ΠΑΝΕΠΙΣΤΗΜΙΟ ΘΕΣΣΑΛΙΑΣ

ΤΜΗΜΑ ΜΗΧΑΝΙΚΩΝ ΗΛΕΚΤΡΟΝΙΚΩΝ
ΥΠΟΛΟΓΙΣΤΩΝ ΤΗΛΕΠΙΚΟΙΝΩΝΙΩΝ & ΔΙΚΤΥΩΝ

ΔΙΠΛΩΜΑΤΙΚΗ ΔΙΑΤΡΙΒΗ

ΚΩΣΤΑΡΑΣ ΠΑΝΑΓΙΩΤΗΣ

Μελέτη απαιτήσεων και πραγματοποίηση μετρήσεων για τη χρήση κρυπτογράφησης στις επικοινωνίες VoIP

Επιβλέπων Καθηγητής : Λέανδρος Τασιούλας
Καθηγητής ΤΜΗΥΤΔ

Πίνακας Περιεχομένων

Ευχαριστίες

Θα ήθελα να ευχαριστήσω τον καθηγητή κύριο Λέανδρο Τασιούλα που δέχτηκε τη συνεργασία μαζί μου στα πλαίσια της διπλωματικής μου εργασίας. Επίσης ένα μεγάλο ευχαριστώ στον κύριο Κοψιδά Σπύρο για τις συμβουλές σε θέματα VoIP και στον κύριο Ζησιάδη Δημήτριο για τη βοήθειά του σε θέματα δικτύων και στη σύνταξη του κειμένου.

Ευχαριστώ την οικογένειά μου για την ηθική, οικονομική και ψυχολογική συμπαράσταση όλα αυτά τα χρόνια.

1. Εισαγωγή

Η ανάπτυξη των δικτύων υπολογιστών τα τελευταία χρόνια υπήρξε ραγδαία. Ενώ πριν από μερικές δεκαετίες η δυνατότητα πρόσβασης σε ένα δίκτυο αποτελούσε προνόμιο για πολύ λίγους ανθρώπους, σήμερα με την τεράστια τεχνολογική ανάπτυξη και τη δημιουργία πλήθους επικοινωνιακών αναγκών, η χρήση ενός δικτύου υπολογιστών αποτελεί πλέον το μοναδικό μέσο για να καταφέρουμε να ανταποκριθούμε. Δίκτυα υπολογιστών χρησιμοποιούνται σε κάθε τομέα. Στην παιδεία, στην ιατρική, στη βιομηχανία τα δίκτυα υπολογιστών συμβάλλουν στην επιτάχυνση των διαδικασιών και στην βελτίωση της παραγωγικότητας και της αποδοτικότητας παρέχοντας δυνατότητες επικοινωνίας και ανταλλαγής πληροφοριών μεταξύ ανθρώπων που απέχουν μεταξύ τους εκατοντάδες χιλιόμετρα. Το μεγαλύτερο δίκτυο που υπάρχει αυτή τη στιγμή και αριθμεί εκατομμύρια χρήστες είναι το Internet (Διαδίκτυο).

Το Internet ξεκίνησε σαν ένα project του αμερικανικού στρατού, του οποίου στόχος ήταν η δημιουργία ενός δικτύου μεταφοράς δεδομένων μεταξύ υπολογιστών. Αρχικά δημιουργήθηκε το πειραματικό δίκτυο ARPANET που περιελάμβανε ένα μικρό αριθμό υπολογιστών. Σήμερα το Internet αποτελεί ένα παγκόσμιο δίκτυο που προσφέρει τεράστιες δυνατότητες, μία από τις οποίες είναι και η τεχνολογία VoIP.

Σε όλο τον κόσμο η τηλεφωνία μέσω Internet (VoIP) αναπτύσσεται με ταχύτατους ρυθμούς, συνήθως στα πλαίσια του double-play, δηλαδή της παροχής ευρυζωνικής πρόσβασης και τηλεφωνίας ταυτόχρονα. Η τεχνολογία VoIP έχει φέρει επανάσταση στο χώρο της σταθερής τηλεφωνίας και απειλεί άμεσα όλους τους μεγάλους τηλεπικοινωνιακούς οργανισμούς. Καθώς με τη VoIP επιτυγχάνεται η ενοποίηση δικτύων (δηλαδή η πρόσβαση στο Internet και η τηλεφωνία πάνω από ένα δίκτυο), το αποτέλεσμα είναι -ιδιαίτερα στα υπεραστικά τηλεφωνήματα- οι χρεώσεις μέσω Διαδικτύου να είναι εξαιρετικά χαμηλές και συχνά να βρίσκονται κάτω από αυτές των αστικών κλήσεων. Αντιλαμβάνεται κανείς πόσο σημαντικά είναι τα πλεονεκτήματα για τις επιχειρήσεις, οι οποίες προσπαθούν να μειώσουν τα κόστη τους στο έντονα ανταγωνιστικό περιβάλλον, και ιδίως για εκείνες που συναλλάσσονται με το εξωτερικό. Ήδη στη Βρετανία τα VoIP τηλέφωνα έχουν λάβει δικό τους κωδικό

περιοχής, ενώ πρόγραμμα που προσφέρει δωρεάν τηλεφωνία ανάμεσα σε χρήστες του Internet ήδη έχει περάσει τα 50 εκατομμύρια χρήστες.

Το Διαδίκτυο μπορεί να θεωρηθεί ένας χώρος επικοινωνίας, εκπαίδευσης και οικονομικής δραστηριότητας με διαρκώς αυξανόμενη δύναμη. Η νέα αυτή ψηφιακή κοινωνία οφείλει να παρέχει μηχανισμούς προστασίας του απαραβίαστου της προσωπικής ζωής των μελών της, το οποίο αποτελεί θεμελιώδες ανθρώπινο δικαίωμα.

Σε νομικό και κοινωνικό επίπεδο, τίθεται ζήτημα προστασίας του απορρήτου της ηλεκτρονικής αλληλογραφίας (e-mail), των συναλλαγών (αριθμός πιστωτικής κάρτας, τραπεζικό απόρρητο), του ιατρικού απορρήτου και γενικότερα το ζήτημα της προστασίας προσωπικών στοιχείων και δεδομένων του κάθε χρήστη του Διαδικτύου, που με διάφορους τρόπους μπορούν να συλλεχθούν από τρίτους και να χρησιμοποιηθούν για οποιονδήποτε σκοπό χωρίς τη συγκατάθεση του.

Σε ακαδημαϊκό επίπεδο, τίθεται θέμα προστασίας αποτελεσμάτων ακαδημαϊκής έρευνας, ευαίσθητων προσωπικών δεδομένων (βαθμολογία φοιτητών), ακαδημαϊκών μελετών και γενικότερα προστασίας των πνευματικών δικαιωμάτων των μελών της ακαδημαϊκής κοινότητας.

Σε οικονομικό επίπεδο, η ασφάλεια και προστασία των εμπορικών πλέον δεδομένων, όπως η εξασφάλιση της εγκυρότητας των συναλλαγών μέσω της αποδοχής μίας ηλεκτρονικής υπογραφής και η ασφάλεια των συναλλαγών είναι κρίσιμα ζητήματα, που αποτελούν το υπόβαθρο της ψηφιακής παγκόσμιας αγοράς.

Η κρυπτογραφία εξασφαλίζει το απόρρητο των προσωπικών πληροφοριών και είναι η τεχνολογική πλευρά της λύσης στα προαναφερθέντα ζητήματα ασφαλείας.

Η κατοχύρωση της ασφάλειας των επικοινωνιών πραγματοποιείται με τη χρήση πρωτοκόλλων που διασφαλίζουν την προστασία των προσωπικών δεδομένων των χρηστών του Διαδικτύου και των συναλλαγών. Ένα από αυτά είναι και το VoIPSec. Το μεγαλύτερο μέρος του συγκεκριμένου συγγράμματος ασχολείται με την προσομοίωση λειτουργίας του συγκεκριμένου πρωτοκόλλου (έχουν υλοποιηθεί και animations για τη προσομοίωση της λειτουργίας του) καθώς και τη πραγματοποίηση μετρήσεων με τη χρήση ποικίλων αλγορίθμων κρυπτογράφησης.

Η παρούσα γραπτή αναφορά χωρίζεται σε έξι κύρια τμήματα. Στο πρώτο πραγματοποιείται ανάλυση της τεχνολογίας VoIP και των παραγόντων που την επηρεάζουν. Στο δεύτερο ακολουθεί ανάλυση των μεθόδων συμμετρικής και ασύμμετρης κρυπτογράφησης με παρουσίαση του τρόπου λειτουργίας ποικίλων αλγορίθμων κάθε κατηγορίας. Στο τρίτο τμήμα παρατίθεται η παρουσίαση του προσομοιωτή Simics [2] και η ανάλυση διαφόρων χαρακτηριστικών του. Στο τέταρτο ακολουθεί η παρουσίαση των μετρήσεων που πραγματοποιήθηκαν στον προσομοιωτή Simics. Η πραγματοποίηση μετρήσεων με τη χρήση ποικίλων αλγορίθμων κρυπτογράφησης χωρίς τη χρήση προσομοιωτή αποτελεί το θέμα ανάπτυξης του πέμπτου τμήματος, ενώ το έκτο τμήμα παρουσιάζει τα animations που υλοποιήθηκαν με χρήση της Java για την αναπαράσταση της λειτουργίας του πρωτοκόλλου VoIPSEC [7].

2. Επικοινωνίες VoIP

Η υπηρεσία Voice over IP (VoIP) χρησιμοποιεί το πρωτόκολλο του Διαδικτύου (Internet Protocol) για να μεταφέρει τηλεφωνικές συνομιλίες, μετατρέποντας τη φωνή σε πακέτα δεδομένων. Το υπάρχον μοντέλο τηλεπικοινωνιών επικεντρώνεται στη φωνή και την παροχή σχετικών υπηρεσιών, στην ασύρματη και ενσύρματη τηλεφωνία. Η υπηρεσία Voice over IP αποτελεί μέρος των υπηρεσιών μετάδοσης σε πραγματικό χρόνο, η οποία τείνει να αντικαταστήσει τη συμβατική τεχνολογία του τηλεφώνου ανατρέποντας τα δεδομένα και τις τιμές των τηλεφωνικών υπηρεσιών παγκοσμίως.

Οι κλήσεις μέσω VoIP είναι οικονομικότερες σε σχέση με τις κλήσεις μέσω του παραδοσιακού τηλεπικοινωνιακού δικτύου. Το χαρακτηριστικό αυτό έχει ωθήσει πολλές ευρωπαϊκές, αλλά και ελληνικές, εταιρίες να επενδύσουν δυναμικά στην τεχνολογία VoIP. Υπολογίζεται ότι μέχρι το 2009 όλες οι υπηρεσίες των εταιριών αυτών (φωνή, fax, μεταφορά δεδομένων, video conferencing κλπ) θα παρέχονται μόνο μέσω IP [5].

2.1 Τεχνολογικά χαρακτηριστικά

Οι παράγοντες που επηρεάζουν τη τεχνολογία Voice over IP (VoIP) είναι οι εξής:

- Καθυστέρηση (Delay/Latency)
- Jitter
- Συμπίεση φωνής (Voice Compression)
- Echo
- Απώλεια πακέτων (Packet loss)
- Μετατροπή ψηφιακού σε αναλογικό (Digital-to-Analog Conversion)

Στη συνέχεια θα αναλύσουμε τον κάθε παράγοντα ξεχωριστά.

2.1.1 Delay/Latency

Ως καθυστέρηση VoIP ορίζουμε το χρόνο που απαιτείται για να φτάσει η φωνή από το στόμα του εκφωνητή στο αυτί του αποδέκτη. Υπάρχουν τέσσερις παράγοντες καθυστέρησης στα σημερινά δίκτυα φωνής:

1. Καθυστέρηση διάδοσης (Propagation Delay)
2. Handling Delay
3. Καθυστέρηση μετάδοσης (Serialization Delay)
4. Καθυστέρηση σε ουρές (Queuing Delay)

Η καθυστέρηση στη διάδοση προκαλείται από την απόσταση την οποία το σήμα πρέπει να διανύσει είτε μέσω οπτικών ινών, είτε μέσω ηλεκτρικών παλμών για δίκτυα με καλώδια χαλκού [10]. Η καθυστέρηση Handling Delay περιλαμβάνει διάφορες καθυστερήσεις που οφείλονται στη χρήση τεχνολογιών, όπως packet switching και τεχνικές συμπίεσης. Ο τρίτος τύπος καθυστέρησης (Serialization Delay) αποτελεί το ποσοστό του χρόνου που απαιτείται για την τοποθέτηση ενός bit ή byte πάνω σε μία διεπιφάνεια (interface).

Propagation Delay

Το φως ταξιδεύει διαμέσου του κενού με ταχύτητα 186.000 μιλίων ανά δευτερόλεπτο, ενώ τα ηλεκτρόνια μέσω οπτικών ινών ή καλωδίων χαλκού με 125.000 μίλια ανά δευτερόλεπτο. Ένα δίκτυο οπτικών ινών απλωμένο γύρω από τη γη (13.000 μίλια) προκαλεί συνολική καθυστέρηση της τάξης των 70ms. Αν και μία τόσο μικρή καθυστέρηση είναι σχεδόν ανεπαίσθητη για το ανθρώπινο αυτί, οι καθυστερήσεις διάδοσης σε συνδυασμό με καθυστερήσεις τύπου Handling Delay ενδεχομένως να προκαλέσουν αξιοσημείωτες επιπτώσεις στην ποιότητα των VoIP επικοινωνιών.

Handling Delay

Οι συσκευές οι οποίες προωθούν τα σήματα σε ένα δίκτυο προκαλούν καθυστερήσεις. Οι συγκεκριμένες καθυστερήσεις απαντώνται τόσο στα παραδοσιακά τηλεφωνικά δίκτυα όπου η φωνή μεταδίδεται με τη χρήση πακέτων, όσο και σε δίκτυα νέας τεχνολογίας με σύγχρονους τρόπους μεταφοράς δεδομένων.

Στη συνέχεια ακολουθεί ένα τυπικό παράδειγμα για την παρατήρηση της καθυστέρησης που προκαλεί μία συσκευή VoIP. Ο επεξεργαστής ψηφιακού σήματος (Digital Signal Processor) παράγει δείγματα φωνής κάθε 10 ms χρησιμοποιώντας G.729 (Ο G.729 είναι ένας αλγόριθμος συμπίεσης δεδομένων φωνής. Συμπιέζει τη φωνή σε πακέτα των 10ms). Δύο από αυτά τα δείγματα φωνής (και τα δύο με καθυστέρηση 10ms) τοποθετούνται σε ένα πακέτο. Η συνολική καθυστέρηση του πακέτου είναι επομένως 20ms. Η χρήση του αλγορίθμου G.729 συνεπάγεται αρχική καθυστέρηση look-ahead 5ms, οδηγώντας σε συνολική αρχική καθυστέρηση της τάξης των 25ms για το πρώτο frame φωνής. Εξαιτίας του γεγονότος ότι ο αλγόριθμος G.729 χρησιμοποιεί δείγματα με 10ms καθυστέρηση, συνεπάγεται ότι κάθε αύξηση στον αριθμό των δειγμάτων θα αυξάνει τη συνολική καθυστέρηση κατά 10ms. Ο λόγος για τον οποίο οι επιχειρήσεις προσφέρουν αυτές τις δυνατότητες στον DSP (Digital Signal Processor) είναι γιατί επιδιώκουν να διατηρήσουν χαμηλά το overhead στους router/gateway.

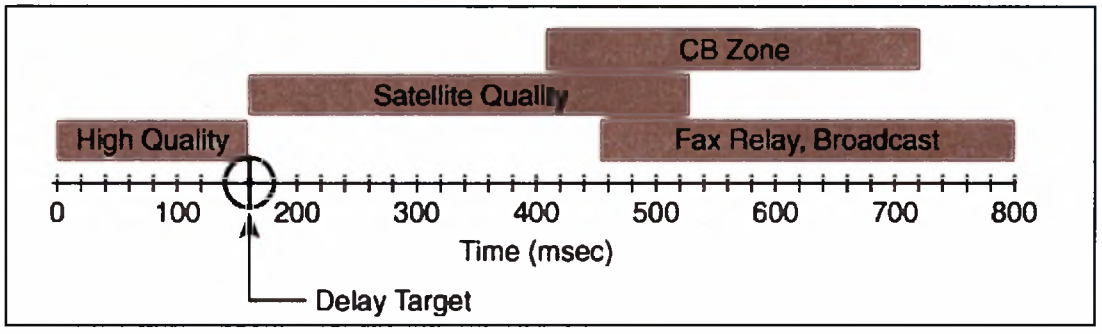
Queuing Delay

Σε ένα δίκτυο στο οποίο τα δεδομένα μεταφέρονται με τη χρήση πακέτων παρατηρούνται καθυστερήσεις και για επιπλέον λόγους. Δύο από αυτούς είναι το packet switching και το queuing delay.

Σε ένα δίκτυο στο οποίο τα δεδομένα μεταφέρονται με τη χρήση πακέτων εφαρμόζεται η τεχνική Store and Forward (η πληροφορία αποστέλλεται σε έναν ενδιάμεσο κόμβο όπου και αποθηκεύεται και στη συνέχεια είτε κατευθύνεται προς τον τελικό προορισμό είτε προς κάποιον άλλο ενδιάμεσο σταθμό). Όταν δεν υπάρχει φορτίο στο δρομολογητή, δεν υφίσταται καθυστέρηση. Ωστόσο όταν τα πακέτα τοποθετούνται σε ουρά (queue) λόγω συμφόρησης στο δίκτυο, το αποτέλεσμα είναι η πρόκληση καθυστέρησης (queuing delay).

Το πρότυπο ITU-T G.114 (International Telecommunication Union Telecommunication Standardization Sector) προτείνει, για αποδεκτή ποιότητα φωνής, καθυστέρηση όχι μεγαλύτερη των 150ms. Ωστόσο, σε κάποιες περιπτώσεις τα αποδεκτά επίπεδα καθυστέρησης είναι μεγαλύτερα ανάλογα με τους τεχνολογικούς παράγοντες που τα καθορίζουν. Συγκεκριμένα σε μεταδόσεις μέσω δορυφόρου, απαιτούνται 180ms–250ms για να φτάσει η

μετάδοση το δορυφόρο και άλλα 180ms–250ms για να επιστρέψει στη γη. Έχουμε δηλαδή συνολική καθυστέρηση της τάξης των 360ms-500ms.



