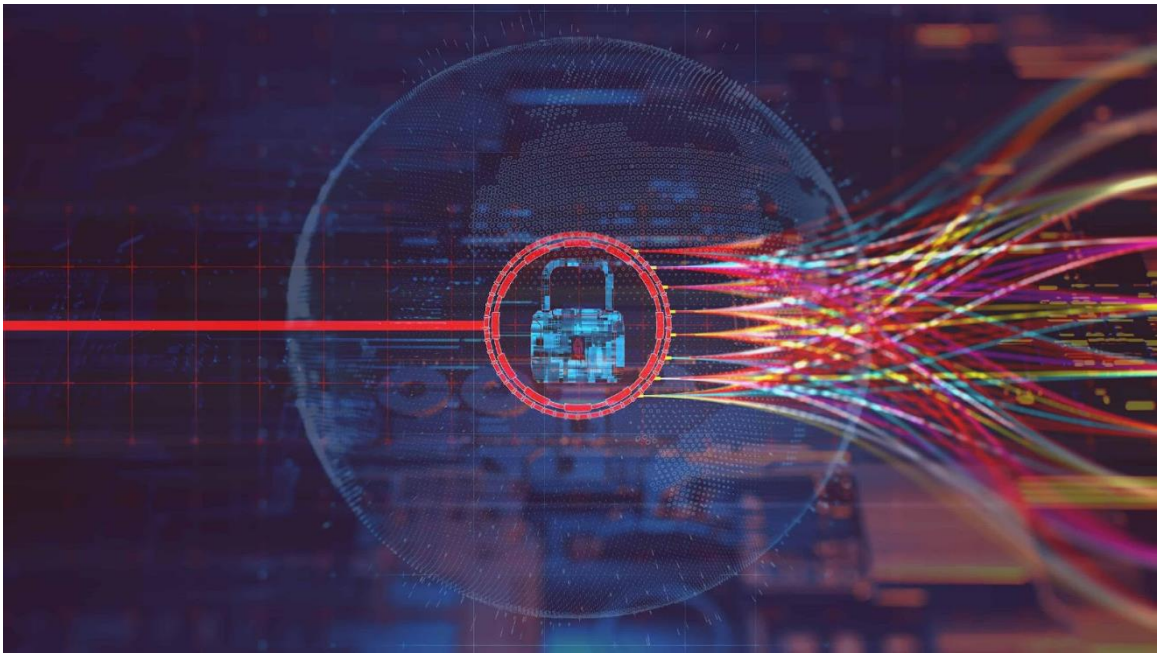
ΔΙΕΘΝΕΣ ΠΑΝΕΠΙΣΤΗΜΙΟ ΤΗΣ ΕΛΛΑΔΟΣ

ΣΧΟΛΗ ΜΗΧΑΝΙΚΩΝ

ΤΜΗΜΑ ΜΗΧΑΝΙΚΩΝ ΠΛΗΡΟΦΟΡΙΚΗΣ
ΚΑΙ ΗΛΕΚΤΡΟΝΙΚΩΝ ΣΥΣΤΗΜΑΤΩΝ

ΠΤΥΧΙΑΚΗ ΕΡΓΑΣΙΑ

«Σχεδιασμός και ανάπτυξη συστήματος ανταλλαγής μηνυμάτων με χρήση κρυπτογράφησης»



Του φοιτητή
Κοκοβίδη Αλέξανδρου
Αρ. Μητρώου: 134011

Επιβλέπων
Αμανατιάδης
Δημήτριος

Ιούνιος 2023

Τίτλος Π.Ε – Σχεδιασμός και ανάπτυξη συστήματος ανταλλαγής μηνυμάτων με χρήση κρυπτογράφησης

Κωδικός Π.Ε. 22281
Ονοματεπώνυμο φοιτητή/τών – Κοκοβίδης Αλέξανδρος
Ονοματεπώνυμο εισηγητή – Αμανατιάδης Δημήτριος
Ημερομηνία ανάληψης Π.Ε. 22 Οκτωβρίου 2022
Ημερομηνία περάτωσης Π.Ε. 25 Μαΐου 2023

Βεβαιώνω ότι είμαι ο συγγραφέας αυτής της εργασίας και ότι κάθε βοήθεια την οποία είχα για την προετοιμασία της είναι πλήρως αναγνωρισμένη και αναφέρεται στην εργασία. Επίσης, έχω καταγράψει τις όποιες πηγές από τις οποίες έκανα χρήση δεδομένων, ιδεών, εικόνων και κειμένου, είτε αυτές αναφέρονται ακριβώς είτε παραφρασμένες. Επιπλέον, βεβαιώνω ότι αυτή η εργασία προετοιμάστηκε από εμένα προσωπικά, ειδικά ως διπλωματική εργασία, στο Τμήμα Μηχανικών Πληροφορικής και Ηλεκτρονικών Συστημάτων του ΔΙ.ΠΑ.Ε.

Η έγκριση της διπλωματικής εργασίας από το Τμήμα Μηχανικών Πληροφορικής και Ηλεκτρονικών Συστημάτων του Διεθνούς Πανεπιστημίου της Ελλάδος, δεν υποδηλώνει απαραιτήτως και αποδοχή των απόψεων του συγγραφέα, εκ μέρους του Τμήματος.

Πρόλογος

Ως φοιτητής του τμήματος πληροφορικής, από τις πρώτες διαλέξεις κατάλαβα ότι ο προγραμματισμός είναι κάτι που μου αρέσει και μου διεγείρει το ενδιαφέρον για μάθηση και εξερεύνηση τεχνολογιών που αφορούν τον συγκεκριμένο κλάδο. Επιπλέον με την ραγδαία ανάπτυξη της τεχνολογίας, τα πολύτιμα δεδομένα που αποτελούν δομικό λίθο της πληροφορικής, άρχισαν να γίνονται εργαλείο όχι μόνο χρήσιμο αλλά και εξαιρετικά επικίνδυνο σε λάθος χέρια. Δεν άργησε να εμφανιστεί βέβαια και το θέμα της κρυπτογράφησης, αφού αποτελεί πρόκληση για όλους γενικότερα.

Η ιδέα μιας εφαρμογής μέσω της οποίας οι χρήστες θα μπορούσαν να επικοινωνούν ήρθε έπειτα από διάφορες και ποικίλες συζητήσεις γύρω από ιδέες νέων εφαρμογών και τεχνολογιών που θα μπορούσαμε να αναπτύξουμε μελλοντικά. Εφόσον η ιδέα και το ενδιαφέρον υπήρχε πλέον, σειρά είχε η έρευνα που θα βοηθούσε να υλοποιηθούν οι σκέψεις μας. Πάρα πολλές εφαρμογές είχαν ήδη δημιουργηθεί από πιο έμπειρους προγραμματιστές, με διαφορετικούς αλγόριθμους κρυπτογράφησης, διαφορετικές κλήσεις και επικοινωνίες των εμπλεκόμενων services, αλλά και προβλήματα και παράπονα από τους χρήστες που τις χρησιμοποιούν. Έτσι στόχος ήταν η επίλυση των ήδη υπαρχόντων προβλημάτων αλλά και η εύρεση του καλύτερου δυνατού αλγορίθμου κρυπτογράφησης, ώστε να επιτευχθεί ο κύριος στόχος, η ασφάλεια των δεδομένων των μελλοντικών χρήστών.

Περίληψη

Η παρούσα εργασία πραγματεύεται την ανάπτυξη ενός λογισμικού το οποίο θα προσφέρει στους χρήστες του την αξία της επικοινωνίας με το επιπλέον χαρακτηριστικό της ασφάλειας το οποίο γίνεται όλο και πιο απαραίτητο αλλά και πιο δυσεύρετο με την ραγδαία εξάπλωση των δεδομένων. Οι χρήστες, ομάδες ατόμων, εταιρειών αλλά και μεμονωμένα άτομα θα μπορούν να δημιουργούν κείμενο το οποίο θέλουν να στείλουν όπως ακριβώς γίνεται μέχρι και σήμερα με τις περισσότερες εφαρμογές ανταλλαγής μηνυμάτων, χωρίς να αλλάξουν κάτι στις συνήθειές τους. Το ενδιάμεσο επίπεδο της επικοινωνίας είναι το σημείο που η ασφάλεια παίρνει θέση. Κάθε κείμενο / μήνυμα του χρήστη που στέλνει / εκπέμπει δεδομένα κωδικοποιείται με ένα αλγόριθμο κρυπτογράφησης ώστε να αλλοιωθεί η μορφή του.

Ο συγκεκριμένος αλγόριθμος που χρησιμοποιήθηκε αποτελεί τον ασφαλέστερο μέχρι την παρούσα χρονική στιγμή σύμφωνα με μελέτες και πειραματικές προσπάθειες που έγιναν, με σκοπό την παραβίαση του και την κλοπή των δεδομένων.

Με την ύπαρξη μιας τέτοιας εφαρμογής το αίσθημα της ασφάλειας θα αυξηθεί και έτσι οι επικοινωνία θα αξιοποιείται στο έπακρο, αφού οι χρήστες δεν θα έχουν το φόβο μια επίθεσης με σκοπό την κλοπή των δεδομένων τους και ίσως πολλά περισσότερα.

Η συγκεκριμένη εφαρμογή έρχεται να προσθέσει ένα επιπλέον βαθμό ασφάλειας λόγω του πιο σύγχρονου αλγορίθμου κρυπτογράφησης, την χρονική στιγμή που πραγματοποιείται. Επίσης είναι αυξημένη και η ασφάλεια των κλειδιών, δημόσιο και ιδιωτικό, που χρησιμοποιούνται για την κρυπτογράφηση και αποκρυπτογράφηση αντιστοιχα.

Design and development of messaging system using encryption

Alexandros Kokovidis

Abstract

The present paper deals with the development of software that will provide its users with the value of communication, with the additional feature of security, which is becoming increasingly necessary but also more elusive with the rapid proliferation of data. Users, groups of individuals, companies, as well as individual users, will be able to create text that they want to send, just as they do today with most messaging applications, without changing their habits. The intermediate level of communication is where security takes place. Each user's text/message that is sent/transmitted is encoded with a cryptographic algorithm to alter its form.

The specific algorithm used is considered the most secure up to the present moment, according to studies and experimental efforts made to breach it and steal the data. With the existence of such an application, the sense of security will increase, allowing communication to be fully utilized, as users will no longer fear attacks aimed at stealing their data and possibly much more.

This particular application adds an additional level of security due to the use of a more modern encryption algorithm at the time of its implementation. Moreover, the security of the keys, both public and private, used for encryption and decryption respectively, is enhanced.

Ευχαριστίες

Η συγκεκριμένη πτυχιακή εργασία ολοκληρώθηκε στα πλαίσια μελέτης για το ενδιαφέρον που προέκυψε από διάφορα ερεθίσματα σε προσωπικό επίπεδο μέσα από το περιβάλλον της ακαδημαϊκής εκπαίδευσης αλλά και ευρύτερων συζητήσεων στην καθημερινότητα.

Επίσης, θα ήθελα να εκφράσω τις ιδιαίτερες ευχαριστίες μου στον κύριο Δημήτριο Αμανατιάδη, για το ιδιαίτερο ενδιαφέρον και ζήλο που έδειξε για το θέμα τόσο σε πρακτικό όσο και θεωρητικό επίπεδο. Ακόμη για τις πολύ σημαντικές παρατηρήσεις και συμβουλές του αλλά και την γενικοτερη βοήθεια του σε όλη την ακαδημαική μου διαδρομή που με οδήγησε σε αυτό το αποτέλεσμα ως μηχανικό ανάπτυξης λογισμικού. Κλείνοντας, θα ήθελα να διευκρινίσω ότι τυχόν λάθη και παραλείψεις σε σχέση με το θέμα βαρύνουν αποκλειστικά τον υπεύθυνο σπουδαστή.

