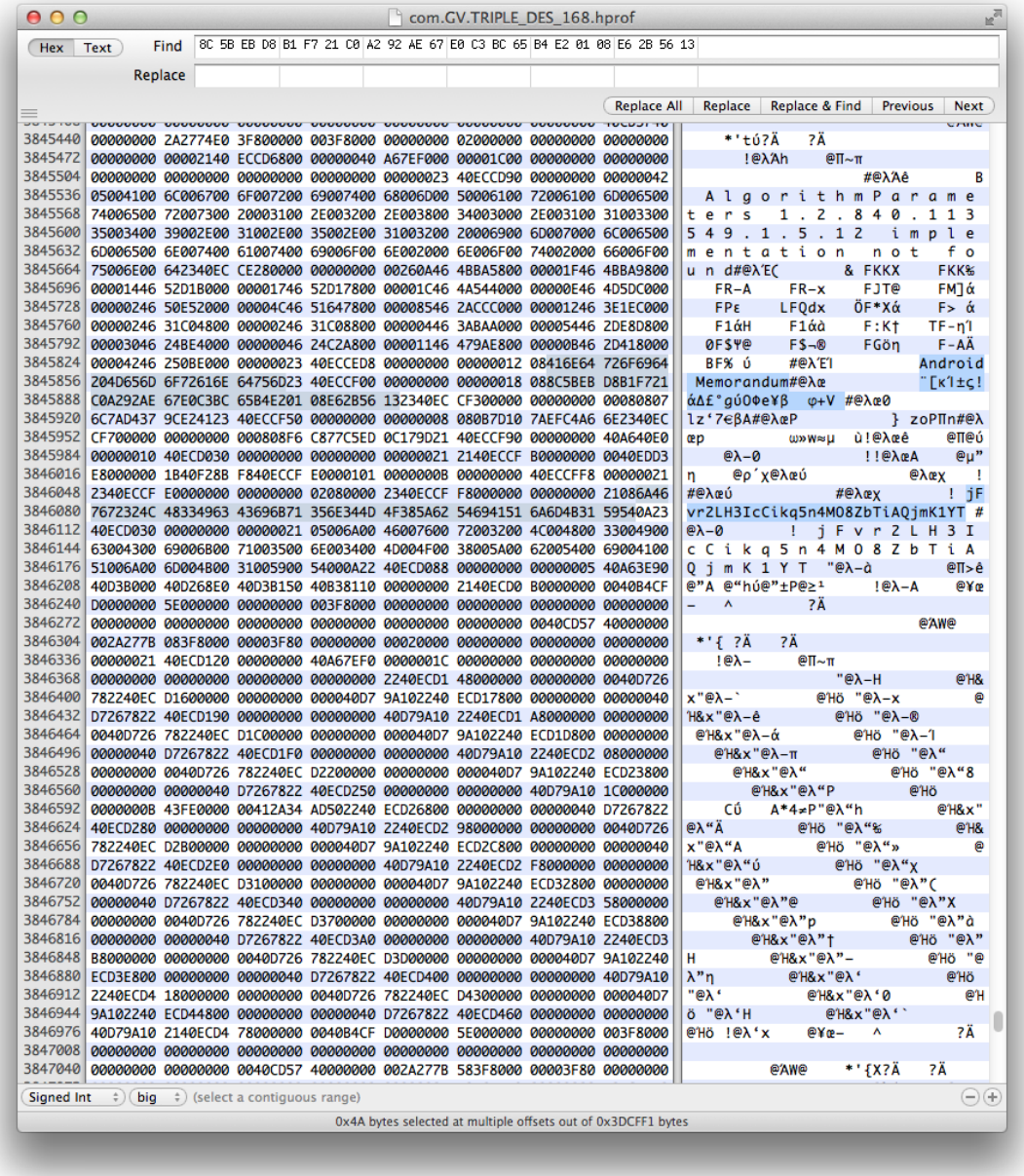

Figure 4-18 *Κοινή Εμφάνιση Plain & Cipher Text*

Το κλειδί σε Base-64, εμφανίζεται μία φορά σε αναζήτηση απλού κειμένου.