Εικόνα 1 : End-to-end delay

2.1.2 Jitter

Jitter ονομάζεται κάθε μεταβολή στο χρόνο άφιξης των πακέτων στο δίκτυο. Οι μεταβολές αυτές οφείλονται σε φαινόμενα συμφόρησης του δικτύου ή σε τροποποιήσεις των δρομολογίων των πακέτων. Σε ένα περιβάλλον ανταλλαγής πακέτων φωνής, ο αποστολέας αναμένεται να μεταδίδει πακέτα σε τακτικά χρονικά διαστήματα (για παράδειγμα ένα frame κάθε 20ms). Ωστόσο τα πακέτα αυτά ενδεχομένως να αντιμετωπίσουν συμφόρηση στο δίκτυο και να μην φτάσουν στον αποδέκτη εντός των προκαθορισμένων χρονικών ορίων. Η διαφορά ανάμεσα στο πότε ένα πακέτο αναμένεται να φτάσει στον τελικό προορισμό του και στο πότε πραγματικά παραλαμβάνεται ορίζεται ως Jitter [10]. Στο σημείο αυτό πρέπει να αναφέρουμε ότι το jitter και η συνολική καθυστέρηση δεν είναι το ίδιο, αν και η ύπαρξη μεγάλου jitter σε ένα δίκτυο ανταλλαγής πακέτων μπορεί να αυξήσει το ποσοστό της συνολικής καθυστέρησης στο δίκτυο. Αυτό οφείλεται στο γεγονός, ότι όσο περισσότερο είναι το jitter στο δίκτυο, τόσο μεγαλύτερο jitter buffer απαιτείται για την αντιστάθμιση της απρόβλεπτης φύσης των δικτύων ανταλλαγής πακέτων.

2.1.3 Συμπίεση φωνής

PCM είναι η ψηφιακή αναπαράσταση ενός αναλογικού σήματος, όπου οι διαστάσεις του σήματος δειγματοληπτούνται περιοδικά σε ομοιόμορφα διαστήματα και έπειτα ακολουθεί κβαντοποίηση σε μία σειρά συμβόλων ενός ψηφιακού κώδικα [6]. Στην τεχνολογία VoIP δύο τροποποιήσεις 64Kbps PCM χρησιμοποιούνται: μ-law και a-law. Και στις δύο περιπτώσεις γίνεται χρήση λογαριθμικής συμπίεσης με στόχο την επίτευξη 12 με 13 bits γραμμικής PCM

ποιότητας 8 bits. Οι δύο τεχνολογίες διαφέρουν σε κάποιες λεπτομέρειες διεξαγωγής του τρόπου συμπίεσης.

Μία άλλη μέθοδος συμπίεσης φωνής που χρησιμοποιείται είναι η ADPCM (adaptive differential pulse code modulation). Μια συνηθισμένη περίπτωση χρήσης της παραπάνω μεθόδου είναι το πρότυπο ITU-T G.726, στο οποίο δείγματα μεγέθους 4 bits κρυπτογραφούνται παρέχοντας ρυθμό μετάδοσης της τάξης των 32Kbps.

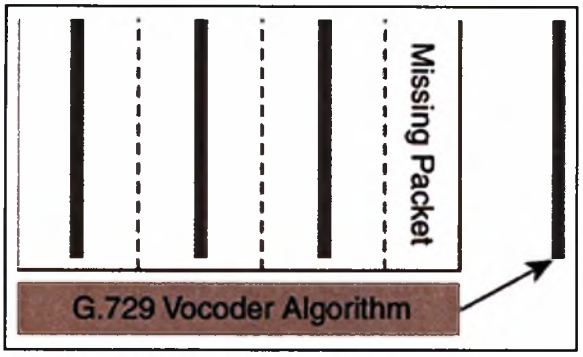
2.1.4 Echo

Το φαινόμενο echo (ανάκλαση των ηχητικών κυμάτων όταν προσκρούσουν σε ορισμένους τύπους επιφανειών) είναι ιδιαίτερα διασκεδαστικό να το βιώνει κανείς στο Grand Canyon, αλλά στις επικοινωνίες η παρουσία του είναι ιδιαίτερα ενοχλητική. Στα δίκτυα μεταγωγής πακέτων υπάρχει η δυνατότητα υλοποίησης συσκευών που παρεμποδίζουν το συγκεκριμένο φαινόμενο (echo cancellers) και τοποθέτησής τους σε κάθε DSP. Αξίζει να αναφερθεί ότι σε κάποιες από αυτές τις υλοποιήσεις, η παρεμπόδιση πραγματοποιείται σε επίπεδο λογισμικού.

2.1.5 Packet loss

Η απώλεια πακέτων στα δίκτυα μεταφοράς δεδομένων είναι ένα φαινόμενο συχνό και αναμενόμενο. Εμφανίζεται όταν υπάρχει συμφόρηση στο δίκτυο. Πολλά πρωτόκολλα δεδομένων στην πραγματικότητα, «χρησιμοποιούν» την απώλεια πακέτων ώστε να γνωρίζουν την κατάσταση του δικτύου και να μπορούν να μειώσουν τον αριθμό των χαμένων πακέτων που στέλνουν.

Όταν εισάγεται φωνή σε δίκτυα δεδομένων, είναι σημαντική η διαμόρφωση του δικτύου με τέτοιο τρόπο ώστε να μπορεί να μεταφέρει φωνή αξιόπιστα και γρήγορα. Επίσης θα ήταν πολύ σημαντική η χρήση κάποιου μηχανισμού που να θωρακίζει τη φωνή απέναντι στο φαινόμενο της απώλειας πακέτων. Ένας τέτοιος μηχανισμός είναι και ο ακόλουθος. Όταν κάποιο πακέτο φωνής δεν παραλαμβάνεται στον προκαθορισμένο χρόνο, χαρακτηρίζεται σαν «χαμένο», και το τελευταίο πακέτο που παραλήφθηκε επαναλαμβάνεται ώστε ο μέσος χρήστης να μην αντιληφθεί κενά.



Εικόνα 2 : Απώλεια πακέτων με G.729

Χρησιμοποιώντας την υλοποίηση G.729 της Cisco για επικοινωνίες VoIP, ας υποθέσουμε ότι κάθε γραμμή στην εικόνα 2 αντιπροσωπεύει και ένα πακέτο. Τα πακέτα 1,2 και 3 φτάνουν στον προορισμό τους, αλλά το 4 χάθηκε κατά τη διάρκεια της μετάδοσης. Ο δέκτης, όταν αντιληφθεί την απώλεια, αντικαθιστά το πακέτο 4 με το τελευταίο πακέτο που παρέλαβε (το 3 στην συγκεκριμένη περίπτωση) έτσι ώστε ο ακροατής να μην αντιληφθεί κάποιο κενό.

2.1.6 Μετατροπή ψηφιακού σε αναλογικό

Αν και η πλειοψηφία των τηλεφωνικών δικτύων στις πιο αναπτυγμένες χώρες σήμερα χρησιμοποιεί ψηφιακή τεχνολογία, πολλές φορές πραγματοποιούνται μετατροπές ψηφιακού σε αναλογικό. Κάθε φορά που λαμβάνει χώρα μία τέτοια μετατροπή, έχουμε αλλοίωση στην φωνή. Τα σημερινά δίκτυα φωνής έχουν τη δυνατότητα υποστήριξης έως και 7 τέτοιων μετατροπών. Κάθε επιπλέον μετατροπή αλλοιώνει τη φωνή σε σημείο που να μην υπάρχει η δυνατότητα αναπαραγωγής του πρωτοτύπου που έστειλε ο αποστολέας.

2.1.7 Άλλοι παράγοντες

Ένας άλλος παράγοντας που επηρεάζει τις επικοινωνίες VoIP είναι το bandwidth που χάνεται εξαιτίας των επικεφαλίδων (headers) στα πακέτα [6]. Τυπικά, για να σταλεί ένα συμπιεσμένο αρχείο ήχου G.723.1 (codec που συμπιέζει αρχεία φωνής σε frames των 30ms με απαιτήσεις 5.6Kbit/s για τη μεταφορά των δεδομένων) χρησιμοποιείται συνολικό bandwidth 18Kbit/s. Η διαφορά ανάμεσα στους δύο ρυθμούς είναι χαρακτηριστική του ποσοστού του bandwidth που καταλαμβάνουν οι επικεφαλίδες των αρχείων (packet headers). Για την αντιμετώπιση του φαινομένου υπάρχουν πολλές τεχνικές

βελτιστοποίησης, όπως συμπίεση επικεφαλίδων (header compression) και silence suppression (Τεχνική που χρησιμοποιείται στην τηλεφωνία και στην οποία δεν έχουμε μετάδοση καμίας πληροφορίας στο δίκτυο όταν κάποιο από τα επικοινωνούντα μέρη δεν μιλά, με αποτέλεσμα την εξοικονόμηση bandwidth). Οι δύο προηγούμενες τεχνικές μπορεί να εξοικονομήσουν μέχρι και 70% του συνολικού bandwidth.

2.2 Πλεονεκτήματα του Voice over IP

Η χρήση υπηρεσιών Voice over IP έχουν ως άμεσο αποτέλεσμα την εξοικονόμηση οικονομικών και διαχειριστικών πόρων. Προσφέρει στις επιχειρήσεις τη δυνατότητα χρήσης του δικτύου τους (LAN, WAN) τόσο για τη μεταφορά δεδομένων (αρχεία, λογιστήριο κ.λπ.) όσο και για τις εσωτερικές επικοινωνίες φωνής.

Τα βασικά πλεονεκτήματα της υπηρεσίας Voice over IP συνοψίζονται στα παρακάτω σημεία :

- Μειωμένο κόστος απομακρυσμένων επικοινωνιών
- Μείωση του χρόνου για την προσθήκη νέων χρηστών στο δίκτυο μέσα από απλοποιημένες ρουτίνες, κινήσεις και αλλαγές
- Οι χρήστες έχουν πρόσβαση σε όλες τις υπηρεσίες του δικτύου
- Ευκολία χρήσης
- Κεντρική διαχείριση
- Χρήση των IP τηλεφώνων για εμφάνιση πληροφοριών και μηνυμάτων
- Εύκολη ενσωμάτωση και χρήση νέων εφαρμογών όπως: Unified Messaging, Call Centres, Web/Mail Collaboration Servers, Personal Assistant

2.3 Υπηρεσίες και εφαρμογές του VoIP

Η τεχνολογία VoIP προσφέρει πλήθος υπηρεσιών και εφαρμογών. Στη συνέχεια αναφέρουμε κάποιες από αυτές [5] :

- Επικοινωνία μέσω μηνυμάτων. Δυνατότητα επικοινωνίας με πελάτες μέσω ηλεκτρονικών μηνυμάτων, φαξ και ευφυών φωνητικών μηνυμάτων (φωνητικό ταχυδρομείο) μέσα σε ένα και μόνο φάκελο αλληλογραφίας (inbox).
- Πρόσβαση στο ηλεκτρονικό ταχυδρομείο μέσω τηλεφώνου (κινητού και σταθερού), με χρήση της τεχνολογίας μετατροπής "κειμένου σε ομιλία" (text to speech).
- Το κέντρο επικοινωνίας IP προσφέρει υπηρεσίες έξυπνης δρομολόγησης κλήσεων, μεταφορά τηλεφωνικών κλήσεων από το δίκτυο στον προσωπικό υπολογιστή και διαχείριση των επαφών με πολυμέσα για την επικοινωνία με τους αντιπροσώπους του κέντρου μέσω δικτύου IP.
- Αυτόματη διανομή κλήσεων και ενσωμάτωση με βάσεις δεδομένων.
- Ομαδική τηλεφωνική συνδιάσκεψη.
- Διατήρηση των εσωτερικών τηλεφωνικών αριθμών χωρίς να είναι απαραίτητη η ύπαρξη τμήματος υποστήριξης για τη διεκπεραίωση των αλλαγών αυτών (δυνατότητα μεταφοράς εσωτερικού αριθμού).
- Υπηρεσίες καταλόγου για την απευθείας επιλογή εσωτερικού τηλεφώνου, χωρίς η διαδικασία να πραγματοποιείται μέσω του τηλεφωνικού κέντρου.
- Τοποθέτηση της υπηρεσίας υποδοχής σε οποιοδήποτε σημείο. Κάποιος εργαζόμενος σε ένα απομακρυσμένο γραφείο μπορεί να αναλάβει τη διεκπεραίωση των υπηρεσιών υποδοχής, εάν παραστεί ανάγκη.

Η τεχνολογία VoIP υποστηρίζεται από πλήθος εφαρμογών. Στη συνέχεια αναφέρουμε κάποια ενδεικτικά παραδείγματα :

- **MSN Messenger**: μέσω του msn messenger, προγράμματος για τη μεταφορά μηνυμάτων μέσω του Διαδικτύου το οποίο ενσωματώνεται στο λειτουργικό σύστημα των Windows, παρέχεται η υπηρεσία .NET Voice Service για τηλεφωνικές κλήσεις απευθείας από τον υπολογιστή. Προϋπόθεση για την ικανοποιητική λειτουργία της υπηρεσίας αποτελεί το

γεγονός ότι οι χρήστες πρέπει να έχουν τουλάχιστον την έκδοση 4.5 του MSN Messenger.

- **Skype**: το skype είναι ένα απλό πρόγραμμα που προσφέρεται δωρεάν και επιτρέπει τηλεφωνικές κλήσεις μέσω του Διαδικτύου σε ολόκληρο τον κόσμο. Χρησιμοποιεί τεχνολογία P2P (peer to peer) για τη διασύνδεση όλων των χρηστών του skype.
- **Firefly:** το Firefly είναι ένα εργαλείο, το οποίο συνδυάζει το instant messaging και την τεχνολογία VoIP, όπως ακριβώς και το Skype.
- **Yahoo! Business Messenger:** Πρόκειται για ένα εργαλείο που απευθύνεται κυρίως σε επιχειρήσεις. Η υπηρεσία της Yahoo! παρέχει ένα πλήρες πακέτο instant messaging και τηλεδιάσκεψης, ανταλλαγής κάθε είδους δεδομένων και τηλεφωνίας μέσω Internet, δίνοντας ιδιαίτερη έμφαση στην ασφάλεια. Επιπρόσθετα δίνει τη δυνατότητα αποστολής άμεσων μηνυμάτων (instant messages) απευθείας από τον υπολογιστή σε κινητά τηλέφωνα των εταιριών Verizon Wireless, Cingular και AT&T Wireless.
- **NetMeeting:** το NetMeeting της Microsoft αποτελεί τμήμα του λειτουργικού συστήματος Windows. Πρόκειται για ένα εύχρηστο, απλό και λειτουργικό web phone, το οποίο υποστηρίζει συνομιλία καθώς και ανταλλαγή δεδομένων ήχου, εικόνας, κειμένου και video.
- **ICQ:** το πρόγραμμα instant messaging ICQ υποστηρίζει τις εξής τηλεφωνικές υπηρεσίες:
    1. Call PC to Phone (κλήσεις από τον υπολογιστή σε τηλέφωνο)
    2. Call PC to PC (κλήση από υπολογιστή σε υπολογιστή)
    3. Call Phone to PC (κλήση από τηλέφωνο σε υπολογιστή)
    4. Call Phone to Phone(κλήση από τηλέφωνο σε τηλέφωνο μέσω του λογαριασμού ICQphone)

Επιπλέον το ICQ παρέχει τη δυνατότητα αποστολής γραπτών μηνυμάτων σε κινητά τηλέφωνα σε ολόκληρο τον κόσμο.

3. Ασφάλεια – Κρυπτογραφικά συστήματα

Δεν είναι λίγοι αυτοί που πιστεύουν ότι η χρήση κρυπτογραφικών εργαλείων αφορά μόνο... κατασκόπους ή μανιώδεις χρήστες υπολογιστών. Στην πραγματικότητα, όταν κάποιος αποστέλλει ένα προσωπικό e-mail ή ανταλλάσσει εμπιστευτικές εμπορικές πληροφορίες για ένα έργο μέσω του ηλεκτρονικού ταχυδρομείου, οφείλει να γνωρίζει ότι, εάν δεν έχει κρυπτογραφηθεί, είναι σαν να το στέλνει με καρτ-ποστάλ: μπορεί να το διαβάσει σχεδόν οποιοσδήποτε.

Ένα e-mail, εκτός από τον αποστολέα και τον παραλήπτη, μπορεί να διαβαστεί εύκολα και από τους εργαζόμενους στον ISP (εταιρία παροχής Internet) του αποστολέα, τους εργαζόμενους στον ISP του παραλήπτη, από οποιονδήποτε ελέγχει τους routers από τους οποίους θα περάσουν τα "πακέτα" του μηνύματος και από οποιονδήποτε έχει πρόσβαση στον εξοπλισμό τηλεφωνίας στην τηλεφωνική εταιρία. Αν το μήνυμα αποστέλλεται ή παραλαμβάνεται από κινητό τηλέφωνο με σύνδεση στο Διαδίκτυο, τότε μπορεί να υποκλαπεί από άτομα με ειδικές συσκευές υποκλοπής συνομιλιών και μηνυμάτων κινητής τηλεφωνίας. Επιπλέον, είναι πολύ απλό να πλαστογραφηθεί η διεύθυνση αποστολής, ακόμα και με ένα τυπικό πρόγραμμα e-mail. Με λίγο περισσότερη δουλειά, κάποιος επιτήδειος μπορεί να αποκρύψει και άλλα σημάδια που δείχνουν από πού πραγματικά προέρχεται ένα μήνυμα.

Λύση στα παραπάνω προβλήματα δίνουν οι τεχνολογίες κρυπτογράφησης. Οι τεχνολογίες αυτές εξασφαλίζουν ότι το μήνυμα θα μπορεί να το διαβάσει μόνο ο παραλήπτης του, καθώς στα ενδιάμεσα στάδια το μήνυμα εμφανίζεται με ακατάληπτους χαρακτήρες, είναι δηλαδή μη αναγνώσιμο. Υπάρχουν δύο τεχνολογίες κρυπτογράφησης, η συμμετρική και η ασύμμετρη κρυπτογράφηση.

3.1 Συμμετρική κρυπτογράφηση

Οι αλγόριθμοι συμμετρικής κρυπτογραφίας βασίζονται στην ύπαρξη ενός μόνο μυστικού κλειδιού που είναι γνωστό μόνο στα συναλλασσόμενα μέρη.

Αυτό το κλειδί χρησιμοποιείται τόσο για την κρυπτογράφηση, όσο και για την αποκρυπτογράφηση του μηνύματος.

Η συμμετρική κρυπτογραφία εγγυάται την εμπιστευτικότητα (confidentiality) των δεδομένων αφού κρυπτογραφεί το μήνυμα με ένα μυστικό κλειδί. Το μήνυμα που παράγεται αποκρυπτογραφείται από τον παραλήπτη με τη βοήθεια του ίδιου κλειδιού, το οποίο πρέπει να μένει μυστικό μεταξύ των δύο.