Περιεχόμενα

Συντομογραφίες

AES	Advanced Encryption Standard
ASCII	American Standard Code for Information Interchange
ECC	Elliptic Curve Cryptography
FDX	full duplex
FDDI	Fiber Distributed Data Interface
HDX	half-duplex
HTTP	Hypertext Transfer Protocol
HTTPS	Hypertext Transfer Protocol Secure
IMAP	Internet Message Access Protocol
IP	Internet Protocol
JVM	Virtual Machine
MAC	Message Authentication Code
OSI	Open Systems Interconnection
POP3	Post Office Protocol version 3
RSA	Ron Rivest, Adi Shamir και Len Adleman
SMTP	Simple Mail Transfer Protocol
SSL	Secure socket layer
TCP	Transmission Control Protocol
XML	*Extensible Markup Language*

Κεφάλαιο 1ο: Ιστορική αναδρομή στην επικοινωνία

1.1 Εισαγωγή

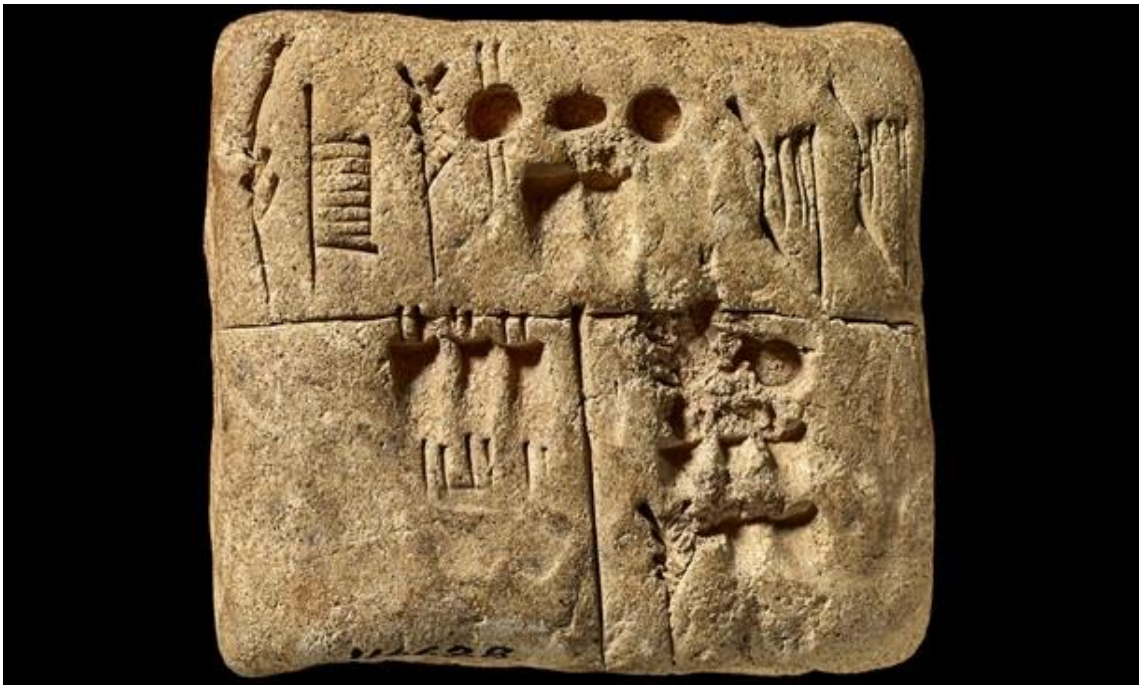
Η επικοινωνία αποτελεί ένα βασικό στοιχείο της ανθρώπινης κοινωνίας και αναπόσπαστο κομμάτι της καθημερινότητάς μας. Η ιστορία της επικοινωνίας εκτείνεται πίσω στους αρχαίους χρόνους, όπου η επικοινωνία βασιζόταν κυρίως στην προφορική και γραπτή γλώσσα και σε συμβολικά συστήματα, όπως οι ιερογλυφικές γραφές των αρχαίων Αιγυπτίων.

Με την πάροδο του χρόνου, η επικοινωνία εξελίχθηκε δραματικά και εμπλούτισε τη ζωή των ανθρώπων με νέα και πιο αποτελεσματικά μέσα επικοινωνίας. Η εφεύρεση του τηλεγράφου και του τηλεφώνου στα τέλη του 19ου αιώνα επέτρεψαν στους ανθρώπους να επικοινωνούν γρήγορα και αποτελεσματικά ακόμη και από μακρινές αποστάσεις.

Σήμερα, η επικοινωνία βασίζεται σε μια ποικιλία μέσων, όπως η τηλεόραση, το ραδιόφωνο, η διαδικτυακή επικοινωνία, οι κοινωνικές πλατφόρμες και άλλα. Η εξέλιξη της τεχνολογίας συνεχίζει να επιτρέπει τη δημιουργία νέων μέσων επικοινωνίας

1.2 Πρώτες προσπάθειες επικοινωνίας

Ως πρώτοι τρόποι επικοινωνίας έχουν καταγραφεί, σύμφωνα με ιστορικές μελέτες και ανακαλύψεις, σχεδιασμοί σε πέτρες, βράχους ή οτιδήποτε άλλο προσέφερε στον άνθρωπο αυτή την δυνατότητα, να καταγράψει δηλαδή αυτό που σκεφτόταν και δεν μπορούσε να εκφράσει με λέξεις, σκαλίζοντας διάφορα σχέδια.



Εικόνα 1, πρώτες προσπάθειες επικοινωνίας.

Άλλες μορφές επικοινωνίας που χρησιμοποιούσαν οι ζωντανοί οργανισμοί και χρησιμοποιούν ακόμα και σήμερα, είναι οι μη λεκτικές μορφές, οι χειρονομίες, η γλώσσα, η στάση του σώματος ακόμα και

ο τόνος της φωνής μπορεί να καταταχθεί σε αυτή την κατηγορία και με βεβαιότητα πλέον αποτελεί μια μορφή επικοινωνίας.

Περνώντας ειδικότερα στον άνθρωπο, η ιστορία της επικοινωνίας είναι μία από τις βασικότερες διαδικασίες στην ιστορία της ανθρωπότητας αφού αποτελεί δομικό συστατικό για :

- την επιβίωση
- την κοινωνικοποίηση
- την εξέλιξη
- ακόμη και για την μεταβίβαση πληροφοριών στον χώρο αλλά και στον χρόνο.

Λέγεται ότι η ιστορία της επικοινωνίας αρχίζει με την δημιουργία της γλώσσας. Η γλώσσα θεωρείται ως μια μοναδική ικανότητα της ανθρώπινης φυλής και το χαρακτηριστικό που είναι υπεύθυνο για την ανάπτυξη της κοινωνίας, διότι η μετάδοση του μηνύματος είναι δυνατή ανεξάρτητα από την πολυπλοκότητα του, σε αντίθεση με παλαιότερες χρονολογικές περιόδους, όπου η γλώσσα ως μορφή επικοινωνίας ήταν σε πρώιμο στάδιο (φωνές, κραυγές κ.α.), περιορίζοντας και δυσκολεύοντας την επικοινωνία.

Έτσι ο άνθρωπος κατάλαβε ότι αυτό το μέσο εξυπηρετούσε αποτελεσματικότερα τις ανάγκες του και είχε μεγάλες δυνατότητες. Με την πάροδο των χρόνων η γλώσσα αλλά και η επικοινωνία γενικότερα αναπτύχθηκαν. Με μια σύντομη έρευνα στην ιστορία μπορεί κανείς να γνωρίσει διαφορές μορφές που αποτυπώθηκαν.

1.3 Επικοινωνία μέσω σημάτων καπνού

Η επικοινωνία μέσω σημάτων καπνού, γνωστή και ως "σημάδια καπνού", ήταν μια μέθοδος επικοινωνίας που χρησιμοποιούνταν από διάφορες φυλές και κουλτούρες σε όλο τον κόσμο. Η μέθοδος αυτή βασιζόταν στην παραγωγή καπνού και τη χρήση ενός συγκεκριμένου τύπου φωτιάς για να παραχθούν οι σημάνσεις.

Από τις πρώτες αναφορές φαίνονται σε διάφορα βιβλία να υπάρχει η επικοινωνία μέσω σημάτων καπνού. Με την βοήθεια μιας κουβέρτας ή κάποιο παρόμοιο ύφασμα που σκέπαζαν και αποκάλυπταν την εστία της φωτιάς δημιουργούσαν σύννεφα καπνού τα οποία είχαν περιορισμένη εμβέλεια μετάδοσης αλλά μετέφεραν εξαιρετικά σημαντική πληροφόρηση για τον παρατηρητή.

Εικόνα 2, σήματα καπνού.

Οι σημαδούρες ήταν οι άνθρωποι που είχαν εξειδικευτεί στην χρήση της μεθόδου αυτής και μπορούσαν να στείλουν και να λάβουν σημάδια καπνού με εξαιρετική ακρίβεια. Η επικοινωνία μέσω

σημάτων καπνού ήταν ιδιαίτερα χρήσιμη σε περιοχές όπου οι αποστάσεις ήταν μεγάλες και η επικοινωνία με άλλα μέσα ήταν δύσκολη.

Παρόλο που η μέθοδος αυτή ήταν αποτελεσματική, είχε και τα μειονεκτήματά της, όπως την ανάγκη για σαφή και συνεννοήσιμα σήματα και την εξάρτησή της από κατάλληλες καιρικές συνθήκες. Με την εξέλιξη της τεχνολογίας, η επικοινωνία μέσω σημάτων καπνού έχει αντικατασταθεί από πιο εξελιγμένες μορφές.

1.4 Επικοινωνία μέσω ταχυδρομικών περιστεριών

Μία άλλη μορφή επικοινωνίας ήταν τα ταχυδρομικά περιστέρια. Πιστεύεται ότι η πρώτη αναφορά γίνεται στην Αρχαία Αίγυπτο περίπου τον 5ο αιώνα π.Χ. ενώ για κατοικίδια περιστέρια φτάνουμε στο 3.000 π.Χ. Τρόπος επικοινωνίας που χρησιμοποιήθηκε και πολύ αργότερα στην ιστορία, κατά τον πρώτο αλλά ακόμη και στον δεύτερο Παγκόσμιο πόλεμο. Αυτός ο τρόπος παρέχει μεγαλύτερη εμβέλεια, ακεραιότητα μηνύματος και περισσότερη σαφήνεια από τον προηγούμενο χρονολογικά αλλά αποτελεί και μία πιο ανεπτυγμένη μορφή, απαιτώντας όμως την ανάπτυξη της γλώσσας ακόμα περισσότερο σε σύγκριση με τον πρώτο τρόπο. Βέβαια ήταν πιο δύσκολος και ήθελε μεγαλύτερη προετοιμασία ώστε να επιτευχθεί.

Το χαρακτηριστικό των περιστεριών που τα βοηθάει να λειτουργούν ως “ταχυδρόμοι” και κατά συνέπεια ώς τα μέσα για να επιτευχθεί η επικοινωνία, είναι η ιδιότητα τους να επιστρέφουν στη φωλιά τους από εξαιρετικά μακρινές αποστάσεις. Πάνω σε αυτή την ιδιότητα βασίστηκαν οι άνθρωποι ώστε να μεταφέρουν τα γράμματά τους γρήγορα και αξιόπιστα. Δηλαδή, δεν μπορούμε να στείλουμε ένα περιστέρι σε κάποιο προορισμό. Αυτό που μπορεί να γίνει είναι να κρατάμε το περιστέρι σε ένα μέρος (διαφορετικό από τη φωλιά του) και να το αφήσουμε να γυρίσει στο σπίτι του μεταφέροντας και το γράμμα μας εκεί.

Εικόνα 3, ταχυδρομικά περιστέρια.

Όπως είναι προφανές, για να λειτουργήσει ένα τέτοιο ταχυδρομείο, έπρεπε κάποιος να διαθέτει περιστέρια γεννημένα και μεγαλωμένα σε διάφορες περιοχές, ώστε να μπορεί να στείλει τα απαραίτητα μηνύματα και να επικοινωνεί από μεγάλες αποστάσεις.