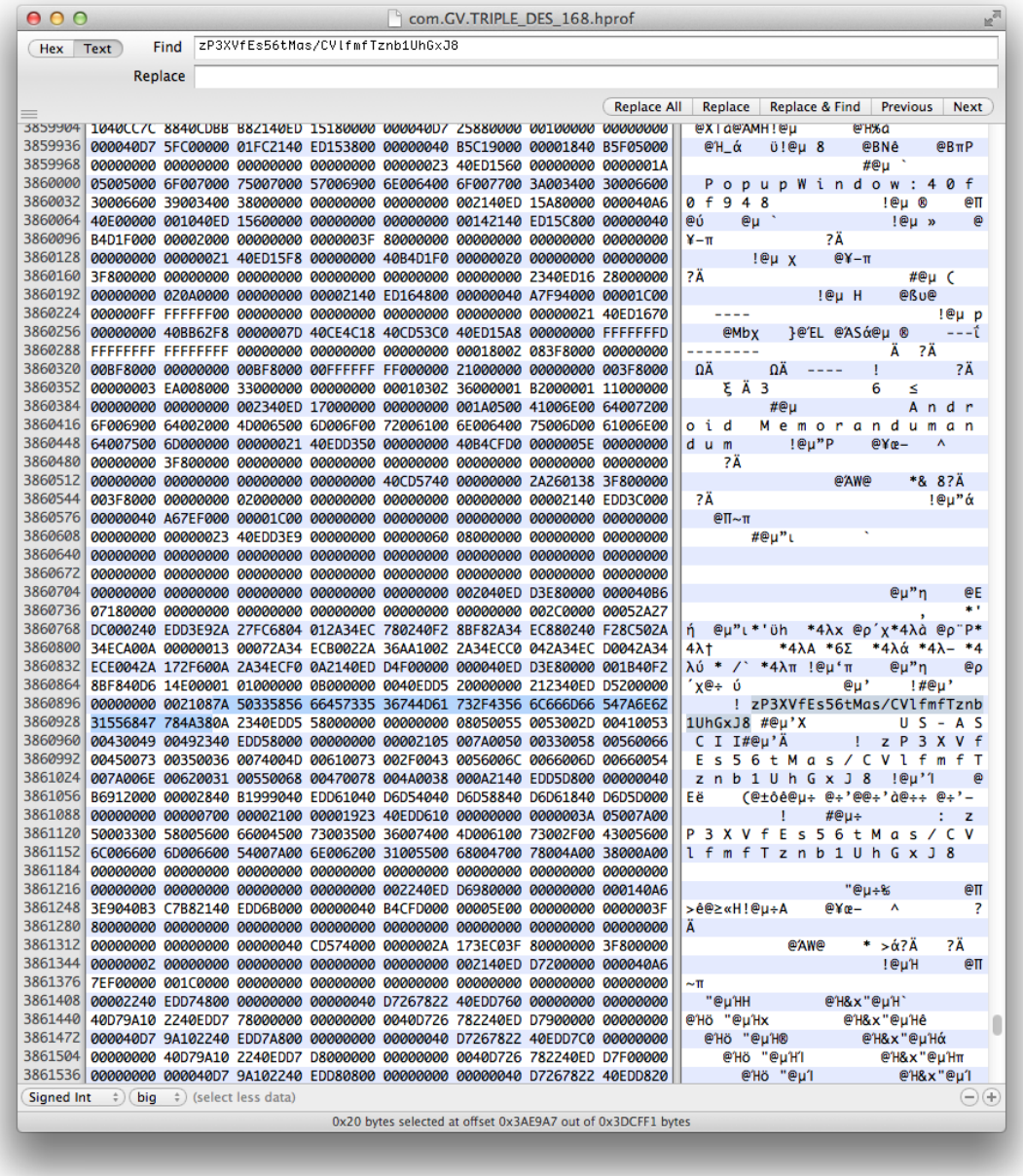

Figure 4-19 *Key (Base64)*

Το κλειδί σε hex, εμφανίζεται δύο φορές στην αναζήτηση. Μια κοντά στα iterations

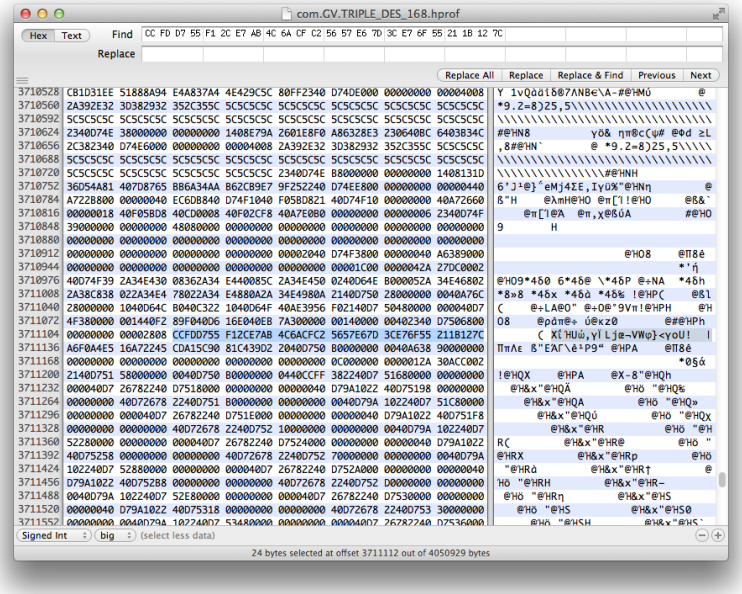

Figure 4-20 *Πρώτη Εμφάνιση Key*

και μια κοντά στο SecretKey

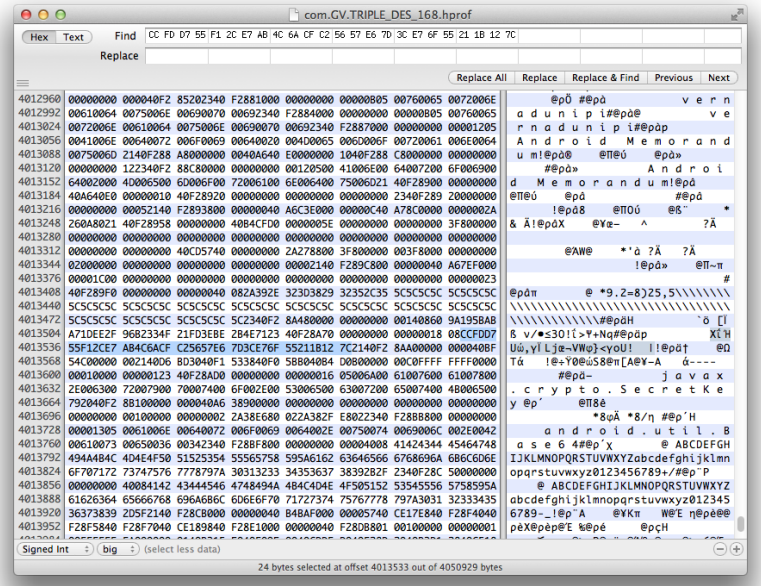

Figure 4-21 *Δεύτερη Εμφάνιση Key*

4.3.1 Ανάλυση Παραμέτρων Triple DES

Για τις παραμέτρους του 3DES, τόσο σε αυτή τη δοκιμή όσο και σε άλλες οι οποίες διεξήχθησαν με παρόμοιες τιμές, προέκυψαν συμπεράσματα τα οποία παρουσιάζονται συνοπτικά σε αυτή την ενότητα.

Καθώς οι παρόμοιες εφαρμογές οι οποίες χρησιμοποιούν κρυπτογράφηση κειμένου με βάση κωδικό, δεν εμφανίζουν το κλειδί κρυπτογράφησης σε οποιαδήποτε μορφή, δόθηκε ιδιαίτερη έμφαση στην αναζήτηση του κλειδιού

κρυπτογράφησης σε δεκαεξαδική μορφή, και όχι σε Base-64. Τα αποτελέσματα της αναζήτησης αυτής παρουσιάζονται παρακάτω.