Παρόλο που η συμμετρική κρυπτογράφηση εγγυάται την εμπιστευτικότητα, δεν μπορεί να εγγυηθεί για το πως θα γίνει η ανταλλαγή του κλειδιού. Για να είναι ασφαλής η επικοινωνία θα πρέπει με κάποιο ασφαλή τρόπο να γίνει η ανταλλαγή του μυστικού κλειδιού. Σε περιπτώσεις που αποστολέας και παραλήπτης δεν γνωρίζονται, απαιτείται η ύπαρξη ενός ασφαλούς καναλιού επικοινωνίας για τη μεταφορά του κλειδιού. Συστήματα που επιτρέπουν την ασφαλή ανταλλαγή κλειδιών μέσα από δημόσια δίκτυα έχουν ήδη αναπτυχθεί και χρησιμοποιούνται σήμερα, με πιο διαδεδομένο το σύστημα Kerberos του MIT.

Ένα ακόμη σημαντικό θέμα αφορά την ταυτοποίηση μεταξύ του αποστολέα και του παραλήπτη. Το πρόβλημα της ταυτοποίησης έγκειται στο ότι πολλοί άνθρωποι μπορεί να έχουν πρόσβαση στο κοινό κλειδί. Αυτό το πρόβλημα μπορεί να το λύσει κρυπτογραφία δημοσίου κλειδιού που θα συζητηθεί παρακάτω.

Οι πιο γνωστοί αλγόριθμοι συμμετρικής κρυπτογραφίας είναι οι DES, IDEA, AES, RC2, RC4.

3.1.1 DES

Ο αλγόριθμος DES (Data Encryption Standard) αναπτύχθηκε από την IBM το 1970 και υιοθετήθηκε από την κυβέρνηση των ΗΠΑ το 1977. Χρησιμοποιεί το ίδιο κλειδί τόσο για την κρυπτογράφηση όσο και για την αποκρυπτογράφηση. Χρησιμοποιείται κυρίως σε εμπορικές εφαρμογές.

Ο κρυπτογραφικός αλγόριθμος DES είναι ένας αλγόριθμος τύπου Feistel [9], περιγραφή του οποίου υπάρχει στο παράρτημα, με δεκαέξι (16) ανακυκλώσεις (n=16). Το μήκος δέσμης αρχικού και κρυπτογραφημένου κειμένου είναι 64 και το μήκος του κλειδιού k είναι 56 bits. Αξίζει να σημειωθεί εδώ ότι τα κλειδιά του DES συνήθως αναπαρίστανται ως σειρές χαρακτήρων

των 64-bit, όπου 8 από τα bits παράγονται ως ψηφία ισοτιμίας (parity bits) των υπολοίπων 56. Ως αποτέλεσμα, μπορούν να υπάρξουν μόνο 2^{56} διαφορετικά κλειδιά για τον αλγόριθμο DES και για αυτό πρέπει να θεωρείται ότι το μήκος κλειδιού του αλγορίθμου DES είναι 56 bits [9].

3.1.2 IDEA

Ο αλγόριθμος IDEA (International Data Encryption Algorithm) αναπτύχθηκε από το Swiss Federal Institute of Technology το 1991. Χρησιμοποιεί κλειδιά των 128 bit και παρέχει ανθεκτικότερη κρυπτογράφηση από τον αλγόριθμο DES.

3.1.3 RC2, RC4 και AES

Οι κρυπτογραφικοί αλγόριθμοι RC2 και RC4 αναπτύχθηκαν από τον Ron Rivest της εταιρίας RSA Security. Βασικό χαρακτηριστικό τους είναι ότι υποστηρίζουν κλειδιά μεταβλητού μεγέθους. Αν το μέγεθος του κλειδιού είναι μεγαλύτερο των 56 bits είναι ανθεκτικότεροι από τον αλγόριθμο DES.

Ο αλγόριθμος AES (Advanced Encryption Standard) αναπτύχθηκε με πρωτοβουλία των ΗΠΑ (από το ινστιτούτο National Institute of Standards and Technology) με σκοπό την αντικατάσταση του DES και αναμένεται να αποτελέσει το νέο πρότυπο κρυπτογραφικού αλγόριθμου δέσμης. Ο αλγόριθμος AES έχει μήκος δέσμης και κλειδιού των 128bits.

3.2 Ασύμμετρη κρυπτογράφηση

Στο τέλος της δεκαετίας του 1970 οι Diffie και Hellman εφεύραν την κρυπτογραφία δημοσίου κλειδιού ή ασύμμετρη κρυπτογράφηση. Η βασική ιδέα είναι ότι ο αποστολέας και ο παραλήπτης δεν διαμοιράζονται ένα μυστικό κλειδί αλλά αντιθέτως έχουν διαφορετικά κλειδιά για διαφορετικές λειτουργίες.

Η κρυπτογράφηση δημοσίου κλειδιού περιλαμβάνει τη χρήση δύο κλειδιών:

- Ενός δημοσίου κλειδιού (public key)
- Ενός προσωπικού κλειδιού (private key)

Τα δεδομένα κρυπτογραφούνται με το δημόσιο κλειδί του παραλήπτη και αποστέλλονται. Όταν παραληφθούν αποκρυπτογραφούνται με το προσωπικό κλειδί του παραλήπτη. Τα δύο κλειδιά έχουν μαθηματική σχέση μεταξύ τους. Εάν το ένα χρησιμοποιηθεί για την κρυπτογράφηση της πληροφορίας το άλλο

θα χρησιμοποιηθεί για την αποκρυπτογράφησή της και αντίστροφα. Το όλο σύστημα βασίζεται στην παραδοχή ότι η γνώση του δημοσίου κλειδιού κρυπτογράφησης δεν επιτρέπει την ανακάλυψη του ιδιωτικού κλειδιού αποκρυπτογράφησης, δηλαδή είναι υπολογιστικά αδύνατο να βρει κανείς το κλειδί της αποκρυπτογράφησης από τη γνώση και μόνο του κλειδιού κρυπτογράφησης και του αλγορίθμου που χρησιμοποιήθηκε.

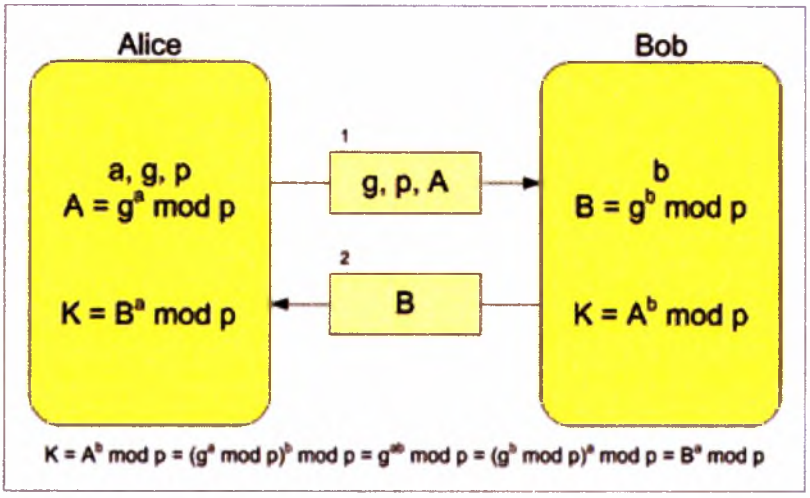
Οι πιο γνωστοί αλγόριθμοι ασύμμετρης κρυπτογραφίας είναι οι Diffie-Hellman, DSA και RSA. Ο τρόπος λειτουργίας των αλγορίθμων DH και RSA παρουσιάζεται στη συνέχεια.

3.2.1 Diffie-Hellman

Ο αλγόριθμος Diffie-Hellman (DH) ανακαλύφθηκε το 1976 από τους Whitfield Diffie και Martin Hellman. Υποθέτοντας ότι οι χρήστες Alice και Bob επιθυμούν να επικοινωνήσουν, ο αλγόριθμος DH [12] προτείνει τα ακόλουθα βήματα:

1. Οι δύο χρήστες καθορίζουν ένα σύνολο G (cyclic group) και την γεννήτρια του συνόλου g. Κάθε στοιχείο του συνόλου προκύπτει ως δύναμη του g. Η γεννήτρια g υποτίθεται ότι είναι γνωστή από όλους τους επίδοξους εχθρούς.
2. Η Alice επιλέγει έναν τυχαίο φυσικό αριθμό a και στέλνει στον Bob το g^a
3. Ο Bob επιλέγει με τη σειρά του ένα τυχαίο φυσικό αριθμό b και στέλνει στην Alice το g^b
4. Η Alice υπολογίζει το $(g^b)^a$.
5. Ο Bob υπολογίζει το $(g^a)^b$.

Στο τέλος της διαδικασίας οι δύο χρήστες έχουν στην κατοχή τους το στοιχείο του συνόλου G g^{ab} ($(g^b)^a = (g^a)^b$) το οποίο αποτελεί και το μυστικό κλειδί.



Εικόνα 3 : Diffie-Hellman key exchange

3.2.2 RSA

Το πρώτο πρακτικά χρήσιμο σύστημα δημοσίου κλειδιού αναπτύχθηκε από τους Rivest, Shamir και Adleman στα τέλη της δεκαετίας του 1970. Η ασφάλεια του συστήματος RSA βασίζεται στην δυσκολία εύρεσης των κοινών παραγόντων πολύ μεγάλων αριθμών.

Η επιλογή του δημόσιου και του κρυφού κλειδιού στον αλγόριθμο RSA [11] γίνεται με την ακόλουθη διαδικασία:

1. Επιλογή δύο τυχαίων μεγάλων πρώτων αριθμών p, q, λόγου χάριν, τουλάχιστον 200 bits.
2. Υπολογισμός του γινομένου n = p*q
3. Επιλογή ενός μικρού περιττού ακεραίου e, ο οποίος είναι σχετικώς πρώτος με το φ(n) = (p-1)(q-1)
4. Υπολογισμός του $d = e^{-1} \bmod \varphi(n)$
5. Ανακήρυξη του ζεύγους P = (e, n) ως δημοσίου κλειδιού RSA
6. Ορισμός του ζεύγους S = (d, n) ως μυστικού κλειδιού RSA

3.3 Σύγκριση Συμμετρικής και Ασύμμετρης κρυπτογράφησης

Το μεγαλύτερο πρόβλημα της συμμετρικής κρυπτογραφίας είναι η συνεννόηση και ανταλλαγή του κλειδιού, χωρίς κάποιος τρίτος να μάθει για αυτό. Η μετάδοση μέσα από το Διαδίκτυο δεν είναι ασφαλής γιατί οποιοσδήποτε γνωρίζει για την συναλλαγή και έχει τα κατάλληλα μέσα μπορεί να καταγράψει όλη την επικοινωνία μεταξύ αποστολέα και παραλήπτη και να

αποκτήσει το κλειδί. Έπειτα, μπορεί να διαβάσει, να τροποποιήσει και να πλαστογραφήσει όλα τα μηνύματα που ανταλλάσσουν οι δύο ανυποψίαστοι χρήστες. Βέβαια, μπορούν να βασισθούν σε άλλο μέσο επικοινωνίας για την μετάδοση του κλειδιού (π.χ. τηλεφωνία), αλλά ακόμα και έτσι δεν μπορεί να εξασφαλιστεί ότι κανείς δεν παρεμβάλλεται μεταξύ της γραμμής επικοινωνίας των χρηστών. Η ασύμμετρη κρυπτογραφία δίνει λύση σε αυτό το πρόβλημα αφού σε καμία περίπτωση δεν "ταξιδεύουν" στο δίκτυο οι εν λόγω ευαίσθητες πληροφορίες.

Άλλο ένα πλεονέκτημα των ασύμμετρων κρυπτοσυστημάτων είναι ότι μπορούν να παρέχουν ψηφιακές υπογραφές που δεν μπορούν να αποκηρυχθούν από την πηγή τους. Η πιστοποίηση ταυτότητας μέσω συμμετρικής κρυπτογράφησης απαιτεί την κοινή χρήση του ίδιου κλειδιού και πολλές φορές τα κλειδιά αποθηκεύονται σε υπολογιστές που κινδυνεύουν από εξωτερικές επιθέσεις. Σαν αποτέλεσμα, ο αποστολέας μπορεί να αποκηρύξει ένα πρωτύτερα υπογεγραμμένο μήνυμα, υποστηρίζοντας ότι το μυστικό κλειδί είχε κατά κάποιον τρόπο αποκαλυφθεί. Στην ασύμμετρη κρυπτογραφία δεν επιτρέπεται κάτι τέτοιο αφού κάθε χρήστης έχει αποκλειστική γνώση της ιδιωτική του κλείδας και είναι δικιά του ευθύνη η φύλαξη του.

Μειονέκτημα της ασύμμετρης κρυπτογραφίας είναι η ταχύτητα. Κατά κανόνα, η διαδικασία κρυπτογράφησης και πιστοποίησης ταυτότητας με συμμετρικό κλειδί είναι σημαντικά ταχύτερη από την κρυπτογράφηση και ψηφιακή υπογραφή με ζεύγος ασύμμετρων κλειδιών. Η ιδιότητα αυτή καλείται διασφάλιση της μη αποκήρυξης της πηγής (non-repudiation). Επίσης, τεράστιο μειονέκτημα της ασύμμετρης κρυπτογραφίας είναι η ανάγκη για πιστοποίηση και επαλήθευση των δημόσιων κλείδων από οργανισμούς (Certificate Authority) ώστε να διασφαλίζεται η κατοχή τους από τους νόμιμους χρήστες. Όταν κάποιος απατεώνας κατορθώσει και ξεγελάσει τον οργανισμό, μπορεί να συνδέσει το όνομα του με την δημόσια κλείδα ενός νόμιμου χρήστη και να προσποιείται την ταυτότητα αυτού του νόμιμου χρήστη.

Σε μερικές περιπτώσεις, η ασύμμετρη κρυπτογραφία δεν είναι απαραίτητη και η συμμετρική κρυπτογραφία από μόνη της είναι αρκετή. Τέτοιες περιπτώσεις είναι περιβάλλονται κλειστά, που δεν έχουν σύνδεση με

το Διαδίκτυο. Ένας υπολογιστής μπορεί να κρατά τα μυστικά κλειδιά των χρηστών που επιθυμούν να εξυπηρετηθούν από αυτόν, μια και δεν υπάρχει ο φόβος για κατάληψη της μηχανής από εξωτερικούς παράγοντες. Επίσης, στις περιπτώσεις που οι χρήστες μπορούν να συναντηθούν και να ανταλλάξουν τα κλειδιά ή όταν η κρυπτογράφηση χρησιμοποιείται για τοπική αποθήκευση κάποιων αρχείων, η ασύμμετρη κρυπτογραφία δεν είναι απαραίτητη.

Τα δύο κρυπτοσυστήματα μπορούν να εφαρμοστούν μαζί, συνδυάζοντας τα καλά τους χαρακτηριστικά και εξαλείφοντας τα μειονεκτήματα τους. Ένα παράδειγμα τέτοιου συνδυασμού είναι οι ψηφιακοί φάκελοι.

4. Simics

Το Simics είναι ένας αποδοτικός και «έξυπνος» προσομοιωτής. Δεν αποτελεί ένα μονοδιάστατο πρόγραμμα αλλά μία ολοκληρωμένη πλατφόρμα πάνω στην οποία ποικίλες εφαρμογές μπορούν να υλοποιηθούν. Η αποδοτικότητα συνδέεται με το γεγονός ότι το Simics είναι σχεδιασμένο να τρέχει προσομοιώσεις πολύ γρήγορα. Συχνά μία προσομοίωση στο Simics θα διαρκέσει τόσο χρόνο, όσο απαιτεί η αντίστοιχη εφαρμογή σε πραγματικό hardware, ή και ακόμα γρηγορότερα. Συγκεκριμένα, στην κατηγορία του, το Simics αποτελεί το γρηγορότερο προσομοιωτή που έχει υλοποιηθεί. Επιπλέον, το Simics δεν σχεδιάστηκε ώστε απλά να τρέχει μία εφαρμογή όσο το δυνατόν γρηγορότερα, αλλά να συλλέγει πλήθος πληροφοριών κατά τη διάρκεια της προσομοίωσης. Το χαρακτηριστικό της καλής απόδοσης επιτυγχάνεται ακόμα και με εφαρμογές με υψηλή πολυπλοκότητα και μεγάλο όγκο δεδομένων προς επεξεργασία παρέχοντας μία ποικιλία δυνατοτήτων και διαφόρων στατιστικών για ανάλυση.

Το Simics παρέχει δυνατότητες προσομοίωσης διαφόρων τεχνολογιών, μεγάλος αριθμός των οποίων είναι διαθέσιμος προς τους χρήστες είτε για ακαδημαϊκή είτε για προσωπική χρήση και έρευνα. Μερικά παραδείγματα αποτελούν οι επεξεργαστές x86 με δυνατότητες υποστήριξης από τον 486sx έως και τους Pentium 4 και AMD64, ο επεξεργαστής 64-bit PowerPC 970FX, ο 32-bit PowerPC 750, ο ARM SA1110 που μοντελοποιεί ένα ARMv5 επεξεργαστή καθώς και πολλοί άλλοι [2]. Ο ARM SA1110 είναι η πλατφόρμα η οποία χρησιμοποιήθηκε για την πραγματοποίηση των μετρήσεων που παρατίθενται στο πέμπτο κεφάλαιο.

Το σύστημα ARM SA1110 περιλαμβάνει ένα επεξεργαστή ARMv5 με συχνότητα λειτουργίας 30 MHz, 32MB μνήμης και υποστηρίζει μία έκδοση του Linux με ιδιαίτερα περιορισμένες δυνατότητες. Περιλαμβάνει άλλα δύο αρχεία, το vmlinux (το αρχείο αυτό περιλαμβάνει το πυρήνα Linux Kernel) και το initrd (το συγκεκριμένο αρχείο περιλαμβάνει το initrd δίσκο RAM για το Linux), τα οποία φορτώνονται απευθείας στην κύρια μνήμη του υπολογιστή καθώς δεν υπάρχουν μοντελοποιημένες άλλες συσκευές αποθήκευσης. Επιπλέον είναι διαθέσιμη και μία δεύτερη έκδοση του ARM SA1110 με αναβαθμισμένα χαρακτηριστικά ταχύτητας και δυνατοτήτων αποθήκευσης. Διαθέτει 128 MB

μνήμης και 32 MB initrd. Αντίθετα με την πρώτη έκδοση του ARM η συγκεκριμένη περιλαμβάνει το χαρακτηριστικό simicsfs. Το simicsfs προσφέρει πρόσβαση στα αρχεία του πραγματικού υπολογιστικού συστήματος μέσα από τη πλατφόρμα προσομοίωσης (simulated machine). Η ευχρηστία που προσδίδει είναι τεράστια με την απλοποίηση της διαδικασίας εισαγωγής αρχείων στο σύστημα που προσομοιώνεται.