1.5 Επικοινωνία μέσω αγγελιοφόρων

Ένα παρόμοιο μέσο επικοινωνίας που ήρθε να εξαλείψει τα ελαττώματα των προηγούμενων είναι οι αγγελιοφόροι (έφιπποι ή πεζοί), άνθρωποι αυτή την φορά και όχι περιστέρια, είναι το μέσο που μεταφέρει το μήνυμα και ουσιαστικά επιτυγχάνει την επικοινωνία. Πιο έμπιστο μέσο, σε περίπτωση επιθέσεων, έλυσε το πρόβλημα του περιορισμού του τόπου γέννησης και ανατροφής που προϋπήρχε στην περίπτωση των περιστεριών, αυξάνοντας ωστόσο τον χρόνο και τις ανάγκες αυτής της ενέργειας μετάδοσης. Οι Αγγελιοφόροι πεζοί ή με άλογα ήταν κοινό φαινόμενο στην Αίγυπτο και στην Κίνα. Είχαν χτιστεί ακόμα και σταθμοί ανεφοδιασμού για αγγελιοφόρους.

Εικόνα 4, αγγελιοφόρος.

Δοκιμάζοντας και άλλες μορφές επικοινωνίας ανά τους αιώνες οι άνθρωποι προσπαθούσαν να κάνουν πιο ασφαλή, ακέραιο, αμεσότερο και γενικά να εξαλείψουν κινδύνους και απώλειες από την επικοινωνίας τους. Διάφορες μορφές όπως ο ηλιογράφος, πυρσίες, υδραυλικός τηλέγραφος του Αινεία, σηματοφόρος δείχνουν την ύπαρξη ποικίλων προβλημάτων αλλά και την ανάγκη του ανθρώπου να βρει το βέλτιστο σύστημα ώστε να επιτύχει την επικοινωνία εξαλείφοντας τα. Αυτό το στοιχείο δείχνει από μόνο του την αναγκαιότητα της επικοινωνίας στη ζωή των ανθρώπων, σε όλους τους τομείς της ανάπτυξης, της εξέλιξης, της άμυνας, ακόμη και της μετάβασης πληροφοριών στο χρόνο αλλά και σε άλλους τομείς.

1.6 Η πρώτη εφημερίδα

Έτσι φτάνουμε σε ένα πιο σύγχρονο μέσο επικοινωνίας το οποίο χρησιμοποιείται μέχρι σήμερα, την εφημερίδα, η οποία βασίζεται στο γραπτό λόγο για την μετάδοση της πληροφορίας.

Οι πρώτες εφημερίδες εντοπίστηκαν αρχικά στην εποχή του Μ. Αλεξάνδρου. Οι «Βασίλειες Εφημερίδες» όπως τις αποκαλούσαν ήταν ημερήσια φύλλα όπου περιέγραφαν ότι συνέβαινε καθημερινά στο βασίλειο της Μακεδονίας. Επίσης περιείχε λεπτομερή καταγραφή των γεγονότων του πολιτικού και στρατιωτικού κόσμου καθώς και τις προσωπικές ασχολίες του βασιλιά, ακροάσεις και μερικές πληροφορίες όσον αφορά το οικονομικά του κράτους. Τα αντίγραφα αυτών των εφημερίδων φυλάσσονταν και ήταν απόρρητα στο ευρύ κοινό. γεγονός που δείχνει την αναγκαιότητα της ασφάλειας και κατ’ επέκταση την ύπαρξη υποκλοπής δεδομένων που αποτυπώνονταν στις εφημερίδες

Εικόνα 5, εφημερίδα.

1.7 Ο Τηλέγραφος Μορς

Μία ακόμη πιο σύγχρονη μέθοδος επικοινωνίας, με μία μορφή κωδικοποίησης αυτή την φορά, ήρθε να καλύψει τις αδυναμίες των προηγούμενων προσφέροντας ασφάλεια, αποκλείοντας τους μη επιθυμητούς συμμετέχοντες στην επικοινωνίας που κάποιος ήθελε να δημιουργήσει ανάμεσα σε πομπό και δέκτη. Αυτή η μέθοδος δεν είναι άλλη από την πρώτη τηλεγραφική μηχανή που εφευρέθηκε από τον Samuel Morse το 1838. Ένας ηλεκτρικός τηλέγραφος ο οποίος αποτελείται από μια διάταξη με την οποία γραπτά σημεία μεταδίδονται από τον ένα σταθμό στον άλλο με τη βοήθεια του ηλεκτρικού ρεύματος. Κάθε τηλεγραφικό σύστημα αποτελείται από :

- την πηγή της ηλεκτρικής ενέργειας, που είναι ηλεκτρική στήλη, γεννήτρια ή συσσωρευτής
- το μηχάνημα - πομπό για την παραγωγή διακοπτόμενου ηλεκτρικού ρεύματος
- τη γραμμή για τη μεταβίβαση του ρεύματος από τον ένα σταθμό στον άλλο
- το μηχάνημα - δέκτη για τη λήψη των διακοπτόμενων ρευμάτων και τη μετατροπή τους σε γραπτά, ηχητικά ή οπτικά σημεία.

Εικόνα 6 τηλέγραφος Μορς.

Ο Μορς σκέφτηκε ότι θα μπορούσε να διαβιβάσει με δύο σύρματα ηλεκτρικό ρεύμα με 11 διακοπές. Οι διακοπές θα αντιπροσώπευαν τα γράμματα του αλφαβήτου. Έτσι επινόησε ένα αλφάβητο, που αποτελείται από ρεύμα μικρής και μεγάλης διάρκειας (στιγμές και γραμμές ή παύλες). Ο συνδυασμός στιγμών και γραμμών δίνει όλο το αλφάβητο και τους αριθμούς 0 έως 9. Η πρώτη σπουδαία τηλεγραφική επικοινωνία έγινε μεταξύ Ουάσιγκτον και Βαλτιμόρης στις Η.Π.Α. Αργότερα η ενσύρματη τηλεπικοινωνία τελειοποιήθηκε. Στην αρχή τα σήματα Μορς τα κατέγραφε η συσκευή λήψης πάνω σε ταινία. Κατόπιν χρησιμοποιήθηκαν ηχεία και η λήψη γινόταν κυρίως με το αφτί. Ο ενσύρματος τηλέγραφος αποτελείται από ένα διακόπτη, από έναν ηλεκτρονόμο, από μια μπαταρία και τις γραμμές σύνδεσης. Μαζί με αυτά υπάρχει και ένας ωρολογιακός μηχανισμός, που ξετυλίγει μια χάρτινη κορδέλα, πάνω στην οποία γίνεται η εγγραφή σημάτων του Μορς που εκπέμπει ο ανταποκριτής. Γράφονται δηλαδή αυτόματα κατά τη λήψη των σημάτων οι στιγμές και οι γραμμές που αποτελούν τα γράμματα των λέξεων.

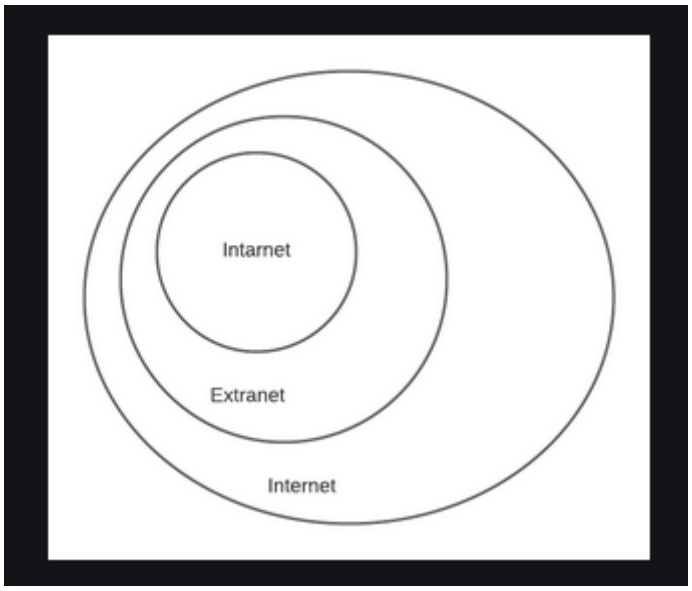
Φτάνοντας στο σημερινό ηλεκτρονικό ταχυδρομείο έχουμε πολλές περισσότερες δυνατότητες αλλά και πολλούς περισσότερους κινδύνους. Το ηλεκτρονικό ταχυδρομείο είναι μια υπηρεσία του Διαδικτύου, η οποία επιτρέπει τη συγγραφή, αποστολή, λήψη και αποθήκευση μηνυμάτων με χρήση ηλεκτρονικών συστημάτων τηλεπικοινωνιών. Γενικά ο όρος «ηλεκτρονικό ταχυδρομείο» αναφέρεται στο σύστημα ηλεκτρονικού ταχυδρομείου του Διαδικτύου που χρησιμοποιεί το Simple Mail Transfer Protocol πρωτόκολλο, σε δικτυακά συστήματα που βασίζονται σε άλλα πρωτόκολλα μεταφοράς μηνυμάτων, αλλά και σε διάφορα συστήματα μηνυμάτων σε μικρά δίκτυα, υπερυπολογιστές, κλπ που επιτρέπουν στους χρήστες τους να στέλνουν μηνύματα μεταξύ τους για την υποστήριξη ομαδικής επικοινωνίας. Τα συστήματα σε τοπικά δίκτυα ή σε δίκτυα intranet (intranet ορίζεται ως ένα ιδιωτικό δίκτυο μιας επιχείρησης ή οργανισμού) είναι πιθανόν να βασίζονται σε ιδιωτικά πρωτόκολλα, που υποστηρίζονται από το συγκεκριμένο σύστημα, ή να είναι τα ίδια πρωτόκολλα που χρησιμοποιούνται στα δημόσια δίκτυα.

1.8 Δίκτυα intranet, extranet & internet

Το intranet αναφέρεται συχνά σαν internet μέσα στην επιχείρηση. Οι πληροφορίες που διακινούνται δια μέσω ενός Intranet, δομούνται, αποθηκεύονται και παρουσιάζονται με χρήση τεχνολογίας Web. Οι

εργαζόμενοι έχουν πρόσβαση στο intranet μέσω των φυλλομετρητών τους που συνήθως είναι ρυθμισμένοι ώστε να ξεκινούν από την αρχική σελίδα του εταιρικού intranet. Από εκεί, οι εργαζόμενοι μπορούν να οδηγηθούν σε διάφορες εφαρμογές που βρίσκονται στο δίκτυο.

Ένα intranet μπορεί να αποτελείται από πολλά Local Area Networks μπορεί να χρησιμοποιεί επίσης γραμμές σε ένα Wide Area Network. Συνήθως, ένα intranet επικοινωνεί με το internet μέσω ενός ή περισσότερων πυλών (gateways). Ο κύριος σκοπός του είναι να διαμοιράσει τις πληροφορίες μιας εταιρείας και τους υπολογιστικούς πόρους, στους εργαζόμενους. Μπορεί επίσης να χρησιμοποιηθεί για να διευκολύνει την ομαδική εργασία και γενικά την επικοινωνία. Ένα intranet χρησιμοποιεί TCP/IP, HTTP και άλλα πρωτόκολλα του Internet. Συνήθως οι μεγάλες εταιρείες αφήνουν εξωτερικούς χρήστες να έχουν πρόσβαση στα intranets, μέσω firewalls (προγράμματα φιλτραρίσματος δεδομένων με σκοπό την ασφάλεια) έτσι ώστε να διασφαλίζεται η ακεραιότητα του intranet. Όταν ένα μέρος του Intranet μπορεί να προσεγγιστεί από πελάτες, προμηθευτές, κ.τ.λ., εκείνο το κομμάτι του δικτύου γίνεται extranet.