1. Το κλειδί κρυπτογράφησης βρίσκεται δύο φορές στο αποτύπωμα μνήμης.
2. Αμφότερα τα εύρηματά του έχουν ιδιαίτερη υψηλή μετατόπιση (offset) καθώς βρίσκονται σε τιμές προς το τέλος των διευθύνσεων του αποτυπώματος μνήμης.
3. Η πρώτη εύρεση του κλειδιού είναι στο offset 3711112 bytes από τα συνολικά 4050929 bytes που περιέχονται στο αποτύπωμα μνήμης. 91.61% του μεγέθους του αποτυπώματος μνήμης.
4. Η δεύτερη εύρεση του κλειδιού είναι στο offset 4013533 bytes από τα συνολικά 4050929 bytes που περιέχονται στο αποτύπωμα μνήμης. 99.07% του μεγέθους του αποτυπώματος μνήμης.
5. Βρίσκεται σε offsets κοντά στη διεπαφή javax.crypto.SecretKey, το οποίο είναι αναμενόμενο καθώς είναι υπεύθυνη για τη δημιουργία του κλειδιού .

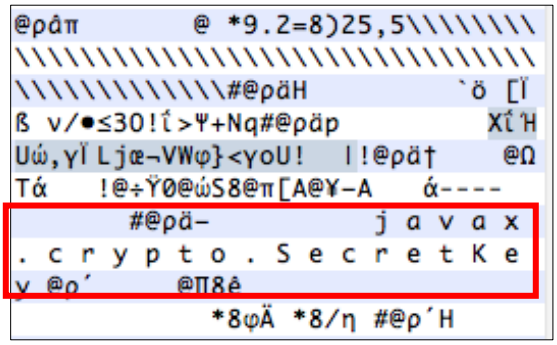

Figure 4-22 *Κλειδί Κρυπτογράφησης και javax.crypto.SecretKey*

Για το **διάνυσμα αρχικοποίησης (IV)** και το **αλάτι (Salt)** παρατηρήθηκαν τα εξής:

Εμφανίζονται κοντά το ένα στο άλλο. Το **IV** σε offset πολύ κοντινά με τη class IvParameterSpec καθώς αυτή είναι υπεύθυνη για τη δημιουργία του, ενώ το **Salt** βρίσκεται αμέσως πριν:

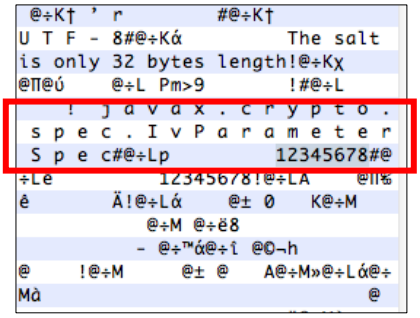

Figure 4-23 *Διάνυσμα αρχικοποίησης και javax.crypto.spec.IvParameterSpec*

Για το **salt** παρατηρήθηκαν τα εξής:

1. Όπως αναφέρθηκε ένα εύρημα του βρίσκεται κοντά στο διάνυσμα αρχικοποίησης λίγο πριν το offset της javax.crypto.spec.IvParameterSpec:
2. Ένα εύρημά του βρίσκεται κοντά στην class PBEKeySpec, καθώς είναι αυτή που δέχεται τις παραμέτρους για κρυπτογράφηση με βάση κωδικό.
3. Τέλος ένα άλλο εύρημά του βρίσκεται σε κοντινό offset με τον αλγόριθμο που χρησιμοποιείται από τη συνάρτηση PBDFK2 για δημιουργία του κλειδιού. (PBKDF2WithHmacSHA1And8bit).

Η λειτουργία του αλγόριθμου κρυπτογράφησης **3DES** καθορίζεται από την εντολή του προγράμματος:

Cipher cipher = Cipher.getInstance("DESede/CBC/PKCS5Padding");

Δεν είναι δύσκολο να αναζητηθεί στο αποτύπωμα μνήμης η τιμή javax.crypto.Cipher σε Unicode μορφή και παρατηρήθηκε ότι σε κοντινό offset από το εύρημα αυτό εμφανίζεται η τιμή που δόθηκε στην παραπάνω εντολή.

Παρατηρήθηκε ότι η συνάρτηση Garbage_Function δεν είχε εμφανή επιρροή στα ευρήματα και στο μέγεθος του αρχείου αποτυπώματος μνήμης.

Εν κατακλείδι άξιο παρατήρησης είναι ότι οι μόνες μεταβλητές οι οποίες δε χρησιμοποιούν κάποια συγκεκριμένη κλάση της java για τη δημιουργία τους είναι το αλάτι και ο αριθμός των επαναλήψεων, οι οποίες είναι αρκετά δύσκολο να εντοπιστούν σε ένα αποτύπωμα μνήμης μιας και αμφότερες οι μεταβλητές αυτές μπορεί να δηλωθούν σαν απλές μεταβλητές ακολουθίας (String) και ακέραιου (int) αντίστοιχα.