Μετά τη δημιουργία του προσωπικού χώρου αποθήκευσης ακολουθεί η εκκίνηση του Simics. Εμφανίζεται ένα περιβάλλον εντολών όπου αρχικά πρέπει να γίνει η επιλογή της πλατφόρμας η οποία πρόκειται να μελετηθεί. Επιπλέον, στο σημείο αυτό υπάρχει η δυνατότητα καθορισμού της συχνότητας λειτουργίας καθώς και του επιθυμητού μεγέθους της μνήμης με απλή ανάθεση τιμών σε δύο μεταβλητές. Συγκεκριμένα χρησιμοποιείται η ακόλουθη εντολή στη γραμμή εντολών του Simics:

- $freq_mhz = 200,

για τον ορισμό της ταχύτητας στα 200 MHz, ενώ η εντολή

- $memory_megs = 32

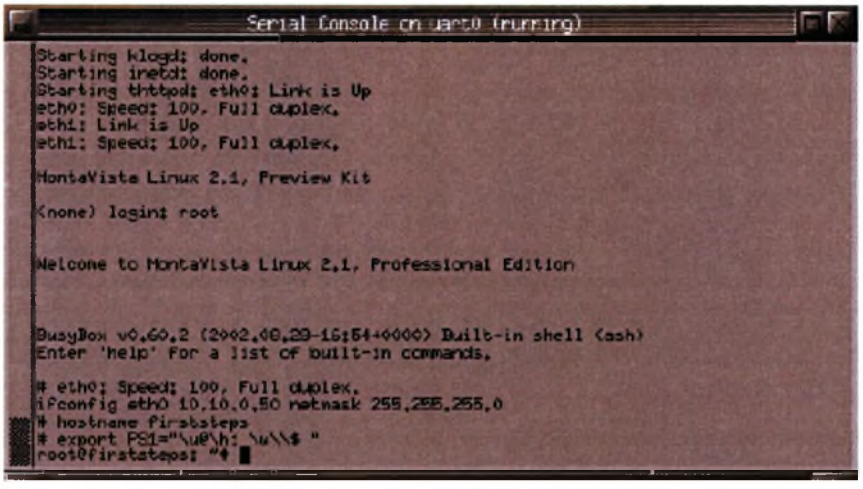
θέτει το μέγεθος της RAM στα 32 MB. Κάνοντας χρήση των παραπάνω εντολών και υποθέτοντας ότι ο ARM αποτελεί την πλατφόρμα επιλογής, τότε θα λειτουργεί στα 200 MHz και θα διαθέτει 32 MB ram. Δηλαδή υπάρχει η δυνατότητα μεταβολής της συχνότητας λειτουργίας του ρολογιού του συστήματος προσομοίωσης. Ωστόσο στο σημείο αυτό πρέπει να τονιστεί ότι η μεταβολή αυτή στην ταχύτητα δεν επηρεάζει την πραγματική ταχύτητα της προσομοίωσης, αλλά μόνο τον αριθμό των εντολών που πρέπει να εκτελεστούν σε ένα συγκεκριμένο διάστημα χρόνου προσομοίωσης. Δηλαδή αν η εφαρμογή βασίζεται αποκλειστικά σε ένα συγκεκριμένο αριθμό εντολών οι οποίες πρέπει να εκτελεστούν, τότε αυξάνοντας τη συχνότητα ρολογιού ο χρόνος εκτέλεσης θα παραμείνει ίδιος για το πραγματικό υπολογιστικό σύστημα (αλλά η εφαρμογή για το σύστημα προσομοίωσης θα εκτελεστεί γρηγορότερα).

Η επιλογή της πλατφόρμας ARM SA1110 πραγματοποιείται ως εξής :

pakostar@computer: simics-workspace$ **./simics /targets/arm-sa1110/ sa1110-linux-large-common.simics**

Πληκτρολογώντας continue στη γραμμή εντολών του Simics ξεκινά η διαδικασία εκκίνησης προσομοίωσης της πλατφόρμας επιλογής και τελικά

εμφανίζεται ένα παράθυρο σαν αυτό εικόνας 4 (η συγκεκριμένη εικόνα αποτελεί στιγμιότυπο της διαδικασία εκκίνησης του Montavista Linux). Η διαχείριση των αρχείων της κονσόλας του ARM πραγματοποιείται με τη χρήση του busybox. Το busybox αποτελεί μία εφαρμογή που περιλαμβάνει υλοποιήσεις περιορισμένου αριθμού εντολών διαχείρισης δεδομένων. Εντολές όπως busybox mkdir temp για τη δημιουργία ενός φακέλου με την ονομασία temp και busybox rmdir temp για τη διαγραφή του φακέλου temp αποτελούν δύο παραδείγματα. Η χρήση του συνδυασμού πλήκτρων Ctrl-C διακόπτει τη διαδικασία λειτουργίας της πλατφόρμας προσομοίωσης ώστε να επιστρέψει ο έλεγχος στη γραμμή εντολών του Simics.



Εικόνα 4 : Montavista Linux

Αρχικός στόχος ήταν η πραγματοποίηση μετρήσεων χρόνων παραγωγής κλειδιών και διάρκειας κρυπτογράφησης–αποκρυπτογράφησης ενός αρχείου φωνής, χρησιμοποιώντας ως πλατφόρμα τον επεξεργαστή ARM SA1110 και η ανάδειξη της ελάχιστης συχνότητας ρολογιού και μνήμης RAM οι οποίες θα μπορούσαν να υποστηρίξουν ικανοποιητικά τις δύο διαδικασίες. Συγκεκριμένα, επειδή πρόκειται για voice communications πρέπει να μην υπάρχει καθυστέρηση σε επίπεδο CPU για τις διαδικασίες encoding–decoding. Επομένως ο στόχος ήταν ο καθορισμός του «ελάχιστου» εκείνου configuration για τον ARM που επιτρέπει τη λειτουργία των εφαρμογών χωρίς διακοπές (ο επεξεργαστής δεν πρέπει να φτάνει ποτέ το 100% των δυνατοτήτων του καθώς εκτελεί όλες μαζί τις διεργασίες). Σε πρώτη φάση η βιβλιοθήκη που χρησιμοποιήθηκε για τη δημιουργία των προγραμμάτων ήταν η OpenSSL crypto [4]. Η συγκεκριμένη βιβλιοθήκη περιλαμβάνει μεγάλη

ποικιλία τόσο συμμετρικών αλγορίθμων (blowfish, idea, rc5, des), όσο και ασύμμετρων (Diffie-Helmann, DSA) που χρησιμοποιούνται σήμερα σε διάφορα πρότυπα στο διαδίκτυο. Για κάθε αλγόριθμο διαθέτει πλήθος συναρτήσεων όπως παραγωγή κλειδιών με μέγεθος καθορισμένο από το χρήστη, συναρτήσεις κρυπτογράφησης–αποκρυπτογράφησης αρχείων, συναρτήσεις για το καθορισμό παραμέτρων του εκάστοτε αλγορίθμου κ.α.

Με την ολοκλήρωση των προγραμμάτων έπρεπε να βρεθεί κάποιος τρόπος γνώσης της διάρκειας εκτέλεσής τους στο Simics. Η απουσία compiler, καθώς και οποιουδήποτε άλλου εργαλείου που να είναι χρήσιμο για τη διεξαγωγή των μετρήσεων (όπως ειπώθηκε και προηγουμένως η συγκεκριμένη πλατφόρμα είναι ιδιαίτερα περιορισμένη σε ικανότητες και σε διαθέσιμο χώρο) δεν επέτρεπε τη χρήση κάποιας μεθόδου υπολογισμού χρόνου της γλώσσας προγραμματισμού με την οποία υλοποιήθηκαν τα προγράμματα. Λύση στο συγκεκριμένο ζήτημα δόθηκε από το ίδιο το Simics. Χρησιμοποιήθηκαν οι εντολές «magic-breakpoint». Ο τρόπος χρήσης τους είναι ιδιαίτερα απλός. Τοποθετείς δύο εντολές στο κομμάτι κώδικα στο οποίο πρόκειται να πραγματοποιήσεις τις μετρήσεις σου, μία στην αρχή του και μία στο τέλος. Επιπλέον στην αρχή του προγράμματος δηλώνεις και το header file «magic-instruction.h» το οποίο περιλαμβάνει τις υλοποιήσεις των εντολών «magic-breakpoint» για διάφορες τεχνολογίες και πολλούς compiler. Έπειτα ακολουθεί εκτέλεση του προγράμματος. Μόλις ο compiler διαβάσει την εντολή «magic-breakpoint» θα διακόψει τη λειτουργία της πλατφόρμας (ARM) και θα επιστρέψει τον έλεγχο στη γραμμή εντολών του Simics. Στη γραμμή εντολών του Simics χρησιμοποιείται η εντολή «ptime» η οποία και επιστρέφει τον αριθμό των εντολών που έχουν εκτελεστεί και το χρόνο προσομοίωσης που έχει περάσει από τη στιγμή που έχει ξεκινήσει η προσομοίωση. Πραγματοποιώντας την ίδια διαδικασία όταν ο compiler συναντήσει τη δεύτερη εντολή «magic-breakpoint», είναι ιδιαίτερα εύκολο με απλή αφαίρεση των δύο χρόνων να γνωρίζουμε πόσο χρόνο διήρκεσε το κομμάτι κώδικα που μας ενδιαφέρει.

Με την ολοκλήρωση και του δεύτερου προγράμματος, ο στόχος του οποίου ήταν η διεξαγωγή κρυπτογράφησης–αποκρυπτογράφησης ενός αρχείου φωνής, ακολούθησε μελέτη του codec ο οποίος πραγματοποιεί την κωδικοποίηση και την αποκωδικοποίηση των δεδομένων. Η λέξη codec είναι

η συντόμευση των αγγλικών λέξεων compressor/decompressor και αναφέρεται σε κάθε τεχνολογία συμπίεσης και αποσυμπίεσης δεδομένων. Οι codecs μπορούν να υλοποιηθούν σε επίπεδο software, σε επίπεδο hardware ή σε συνδυασμό και των δύο. Ο codec που χρησιμοποιήθηκε ήταν ο speex [1]. Ο κώδικας του είναι διαθέσιμος στο ευρύ κοινό είτε για επιστημονική, είτε για ακαδημαϊκή χρήση. Είναι ιδιαίτερα εύχρηστος και διαθέτει πλήθος επιλογών για τη διαμόρφωση της ποιότητας της κωδικοποίησης. Είναι σχεδιασμένος για 3 διαφορετικές συχνότητες δειγματοληψίας, 8 kHz, 16 kHz και 32 kHz. Επιπλέον παρέχεται η δυνατότητα καθορισμού της ποιότητας της κωδικοποίησης με μία παράμετρο που παίρνει τιμές από μηδέν έως και δέκα με τις μεγαλύτερες τιμές να υποδεικνύουν καλύτερη ποιότητα. Στο πακέτο του Speex συμπεριλαμβάνονται δύο εφαρμογές, τα speexenc και speexdec, τα οποία πραγματοποιούν κωδικοποίηση και αποκωδικοποίηση αντίστοιχα. Δηλαδή μετά την εγκατάσταση του Speex υπάρχει η δυνατότητα χρήσης των ακόλουθων εντολών σε ένα shell του Linux για την πραγματοποίηση κωδικοποίησης-αποκωδικοποίησης ενός αρχείου :

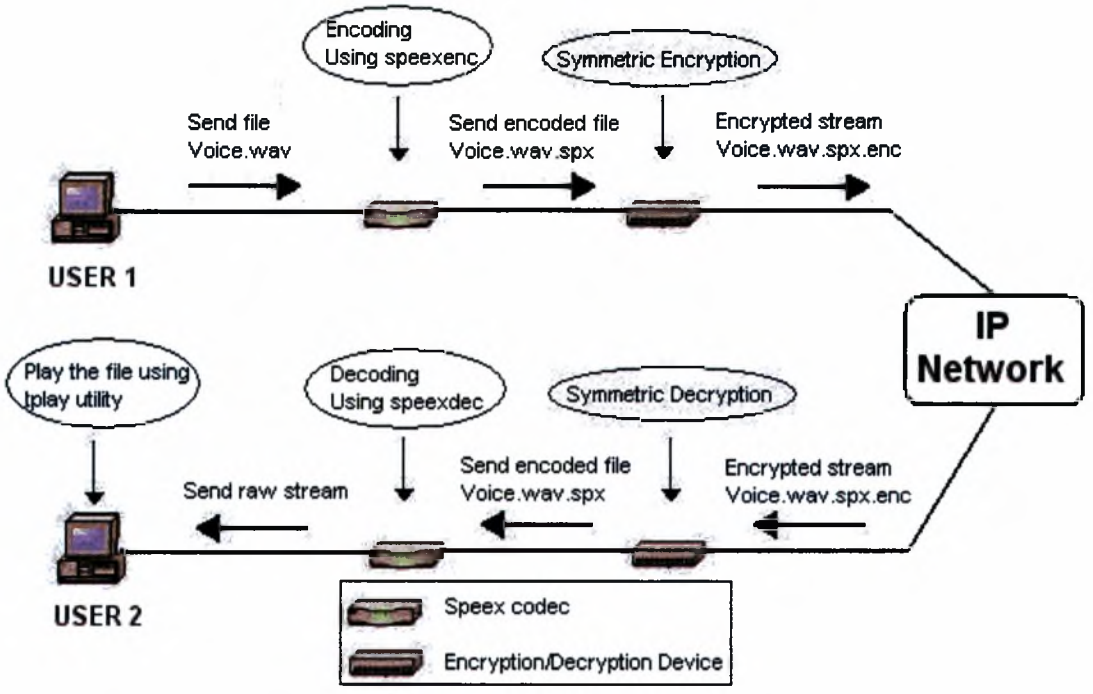
speexenc [options] input_file output_file (κωδικοποίηση)
speexdec [options] speex_file output_file (αποκωδικοποίηση)

Στα "options" παρέχονται ποικίλες δυνατότητες διαμόρφωσης της κωδικοποίησης. Κάποιες από τις διαθέσιμες επιλογές είναι :

- ο καθορισμός της ποιότητας κωδικοποίησης (-quality n, όπου το n παίρνει τιμές από 0 έως 10),
- υπόδειξη της συχνότητας δειγματοληψίας (-narrowband για δειγματοληψία στα 8 kHz, -wideband για δειγματοληψία στα 16 kHz και -ultra-wideband για δειγματοληψία στα 32 kHz),
- εμφάνιση στην οθόνη ενός εγχειριδίου βοήθειας του Speex με επεξήγηση κάθε πιθανής επιλογής διαμόρφωσης με χρήση της παραμέτρου –help.

Μετά την κατανόηση της λειτουργίας του Speex είχε πλέον διαμορφωθεί το τελικό σχήμα για το οποίο έπρεπε να πραγματοποιηθούν οι μετρήσεις για επεξεργασία σε πραγματικό χρόνο (real time processing).

ΣΧΗΜΑ 1



Πρέπει να αναφερθεί ότι οι συσκευές που χρησιμοποιούνται στο σχήμα 1 ως μεμονωμένοι σταθμοί στην πραγματικότητα αποτελούν κομμάτι του υπολογιστή του εκάστοτε χρήστη. Η συγκεκριμένη απλοποίηση έγινε για λόγους εμπέδωσης του συνόλου της διαδικασίας. Αρχικά ο πρώτος χρήστης (USER 1) στέλνει ένα αρχείο ήχου, το voice.wav, το οποίο κωδικοποιείται με τη χρήση της εφαρμογής που ο Codec Speex προσφέρει, speexenc, και προκύπτει το αρχείο voice.wav.spx. Έπειτα το κωδικοποιημένο αρχείο χρησιμοποιείται ως είσοδος για το πρόγραμμα το οποίο και εκτελεί την κρυπτογράφηση (στην εικόνα αντί για το πρόγραμμα χρησιμοποιείται μία συσκευή για τις διαδικασίες κρυπτογράφησης–αποκρυπτογράφησης αποκλειστικά για λόγους απεικόνισης) και τελικά προκύπτει το κρυπτογραφημένο αρχείο voice.wav.spx.encrypted. Το συγκεκριμένο αρχείο αποκρυπτογραφείται για να προκύψει το αρχείο με κατάληξη .spx, το οποίο αποκωδικοποιείται για την απόκτηση του αρχείου ήχου που τελικά παραλαμβάνεται από τον χρήστη 2 (USER 2). Τέλος χρησιμοποιείται μία ειδική εφαρμογή, ικανή για την αναπαραγωγή του αρχείου ήχου στην τελική του μορφή. Το πρόγραμμα που χρησιμοποιήθηκε για την αναπαραγωγή των αρχείων που προκύπτουν από τη συγκεκριμένη διαδικασία είναι ο tplay [13].

Τέλος σημειώνεται ότι οι μετρήσεις αφορούν αποκλειστικά χρόνους ταυτόχρονης κρυπτογράφησης-αποκρυπτογράφησης και όχι χρόνους διέλευσης των πακέτων στο δίκτυο.