Εικόνα 7, intranet, extranet, internet.

Το intranet θα μπορούσε να περιγραφεί σαν το νευρικό σύστημα της εταιρείας. Σε αυτό αποθηκεύονται δομημένες πληροφορίες οι οποίες μπορούν να επεξεργαστούν, να χρησιμοποιηθούν από όλους και συνεχώς και να διακινούνται μέσω μιας εικονικής κοινότητας η οποία μπορεί να βρίσκεται διασκορπισμένη στη χώρα και να επικοινωνεί με ένα απόλυτα διαφανές δίκτυο. Αν υποθέσουμε δηλαδή ότι μία εταιρεία ή οργανισμός έχει εγκαταστήσει ένα intranet το οποίο επεκτείνεται μέσω γραμμών από τη Θεσσαλονίκη στην Αθήνα το Κιλκίς και την Ξάνθη, οι χρήστες μπορούν να έχουν διαφανή πρόσβαση στις πληροφορίες που χρειάζονται, ανεξάρτητα από το σημείο στο οποίο βρίσκονται. Για να υλοποιηθεί ένα intranet, συνήθως είναι αρκετός ο υπάρχων εξοπλισμός μιας επιχείρησης.

1.9 Επίλογος

Η ιστορία της επικοινωνίας είναι μακρά και πολυσύνθετη, καθώς έχει εξελιχθεί από την ανθρώπινη φωνή και την ανταλλαγή συμβόλων μέχρι την ψηφιακή εποχή. Μπορεί να διακριθεί σε διάφορες περιόδους και εξελίξεις, όπως ακολούθως:

1. Προϊστορική εποχή: Η επικοινωνία βασιζόταν στη φωνή και στη γλώσσα του σώματος.
2. Αρχαίος κόσμος: Η επικοινωνία εξελίχθηκε σε γραπτή μορφή με τη χρήση πινάκων και την ανάπτυξη της γλώσσας.
3. Μεσαίωνας: Η επικοινωνία εξελίχθηκε με την εφεύρεση των τύπων και των βιβλίων, καθώς και με την ανάπτυξη των επιστολών και των νέων δικτύων επικοινωνίας.
4. Νεότερη εποχή: Η επανάσταση των μέσων μαζικής επικοινωνίας και η ανάπτυξη των τηλεφώνων, τηλεόρασης, ραδιοφώνου, δορυφορικής επικοινωνίας και διαδικτύου επαναπροσδιόρισαν τον τρόπο που επικοινωνούμε.

Σήμερα, η επικοινωνία έχει γίνει πιο αποτελεσματική και απλή χάρη στη χρήση της τεχνολογίας. Με την ανάπτυξη της τεχνολογίας, η επικοινωνία έχει γίνει πιο άμεση, πιο προσβάσιμη και πιο αποτελεσματική. Μερικά από τα πιο κοινά μέσα επικοινωνίας σήμερα είναι:

1. Τηλέφωνο: Το τηλέφωνο είναι ένα από τα πιο βασικά μέσα επικοινωνίας. Με τη χρήση του τηλεφώνου, μπορούμε να επικοινωνήσουμε άμεσα με άλλα άτομα σε οποιοδήποτε μέρος του κόσμου.
2. Ηλεκτρονική αλληλογραφία: Η ηλεκτρονική αλληλογραφία ή email είναι ένα από τα πιο δημοφιλή μέσα επικοινωνίας. Με την ανάπτυξη της τεχνολογίας, οι άνθρωποι μπορούν να ανταλλάσσουν γρήγορα και εύκολα μηνύματα ηλεκτρονικού ταχυδρομείου ανεξαρτήτως της απόστασης.
3. Κοινωνικά δίκτυα: Τα κοινωνικά δίκτυα όπως το Facebook, το Twitter και το Instagram έχουν επαναπροσδιορίσει τον τρόπο που επικοινωνούμε μεταξύ μας.

Κεφάλαιο 2ο: Ανοικτή διασύνδεση συστημάτων

2.1 Εισαγωγή

Η ανοικτή διασύνδεση συστημάτων αναφέρεται στη δυνατότητα διασύνδεσης διαφορετικών συστημάτων και τεχνολογιών, που κατά κανόνα λειτουργούν ανεξάρτητα το ένα από το άλλο, έχει γίνει ευρέως αποδεκτή στη βιομηχανία τεχνολογίας και στον κόσμο της πληροφορικής, καθώς επιτρέπει στα συστήματα να επικοινωνούν και να συνεργάζονται πιο αποτελεσματικά.Επίσης, επιτρέπει την επαναχρησιμοποίηση και την επέκταση των υφιστάμενων συστημάτων, καθώς και την ενσωμάτωση νέων τεχνολογιών στα υπάρχοντα συστήματα. Αυτό έχει σημαντικές οικονομικές και λειτουργικές επιπτώσεις, καθώς επιτρέπει στις επιχειρήσεις να αναπτύσσονται και να προσαρμόζονται στις αλλαγές της αγοράς. Με αυτό τον τρόπο επιδρά άμμεσα στην κοινωνία, καθώς δίνει τη δυνατότητα στους ανθρώπους να επικοινωνούν και να μοιράζονται πληροφορίες και δεδομένα.

2.2 Τα επίπεδα OSI

Περνώντας στην σύγχρονη εποχή και αφήνοντας πίσω τους παραδοσιακούς τρόπους μετάδοσης μηνυμάτων, που αναφέρθηκαν σε προηγούμενο κεφάλαιο, η υλοποίηση ενός δικτύου επικοινωνίας είτε σε επίπεδο internet είτε σε επίπεδο intranet απαιτεί την παρουσία κατάλληλου μοντέλου αποτελούμενου από διάφορα πρωτόκολλα που ανά καιρούς αναπτύσσονται, επεκτείνονται και αυξάνονται, ώστε να παρέχουν καλύτερη και ασφαλέστερη επικοινωνία στα συστήματα και κατ επέκταση στους χρήστες του.

Ένα τέτοιο μοντέλο είναι το μοντέλο αναφοράς ανοικτής διασύνδεσης συστημάτων ή μοντέλο αναφοράς Open Systems Interconnection (OSI), αφηρημένη περιγραφή για τη σχεδίαση τηλεπικοινωνιακών και δικτυακών πρωτοκόλλων η οποία καθορίστηκε από την πρωτοβουλία Ανοικτή Διασύνδεση Συστημάτων – OSI το οποίο είναι γνωστό και ως *μοντέλο των επτά επιπέδων.*

Το *μοντέλο OSI* υποδιαιρεί τις λειτουργίες ενός τηλεπικοινωνιακού δικτύου σε μια «κατακόρυφη» στοίβα από επίπεδα, για το καθένα από τα οποία μπορεί να οριστεί κάποιο πρωτόκολλο σε μία συγκεκριμένη υλοποίηση. Κάθε επίπεδο αξιοποιεί τις λειτουργίες του κατωτέρου του στη στοίβα επιπέδου, ενώ στόχος του είναι να παρέχει λειτουργικότητα στο αμέσως ανώτερο επίπεδο του. Μία συγκεκριμένη υλοποίηση του μοντέλου, με καθορισμένα πρωτόκολλα για κάθε επίπεδο, ονομάζεται στοίβα πρωτοκόλλων ή απλά *στοίβα*. Το κάθε πρωτόκολλο υλοποιείται είτε σε υλικό είτε σε λογισμικό. Συνήθως τα κατώτερα επίπεδα υλοποιούνται στο υλικό ενώ τα ανώτερα σε λογισμικό.

Το μοντέλο *OSI* είναι στενά συσχετισμένο με τον κλάδο της επιστήμης των υπολογιστών και τη δικτύωση τους. Το βασικό χαρακτηριστικό του είναι η διασύνδεση μεταξύ των επιπέδων, η οποία υπαγορεύει τις προδιαγραφές της αλληλεπίδρασής τους. Αυτό σημαίνει ότι ένα επίπεδο υλοποιημένο με κάποιο συγκεκριμένο πρωτόκολλο μπορεί να συνεργαστεί με το γειτονικό του, στη στοίβα επίπεδο, το οποίο υλοποιείται με κάποιο άλλο πρωτόκολλο, υπό την προϋπόθεση ότι οι προδιαγραφές του καθενός έχουν δημοσιευθεί και έχουν γίνει αντιληπτές σωστά. Αυτές οι προδιαγραφές είναι τυπικά γνωστές ως RFC (*Requests for Comments*) και αποτελούν πρότυπα του Διεθνούς Οργανισμού Τυποποίησης ISO.

Συνήθως τα επίπεδα είναι αυστηρά διαχωρισμένα μεταξύ τους, αξιοποιούν τις υπηρεσίες του κατώτερου επιπέδου τους και προσφέρουν υπηρεσίες στο ανώτερό τους, αλλά το καθένα δεν παρεμβαίνει στις λειτουργίες του άλλου, πιθανόν να μη γνωρίζει καν γι' αυτές. Αυτός ο λογικός διαχωρισμός των επιπέδων διευκολύνει πολύ τη μελέτη της συμπεριφοράς των πρωτοκόλλων και

επιτρέπει τη σχεδίαση πολύπλοκων και αξιόπιστων στοιβών πρωτοκόλλων. Ορισμένες φορές όμως αυτή η αρχή ανεξαρτησίας των επιπέδων παραβιάζεται, για λόγους βελτιστοποίησης της απόδοσης ή αύξησης της λειτουργικότητας, με πρωτόκολλα διαφορετικών επιπέδων να συγχωνεύονται ή να παρεμβαίνουν το ένα στη λειτουργία του άλλου.

Το μοντέλο *OSI* είναι μια ιεραρχική δομή επτά επιπέδων που καθορίζει τις προδιαγραφές επικοινωνίας μεταξύ δύο υπολογιστών, ορίζοντας επακριβώς τον σκοπό κάθε επιπέδου αλλά και τα χρησιμοποιούμενα πρωτόκολλα, και τυποποιήθηκε ως πρότυπο ISO 7498-1. Θεωρήθηκε ότι θα επέτρεπε τη λειτουργική συνεργασία μεταξύ ποικίλων ψηφιακών συσκευών που ήταν διαθέσιμες στην αγορά. Το μοντέλο επιτρέπει σε όλα τα στοιχεία ενός δικτύου να συλλειτουργούν, με κάθε στοιχείο να υλοποιεί ένα ή περισσότερα πρωτόκολλα δικτύωσης, ανεξάρτητα από το ποιος είναι ο κατασκευαστής τους. Περί τα τέλη της δεκαετίας του 1980 ο ISO συνιστούσε την εφαρμογή του μοντέλου *OSI* ως κοινώς αποδεκτού υποδείγματος σχεδιασμού δικτύων.

Μοντέλο OSI			
	Μονάδα δεδομένων	**Επίπεδο**	**Λειτουργία**
Λογισμικό	Δεδομένα	7. Εφαρμογών	Παρέχεται στις εφαρμογές πρόσβαση στο δίκτυο
		6. Παρουσίασης	Αναπαράσταση δεδομένων και κρυπτογράφηση
		5. Συνόδου	Έλεγχος του διαλόγου μεταξύ των άκρων της επικοινωνίας
	Τμήμα	4. Μεταφοράς	Αξιόπιστη επικοινωνία από άκρο σε άκρο
Υλικό	Πακέτο	3. Δικτύου	Καθορισμός διαδρομών και λογικών διευθύνσεων των κόμβων στα πλαίσια ενός διαδικτύου
	Πλαίσιο	2. Ζεύξης δεδομένων	Φυσική διευθυνσιοδότηση (MAC & LLC)
	Bit	1. Φυσικό	Δυαδική μετάδοση σήματος μέσω του φυσικού μέσου

Εικόνα 8, επίπεδα OSI.