5 Συμπέρασμα

Σε αντιπαραβολή με τη ραγδαία ανάπτυξη της σύγχρονης τεχνολογίας, δεν μπορούμε να παραλείψουμε και την αντίστοιχη αλματώδη εξέλιξη που υπάρχει στον τομέα των κακόβουλων χρηστών και προγραμμάτων. Ολοένα και περισσότεροι εισβολείς προσπαθούν να παραβιάσουν την ασφάλεια και να εισβάλουν απρόσκλητα στην προσωπική μας ζωή. Οι κακόβουλοι χρήστες έχοντας στόχο το προσωπικό κέρδος, εξαπατούν, κλέβουν και καταστρέφουν τα προσωπικά μας δεδομένα .

Οι εφαρμογές αποθηκεύοντας πληροφορίες, ιδίως σε κοινά μέσα, συχνά χρησιμοποιούν την κρυπτογράφηση, έτσι ώστε τα στοιχεία να μην είναι ορατά. Ένας προγραμματιστής έχει τη δυνατότητα να χρησιμοποιήσει τις βιβλιοθήκες crypto αλλά συχνά τροποποιεί αυτές τις βιβλιοθήκες ή εφευρίσκει τον δικό του αλγόριθμο κρυπτογράφησης. Αυτό θα μπορούσε να δημιουργήσει τρωτά σημεία στις εφαρμογές. Πολλοί προγραμματιστές πιστεύουν ότι η κωδικοποίηση για παράδειγμα με base64 είναι ένας καλός τρόπος για την κρυπτογράφηση των δεδομένων, αλλά στην πραγματικότητα δεν είναι. Αυτό αποδεικνύεται και με την εφαρμογή της σε εφαρμογή που χρησιμοποιεί κρυπτογράφηση Triple DES, όπως η υλοποιηθείσα. Η λήψη μιας εφαρμογής και εφαρμογή reverse engineering σε αυτήν θα αποκαλύψει τον τρόπο με τον οποίο η κρυπτογράφηση υλοποιήθηκε,

καθιστώντας την ευάλωτη σε έναν πιθανό εισβολέα που θα μπορέσει να αντιστρέψει τη διαδικασία και να αποκρυπτογραφήσει τα δεδομένα, συνεπώς η εφαρμογή κρυπτοσυστήματος Triple DES σε εφαρμογή Android δεν προτείνεται.

6 Βιβλιογραφία

Android Forensics Investigation, Analysis, and Mobile Security for Google Android, Andrew Hoog, 2011 Elsevier, Inc

Live Memory Forensics on Android with Volatility, Holger Macht, January 2013, Department of Computer Science

Android Forensics: Simplifying Cell Phone Examinations, Jeff Lessard, Gary C. Kessler, September 2010

Practical Mobile Forensics, Satish Bommisetty, Rohit Tamma, May 2014

Acquisition and analysis of volatile memory from Android devices, Joe Sylve,

Andrew Case, Lodovico Marziale, Golden G. Richard, Department of Computer Science, University of New Orleans, New Orleans, 2012, USA

Android Memory Capture and Applications for Security and Privacy, Joseph T. Sylve, University of New Orleans, 2011

Forensic analysis of mobile phone internal memory, Svein Y. Willassen, Norwegian University of Science and Technology

Mobile Device Forensics, Andrew Martin, Joey Niem , August 29, 2008

Data Carving Concepts, Antonio Merola, Rick Wanner, November 10th 2008

Analysis of the Android Architecture, Stefan Brahler, 2010

Android Forensics: Automated Data Collection and Reporting from a Mobile Device, Justin Grover, 2013

Comparison of Android Devices, http://en.wikipedia.org/wiki/Comparison_of_Android_devices

Android File System Structure/Architecture/Layout Details, http://techblogon.com/Android-file-system-structure-architecture-layoutdetails/

Mobile Forensics, Javier Martinez Presentation

Android Debug Bridge, http://developer.Android.com/tools/help/adb.html