Ωστόσο κατά τη διάρκεια ελέγχου της λειτουργίας του codec στον ARM προέκυψε ένα σφάλμα. Ένα σφάλμα αρχιτεκτονικής του Simics. Όταν προσπαθούσα να κωδικοποιήσω ή να αποκωδικοποιήσω ένα αρχείο ήχου τότε προέκυπτε segmentation fault. Παρόμοια ήταν τα αποτελέσματα και στην περίπτωση ενός δεύτερου codec, του GSM. Στην εικόνα 5 παρουσιάζονται τα αποτελέσματα της προσπάθειας κωδικοποίησης ενός αρχείου ήχου (male_speex_8.wav) με τη χρήση του codec Speex. Το ίδιο αποτέλεσμα προέκυπτε και για κάθε άλλο αρχείο ήχου που δοκιμάστηκε. Ακολούθησε κοινοποίηση του προβλήματος στους ανθρώπους της Simics, οι οποίοι το έλεγξαν προσωπικά για να διαπιστώσουν αν πραγματικά πρόκειται για ένα σφάλμα του Simics και του ARM ή αν το πρόβλημα οφείλεται στον codec (Speex). Τελικά διαπιστώθηκε ότι το πρόβλημα προέρχεται από την πλατφόρμα του Simics. Ωστόσο, τρεις μήνες μετά, κατά τη διάρκεια συγγραφής της διπλωματικής εργασίας, δεν υπάρχει κάποια πρόοδος παρά τις υποσχέσεις για ταχύτατη διευθέτηση του προβλήματος .

```
/bin # ./speexenc male_speex_8.wav male_speex_8.wav.spx
Encoding 8000 Hz audio using narrowband mode (mono)
Unhandled fault: terminal exception (2) at 0x3fc6dace
pgd = c23e8000
*pgd = 00000000, *pmd = 00000000
Internal error: 0ops: 0
CPU: 0
pc : [<c00dcfec>]    lr : [<coocf988>]   Not tainted
sp : c23edf80  ip : c23ec274  fp : 00000000
r10 : 00010000  r9 : 00000001  r8 : 00000000
r7 : 3fc6daca   r6 : c23ec000  r5 : 3fc6daca  r4 : cd1191b1
r3 : c23ec278  r2 : 00000002  r1 : bfffffc    r0 : 3fc6dace
Flags: nzcv  IRQs on FIQs on Mode SVC_32 Segment user
Control: 317F  Table:  C23E8000  DAC: 00000015
Process speexenc  (pid: 65, stackpage=c23ed000)
Stack:
c23edf60:                                          c00cf988 c00dcfec 00000013 ffffff
ff
c23edf80: cd1191b1 c23ec268 00000000 80000093  40179cf0  c00137bc c001374c c00cff
30
c23edfa0: c00cf634 c23edfb8 40179cf4 80000010 0000317f  c00db508 3fc6dd8e 3fc6dd
8e
c23edfc0: 20000000 7feffffe 3fc6dd8e 20000000 0001bd50 00000004 0001e704  0001f8
38
c23edfe0: 401e4e3c bfffd70c bfffd710 bfffcf84  00000000 40179cf4  80000010 ffffff
ff
Backtrace: no frame pointer
Code: e2411004 e1500001 (94b01000) 93a0000 91a0f00e
Segmentation fault
```

Εικόνα 5 : Simics failure

4.1 Συμπεράσματα

Συνοψίζοντας, στα θετικά του Simics συγκαταλέγεται το πληρέστατο εγχειρίδιο που διαθέτει, το οποίο παρέχει πληροφορίες για κάθε λεπτομέρεια του προγράμματος καθώς και οδηγίες για τη πλήρη εκμετάλλευση όλων των δυνατοτήτων του, το άμεσο forum το οποίο ανανεώνεται και ενημερώνεται ταχύτατα, το γεγονός ότι αποτελεί open-source εφαρμογή και ο καθένας μπορεί να πειραματιστεί τροποποιώντας τον κώδικα του προγράμματος και τέλος η παροχή δυνατοτήτων επεξεργασίας ενός μεγάλου αριθμού πλατφόρμων (ARM, x86, AlphaPC, PowerPC κοκ). Στα αρνητικά συγκαταλέγεται η νεότητα του προγράμματος, με όσα προβλήματα αυτό συνεπάγεται (για παράδειγμα το σφάλμα του ARM που ανέφερα προηγουμένως), το γεγονός ότι ορισμένες πλατφόρμες, με πιο χαρακτηριστική αυτή του ARM, διαθέτουν ιδιαίτερα περιορισμένες δυνατότητες (η αρχική έκδοση του ARM δεν περιλαμβάνει Simicsfs για τη γρήγορη μεταφορά αρχείων από το πραγματικό υπολογιστικό σύστημα στο σύστημα προσομοίωσης και είναι διαθέσιμη αποκλειστικά με 32MB μνήμης – τα 16 χρησιμοποιούνται από το ίδιο το σύστημα, οπότε μπορείς να χρησιμοποιήσεις μόνο 16– χαρακτηριστικό που αποτρέπει τη χρήση benchmarks και βιβλιοθηκών μεγάλου μεγέθους).

5. Μετρήσεις στο Simics (παραγωγή κλειδιών)

Στο Simics πραγματοποιήθηκαν μετρήσεις που αφορούσαν χρόνους παραγωγής κλειδιών. Οι συμμετρικοί αλγόριθμοι που χρησιμοποιήθηκαν στις μετρήσεις ήταν οι ακόλουθοι :

- RC5,
- IDEA,
- Blowfish,
- 3DES,

ενώ οι ασύμμετροι :

- Diffie-Helmann
- DSA

Οι μετρήσεις πραγματοποιήθηκαν για συχνότητες των 100 MHz, 133 MHz, 166 MHz, 200 MHz, 233 MHz, 266 MHz, 300 MHz, 400 MHz και 533 MHz. Τα μεγέθη κλειδιών που χρησιμοποιήθηκαν για τους συμμετρικούς αλγορίθμους είναι 128, 160,192 και 256 bits. Αντίστοιχα, τα μεγέθη για τους αλγορίθμους ασύμμετρης κρυπτογράφησης είναι 1024,2048 και 4096 bits.

Ο πίνακας 1 περιλαμβάνει τις μετρήσεις για τον συμμετρικό αλγόριθμο RC5 στη συχνότητα των 100 MHz. Οι δύο πρώτες στήλες περιλαμβάνουν την ονομασία του αλγορίθμου και το μέγεθος του κλειδιού που χρησιμοποιείται, ενώ οι δύο επόμενες τον αλγόριθμο ασύμμετρης κρυπτογράφησης με το αντίστοιχο μέγεθος ζεύγους κλειδιών. Η στήλη Total time περιλαμβάνει το χρόνο για το σύνολο της διαδικασίας. Περαιτέρω μετρήσεις παρατίθενται στο παράρτημα.

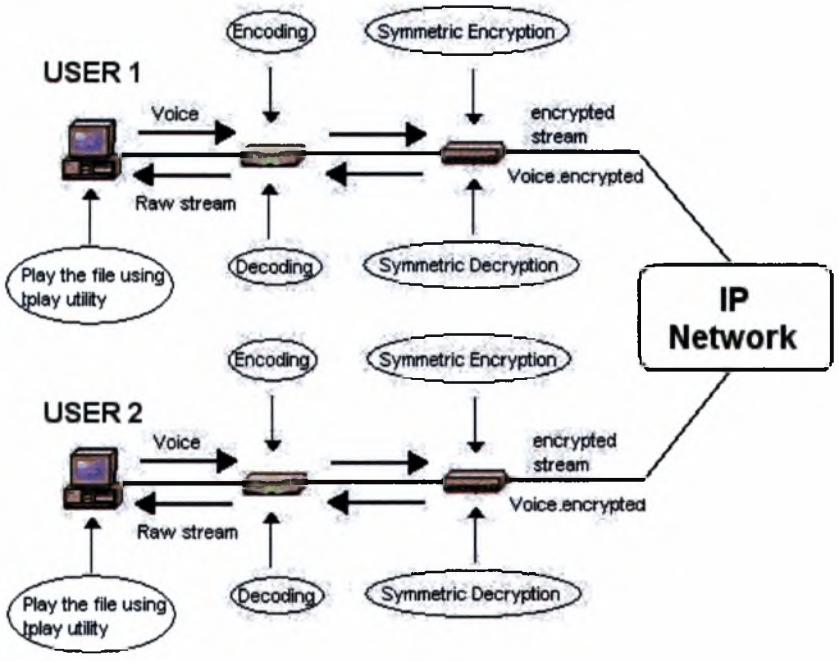
Πίνακας 1 : Μειρήσεις RC5 στα 100 MHz

	Key Length		Key Length			Time 1	Time 2	Total time(seconds)
RC5	128	DH	1024	ARM 100	→	0,006	1,042	**1,048**
RC5	160	DH	1024	ARM 100	→	0,007	1,042	**1,049**
RC5	192	DH	1024	ARM 100	→	0,007	1,042	**1,049**
RC5	256	DH	1024	ARM 100	→	0,007	1,042	**1,049**
RC5	128	DSA	1024	ARM 100	→	0,006	8,084	**8,09**
RC5	160	DSA	1024	ARM 100	→	0,007	8,084	**8,091**
RC5	192	DSA	1024	ARM 100	→	0,007	8,084	**8,091**
RC5	256	DSA	1024	ARM 100	→	0,007	8,084	**8,091**
RC5	128	DH	2048	ARM 100	→	0,006	5,151	**5,157**
RC5	160	DH	2048	ARM 100	→	0,007	5,151	**5,158**
RC5	192	DH	2048	ARM 100	→	0,007	5,151	**5,158**
RC5	256	DH	2048	ARM 100	→	0,007	5,151	**5,158**
RC5	128	DSA	2048	ARM 100	→	0,006	8,331	**8,337**
RC5	160	DSA	2048	ARM 100	→	0,007	8,331	**8,338**
RC5	192	DSA	2048	ARM 100	→	0,007	8,331	**8,338**
RC5	256	DSA	2048	ARM 100	→	0,007	8,331	**8,338**
RC5	128	DH	4096	ARM 100	→	0,006	32,051	**32,057**
RC5	160	DH	4096	ARM 100	→	0,007	32,051	**32,058**
RC5	192	DH	4096	ARM 100	→	0,007	32,051	**32,058**
RC5	256	DH	4096	ARM 100	→	0,007	32,051	**32,058**
RC5	128	DSA	4096	ARM 100	→	0,006	9,449	**9,455**
RC5	160	DSA	4096	ARM 100	→	0,007	9,449	**9,456**
RC5	192	DSA	4096	ARM 100	→	0,007	9,449	**9,456**
RC5	256	DSA	4096	ARM 100	→	0,007	9,449	**9,456**

6. Μετρήσεις για παραγωγή κλειδιών – κρυπτογράφηση / αποκρυπτογράφηση φωνής

Μετά την αδυναμία του Simics να εκτελέσει τις διαδικασίες της κρυπτογράφησης και αποκρυπτογράφησης ακολούθησαν μετρήσεις στο υπολογιστικό σύστημα του εργαστηρίου της σχολής, χωρίς τη χρήση του Simics ή κάποιου άλλου προσομοιωτή. Στόχος ήταν η πραγματοποίηση μετρήσεων χρόνου για τη παραγωγή κλειδιών των αλγορίθμων που αναφέρθηκαν προηγουμένως. Επιπλέον έπρεπε να πραγματοποιηθούν μετρήσεις για το παρακάτω σχήμα :

Σχήμα 2



Το σχήμα 2 υποδηλώνει ότι η φωνή ενός από τους δύο χρήστες κωδικοποιείται και στη συνέχεια κρυπτογραφείται με αποτέλεσμα τη δημιουργία ενός αρχείου που εδώ αναφέρεται σαν encrypted stream, ενώ παράλληλα η φωνή του δεύτερου χρήστη αποκρυπτογραφείται και αποκωδικοποιείται για να παραχθεί τελικά το raw stream, το οποίο και αναπαράγεται στον player tplay (utility ικανό να αναπαράγει raw stream).

Τα τεχνικά χαρακτηριστικά του υπολογιστικού συστήματος στο οποίο πραγματοποιήθηκαν οι μετρήσεις καθώς και τα χαρακτηριστικά του αρχείου ήχου που χρησιμοποιήθηκε για τη διεξαγωγή των μετρήσεων παρατίθενται στη συνέχεια :

Τεχνικά χαρακτηριστικά του τερματικού συστήματος

Τα τεχνικά χαρακτηριστικά του υπολογιστικού συστήματος στο οποίο πραγματοποιήθηκαν οι μετρήσεις περιλαμβάνονται στον πίνακα 2 :

Πίνακας 2 : Τεχνικά χαρακτηριστικά του Η/Υ

Επεξεργαστής	Intel Pentium
Ταχύτητα	3.00 GHz
Μνήμη (RAM)	1.00 GB
Λειτουργικό Σύστημα	SUSE Linux 9.3

Χαρακτηριστικά του αρχείου ήχου που χρησιμοποιήθηκε στις μετρήσεις

Στις μετρήσεις που πραγματοποιήθηκαν χρησιμοποιήθηκε ένα αρχείο φωνής με τα ακόλουθα χαρακτηριστικά :

Πίνακας 3 : Χαρακτηριστικά του αρχείου music.wav

Μέγεθος	4.3 MB
Sample rate	8 kHz
Sample size	16 bits
Χρονική διάρκεια αρχείου	4 λεπτά και 40 δευτερόλεπτα

Χρησιμοποιώντας το πρόγραμμα παραγωγής κλειδιών για τους αλγορίθμους συμμετρικής και ασύμμετρης κρυπτογράφησης προέκυψε ο πίνακας 4. Η πρώτη στήλη περιλαμβάνει τους αλγορίθμους συμμετρικής κρυπτογράφησης RC5, IDEA, Blowfish, 3DES και ασύμμετρης κρυπτογράφησης DH, DSA. Η δεύτερη στήλη περιέχει τα μήκη κλειδιών για τα οποία πραγματοποιήθηκαν οι μετρήσεις και συγκεκριμένα 128, 160, 192, 256 για αλγορίθμους συμμετρικής κρυπτογράφησης και 1024, 2048, 4096 για τους αλγορίθμους ασύμμετρης κρυπτογράφησης. Η τελευταία στήλη με τον τίτλο Samples περιέχει τμήμα του συνόλου των μετρήσεων που πραγματοποιήθηκαν για κάθε μήκος κλειδιού, κάθε αλγορίθμου ξεχωριστά. Τέλος η τρίτη στήλη με την ονομασία Time αποτελεί τον τελικό προσεγγιστικό χρόνο για κάθε περίπτωση (ο κάθε χρόνος αποτελεί μέσο όρο από περίπου 20 μετρήσεις που πραγματοποιήθηκαν για κάθε συνδυασμό αλγορίθμου-κλειδιού μέρος των οποίων υπάρχει στην στήλη Samples).

Πίνακας 4 : Χρόνοι παραγωγής κλειδιών αλγορίθμων συμμετρικής και ασύμμετρης κρυπτογράφησης

Algorithm	Key length	Time (in msec)	Samples (msec)
RC5	128 bit	0.565	0.563, 0.566, 0.562, 0.567, 0.567, 0.565, 0.570, 0.569, 0.559, 0.566
	160 bit	0.565	0.563, 0.562, 0.569, 0.568, 0.570, 0.568, 0.558, 0.566, 0.570, 0.558
	192 bit	0.567	0.571, 0.572, 0.568, 0.562, 0.560, 0.560, 0.570, 0.570
	256 bit	0.570	0.576, 0.563, 0.561, 0.575, 0.562, 0.574, 0.568, 0.569, 0.572, 0.582
IDEA	128 bit	0.555	0.554, 0.553, 0.560, 0.554, 0.552, 0.556, 0.553, 0.559
	160 bit	0.562	0.560, 0.567, 0.554, 0.565, 0.566, 0.562, 0.564, 0.562
	192 bit	0.563	0.564, 0.564, 0.557, 0.574, 0.565, 0.566, 0.554, 0.567
	256 bit	0.564	0.564, 0.561, 0.574, 0.557, 0.566, 0.579, 0.554, 0.559
Blowfish	128 bit	0.645	0.646, 0.650, 0.650, 0.646, 0.647, 0.635, 0.647, 0.646
	160 bit	0.683	0.684, 0.683, 0.693, 0.688, 0.684, 0.676, 0.676, 0.684
	192 bit	0.685	0.690, 0.685, 0.686, 0.686, 0.685, 0.676, 0.692, 0.687
	256 bit	0.720	
3DES	128 bit	0.593	0.590, 0.595, 0.587, 0.596, 0.597, 0.597, 0.594, 0.589
	160 bit	0.596	0.592, 0.590, 0.599, 0.601, 0.605, 0.590, 0.591, 0.602
	192 bit	0.614	0.612, 0.608, 0.618, 0.611, 0.609, 0.621, 0.620, 0.619
	256 bit	0.635	0.635, 0.637, 0.639, 0.635, 0.634, 0.638, 0.637, 0.630
DH	1024 bit	24.448	28.978, 24.391, 22.960, 22.823, 21.956, 25.506, 24.528
	2048 bit	98.868	99.189, 97.457, 95.105, 111.482, 90.708, 101.348, 96.787
	4096 bit	525.254	516.537, 525.982, 525.481, 521.821, 530.779, 530.926
DSA	1024 bit	152.193	152.398, 151.486, 152.733, 151.501, 153.115, 151.891, 152.229
	2048 bit	156.891	156.287, 156.689, 156.532, 159.318, 156.277, 156.694, 156.443
	4096 bit	176.004	174.875, 174.587, 174.451, 181.041, 174.255, 174.309, 174.710, 179.804

Στη συνέχεια πραγματοποιήθηκαν μετρήσεις για το καθορισμό της διάρκειας των διαδικασιών κωδικοποίησης-αποκωδικοποίησης και κρυπτογράφησης-αποκρυπτογράφησης. Η ακόλουθη εντολή χρησιμοποιήθηκε στη γραμμή εντολών του Linux (shell) :

- speexenc music.wav - | testenc > music.wav.spx.enc && testdec < music.wav.spx.enc | speexdec - music.wav

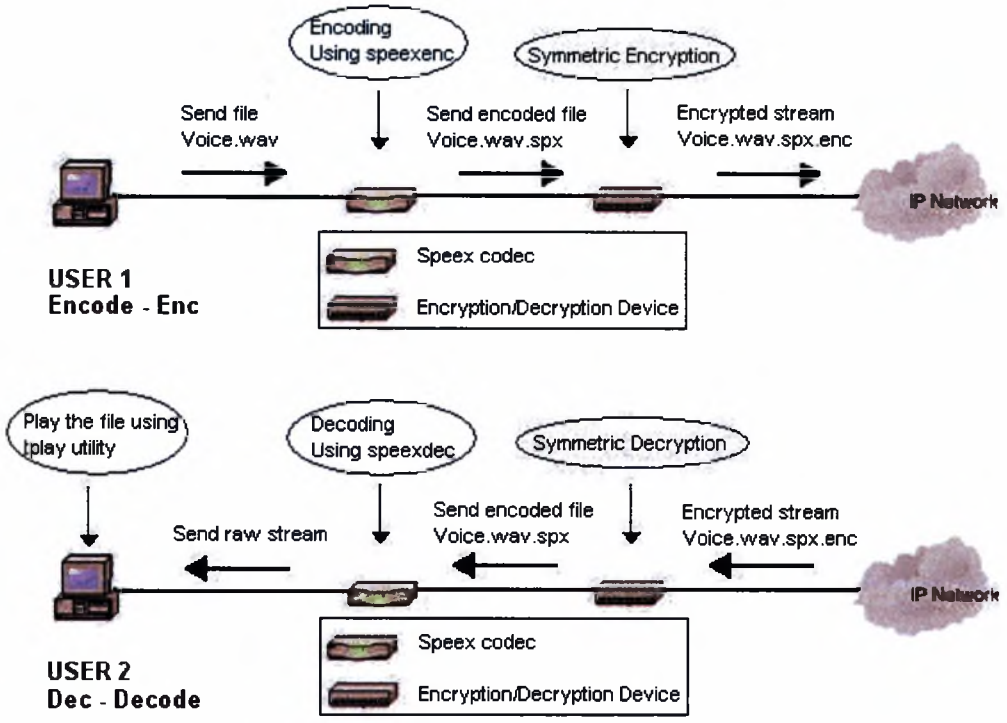
Η συγκεκριμένη εντολή περιγράφει τη λειτουργία της παράστασης του σχήματος 2 που παρουσιάστηκε προηγουμένως. Τα testenc και testdec αποτελούν τις εφαρμογές που πραγματοποιούν κρυπτογράφηση και αποκρυπτογράφηση αντίστοιχα. Πιο συγκεκριμένα το testenc διαβάζει τα δεδομένα από το stdin, τα κρυπτογραφεί και παράγει το αρχείο music.wav.spx.enc, ενώ το testdec αποκρυπτογραφεί το αρχείο music.wav.spx.enc. Το αποτέλεσμα της αποκρυπτογράφησης το μεταφέρει στο stdout από όπου το speexdec, διαβάζοντάς το, πραγματοποιεί αποκωδικοποίηση και τελικά παράγει το αρχείο music.wav το οποίο και αναπαράγουμε στον player. Το σύμβολο && δηλώνει ότι οι δύο διαδικασίες εκκινούν ταυτόχρονα (speexenc- testenc και testdec- speexdec).