Ωστόσο εκείνη την εποχή η στοίβα πρωτοκόλλων Transmission Control Protocol/Internet Protocol *(*TCP/IP), η οποία βασιζόταν σε ελαφρώς διαφορετική διαστρωμάτωση επιπέδων, ήταν ήδη επί πολύ καιρό σε ευρεία χρήση. Το TCP/IP ήταν θεμελιώδες για το δίκτυο ARPANET και τα άλλα δίκτυα που εξελίχθηκαν στο σημερινό διαδίκτυο. Ως αποτέλεσμα το *μοντέλο OSI* παραμερίστηκε και σήμερα

μόνο ένα υποσύνολο του χρησιμοποιείται ακόμη. Η επικρατούσα αντίληψη είναι ότι οι περισσότερες προδιαγραφές του είναι περίπλοκες και η πλήρης λειτουργικότητά του θα χρειαζόταν μεγάλο χρόνο κατασκευής, αν και συνεχίζουν να υπάρχουν σθεναροί υποστηρικτές του.

2.2.1 Επίπεδο Εφαρμογών

Το επίπεδο εφαρμογών (application layer) παρέχει στον χρήστη έναν τρόπο να προσπελάσει μέσω μιας εφαρμογής τις πληροφορίες ενός δικτύου. Αυτό το επίπεδο είναι η κύρια διασύνδεση του χρήστη με την εφαρμογή και, συνεπώς, με το δίκτυο. Στο επίπεδο αυτό γίνεται η διαχείρισητων κατανεμημένων εφαρμογών, η αποστολή του ηλεκτρονικού ταχυδρομείου κλπ. Παραδείγματα πρωτοκόλλων επιπέδου εφαρμογών αποτελούν τα Telnet, FTP, SMTP και http.

2.2.2 Επίπεδο Παρουσίασης

Το επίπεδο παρουσίασης (*presentation layer*) μετασχηματίζει τα δεδομένα σε τυπική μορφή που την αναμένει το επίπεδο εφαρμογών. Στο επίπεδο αυτό τα δεδομένα υφίστανται κρυπτογράφηση, συμπίεση, κωδικοποίηση MIME και όποια άλλη διαμόρφωση απαιτεί η μορφή δεδομένων ή ο σχεδιαστής του πρωτοκόλλου. Παραδείγματα αποτελούν η μετατροπή αρχείων από κώδικα EBCDIC σε κώδικα ASCII και η μετατροπή της δομής των δεδομένων σε μορφή XML ή αντίστροφα (π.χ. από XML σε έγγραφο τύπου DOC).

2.2.3 Επίπεδο Συνόδου

Το επίπεδο συνόδου (session layer) ελέγχει τις συνόδους (δηλαδή τις ανταλλαγές δεδομένων) μεταξύ δύο υπολογιστών, του Α και του Β. Ξεκινά, διαχειρίζεται και τερματίζει τη σύνδεση μεταξύ μιας τοπικής και μιας απομακρυσμένης εφαρμογής. Αντιμετωπίζει λειτουργίες FDX (*full duplex, οι Α και Β μιλούν ταυτόχρονα από δύο κανάλια*) ή HDX (*half-duplex, μιλάει ο Α και μετά απαντάει ο Β από το ένα διαθέσιμο κανάλι*), ενώ υποστηρίζει διαδικασίες αποθήκευσης κατάστασης (checkpoint), αναβολής (adjournment), τερματισμού (termination) και επανεκκίνησης (restart).

Αυτό το επίπεδο είναι υπεύθυνο για το ομαλό κλείσιμο της συνόδου (που είναι ιδιότητα του TCP) και επίσης για την αποθήκευση και ανάκτηση κατάστασης, λειτουργίες οι οποίες δεν χρησιμοποιούνται στην στοίβα πρωτοκόλλων του Διαδικτύου.

2.2.4 Επίπεδο Μεταφοράς

Το επίπεδο μεταφοράς (transport layer) διεκπεραιώνει τη μεταφορά των δεδομένων από διεργασία σε διεργασία, απαλλάσσοντας έτσι τα ανώτερα επίπεδα από κάθε φροντίδα να προσφέρουν αξιόπιστη μεταφορά δεδομένων από το ένα άκρο της επικοινωνίας στο άλλο.

Το επίπεδο μεταφοράς ελέγχει την αξιοπιστία ενός χρησιμοποιούμενου καναλιού με έλεγχο ροής (*flow control*), κατάτμηση και αποτμηματοποίηση (segmentation / desegmentation), καθώς και έλεγχο σφαλμάτων (error control).

Ορισμένα πρωτόκολλα καταγράφουν καταστάσεις και συνδέσεις, οπότε κρατούν λογαριασμό των πακέτων και επανεκπέμπουν αυτά που δεν παρελήφθησαν σωστά. Τα διάφορα πρωτόκολλα μορφοποιούν διαφορετικά τα εκπεμπόμενα πακέτα πληροφοριών, αλλά τα προς αποστολή δεδομένα παραλαμβάνονται αρχικά από τα ανώτερα επίπεδα.

Το συνηθέστερο παράδειγμα πρωτοκόλλου μεταφοράς είναι το TCP (Transmission Control Protocol, πρωτόκολλο ελέγχου μετάδοσης). Άλλα πρωτόκολλα μεταφοράς είναι τα UDP (User Datagram

Protocol, πρωτόκολλο για ασυνδεσμική αποστολή δεδομένων, SCTP (Stream Control Transmission Protocol, πρωτόκολλο ελέγχου της ροής μετάδοσης), κλπ.

2.2.5 Επίπεδο Δικτύου

Το επίπεδο δικτύου (network layer) παρέχει τα λειτουργικά και διαδικαστικά μέσα για τη μεταφορά στοιχειοσειρών δεδομένων μεταβλητού μήκους από μια προέλευση σε έναν προορισμό, μέσα από ένα ή περισσότερα ενδιάμεσα δίκτυα, ενώ διατηρεί την ποιότητα εξυπηρέτησης που απαιτεί το επίπεδο μεταφοράς.

Εικόνα 9, δρομολογητής - router.

Το επίπεδο δικτύου εκτελεί λειτουργίες δρομολόγησης, με πιθανές κατατμήσεις / αποτμηματοποιήσεις, και αναφέρει σφάλματα σχετικά με την παράδοση των πακέτων. Οι δρομολογητές (routers) λειτουργούν στο επίπεδο αυτό· διακινώντας δεδομένα σε διασυνδεδεμένα δίκτυα έκαναν το Διαδίκτυο πραγματικότητα. Υπάρχουν και δικτυακοί διακόπτες που σχετίζονται με τις διευθύνσεις (IP). Εδώ υπάρχει μια λογική οργάνωση και τις τιμές των διευθύνσεων τις καθορίζει ιεραρχικά ο τεχνικός των επικοινωνιών. Το πλέον αναγνωρίσιμο παράδειγμα πρωτοκόλλου δικτύου είναι το Πρωτόκολλο Διαδικτύου (Internet Protocol, IP).

2.2.6 Επίπεδο Ζεύξης Δεδομένων

Το επίπεδο ζεύξης (data link layer) δεδομένων παρέχει τα λειτουργικά και διαδικαστικά μέσα για τη μεταφορά δεδομένων από μια συσκευή ενός τοπικού δικτύου σε άλλη, αλλά και για την ανίχνευση και διόρθωση σφαλμάτων που συμβαίνουν στο φυσικό επίπεδο. Οι μη ιεραρχημένες διευθύνσεις των συσκευών εδώ είναι οι φυσικές (π.χ. MAC διευθύνσεις), δηλαδή είναι προκαθορισμένες και αποθηκευμένες στις κάρτες δικτύου των επικοινωνούντων κόμβων από το εργοστάσιο.

Το πιο γνωστό πρότυπο αυτού του επιπέδου είναι το Ethernet, για τοπικά δίκτυα. Άλλα παραδείγματα πρωτοκόλλων ζεύξης δεδομένων αποτελούν τα:

- HDLC και ADCCP, για συνδέσεις από-σημείο-σε-σημείο (point-to-point).
- 802.11, για ασύρματα τοπικά δίκτυα.

Αυτό το επίπεδο, στα τοπικά δίκτυα της οικογένειας πρωτοκόλλων IEEE 802.X, και σε κάποια άλλα όπως το FDDI, μπορεί να διαιρεθεί σε δύο μικρότερα:

- Ένα επίπεδο ελέγχου πρόσβασης στο κοινό μέσο, το υποεπίπεδο MAC (Media Access Control, Έλεγχος Πρόσβασης Μέσου)

- Ένα ανώτερο επίπεδο ελέγχου λογικών συνδέσεων, το υποεπίπεδο LLC (Logical Link Control, Έλεγχος Λογικών Ζεύξεων), όπου επικρατεί καθολικά το πρωτόκολλο IEEE 802.2 ανεξάρτητα από το υποκείμενο πρωτόκολλο MAC ή φυσικού επιπέδου.

Στο επίπεδο αυτό λειτουργούν οι δικτυακές γέφυρες (bridge) και οι δικτυακοί διακόπτες (switch). Η συνδεσιμότητα παρέχεται μόνο για κόμβους που συνδέονται στο ίδιο κοινό μέσο (τοπικό δίκτυο ή σύνδεση από-σημείο-σε-σημείο).

2.2.7 Φυσικό Επίπεδο

Το φυσικό επίπεδο (physical layer) ορίζει όλες τις ηλεκτρικές και φυσικές προδιαγραφές της επικοινωνίας. Σ' αυτές περιλαμβάνονται οι σχηματισμοί των ακίδων, οι επιτρεπτές τάσεις, οι προδιαγραφές των καλωδίων κλπ. Συσκευές φυσικού επιπέδου είναι οι διανεμητές, οι επαναλήπτες (repeaters), οι κάρτες δικτύου, οι προσαρμοστές διαύλου (bus adapters). Οι κυριότερες λειτουργίες και υπηρεσίες του φυσικού επιπέδου είναι:

- Έναρξη και τερματισμός της ηλεκτρικής σύνδεσης μιας επικοινωνιακής συσκευής.
- Συμμετοχή σε διαδικασίες όπου οι επικοινωνιακές συσκευές εξυπηρετούν αποτελεσματικά πολλούς χρήστες (πολυπλεξία). Επιλύονται προβλήματα προτεραιότητας πρόσβασης και ελέγχου ροής δεδομένων.
- Διαμόρφωση και αποδιαμόρφωση των ψηφιακών δεδομένων κατά τη μετάδοση από συσκευή σε συσκευή. Για παράδειγμα, τα ψηφιακά ηλεκτρικά σήματα μπορεί να ταξιδέψουν ως αναλογικά σε χάλκινο καλώδιο, μετά σε οπτική ίνα, μετά να μεταδοθούν από ραδιοζεύξη ή δορυφορικά, να φτάσουν πάλι αναλογικά σε χάλκινο καλώδιο και να γίνουν ψηφιακά στον παραλήπτη.

Εικόνα 10, διανεμητής.

Οι παράλληλοι δίαυλοι SCSI λειτουργούν στο επίπεδο αυτό. Επίσης τα επίπεδα 1 και 2 αφορούν οι προδιαγραφές των πρωτοκόλλων Ethernet, Token Ring, FDDI (Fiber Distributed Data Interface, Διασύνδεση Κατανεμημένων Δεδομένων με Οπτικές Ίνες) και IEEE 802.11

2.3 Επίλογος

Στον επικοινωνιακό κόσμο, τα επίπεδα OSI παρέχουν ένα κοινό πλαίσιο αναφοράς για τη σχεδίαση, την ανάπτυξη και την κατανόηση των δικτυακών συστημάτων. Από τη φυσική σύνδεση του υλικού

μέχρι την εφαρμογή λογισμικού, τα επίπεδα OSI παρέχουν μια σειρά από πρωτόκολλα και διεπαφές που διασφαλίζουν τη σωστή λειτουργία και την ασφάλεια των δικτύων.

Παρόλο που τα επίπεδα OSI είναι ένα θεωρητικό πλαίσιο, έχουν επιτρέψει στους κατασκευαστές δικτύων και στους προγραμματιστές να αναπτύξουν πρωτόκολλα και εφαρμογές που επιτρέπουν την ανταλλαγή πληροφοριών μεταξύ συσκευών από διαφορετικούς κατασκευαστές και με διαφορετικές λειτουργίες.

Η σημασία των επιπέδων OSI έγκειται στο γεγονός ότι προσφέρουν ένα κοινό πλαίσιο κατανόησης για τους ανθρώπους που εργάζονται σε διαφορετικές πτυχές της δικτυακής τεχνολογίας, από τον σχεδιαστή δικτύων έως τον προγραμματιστή λογισμικού.

Τέλος, τα 7 στρώματα OSI αποτελούν μια κοινή γλώσσα για τους επαγγελματίες δικτύων και τη βιομηχανία επικοινωνιών. Αυτό διευκολύνει την ανταλλαγή ιδεών, τη διεπαφή μεταξύ συστημάτων διαφορετικών κατασκευαστών και την ανάπτυξη κοινών προτύπων και πρακτικών.

Κεφάλαιο 3ο: Επικοινωνία με ασφάλεια

3.1 Εισαγωγή

Η επικοινωνία με ασφάλεια είναι ένα σημαντικό κομμάτι της σύγχρονης κοινωνίας και αποτελεί βασικό πυλώνα για τη διασφάλιση της προστασίας των δεδομένων και της ιδιωτικότητας στον κυβερνοχώρο. Η ασφάλεια της επικοινωνίας αφορά την προστασία των πληροφοριών που ανταλλάσσονται μεταξύ των υπολογιστών, των συστημάτων και των δικτύων, και αυτό μπορεί να επιτευχθεί μέσω της εφαρμογής αποτελεσματικών μέτρων ασφαλείας.

Στη σύγχρονη κοινωνία, η επικοινωνία με ασφάλεια αποτελεί προτεραιότητα για πολλές επιχειρήσεις και οργανισμούς, καθώς η διαρροή ευαίσθητων πληροφοριών μπορεί να έχει σοβαρές συνέπειες για την επιχείρηση ή τους πελάτες της. Επιπλέον, με την αυξανόμενη χρήση του διαδικτύου και της ηλεκτρονικής αλληλογραφίας, η ασφάλεια της επικοινωνίας είναι πιο σημαντική από ποτέ. Οι προσπάθειες για τη διατήρηση της ασφάλειας της επικοινωνίας περιλαμβάνουν την κρυπτογάφηση των δεδομένων προς αποστολή.

3.2 Η άνοδος του διαδικτύου

Με την άνοδο στη χρήση του διαδικτύου, μεταφέραμε σε αυτό ένα τεράστιο μέρος της επικοινωνίας μας. Καθώς το διαδίκτυο ως μέσο επικοινωνίας βασίζεται σε εκατομμύρια υπολογιστές που διαχειρίζονται τη μεταφορά των τμημάτων πληροφοριών που ανταλλάσσουμε, στην πορεία αυτή αφήνουμε ίχνη της επικοινωνίας και δεδομένα προσωπικά (ίσως πολύ σημαντικά) τόσο για εμάς αλλά και για κακόβουλους χρήστες με σκοπό την εκμετάλλευση τους.

Οι πληροφορίες από μία ανταλλαγή μπορεί να μην παρέχουν πολλές σημαντικές λεπτομέρειες σε τρίτους, όμως επειδή χρησιμοποιούμε τόσο πολύ το διαδίκτυο, η τεράστια ποσότητα πληροφοριών που μένει πίσω, όσο κατακερματισμένη και αν είναι, μπορεί τελικά να συνδυαστεί ώστε να ταυτοποιηθείτε και σε πολλές περιπτώσεις να οδηγήσει σε κινδύνους. Μέσα από την αποκάλυψη δεδομένων μπορεί επίσης να διαρρεύσουν οι προσωπικές πληροφορίες στο διαδίκτυο οι οποίες μπορεί να προσελκύσουν ακόμα περισσότερους ενδιαφερόμενους με μη επιθυμητό σκοπό αυξάνοντας τις επιρροές των κινδύνων χωρίς κάποιο τέλος σε όλη αυτή την επιβλαβή διαδικασία.

3.3 Η αναγκαιότητα της ιδιωτικότητας

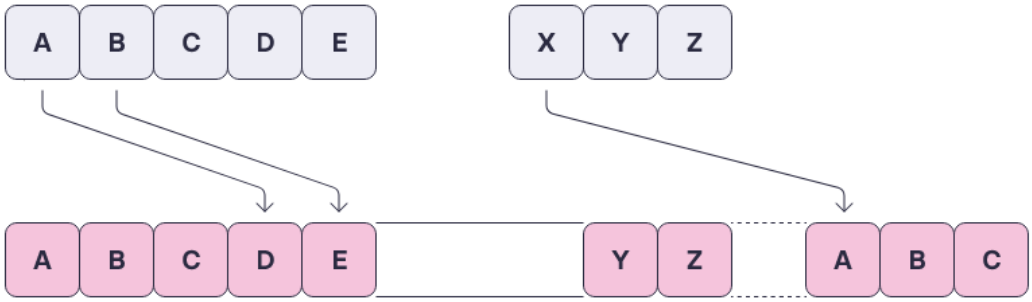
Είναι σημαντικό να διατηρείται ιδιωτική η επικοινωνία προκειμένου να περιοριστούν οι πληροφορίες που αφήνονται πίσω. Όταν προφυλάσσεται η επικοινωνία, ουσιαστικά κρύβονται οι πληροφορίες από πηγές που είναι δημόσια διαθέσιμες. Οι περισσότεροι τρόποι για να διατηρηθεί ιδιωτική η επικοινωνία βασίζονται στην κρυπτογράφηση. Ουσιαστικά, η κρυπτογράφηση κρύβει την επικοινωνία από όλους τους άλλους υπολογιστές μέσα από τους οποίους ταξιδεύουν οι πληροφορίες. Ο αλγόριθμος κρυπτογράφησης είναι αυτός που προσδιορίζει πόσο ασφαλής είναι η κρυπτογράφηση, όμως επειδή τα δεδομένα τα διαχειρίζονται μη ασφαλείς υπολογιστές, ο τρόπος που ανταλλάσσονται τα κλειδιά κρυπτογράφησης μπορεί επίσης να είναι το αδύναμο σημείο.

Δεν χρειάζεται να κατανοηθούν όλες τις λεπτομέρειες της κρυπτογράφησης, ας δούμε όμως κάποιες πολύ βασικές πληροφορίες σχετικά με τις απλές μεθόδους της. Άλλωστε, η κρυπτογραφία χρησιμοποιείται εδώ και χιλιάδες χρόνια με διάφορες μορφές. Οι πρώτοι χρήστες της κρυπτογράφησης που γνωρίζουμε μάλλον ήταν οι Αιγύπτιοι, αν και απλές αντικαταστάσεις

περιεχομένου μηνυμάτων για την απόκρυψη του αρχικού μηνύματος ενδεχομένως να χρησιμοποιούνταν ακόμα και από πιο παλιά.

3.4 Πρώτες μορφές κρυπτογράφησης

Οι Ρωμαίοι χρησιμοποιούσαν αρκετά συχνά την κρυπτογραφία. Ήταν γνωστό ότι ο Ιούλιος Καίσαρας χρησιμοποιούσε κάποια μορφή κώδικα αντικατάστασης, η οποία σήμερα είναι γνωστή ως κώδικας του Καίσαρα. Ο κώδικας είναι ένας όρος που περιγράφει έναν αλγόριθμο που χρησιμοποιείται για την κρυπτογράφηση και αποκρυπτογράφηση δεδομένων. Ο κώδικας αντικατάστασης είναι ένας κώδικας όπου ένας χαρακτήρας αντικαθίσταται από έναν άλλον που προσδιορίζεται με κάποιον τρόπο. Για παράδειγμα, ο Καίσαρας χρησιμοποιούσε έναν κώδικα όπου το κάθε γράμμα ήταν γραμμένο με τέτοιο τρόπο που αντικαθιστούσε τον χαρακτήρα με τον τρίτο από αυτόν σε αλφαβητική σειρά, π.χ. το Α γινόταν Δ, το Β γινόταν Ε κ.ο.κ.



Εικόνα 11, κρυπτογράφηση.

Όπως φαίνεται στην παραπάνω εικόνα, το κλειδί για αυτή την «κρυπτογράφηση» είναι «κινηθείτε τρία βήματα προς τα εμπρός στο αλφάβητο». Ενδέχεται να μπορεί να "αποκρυπτογραφηθεί" αυτό το είδος κώδικα ανάλογα με το πόσο μυστικό μπορεί να διατηρηθεί το σύστημα αντί για το κλειδί. Στο παράδειγμα του κώδικα του Καίσαρα, το κλειδί θα μπορούσε να είναι οτιδήποτε και θα μπορούσατε να υπολογισθεί αρκετά εύκολα απλώς δοκιμάζοντας όλους τους συνδυασμούς (*brute forcing*) ή χρησιμοποιώντας τη συχνότητα των γραμμάτων μιας γλώσσας. Για παράδειγμα, αν το γράμμα Ρ είναι το γράμμα που χρησιμοποιείται πιο συχνά στο κρυπτογραφημένο μήνυμα και η γλώσσα γνωρίζουμε ότι είναι η αγγλική, είναι λογικό να υποθέσουμε ότι το Ρ στο μυστικό μήνυμα είναι το Ε στο μήνυμα απλού κειμένου, καθώς το Ε είναι το πιο κοινό γράμμα στην αγγλική γλώσσα. Διαφορετικές εκδοχές κωδίκων αντικατάστασης χρησιμοποιούνταν για τουλάχιστον χίλια χρόνια μέχρι τα μαθηματικά να προσφέρουν καλύτερους τρόπους κρυπτογράφησης.

Να σημειώσουμε ότι η κρυπτογράφηση δεν χρειάζεται να είναι τέλεια. Σε συγκρούσεις όπως σε πολεμικές συρράξεις, διασφαλίζοντας απλώς ότι το μήνυμα δεν θα διαβαστεί μέσα σε μερικά λεπτά ή μερικές ώρες μπορεί να είναι εξαιρετικά σημαντικό. Όμως, σε περιπτώσεις όπου τα κρυπτογραφημένα δεδομένα είναι εμπιστευτικά και μπορούν να προκαλέσουν ζημιά και αργότερα, θα πρέπει να φροντίσετε ώστε η μέθοδος που χρησιμοποιείται να μην είναι εύκολα διαβλητή.

3.5 Ο κώδικας *Vigenère*

Κατά τον 16ο αιώνα, αναπτύχθηκε ένας καινούριος και καλύτερος τρόπος κρυπτογράφησης που προσέφερε προστασία από τις επιθέσεις συχνότητας. Ο κώδικας *Vigenère* χρησιμοποιεί ένα

επαναλαμβανόμενο κλειδί, νικώντας έτσι την απλή χρήση της ανάλυσης συχνότητας καθώς το γράμμα *P* δεν ταιριάζει πλέον με το γράμμα *E* στα περισσότερα από τα κρυπτογραφημένα κείμενα. Ο κώδικας *Vigenère* χρησιμοποιεί ένα μεταβλητό κλειδί που κάνει τον απλό κώδικα αντικατάστασης πιο ανθεκτικό. Το κλειδί επαναλαμβάνεται ώστε να καλύψει το πλήρες μήκος του μηνύματος. Το μήκος του κλειδιού είναι το πιο σημαντικό μέρος του κώδικα *Vigenère* καθώς με μήκος κλειδιού 1, ο κώδικας είναι βασικά ένας κώδικας του Καίσαρα. Παρακάτω παρατίθεται ένα παράδειγμα.

	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
A	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
B	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A
C	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B
D	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C
E	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D
F	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E
G	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F
H	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G
I	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H
J	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I
K	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J
L	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K
M	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L
N	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M
O	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N
P	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O
Q	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P
R	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q
S	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R
T	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S
U	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T
V	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U
W	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V
X	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W
Y	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X
Z	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y

Εικόνα 12, κωδικας Vigenère.