Τα αποτελέσματα των μετρήσεων έδειξαν ότι η διαδικασία της κωδικοποίησης χρησιμοποιώντας το Speex και την εφαρμογή speexenc είχε διάρκεια 9.9 δευτερόλεπτα ενώ η διαδικασία της αποκωδικοποίησης μέσω του speexdec 1.15 δευτερόλεπτα. Τα αποτελέσματα των μετρήσεων για τις διαδικασίες κρυπτογράφησης και αποκρυπτογράφησης συνοψίζονται στον πίνακα 5. Η πρώτη στήλη του πίνακα περιλαμβάνει την ονομασία του αλγορίθμου, η δεύτερη τη διαδικασία που πραγματοποιείται (κρυπτογράφηση-αποκρυπτογράφηση), η τρίτη το μήκος του κλειδιού και η τέταρτη το χρόνο σε μsec που διήρκεσε η διαδικασία. Ωστόσο, στον πίνακα δεν υπάρχουν μετρήσεις για τον αλγόριθμο IDEA για τη διαδικασία της αποκρυπτογράφησης. Η απουσία αυτή οφείλεται στο γεγονός ότι τα αποτελέσματα που προέκυπταν για τη συγκεκριμένη περίπτωση ήταν λανθασμένα. Σε όλες τις εκτελέσεις που πραγματοποιήθηκαν ο χρόνος που προέκυπτε για τι διαδικασία της αποκρυπτογράφησης ήταν πάντα 14 μsec...

Πίνακας 5 : Αποτελέσματα μετρήσεων χρόνων κρυπτογράφησης-αποκρυπτογράφησης

Algorithm	Type	Key Length	TIME (μsec)
Blowfish	ENCRYPTION	128	39762
Blowfish	ENCRYPTION	160	53323
Blowfish	ENCRYPTION	256	56559
DES	ENCRYPTION	128	57422
DES	ENCRYPTION	160	62349
DES	ENCRYPTION	256	63330
RC5	ENCRYPTION	128	34018
RC5	ENCRYPTION	160	50088
RC5	ENCRYPTION	256	53400
IDEA	ENCRYPTION	128	40947
IDEA	ENCRYPTION	160	46505
IDEA	ENCRYPTION	256	53467
Blowfish	DECRYPTION	128	46241
Blowfish	DECRYPTION	160	48169
Blowfish	DECRYPTION	256	49824
DES	DECRYPTION	128	52932
DES	DECRYPTION	160	53011
DES	DECRYPTION	256	56316
RC5	DECRYPTION	128	44681
RC5	DECRYPTION	160	45170
RC5	DECRYPTION	256	47988

Με συνδυασμό των χρόνων των διαδικασιών κωδικοποίησης (speexenc)-αποκωδικοποίησης (speexdec) και κρυπτογράφησης-αποκρυπτογράφησης προκύπτει ο πίνακας 6 που περιλαμβάνει συνολικούς χρόνους για τις δύο επόμενες περιπτώσεις, των USER 1 και USER 2 :



Η τελευταία στήλη του πίνακα 6 περιλαμβάνει το άθροισμα των χρόνων των διαδικασιών κωδικοποίησης-αποκωδικοποίησης και κρυπτογράφησης-αποκρυπτογράφησης.

Πίνακας 6 : Συνδυασμός μετρήσεων κωδικοποίησης-κρυπτογράφησης

Algorithm	Key Length	TIME (sec)
		encode - enc
Blowfish	128	9.939
Blowfish	160	9.953
Blowfish	256	9.956
DES	128	9.957
DES	160	9.962
DES	256	9.963
RC5	128	9.934
RC5	160	9.95
RC5	256	9.953
IDEA	128	9.94
IDEA	160	9.946
IDEA	256	9.953
		dec - decode
Blowfish	128	1.196
Blowfish	160	1.198
Blowfish	256	1.199
DES	128	1.202
DES	160	1.203
DES	256	1.206
RC5	128	1.194
RC5	160	1.195
RC5	256	1.197

Συνδυάζοντας τα αποτελέσματα των τριών τελευταίων πινάκων προκύπτει ο παρακάτω συγκεντρωτικός πίνακας αποτελεσμάτων που

περιέχει τα τελικά αποτελέσματα για το σχήμα 2 της σελίδας 31. Η τελευταία στήλη του Πίνακα 7 περιλαμβάνει τους συνολικούς χρόνους σε δευτερόλεπτα για το σύνολο της διαδικασίας. Χρησιμοποιώντας για παράδειγμα τον αλγόριθμο Blowfish με κλειδί μεγέθους 128 bits, ο χρόνος για την ταυτόχρονη λειτουργία κωδικοποίησης–κρυπτογράφησης και αποκρυπτογράφησης–αποκωδικοποίησης ανέρχεται στα 11.135 δευτερόλεπτα.

Πίνακας 7

TOTAL	Key Length	TIME in sec
		(encode-enc & dec-decryption)
Blowfish	128	11.135
Blowfish	160	11.151
Blowfish	256	11.155
DES	128	11.159
DES	160	11.165
DES	256	11.169
RC5	128	11.128
RC5	160	11.145
RC5	256	11.15

Σε ένα δίκτυο υπολογιστών η φωνή μεταδίδεται σε μικρά πακέτα. Ο πίνακας 8 περιλαμβάνει μετρήσεις για πακέτα μεγέθους 20 και 40 bytes του ίδιου αρχείου wave που χρησιμοποιήθηκε στις προηγούμενες μετρήσεις.

Πίνακας 8 : Μετρήσεις για πακέτα μεγέθους 20 και 40 bytes

Algorithm	Type	Key Length	Time(μsec)	TIME (μsec)
			20 bytes	40 bytes
Blowfish	ENCRYPTION	128	35	37
Blowfish	ENCRYPTION	160	36	38
Blowfish	ENCRYPTION	256	36	38
DES	ENCRYPTION	128	38	39
DES	ENCRYPTION	160	39	40
DES	ENCRYPTION	256	40	42
RC5	ENCRYPTION	128	30	33
RC5	ENCRYPTION	160	33	35
RC5	ENCRYPTION	256	34	35
IDEA	ENCRYPTION	128	35	36
IDEA	ENCRYPTION	160	38	39
IDEA	ENCRYPTION	256	38	40
Blowfish	DECRYPTION	128	33	35
Blowfish	DECRYPTION	160	35	37
Blowfish	DECRYPTION	256	36	38
DES	DECRYPTION	128	39	40
DES	DECRYPTION	160	40	41
DES	DECRYPTION	256	40	42
RC5	DECRYPTION	128	33	34
RC5	DECRYPTION	160	33	35
RC5	DECRYPTION	256	34	35

Στη διαδικασία της αποκρυπτογράφησης δεν περιλαμβάνονται οι μετρήσεις του αλγόριθμου IDEA καθώς, όπως αναφέρθηκε και παραπάνω, τα

αποτελέσματα δεν ήταν ορθά (υποθέτουμε σφάλμα στον κώδικα υλοποίησης).

Αθροίζοντας τα αποτελέσματα των πινάκων 4 και 7 έχουμε τους τελικούς χρόνους για τις μετρήσεις μας. Συγκεκριμένα αθροίζουμε τους χρόνους παραγωγής κλειδιών με τους τελικούς χρόνους του σχήματος κωδικοποίησης – κρυπτογράφησης. Τα αποτελέσματα συνοψίζονται στον πίνακα 9.

Πίνακας 9 : Αποτελέσματα του συνόλου της διαδικασίας κρυπτογράφησης-κωδικοποίησης για VoIP επικοινωνίες

Algorithm	Key length	Time (sec)
RC5	128 bit	11.693
	160 bit	11.710
	256 bit	11.720
Blowfish	128 bit	11.780
	160 bit	11.834
	256 bit	11.875
3DES	128 bit	11.721
	160 bit	11.761
	256 bit	11.804

7. Παρουσίαση λειτουργίας του πρωτοκόλλου VoIPSec που υλοποιεί κρυπτογράφηση σε VoIP επικοινωνίες

Το VoIPSec είναι ένα καινούργιο πρωτόκολλο το οποίο διασφαλίζει την ασφάλεια της επικοινωνίας μεταξύ δύο τερματικών συστημάτων με τη χρήση βιομετρικών δεδομένων και ενός συμμετρικού κλειδιού. Το κλειδί ανταλλάσσεται μεταξύ των χρηστών ενώ τα δεδομένα εξακριβώνονται με μία απλή διαδικασία με τη χρήση φωνής ή video. Το πρωτόκολλο στηρίζεται αποκλειστικά και μόνο στο χρήστη χωρίς περαιτέρω προϋποθέσεις, όπως για παράδειγμα αξιόπιστοι ISPs, PKI κοκ. Χρησιμοποιεί ένα σύνολο απλών μεν, αλλά αποτελεσματικών δε, μηνυμάτων τα οποία ανταλλάσσουν οι χρήστες μέσω του διαδικτύου. Είναι ιδιαίτερα απλό στη χρήση και απόλυτα κατανοητό εξαιτίας των απλών τεχνικών που εφαρμόζει (χρήση φωνής ή video, προσωπικά δεδομένα).

Υποθέτουμε ότι υπάρχουν δύο χρήστες, η Alice και ο Bob οι οποίοι επιθυμούν να επικοινωνήσουν. Σύμφωνα με το πρωτόκολλο VoIPSec θα ακολουθήσουν τα επόμενα στάδια:

- Στάδιο 1°: Οι δύο χρήστες ανταλλάσσουν τα αντικείμενα επιλογής τους αφού πρώτα τα έχουν κρυπτογραφήσει, ο καθένας με το προσωπικό του ιδιωτικό κλειδί. Τα αντικείμενα αυτά μπορεί να είναι οτιδήποτε, από ένας απλός αριθμός, ένα αλφαριθμητικό μέχρι και ένα αρχείο ήχου ή video.
- Στάδιο 2°: Έπειτα ανταλλάσσουν τα δημόσια κλειδιά τους και ο χρήστης που ξεκίνησε την επικοινωνία στέλνει στον δεύτερο χρήστη το συμμετρικό κλειδί (Session Symmetric Key).
- Στάδιο 3°: Στο τρίτο και τελευταίο στάδιο πραγματοποιείται η επαλήθευση της γνησιότητας των ψηφιακών υπογραφών από τα δύο επικοινωνούντα μέρη με τη χρήση βιομετρικών μεθόδων (επιβεβαίωση με τη χρήση φωνής ή video).

Αν η διαδικασία της επαλήθευσης των αντικειμένων που επέλεξαν αρχικά οι χρήστες παράγει θετικό αποτέλεσμα, τότε η επικοινωνία ανάμεσά τους χαρακτηρίζεται ασφαλής και η λειτουργία του πρωτοκόλλου συνεχίζεται με την κρυπτογράφηση της επικοινωνίας με τη χρήση του συμμετρικού κλειδιού το οποίο ανταλλάχτηκε στο δεύτερο στάδιο. Αν η διαδικασία

επαλήθευσης αποτύχει, τότε οι δύο χρήστες γνωρίζουν ότι τόσο η επικοινωνία όσο και τα δεδομένα που αντάλλαξαν κατά τη διάρκεια της διαδικασίας έχουν υποκλαπεί.

Ο σχεδιασμός και η υλοποίηση του πρωτοκόλλου αποτελεί έργο των κυρίων Κοψιδά Σπύρου, Ζησιάδη Δημήτρη και Τασιούλα Λέανδρου [7].

7.1 Animation για το πρωτόκολλο VoIPSec

7.1.1 Παρουσίαση και επεξήγηση τεχνικών χαρακτηριστικών για το animation

Ως γλώσσα προγραμματισμού επιλέχθηκε η Java λόγω της καταλληλότητάς της για web presentation.

Η περιγραφή της ροής του πρωτοκόλλου πραγματοποιείται με τη χρήση script language. Οι εντολές που χρησιμοποιούνται καθώς και η επεξήγηση της λειτουργικότητας κάθε μιας παρουσιάζονται στη συνέχεια :

- q samplenet.txt : Με την εντολή αυτή καθορίζεται το γράφημα που θα χρησιμοποιηθεί. Υπάρχουν δύο επιλογές, η πρώτη με το γράφημα που περιγράφει τη κανονική περίπτωση λειτουργίας στο οποίο υπάρχουν δύο χρήστες, η Alice και ο Bob και η περίπτωση «επίθεσης» από τρίτο πρόσωπο στο οποίο έχουμε έναν επιπλέον χρήστη, τον malicious user.
- w 1000 : Η συγκεκριμένη εντολή δηλώνει παύση. Ο χαρακτήρας w προέρχεται από την αγγλική λέξη wait. Ο αριθμός 1000 αναφέρεται στον χρόνο παύσης και είναι σε ms. Έτσι η συγκεκριμένη εντολή πραγματοποιεί παύση της κανονικής ροής του animation για 1000 ms, δηλαδή για 1 δευτερόλεπτο.
- f 25 : Η χρήση της συγκεκριμένης εντολής μεταβάλλει το μέγεθος των γραμμάτων των μηνυμάτων που εμφανίζονται στην οθόνη. Επομένως κάθε εντολή η οποία εμφανίζει κάποιο μήνυμα κατά τη λειτουργία του animation, μετά τη χρήση της προηγούμενης εντολής θα το εμφανίζει με μέγεθος γραμματοσειράς 25 (f από fond). Αν δεν χρησιμοποιηθεί η προηγούμενη εντολή τότε κάθε μήνυμα θα εμφανίζεται με μέγεθος χαρακτήρων 14, το οποίο αποτελεί την προκαθορισμένη επιλογή.
- m Bob produces P2/C2 : Η συγκεκριμένη εντολή χρησιμοποιείται για την εμφάνιση ενός μηνύματος στην οθόνη. Το σημείο εμφάνισης όλων των μηνυμάτων είναι προκαθορισμένο. Αν για παράδειγμα χρησιμοποιηθεί η

προηγούμενη εντολή τότε θα εμφανιστεί στην οθόνη το μήνυμα «Bob produces P2/C2».

- c Bob P2 : Η συγκεκριμένη εντολή χρησιμοποιείται στην περίπτωση που ο χρήστης δημιουργεί ένα αντικείμενο, είτε αυτό είναι κλειδί που θα χρησιμοποιηθεί για την κρυπτογράφηση των μηνυμάτων, είτε ένα αντικείμενο όπως ένας αριθμός, ένα αρχείο φωνής, video κοκ.
- x Alice N1 P1 USS1 3500 : Η εντολή αυτή χρησιμοποιείται για να περιγράψει τη διαδικασία της κρυπτογράφησης. Έτσι, η Alice κρυπτογραφεί το αντικείμενό της N1 με το ιδιωτικό της κλειδί P1 και προκύπτει το κρυπτογραφημένο πακέτο USS1. Ο αριθμός 3500 είναι σε ms και εκφράζει τη διάρκεια παραμονής της παράστασης κρυπτογράφησης στην οθόνη.
- d phoncomun 390 400 : Η συγκεκριμένη εντολή εμφανίζει μία εικόνα *.gif στο animation. Οι δύο αριθμοί που ακολουθούν αποτελούν τις συντεταγμένες(x, y) του σημείου όπου θα εμφανιστεί η εικόνα. Έτσι η προηγούμενη εντολή εμφανίζει την εικόνα με την ονομασία phoncomun στο σημείο που περιγράφεται με τις συντεταγμένες x = 390 και y = 400.

Η πρώτη εντολή που χρησιμοποιείται στη περιγραφή του πρωτοκόλλου με τη χρήση της script language είναι η «g samplenet.txt». Όπως αναφέρθηκε και προηγουμένως, samplenet.txt είναι το αρχείο το οποίο περιλαμβάνει τη περιγραφή του πρώτου γραφήματος. Το αρχείο παρατίθεται στη συνέχεια :

```
1  7 800 600
2  1 U Alice 170 400 70 400 1 400
3  2 U Bob 610 400 710 400 780 400
4  4 N 300 250
5  5 N 350 150
6  6 N 400 250
7  7 N 450 150
8  8 N 500 250
9  1 4 D
10 2 8 D
11 4 5 D
12 4 6 D
13 5 7 D
14 5 6 D
15 6 7 D
16 6 8 D
17 7 8 D
```

Samplenet.txt

Η πρώτη γραμμή του αρχείου περιγράφει γενικά τη διάταξη του γραφήματος, δηλώνοντας τον συνολικό αριθμό κόμβων του γραφήματος (7) και τις διαστάσεις του (x, y = 800, 600). Οι γραμμές 2 και 3 περιγράφουν τους δύο χρήστες του πρωτοκόλλου, Alice και Bob. Το πρώτο ζεύγος αριθμών για κάθε χρήστη αποτελεί τις συντεταγμένες εμφάνισης του κόμβου πάνω στο γράφημα, ενώ τα άλλα δύο ζεύγη τους χώρους αποθήκευσης για κάθε κόμβο, των κλειδιών του και των αντικειμένων που λαμβάνει. Οι επόμενες πέντε σειρές (4-8) περιγράφουν τους κόμβους που αποτελούν το δίκτυο στο οποίο συνδέονται οι δύο χρήστες, Alice και Bob, ενώ οι γραμμές 9 έως 17 του τύπου «X Y D»δηλώνουν ύπαρξη ζεύξης-σύνδεσης μεταξύ των κόμβων X και Y.

7.1.2 Ανάλυση των εφαρμογών σε προγραμματιστικό επίπεδο

Οι κλάσεις της εφαρμογής κατηγοριοποιούνται σύμφωνα με τη λειτουργία τους σε δομικές, σε κλάσεις που αφορούν στην είσοδο-έξοδο και σε κλάσεις που αφορούν στην οπτικοποίηση της εφαρμογής.

Δομικές κλάσεις:

- NetEdge.java
- NetNode.java
- NetGraph.java
- NetObject.java

Κλάσεις εισόδου-εξόδου:

- InputTools.java
- EventGenerator.java

Κλάσεις οπτικοποίησης:

- PresentPanel.java
- PresentFrame.java
- PresentApplet.java

NetEdge.java

Η κλάση αυτή απλά κρατάει την πληροφορία της διασύνδεσης μεταξύ δύο κόμβων του δικτύου ώστε το τμήμα της λειτουργικότητας αλλά και της οπτικοποίησης να «γνωρίζουν» τους κόμβους που συνδέονται μεταξύ τους ώστε είτε να ελέγξουν τη δυνατότητα αποστολής ενός πακέτου από τον κόμβο

Α στον Β είτε να συνδέσουν γραφικά τους δύο κόμβους στο πλαίσιο της εφαρμογής.

NetNode.iava

Κάθε αντικείμενο τύπου NetNode έχει ένα όνομα κόμβου και έναν κωδικό κόμβου. Παράλληλα, κάθε κόμβος έχει μια λίστα (στην πραγματικότητα hash table) στην οποία αποθηκεύει τις ακμές με τις οποίες ο τρέχων κόμβος συνδέεται με τους διπλανούς του.

Εδώ πρέπει να γίνει ένας διαχωρισμός μεταξύ των κόμβων. Υπάρχουν δύο είδη κόμβων: το πρώτο είδος κόμβου είναι οι κόμβοι-χρήστες, ενώ το δεύτερο είδος είναι οι ενδιάμεσοι κόμβοι του δικτύου. Αυτός ο διαχωρισμός εκτός από την οντολογική του σημασία, έχει και πρακτική όσον αφορά στο τμήμα του προγραμματισμού, και έγινε για λόγους οικονομίας αριθμού κλάσεων, χωρίς τη χρήση κληρονομικότητας.

Κάθε κόμβος, εκτός από την πληροφορία των προσκείμενων κόμβων, έχει δύο λίστες με αντικείμενα που έχει παραλάβει κατά τη διάρκεια της λειτουργίας του πρωτοκόλλου: μία λίστα που θα περιέχει τα αντικείμενα που έχει δημιουργήσει ο ίδιος ο κόμβος και μια λίστα για τα αντικείμενα που έχει παραλάβει από άλλους κόμβους–οντότητες του δικτύου όπως ο κακόβουλος χρήστης και ο καλόβουλος συνεργάτης του πρώτου χρήστη. Εδώ πρέπει να τονιστεί ότι αυτές οι λίστες καθώς και τα επόμενα πεδία πληροφορίας που θα αναφέρουμε, χρησιμοποιούνται μόνο από τους κόμβους–χρήστες και όχι από τους ενδιάμεσους κόμβους του δικτύου. Κάθε τέτοια λίστα συνοδεύεται και από ένα σημείο θέσης το οποίο υποδηλώνει τη θέση που αυτή η λίστα θα έχει στον δισδιάστατο χώρο της εφαρμογής, η οποία καθορίζεται κατά την περιγραφή του δικτύου μέσα στο αντίστοιχο αρχείο περιγραφής.

Τέλος, κάθε κόμβος γνωρίζει τη θέση στην οποία βρίσκεται μέσα στο δισδιάστατο χώρο του δικτύου ώστε να μπορεί να παρασταθεί γραφικά. Επίσης, δείχνει σε μια εικόνα η οποία χρησιμοποιείται για τη γραφική αναπαράσταση του κόμβου στην οπτικοποιημένη εφαρμογή.

NetGraph.iava

Η κλάση NetGraph εκτός από το ρόλο της ανάγνωσης ενός δικτύου, παρέχει και όλες τις λειτουργίες που μπορούν να γίνουν στο δίκτυο αυτό όπως τη δημιουργία αντικειμένων, την αποστολή τους, το συνδυασμό

υπαρχόντων αντικειμένων για τη δημιουργία νέων κλπ. Δομικά έχει πρόσβαση σε όλους τους κόμβους και ακμές του δικτύου μέσω του αντίστοιχου ονόματος – κωδικού του κάθε κόμβου και ακμής.

NetObject.java

Μέσω της κλάσης αυτής περιγράφονται όλα τα πακέτα που στέλνονται μέσω του δικτύου, τα οποία πρώτα τοποθετούνται στις αντίστοιχες λίστες με τα αντικείμενα που έχει ο κάθε χρήστης υπό την κατοχή του κατά τη διάρκεια της δημιουργίας τους, ενώ στη συνέχεια κατά την περαιτέρω εφαρμογή του πρωτοκόλλου στέλνονται προς άλλους χρήστες και αλλάζουν κατοχή. Όπως και οι κόμβοι, έτσι και τα πακέτα έχουν μια εικόνα μέσω της οποίας απεικονίζονται γραφικά, και μια τρέχουσα θέση στην οποία εμφανίζονται η οποία όμως αλλάζει κατά τη διάρκεια εφαρμογής του πρωτοκόλλου.

Η κίνηση των αντικειμένων με ρεαλιστικό τρόπο, επιτυγχάνεται μέσω της ακόλουθης τεχνικής: κάθε αντικείμενο, ανά πάσα στιγμή έχει μια τρέχουσα θέση, και μια θέση στόχο. Αν οι δυο αυτές θέσεις συμπίπτουν, το αντικείμενο παραμένει ακίνητο. Όταν όμως ένα αντικείμενο σταλεί κάπου, μέσω της κλάσης NetGraph η θέση–στόχος του αντικειμένου γίνεται ίση με τη θέση του κόμβου στον οποίο θέλει το πακέτο να αποσταλεί. Έτσι με την πάροδο του χρόνου (με την πάροδο διαδοχικών frames στο χώρο οπτικοποίησης) η πραγματική θέση του αντικειμένου πλησιάζει διαδοχικά την θέση στόχο.

Αυτή η κίνηση επιτυγχάνεται με τη συνύπαρξη δύο ανεξάρτητων threads στην εφαρμογή όπου το ένα πραγματοποιεί τις πράξεις πάνω στο γράφημα–δίκτυο ενώ το άλλο παίρνοντας σαν είσοδο την κατάσταση του γραφήματος, πραγματοποιεί την κίνηση των κόμβων με ομαλό τρόπο αλλάζοντας διαδοχικά τη θέση των κινούμενων αντικειμένων και εμφανίζοντάς τα στην οθόνη με την πάροδο του κάθε frame.

Στη συνέχεια θα αναφέρουμε τις κλάσεις που επιτελούν λειτουργίες εισόδου – εξόδου.

InputTools.java

Η κλάση αυτή ουσιαστικά χρησιμοποιείται για την ανάγνωση εικόνων από το δίσκο καθώς και των αρχείων που περιγράφουν το δίκτυο και το εκάστοτε σενάριο–εφαρμογή του πρωτοκόλλου.

EventGenerator.java:

Η κλάση αυτή διαβάζει εντολή-εντολή το script, μεταφράζει τις εντολές που διαβάζει και τις εκτελεί πάνω στο γράφημα.

Τέλος, θα αναφέρουμε επιγραμματικά τη λειτουργία των κλάσεων που αφορούν στο γραφικό περιβάλλον της εφαρμογής.

PresentPanel.java, PresentFrame.java, PresentApplet.java:

Η πρώτη από τις τρεις αυτές κλάσεις συνιστά το βασικό χώρο στον οποίο εμφανίζεται το δίκτυο και όλα όσα διεξάγονται πάνω σε αυτό. Οι κλάσεις PresentFrame και PresentApplet είναι πανομοιότυπες με τη διαφορά ότι η πρώτη «τρέχει» την εφαρμογή εμφανίζοντάς την σε παράθυρο ενώ η δεύτερη σε μορφή Applet ώστε να είναι προσβάσιμη μέσα από έναν Internet Browser. Οι δύο αυτές κλάσεις αναλαμβάνουν την υψηλότερου επιπέδου διασύνδεση με τον χρήστη μέσω των αντίστοιχων κουμπιών.

7.2 Παρουσίαση των animation

Αρχικά θα επεξηγήσουμε κάποια χαρακτηριστικά τα οποία απαντώνται και στα δύο animation πριν προχωρήσουμε στην λεπτομερή ανάλυσή τους. Στο κάτω μέρος των εικόνων που παρατίθενται παρακάτω, μπορούμε να παρατηρήσουμε την ύπαρξη δύο πλήκτρων, pause και restart. Το κουμπί «pause» χρησιμοποιείται για την παύση-επανεκκίνηση της ροής του animation ώστε ο χρήστης να παρατηρήσει καλύτερα κάποιο βήμα της διαδικασίας, ενώ το κουμπί «restart» για την επανεκκίνηση της διαδικασίας από την αρχή. Επιπλέον, στις εικόνες πάνω και δεξιά μπορούμε να παρατηρήσουμε την ύπαρξη μίας λεζάντας, η οποία περιέχει πληροφορίες για τη σημασία κάθε συμβόλου που χρησιμοποιείται. Έτσι τα Pi και Ci συμβολίζουν το ιδιωτικό και το δημόσιο κλειδί του χρήστη i αντίστοιχα (έχουμε υποθέσει ότι στον χρήστη Alice αντιστοιχεί ο αριθμός 1 ενώ στον χρήστη Bob ο αριθμός 2), το Ni το τυχαίο αντικείμενο που ο κάθε χρήστης επιλέγει να αποστείλει μέσω του δικτύου, το SSK το συμμετρικό κλειδί που χρησιμοποιείται στις συναλλαγές κοκ.

Pi : Private key of user i
Ci : Common key of user i
SSK : Session Symmetric key
EnSSK : Encrypted SSK
USSi : User Session Signature of user i
Ni: user selected object (random)

7.2.1 Πρώτο animation – Κανονική περίπτωση λειτουργίας

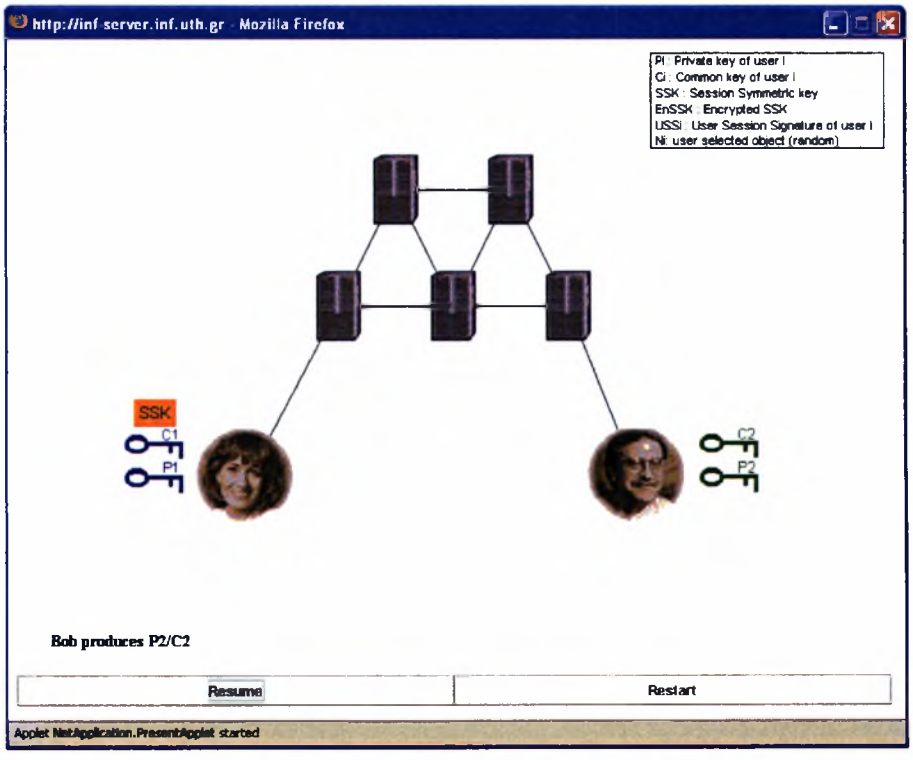
Υποθέτουμε την ύπαρξη δύο χρηστών, του Bob και της Alice, οι οποίοι επιθυμούν να μεταφέρουν κάποια αντικείμενα που έχουν επιλέξει ο ένας στον άλλο, με ασφάλεια και χωρίς να υπάρχει δυνατότητα υποκλοπής.

Η λειτουργία του πρωτοκόλλου διακρίνεται σε τρεις φάσεις :

1. Παραγωγή κλειδιών (Key generation)
2. Ανταλλαγές κλειδιών και ψηφιακών υπογραφών
3. Επαλήθευση (Verification)

Φάση 1 – Παραγωγή κλειδιών

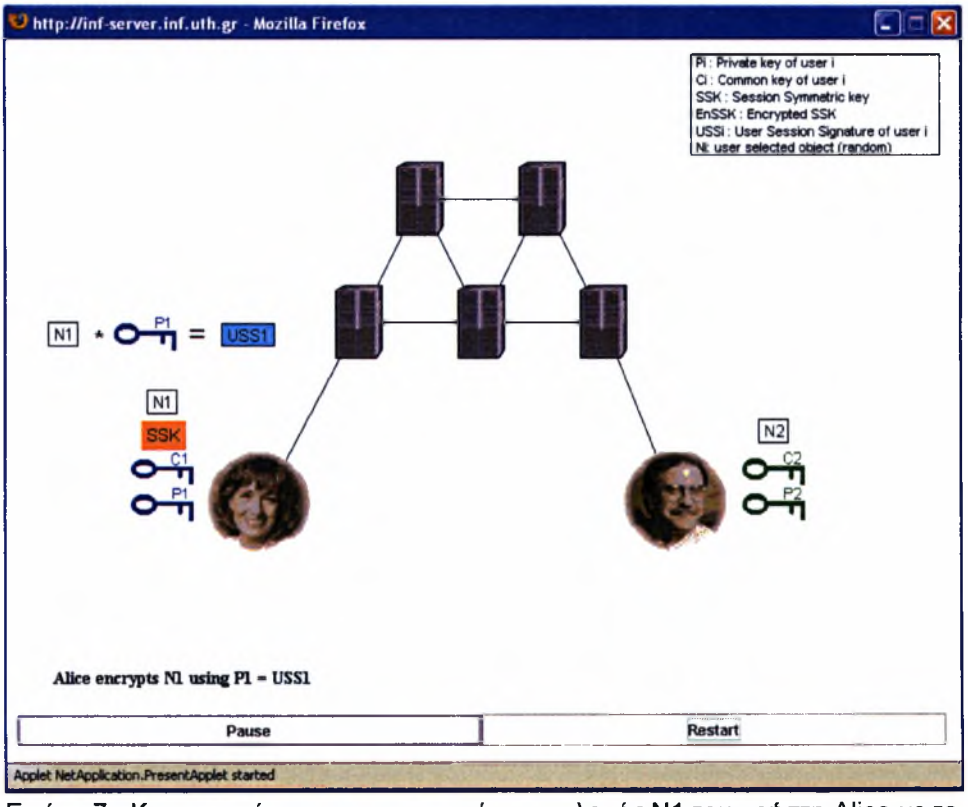
Η παραγωγή κλειδιών αποτελεί τη πρώτη φάση λειτουργίας του πρωτοκόλλου VoIPSec. Στο στάδιο αυτό οι παράγονται τα ιδιωτικά και δημόσια κλειδιά των δύο χρηστών τα οποία θα χρησιμοποιηθούν για τη διασφάλιση της ασφάλειας στην επικοινωνία τους, καθώς και το συμμετρικό κλειδί. Παρατίθεται ένα στιγμιότυπο της συγκεκριμένης φάσης με την ολοκλήρωση της διαδικασίας παραγωγής των κλειδιών και με τον κάθε χρήστη να έχει δημιουργήσει το προσωπικό του ζεύγος.



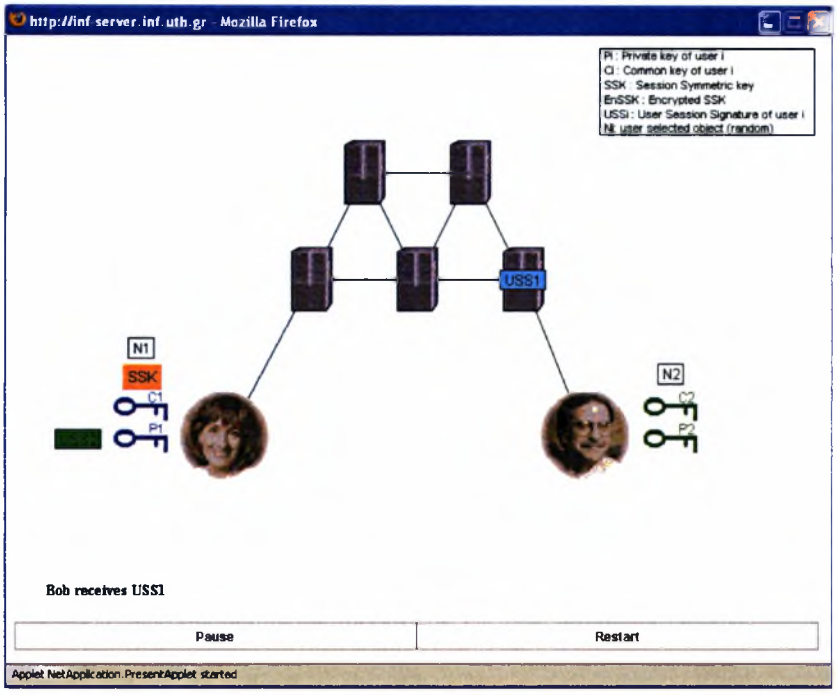
Εικόνα 6 : Στιγμιότυπο της πρώτης φάσης λειτουργίας του πρωτοκόλλου VoIPSec με τους δύο χρήστες να έχουν παράγει τα προσωπικά τους ζεύγη κλειδιών.

Φάση 2 – Ανταλλαγές κλειδιών και ψηφιακών υπογραφών

Στη δεύτερη φάση ανταλλάσσονται τα κλειδιά που παρήχθησαν στην φάση 1. Αρχικά ο κάθε χρήστης επιλέγει κάποιο αντικείμενο (Ni) και το κρυπτογραφεί με το ιδιωτικό του κλειδί (Pi), παράγοντας την ψηφιακή υπογραφή του την οποία και αποστέλλει στον άλλο. Οι εικόνες 7 και 8 επεξηγούν τη διαδικασία για την Alice. Στην πρώτη εικόνα η Alice κρυπτογραφεί το αντικείμενο που έχει επιλέξει (N1) με το ιδιωτικό της κλειδί P1, παράγοντας την ψηφιακή της υπογραφή USS1 την οποία και στέλνει στο χρήστη Bob όπως δείχνει η εικόνα 8. Παρόμοια διαδικασία ακολουθείται και από τον Bob με αποτέλεσμα τη δημιουργία της δικής του ψηφιακής υπογραφής USS2 την οποία και στέλνει στην Alice. Στο τέλος της φάσης 2 η Alice κρυπτογραφεί το συμμετρικό κλειδί SSK με το δημόσιο κλειδί του Bob και στη συνέχεια του το στέλνει. Εκείνος το αποκρυπτογραφεί και λαμβάνει το SSK. Στο σημείο αυτό και οι δύο χρήστες γνωρίζουν το ίδιο συμμετρικό κλειδί (SSK).



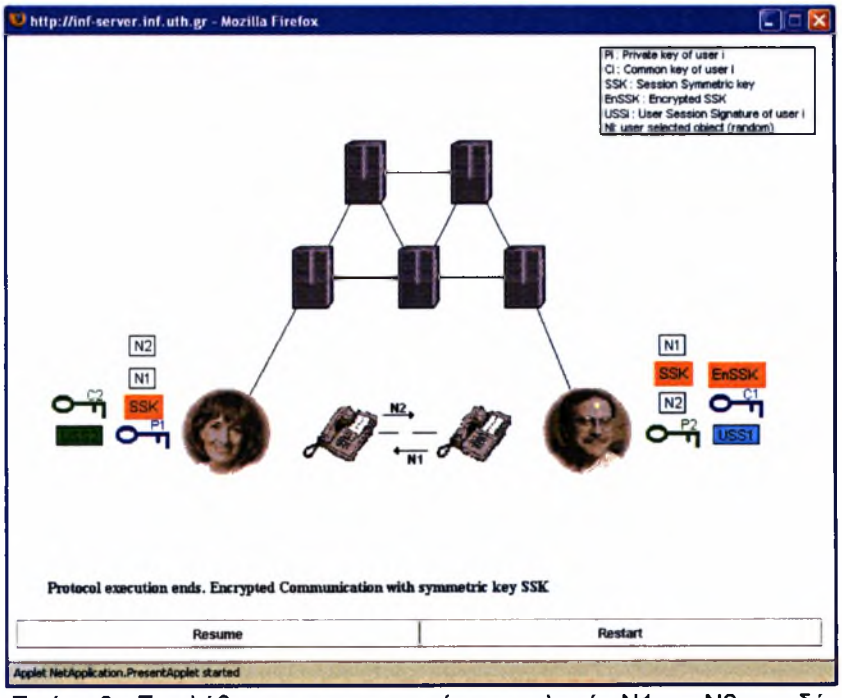
Εικόνα 7 : Κρυπτογράφηση του αντικειμένου επιλογής N1 του χρήστη Alice με το προσωπικό του κλειδί P1. Παραγωγή της ψηφιακής του υπογραφής USS1.



Εικόνα 8 : Αποστολή της ψηφιακής υπογραφής USS1 του χρήστη Alice στον χρήστη Bob.

Φάση 3 – Επαλήθευση

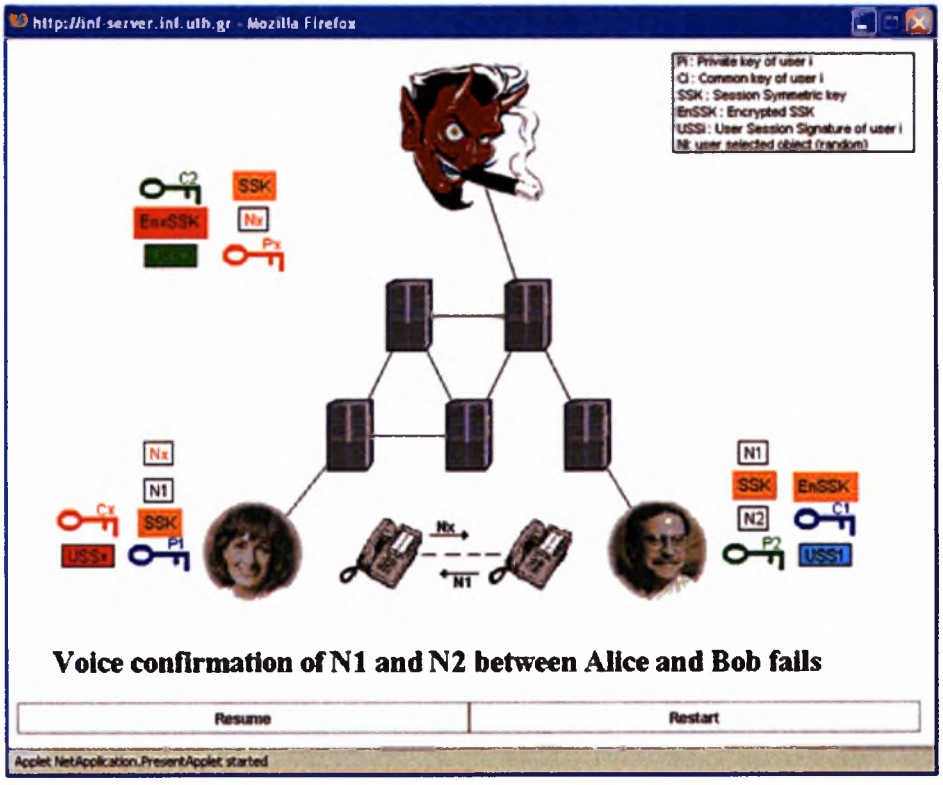
Στην τρίτη και τελευταία φάση οι δύο χρήστες αποκρυπτογραφούν τις ψηφιακές υπογραφές που έχουν λάβει ο ένας από τον άλλο. Πλέον η Alice έχει το αντικείμενο επιλογής του Bob (N2), ενώ ο Bob το αντικείμενο επιλογής της Alice (N1). Η εγκυρότητα των δύο αντικειμένων διασταυρώνεται μέσω τηλεφωνικής επικοινωνίας, όπως φαίνεται και στην εικόνα 9.



Εικόνα 9 : Επαλήθευση των αντικειμένων επιλογής N1 και N2 των δύο χρηστών με τη χρήση φωνής (τηλέφωνο).

7.2.2 Δεύτερο animation – Περίπτωση επίθεσης από τρίτο χρήστη

Σε αυτό το animation παρουσιάζεται μία περίπτωση της ανθεκτικότητας του πρωτοκόλλου απέναντι σε επιτηδευμένες επιθέσεις τρίτων. Ένας κακόβουλος χρήστης προσπαθεί να υποκλέψει τα δεδομένα των Alice και Bob χωρίς να γίνει αντιληπτός. Ωστόσο το πρωτόκολλο, μέσω των μηχανισμών που διαθέτει, αντιλαμβάνεται την ύπαρξη και άλλου χρήστη, εκτός των Alice και Bob, και διακόπτει την επικοινωνία.



Εικόνα 10 : Η διαδικασία επαλήθευσης αποτυγχάνει. Απόκρουση επίθεσης.

8. Επίλογος

Όπως αναφέρθηκε και στην εισαγωγή η κρυπτογράφηση των δεδομένων είναι η μόνη λύση για τη κατοχύρωση της ασφάλειας και της αξιοπιστίας των δεδομένων σε ηλεκτρονικές συναλλαγές. Βασίζεται στους χρήστες και πετυχαίνει να διασφαλίσει το απόρρητο των επικοινωνιών τους εγγυημένα και αξιόπιστα. Η επιβάρυνση για την κρυπτογράφηση φωνής σε συστήματα VoIP είναι αποδεκτή (παραγωγή κλειδιών ~0.5msec και κρυπτογράφηση-κωδικοποίηση ~11sec για το αρχείο ήχου music.wav – καθυστέρηση 33-42 μsec για πακέτα μεγέθους 40 bytes ανάλογα με τον αλγόριθμο και το μήκος κλειδιού που χρησιμοποιείται) ή δεν επηρεάζει τη λειτουργία τους, ενώ πρωτόκολλα διασφάλισης του απορρήτου των επικοινωνιών, όπως το VoIPSec, πετυχαίνουν να παρέχουν στους χρήστες αυτή τη δυνατότητα. Σαν μελλοντική εργασία θα μπορούσαν να πραγματοποιηθούν μετρήσεις σε άλλες συσκευές, όπως PDAs και κινητά τηλέφωνα, για την κατοχύρωση εκείνου του configuration που θα επιφέρει την ελάχιστη επιβάρυνση σε voice communications.

9. Παράρτημα

9.1 Εγκατάσταση Simics

Η εγκατάσταση του Simics περιλαμβάνει τα ακόλουθα βήματα:

1. Κατέβασμα του εκτελέσιμου αρχείου για εγκατάσταση από τη διεύθυνση https://www.simics.net/evaluation/form_dl.php. Υπάρχουν εκδόσεις τόσο για λειτουργικά συστήματα Linux, όσο και για Windows.
2. Αίτηση για άδεια χρήσης του λογισμικού. Στο σημείο αυτό πρέπει απλά να συμπληρώσεις μία αίτηση με τα προσωπικά σου στοιχεία και με τον αριθμό της κάρτας δικτύου του υπολογιστή όπου θα εγκαταστήσεις το λογισμικό.
3. Έπειτα μπορείς να εκκινήσεις το Simics. Χρησιμοποιώντας τη παρακάτω εντολή δημιουργείς το προσωπικό σου χώρο όπου μπορείς να αποθηκεύεις τις εργασίες σου. Με [simics] εννοούμε το μονοπάτι όπου είναι εγκατεστημένο το Simics :

pakostar@computer:`$ [simics]/bin/workspace-setup ~/simics-workspace
Setting up Simics workspace directory: /home/pakostar/simics-workspace

9.2 Arm-linux-gcc

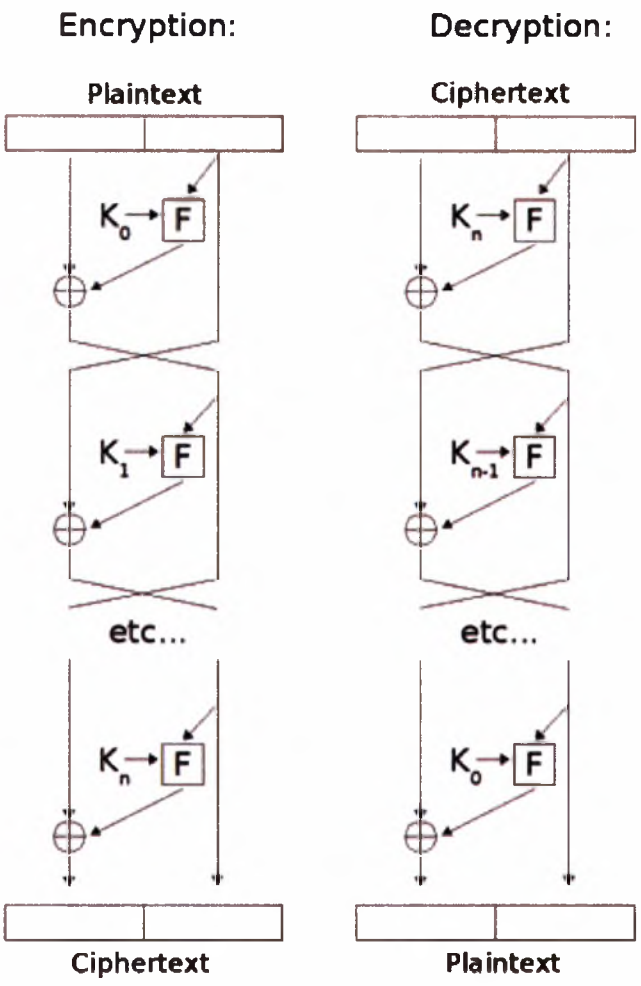
Όπως ανέφερα και προηγουμένως ο επεξεργαστής του συστήματος που πραγματοποίησα τις μετρήσεις ήταν τεχνολογίας Pentium. Τα binary αρχεία που προέκυπταν από το compile των προγραμμάτων έπρεπε με κάποιο τρόπο να είναι συμβατά με τον ARM. Για το λόγο αυτό εγκατέστησα μία εφαρμογή ικανή να πραγματοποιεί compile προγραμμάτων και τα binary που προκύπτουν να είναι αναγνώσιμα από επεξεργαστή τεχνολογίας ARM. Η εντολή που χρησιμοποίησα ήταν η ακόλουθη :

- arm-linux-gcc testenc.c -static -I /opt/arm/openssl-0.9.7d/include/ -L /opt/arm/openssl-0.9.7d –lcrypto –o encryption.out

Το binary αρχείο encryption.out που προκύπτει μπορείς να το χρησιμοποιήσεις στον ARM για να πραγματοποιήσεις τις μετρήσεις σου. Με τα προσδιοριστικά -I /opt/arm/openssl-0.9.7d/include/ και -L /opt/arm/openssl-0.9.7d –lcrypto ορίζουμε το μονοπάτι για την τοποθεσία των βιβλιοθηκών.

9.3 Κρυπτογραφικός αλγόριθμος Feistel

Ο αλγόριθμος Feistel αποτελεί έναν ειδικό τύπο επαναληπτικού κρυπτογραφικού αλγορίθμου δέσμης. Η δέσμη m του αρχικού κειμένου που πρόκειται να κρυπτογραφηθεί διαιρείται αρχικά σε δύο υποδέσμες L_0 και R_0(ίδιου μήκους). Για παράδειγμα, αν το μήκος της δέσμης είναι G, τότε οι υποδέσμες L_0 και R_0 θα έχουν και οι δύο το ίδιο μήκος G/2. Το κλειδί k πρέπει να χρησιμοποιείται για τον υπολογισμό ενός συνόλου από n μέρη κλειδιού k1, k2, k3, …, k_n(ένα για κάθε ανακύκλωση). Το παρακάτω διάγραμμα επιδεικνύει τόσο την κρυπτογράφηση όσο και την αποκρυπτογράφηση.



Feistel Cipher

Η λειτουργία του αλγορίθμου περιγράφεται με τις παρακάτω εξισώσεις :

1. $L_i = R_{i-1}$
2. $R_i = L_{i-1} \oplus f_{ki}(R_{i-1})$, όπου f είναι η κυκλική συνάρτηση.

Μια σημαντική ιδιότητα του κρυπτογραφικού αλγορίθμου Feistel είναι ότι η κυκλική συνάρτηση είναι πάντοτε αντιστρέψιμη ανεξαρτήτως επιλογής της συνάρτησης f($L_i = R_{i-1}$ και $R_i = L_{i-1} \oplus f_{ki}(R_{i-1})$, οπότε έχουμε ότι $R_{i-1} = L_i$ και $L_{i-1} = R_i \oplus f_{ki}(L_i)$).

9.4 Παραδείγματα μετρήσεων στο Simics

Πίνακας : Blowfish - 200 MHz

Blowfish	128	DH	1024	ARM 200	→	0,005	0,732	**0,737**
Blowfish	160	DH	1024	ARM 200	→	0,006	0,732	**0,738**
Blowfish	192	DH	1024	ARM 200	→	0,006	0,732	**0,738**
Blowfish	256	DH	1024	ARM 200	→	0,007	0,732	**0,739**
Blowfish	128	DSA	1024	ARM 200	→	0,005	4,017	**4,022**
Blowfish	160	DSA	1024	ARM 200	→	0,006	4,017	**4,023**
Blowfish	192	DSA	1024	ARM 200	→	0,006	4,017	**4,023**
Blowfish	256	DSA	1024	ARM 200	→	0,007	4,017	**4,024**
Blowfish	128	DH	2048	ARM 200	→	0,005	2,396	**2,401**
Blowfish	160	DH	2048	ARM 200	→	0,006	2,396	**2,402**
Blowfish	192	DH	2048	ARM 200	→	0,006	2,396	**2,402**
Blowfish	256	DH	2048	ARM 200	→	0,007	2,396	**2,403**
Blowfish	128	DSA	2048	ARM 200	→	0,005	4,168	**4,173**
Blowfish	160	DSA	2048	ARM 200	→	0,006	4,168	**4,174**
Blowfish	192	DSA	2048	ARM 200	→	0,006	4,168	**4,174**
Blowfish	256	DSA	2048	ARM 200	→	0,007	4,168	**4,175**
Blowfish	128	DH	4096	ARM 200	→	0,005	16,07	**16,075**
Blowfish	160	DH	4096	ARM 200	→	0,006	16,07	**16,076**
Blowfish	192	DH	4096	ARM 200	→	0,006	16,07	**16,076**
Blowfish	256	DH	4096	ARM 200	→	0,007	16,07	**16,077**
Blowfish	128	DSA	4096	ARM 200	→	0,005	4,725	**4,73**
Blowfish	160	DSA	4096	ARM 200	→	0,006	4,725	**4,731**
Blowfish	192	DSA	4096	ARM 200	→	0,006	4,725	**4,731**
Blowfish	256	DSA	4096	ARM 200	→	0,007	4,725	**4,732**

Πίνακας : IDEA - 266 MHz

IDEA	128	DH	1024	ARM 266	→	0,003	0,498	**0,501**
IDEA	160	DH	1024	ARM 266	→	0,003	0,498	**0,501**
IDEA	192	DH	1024	ARM 266	→	0,003	0,498	**0,501**
IDEA	256	DH	1024	ARM 266	→	0,003	0,498	**0,501**
IDEA	128	DSA	1024	ARM 266	→	0,003	3,021	**3,024**
IDEA	160	DSA	1024	ARM 266	→	0,003	3,021	**3,024**
IDEA	192	DSA	1024	ARM 266	→	0,003	3,021	**3,024**
IDEA	256	DSA	1024	ARM 266	→	0,003	3,021	**3,024**
IDEA	128	DH	2048	ARM 266	→	0,003	1,929	**1,932**
IDEA	160	DH	2048	ARM 266	→	0,003	1,929	**1,932**
IDEA	192	DH	2048	ARM 266	→	0,003	1,929	**1,932**
IDEA	256	DH	2048	ARM 266	→	0,003	1,929	**1,932**
IDEA	128	DSA	2048	ARM 266	→	0,003	3,138	**3,141**
IDEA	160	DSA	2048	ARM 266	→	0,003	3,138	**3,141**
IDEA	192	DSA	2048	ARM 266	→	0,003	3,138	**3,141**
IDEA	256	DSA	2048	ARM 266	→	0,003	3,138	**3,141**
IDEA	128	DH	4096	ARM 266	→	0,003	12,211	**12,214**
IDEA	160	DH	4096	ARM 266	→	0,003	12,211	**12,214**
IDEA	192	DH	4096	ARM 266	→	0,003	12,211	**12,214**
IDEA	256	DH	4096	ARM 266	→	0,003	12,211	**12,214**
IDEA	128	DSA	4096	ARM 266	→	0,003	3,574	**3,577**
IDEA	160	DSA	4096	ARM 266	→	0,003	3,574	**3,577**
IDEA	192	DSA	4096	ARM 266	→	0,003	3,574	**3,577**
IDEA	256	DSA	4096	ARM 266	→	0,003	3,574	**3,577**

10. Βιβλιογραφία

[1]. www.speex.org
[2]. www.simics.net
[3]. www.virtutech.com
[4]. www.openssl.org
[5]. www.go-online.gr
[6]. http://el.wikipedia.org/
[7]. S. Kopsidas, D. Zisiadis, L. Tassiulas, "*Voice Interactive Personalized Security (VoIPSec) protocol: Fortify Internet telephony by providing end-to-end security through inbound key exchange and biometric verification*", In Proceedings of the First IEEE Workshop on Hot Topics in Web Systems and Technologies HotWeb2006, Nov 2006
[8]. simics-user-guide-unix.pdf
[9]. Σύγγραμμα «Ασφάλεια Πληροφοριακών συστημάτων και δικτύων», Γ. Παγκάλου και Ι. Μαυρίδη
[10]. Άρθρο «VoIP: An In-Depth Analysis» της Cisco, http://www.ciscopress.com/articles
[11]. Σύγγραμμα «Αλγόριθμοι, Σχεδιασμός και Ανάλυση», Π. Μποζάνης
[12]. http://en.wikipedia.org/wiki/Diffie-Hellman
[13]. http://www.ibiblio.org/pub/Linux/apps/sound/players/ (στον κατάλογο !INDEX.short.html)
[14]. http://www.spectrum.ieee.org/oct05/1846
[15]. http://www.tech-faq.com/what-is-voip.shtml