Ένα παράδειγμα ενός τετραγώνου *Vigenère.* Διαπιστώνεται εύκολα ότι αυτή η έκδοση του κώδικα *Vigenère* είναι κατά βάση ένας κώδικας του Καίσαρα που μετατοπίζεται κυκλικά.

Όπως φαίνεται στον παραπάνω πίνακα, χρησιμοποιώντας ένα κλειδί με μόνο τον χαρακτήρα «D», ο κώδικας είναι πανομοιότυπος με τον κώδικα που χρησιμοποιούσε ο Καίσαρας στα μηνύματά του. Χρησιμοποιώντας τον πίνακα, αν παρατηρηθεί η σειρά D και από τη στήλη A θα βρούμε το γράμμα A να είναι κρυπτογραφημένο ως το γράμμα D, όπως στον κώδικα του Καίσαρα.

Για να κατανοήσουμε την ισχύ του κώδικα *Vigenère*, ας δούμε ένα πιο ολοκληρωμένο παράδειγμα με ένα μεγαλύτερο κλειδί. Χρησιμοποιώντας το τετράγωνο *Vigenère* παραπάνω (ονομάζεται και πίνακας *Vigenère*), μπορούμε να κρυπτογραφήσουμε το μήνυμα απλού κειμένου «CYBERSECURITY» με το κλειδί «SECRET» επαναλαμβάνοντας το τόσες φορές ώστε να ταιριάξει το μήκος του κλειδιού με το επιθυμητό κείμενο.

Βήμα 1ο :

Μήνυμα: CYBERSECURITY

Κλειδί: SECRETSECRETS

Κρυπτογραφημένο κείμενο:

Πρώτα πρέπει να βρεθεί η στήλη που αντιστοιχεί στο γράμμα C στη σειρά S στον πίνακα. Χρησιμοποιώντας τον πίνακα βρίσκεται ότι είναι το γράμμα U. Εισάγεται ως το πρώτο γράμμα του κρυπτογραφημένου κειμένου.

Βήμα 2ο :

Μήνυμα: CYBERSECURITY

Κλειδί: SECRETSECRETS

Κρυπτογραφημένο: U

Το επόμενο γράμμα του μηνύματος είναι το Y στη σειρά E (δεύτερο γράμμα του κλειδιού κρυπτογράφησης). Το αποτέλεσμα είναι το γράμμα C. Προσθέτοντάς το στην κρυπτογράφηση βλέπουμε ότι τα δύο πρώτα γράμματα του κρυπτογραφημένου κειμένου (κρυπτοκείμενο) είναι UC.

Βήμα 3ο :

Μήνυμα: CYBERSECURITY

Κλειδί: SECRETSECRETS

Κρυπτογραφημένο: UC

Ακολουθώντας την ίδια διαδικασία, καταλήγουμε με το τελικό κρυπτογραφημένο κείμενο:

Βήμα 14ο :

Μήνυμα: CYBERSECURITY

Κλειδί: SECRETSECRETS

Κρυπτογραφημένο: UCDVVLWGWIMMQ

Έτσι κρυπτογραφούμε με τον κώδικα *Vigenère*. Ο κώδικας χρησιμοποιήθηκε επιτυχώς για περίπου τρεις αιώνες μέχρι που ανακαλύφθηκε μια μέθοδος γενικής αποκρυπτογράφησης. Παρ' όλα αυτά, κάποια μηνύματα είχαν πιθανότατα αποκρυπτογραφηθεί νωρίτερα καθώς η μυστικότητα του μηνύματος εξαρτάται από τη μυστικότητα και την ποιότητα του κλειδιού.

Ο κώδικας *Vigenère* παρέμεινε ασφαλής για μεγάλο χρονικό διάστημα, όμως τον 19ο αιώνα αναγνωρίστηκαν και δημοσιεύτηκαν γενικές αδυναμίες. Με τη χρήση αυτών των μεθόδων, η κρυπτογράφηση παραβιάζοταν ανεξάρτητα από το κλειδί που χρησιμοποιούταν. Οι επιθέσεις βασίζονται σε αδυναμίες και στην επανάληψη του κλειδιού στον αλγόριθμο για την εύρεση του μήκους του κλειδιού (ή τα πιθανά μήκη του κλειδιού) και με αυτή την πληροφορία μπορεί να χρησιμοποιηθεί μια επίθεση αποκλεισμού κλειδιών ώστε να βρεθεί το κλειδί που χρησιμοποιήθηκε. Μπορούν να χρησιμοποιηθούν πολλές διαφορετικές μέθοδοι για την εύρεση του μήκους του κλειδιού με υψηλό ποσοστό βεβαιότητας.

Μια μορφή του κώδικα *Vigenère* χρησιμοποιήθηκε επίσης από τις δυνάμεις της συνομοσπονδίας κατά τον αμερικανικό εμφύλιο πόλεμο. Μέχρι τότε, οι δυνάμεις της ένωσης αποκρυπτογραφούσαν συχνά τα μηνύματά τους καθώς είχαν βρεθεί πολλές αδυναμίες στον κώδικα.

Ένας κώδικας *Vigenère* που χρησιμοποιεί ένα πραγματικά τυχαίο κλειδί με μήκος κλειδιού ίδιο με εκείνο του μηνύματος απλού κειμένου θεωρείται κωδικός που δεν αποκρυπτογραφείται και ονομάζεται **one-time pad** (σημειωματάριο μιας χρήσης). Το σημειωματάριο μιας χρήσης δεν φέρει τις αδυναμίες που σχετίζονται με το επαναλαμβανόμενο κλειδί. Καθώς οι επιθέσεις λεξικού δεν έχουν εφαρμογή σε πραγματικά τυχαία κλειδιά, η μυστικότητα του μηνύματος βασίζεται στο κλειδί και όχι στον κώδικα. Όμως, η χρήση του σημειωματαρίου μίας χρήσης είναι δύσκολη καθώς το αδύνατο σημείο θα είναι ο τρόπος ανταλλαγής του κλειδιού μεταξύ των μερών.

Με την εφεύρεση της μηχανολογίας, νέες και καλύτερες μέθοδοι εφευρέθηκαν στο πεδίο της κρυπτογράφησης. Δημιουργήθηκαν μηχανές όπου το πάτημα ενός πλήκτρου άναβε το κρυπτογραφημένο γράμμα. Αυτές οι πρώτες μηχανές μηχανικής κρυπτογράφησης επέκτειναν επίσης το μήκος του λεξιλογίου προσθέτοντας περιστρεφόμενα γρανάζια το ένα δίπλα στο άλλο. Όταν ένα γρανάζι με 26 χαρακτήρες περιστρέφονταν από το A έως το Z, ένα άλλο μετακινούνταν κατά ένα βήμα παρακάτω με αποτέλεσμα να αποκρύπτεται το επαναλαμβανόμενο μοτίβο του κλειδιού. Ένα μόνο γρανάζι παρείχε ένα κλειδί μήκους 26 χαρακτήρων. Προσθέτοντας ακόμα ένα γρανάζι που κινείται, επέκτεινε τις διαθέσιμες θέσεις σε 26 x 26 = 676. Για τη ρύθμιση του κοινού κλειδιού θα έπρεπε απλώς να ενημερώσετε το άλλο μέρος για την αρχική κατάσταση των δύο γραναζιών.

Αν υποθέσουμε ότι έχουμε τρία γρανάζια και η αρχική ρύθμιση για όλα είναι A, θα έχουμε τις ακόλουθες θέσεις για κάθε διαδοχικό πάτημα πλήκτρου:

A A A

B A A

C A A

D A A

…

Z A A

A B A

B B A

…

Y Z Z

Z Z Z

A A A

Η πραγματική εγκατάσταση, η καλωδίωση και ο τρόπος που λειτουργούν οι μηχανές είναι πιο περίπλοκος από το παράδειγμα, όμως δείχνει την ισχύ της αυτοματοποίησης της δημιουργίας του πραγματικού κλειδιού κρυπτογράφησης από την αρχική ρύθμιση των μηχανών.

3.6 Σύγχρονοι τρόποι κρυπτογράφησης

Οι σύγχρονοι τρόποι κρυπτογράφησης περιλαμβάνουν τη συμμετρική και την ασύμμετρη κρυπτογράφηση. Η συμμετρική κρυπτογράφηση αναφέρεται σε μια διαδικασία κρυπτογράφησης, όπου τα ίδια κλειδιά χρησιμοποιούνται τόσο για την κρυπτογράφηση όσο και για την αποκρυπτογράφηση των δεδομένων. Η ασυμμετρη κρυπτογράφηση σε αντίθεση, αναφέρεται στην κρυπτογράφηση όπου τα δύο κλειδιά που χρησιμοποιούνται για την κρυπτογράφηση και αποκρυπτογράφηση είναι διαφορετικά. Αυτό σημαίνει ότι το κλειδί που χρησιμοποιείται για την κρυπτογράφηση δεν μπορεί να χρησιμοποιηθεί για την αποκρυπτογράφηση και αντίστροφα.

3.6.1 Συμμετρική κρυπτογράφηση

Η συμμετρική κρυπτογράφηση είναι ένας τύπος κρυπτογράφησης όπου η ίδια μέθοδος κλειδιού χρησιμοποιείται τόσο για την κρυπτογράφηση όσο και για την αποκρυπτογράφηση των δεδομένων. Αυτό σημαίνει ότι ο αποστολέας και ο παραλήπτης χρησιμοποιούν το ίδιο κλειδί για την ασφαλή μεταφορά των πληροφοριών. Το συμμετρικό κλειδί είναι μια ακολουθία ψηφίων ή χαρακτήρων που χρησιμοποιείται τόσο για την κρυπτογράφηση όσο και για την αποκρυπτογράφηση των δεδομένων. Αυτό το κλειδί είναι μυστικό και πρέπει να είναι γνωστό μόνο από τον αποστολέα και τον παραλήπτη των κρυπτογραφημένων δεδομένων. Ο αποστολέας χρησιμοποιεί το συμμετρικό κλειδί για να μετασχηματίσει τα αρχικά δεδομένα σε κρυπτογραφημένα δεδομένα με τη χρήση ενός αλγορίθμου κρυπτογράφησης. Στη συνέχεια, τα κρυπτογραφημένα δεδομένα μπορούν να αποσταλούν ασφαλώς στον παραλήπτη. Ο παραλήπτης, γνωρίζοντας το ίδιο συμμετρικό κλειδί, μπορεί να το χρησιμοποιήσει για να αποκρυπτογραφήσει τα δεδομένα και να τα επαναφέρει στην αρχική τους αναγνώσιμη μορφή. Η ασφάλεια της συμμετρικής κρυπτογραφίας εξαρτάται από την ασφάλεια του κλειδιού. Είναι σημαντικό να διατηρείται το κλειδί μυστικό και να μην πέφτει σε ανεπιθύμητα χέρια, καθώς η γνώση του κλειδιού επιτρέπει σε οποιονδήποτε το διαθέτει να αποκρυπτογραφήσει τα δεδομένα. Επειδή η ίδια μέθοδος παραγωγής κλειδιού χρησιμοποιείται για την κρυπτογράφηση και την αποκρυπτογράφηση, η διαδικασία είναι συνήθως πολύ γρήγορη και αποδοτική. Ωστόσο, η πρόκληση με τη συμμετρική κρυπτογράφηση είναι η ασφάλεια του κλειδιού. Ο αποστολέας και ο παραλήπτης πρέπει να γνωρίζουν και να διατηρούν μυστικό το κλειδί που χρησιμοποιείται. Εάν ένας επιτιθέμενος αποκτήσει πρόσβαση στο κλειδί, μπορεί να αποκρυπτογραφήσει τα δεδομένα και να έχει πρόσβαση σε ευαίσθητες πληροφορίες. Για την ασφάλεια, είναι σημαντικό να χρησιμοποιούνται ασφαλή κλειδιά και να εφαρμόζονται κατάλληλες πρακτικές για τη διαχείριση των κλειδιών. Επίσης, η ασφάλεια μπορεί να ενισχυθεί με τη χρήση προηγμένων αλγορίθμων κρυπτογράφησης και την εφαρμογή κατάλληλων πρωτοκόλλων ασφαλείας. Τα πλεονεκτήματά της είναι:

- Ταχύτητα: Οι αλγόριθμοι συμμετρικής κρυπτογράφησης είναι συνήθως γρήγοροι και αποδοτικοί σε σχέση με τους αλγορίθμους ασύμμετρης κρυπτογραφίας για την κρυπτογράφηση και αποκρυπτογράφηση μεγάλου όγκου δεδομένων ή σε εφαρμογές που απαιτούν υψηλή απόδοση.
- Απλότητα: Η συμμετρική κρυπτογραφία είναι συνήθως πιο απλή στην υλοποίηση και στη χρήση από την ασύμμετρη κρυπτογραφία. Απαιτεί μικρότερο αριθμό υπολογιστικών πόρων και λιγότερη υπολογιστική ισχύ σε σύγκριση με την ασύμμετρη κρυπτογραφία.
- Αποδοτική αποθήκευση: Τα συμμετρικά κλειδιά είναι συνήθως πολύ μικρότερα από τα κλειδιά της ασύμμετρης κρυπτογραφίας, οπότε απαιτείται μικρότερος χώρος αποθήκευσης για τα κλειδιά.
- Ευελιξία: Τα συμμετρικά κρυπτογραφικά συστήματα μπορούν να χρησιμοποιηθούν για πολλούς σκοπούς, όπως η εμπιστευτική επικοινωνία, η προστασία δεδομένων και η αυθεντικοποίηση.

Επίσης πολλές γνώμες υποστηρίζουν και τα παρακάτω πλεονεκτήματα

- Κατάλληλη για μεγάλα συστήματα: Η συμμετρική κρυπτογραφία είναι εξαιρετικά κατάλληλη για εφαρμογές που απαιτούν μεγάλη απόδοση και αποτελεσματική χρήση πόρων, όπως μεγάλα δίκτυα και επιχειρηματικά συστήματα.
- Χρησιμοποιεί ένα κοινό κλειδί για την κρυπτογράφηση και την αποκρυπτογράφηση των δεδομένων.
- Κατάλληλη για την κρυπτογράφηση μικρού όγκου δεδομένων ή για τη δημιουργία συμμετρικών κλειδιών για την ασφάλεια των δεδομένων σε ασύμμετρα συστήματα.

Παρόλα αυτά, πρέπει να ληφθεί υπόψη ότι η συμμετρική κρυπτογραφία δεν παρέχει την ίδια ευελιξία και ασφάλεια όπως η ασύμμετρη κρυπτογραφία, καθώς απαιτεί την ασφαλή διανομή του κλειδιού. Έτσι παρά τα πλεονεκτήματά της, υπάρχουν και μειονεκτήματα που πρέπει να ληφθούν υπόψη:

- Κοινό κλειδί: Στη συμμετρική κρυπτογραφία, απαιτείται η ασφαλής διανομή του κοινού κλειδιού μεταξύ των εμπλεκομένων μερών. Αυτό μπορεί να αποτελέσει πρόκληση, ειδικά αν οι εμπλεκόμενοι χρήστες βρίσκονται σε απομακρυσμένες τοποθεσίες ή αν ο αριθμός των χρηστών είναι μεγάλος.
- Ασφάλεια κλειδιού: Η ασφάλεια του κλειδιού είναι κρίσιμη στη συμμετρική κρυπτογραφία. Αν το κλειδί είναι ευάλωτο ή διαρρεύσει, οι επιτηθέμενοι μπορούν να αποκρυπτογραφήσουν τα δεδομένα. Η ασφαλής διαχείριση των κλειδιών μπορεί να είναι προκλητική, ειδικά για μεγάλες κατανομές κλειδιών.
- Έλλειψη εμπιστοσύνης: Στη συμμετρική κρυπτογραφία, οι εμπλεκόμενοι πρέπει να εμπιστεύονται τον αποστολέα των κρυπτογραφημένων δεδομένων, καθώς ο αποστολέας και ο παραλήπτης χρησιμοποιούν το ίδιο κλειδί. Αυτό μπορεί να προκαλέσει ανησυχία αν υπάρχει αμφιβολία για την ασφάλεια ή την εμπιστοσύνη του αποστολέα.
- Ο κίνδυνος απώλειας του κλειδιού μπορεί να οδηγήσει στην αποκάλυψη των δεδομένων.
- Ανανεώσιμα κλειδιά: Εάν επιθυμείτε να αλλάξετε το κλειδί για λόγους ασφαλείας, πρέπει να μοιραστεί το νέο κλειδί σε όλους τους εμπλεκόμενους χρήστες. Αυτό μπορεί να είναι περίπλοκο και χρονοβόρο, ειδικά σε μεγάλες κλίμακες.

Είναι σημαντικό να επιλέξετε το κατάλληλο σύστημα κρυπτογράφησης ανάλογα με τις ανάγκες ασφαλείας και απόδοσης του συστήματός σας. Σε ορισμένες περιπτώσεις, μπορεί να απαιτείται η συνδυασμένη χρήση συμμετρικής και ασύμμετρης κρυπτογραφίας για την επίτευξη των βέλτιστων αποτελεσμάτων.

3.6.2 Ασύμμετρη Κρυπτογράφηση

Με την πάροδο των χρόνων, αναπτύχθηκαν μέθοδοι που δεν απαιτούν τη μετάδοση του μυστικού κλειδιού στον αποδέκτη του μηνύματος. Αυτές οι μέθοδοι ονομάζονται ασύμμετρη κρυπτογράφηση. Στην ασύμμετρη κρυπτογράφηση, το μήνυμα είναι κρυπτογραφημένο με ένα δημόσιο κλειδί που προκύπτει από το μυστικό κλειδί του αποδέκτη του μηνύματος. Για παράδειγμα, αν θέλουμε μια ομάδα ατόμων να κρυπτογραφούν τα μηνύματα που αποστέλλουν μεταξύ τους, θα διαμοίραζαν το δημόσιο τους κλειδί μεταξύ τους και ο καθένας θα το χρησιμοποιούσε για να κρυπτογρφήσει τα μηνύματα που ήθελε να στείλει στους υπόλοιπους. Αφού τα μηνύματα κρυπτογραφηθούν, μόνο κάποιος που διαθέτει το αντίστοιχο μυστικό κλειδί μπορεί να αποκρυπτογραφήσει το μήνυμα. Η κρυπτογραφία δημόσιου κλειδιού χρησιμοποιεί ένα δημόσιο κλειδί για την κρυπτογράφηση. Τα πλεονεκτήματά της είναι:

- Διανομή κλειδιών: Στην ασύμμετρη κρυπτογραφία, υπάρχουν δύο κλειδιά: ένα ιδιωτικό κλειδί και ένα δημόσιο κλειδί. Το δημόσιο κλειδί μπορεί να διανεμηθεί ελεύθερα σε οποιονδήποτε, ενώ το ιδιωτικό κλειδί παραμένει μυστικό. Αυτό καθιστά ευκολότερη τη διανομή κλειδιών, καθώς δεν απαιτείται η ασφαλής και εμπιστευτική ανταλλαγή κλειδιών.

- Αυθεντικότητα και υπογραφές: Η ασύμμετρη κρυπτογραφία μπορεί να χρησιμοποιηθεί για τη δημιουργία ψηφιακών υπογραφών. Με τη χρήση του ιδιωτικού κλειδιού, μπορεί να διαπιστωθεί η αυθεντικότητα των δεδομένων και η ταυτότητα του αποστολέα. Αυτό είναι σημαντικό για την επαλήθευση της αυθεντικότητας των μηνυμάτων και των αρχείων.
- Κρυπτογραφία κλειδιού: Με τη χρήση του δημόσιου κλειδιού, μπορεί να κρυπτογραφηθεί ένα μήνυμα και μόνο ο κάτοχος του ιδιωτικού κλειδιού μπορεί να το αποκρυπτογραφήσει. Αυτό επιτρέπει την εμπιστευτική ανταλλαγή πληροφοριών, χωρίς την ανάγκη κοινού κλειδιού.
- Κατάλληλη για κρυπτογραφία μικρής κλίμακας: Η ασύμμετρη κρυπτογραφία είναι ιδανική για μικρές επικοινωνίες και αποστολή απομονωμένων μηνυμάτων. Είναι πιο ασφαλής για αυτές τις περιπτώσεις, επειδή δεν απαιτείται η ασφαλής διανομή ενός κοινού κλειδιού.

Επίσης πολλές γνώμες υποστηρίζουν :

- Οι αλγόριθμοι κρυπτογράφησης ασύμμετρης κρυπτογραφίας είναι πιο ασφαλείς, αλλά πιο αργοί και απαιτούν περισσότερους υπολογιστικούς πόρους σε σύγκριση με τη συμμετρική κρυπτογραφία.
- Η κλειδοχώρος είναι μεγαλύτερος, επιτρέποντας μεγαλύτερη ασφάλεια και πιθανότητα ανεξάρτητης δημιουργίας κλειδιών.
- Παρέχει ανώνυμη ασφάλεια, καθώς το δημόσιο κλειδί μπορεί να διανεμηθεί ελεύθερα.
- Κατάλληλη για την υπογραφή ψηφιακών πιστοποιητικών.

Παρά τα πλεονεκτήματα της ασύμμετρης κρυπτογραφίας, υπάρχουν και ορισμένα μειονεκτήματα που πρέπει να ληφθούν υπόψη:

- Υπολογιστική πολυπλοκότητα: Οι αλγόριθμοι ασύμμετρης κρυπτογραφίας είναι πιο χρονοβόροι σε σχέση με τους αλγορίθμους συμμετρικής κρυπτογραφίας. Αυτό οφείλεται στη μεγαλύτερη απαιτούμενη υπολογιστική ισχύ για τις αριθμητικές πράξεις που συμπεριλαμβάνονται στη διαδικασία της κρυπτογράφησης και αποκρυπτογράφησης.
- Απαιτήσεις αποθήκευσης κλειδιών: Η ασύμμετρη κρυπτογραφία απαιτεί τη διαχείριση και αποθήκευση δημόσιων και ιδιωτικών κλειδιών. Αυτό μπορεί να αποτελέσει πρόκληση ειδικά σε μεγάλες κλίμακες ή όταν απαιτούνται πολλά κλειδιά για διάφορες χρήσεις.
- Πιθανή ασφάλεια κλειδιού: Ενώ η ασύμμετρη κρυπτογραφία παρέχει ασφάλεια σε επίπεδο κλειδιού, υπάρχει πιθανότητα να παραβιαστεί η ασφάλεια του ιδιωτικού κλειδιού. Εάν ένας επιτιθέμενος αποκτήσει πρόσβαση στο ιδιωτικό κλειδί, μπορεί να αποκρυπτογραφήσει τα μηνύματα που έχουν κρυπτογραφηθεί με το αντίστοιχο δημόσιο κλειδί.
- Περιορισμένη απόδοση σε μεγάλα δεδομένα: Η ασύμμετρη κρυπτογραφία είναι πιο αργή σε σχέση με τη συμμετρική κρυπτογραφία, ειδικά όταν πρέπει να κρυπτογραφηθούν ή να αποκρυπτογραφηθούν μεγάλα δεδομένα. Αυτό μπορεί να οδηγήσει σε μειωμένη απόδοση συστημάτων που απαιτούν γρήγορη επεξεργασία μεγάλου όγκου δεδομένων.

Η συμμετρική και η ασύμμετρη κρυπτογραφία έχουν τις δικές τους πλευρές και χρησιμοποιούνται σε διαφορετικά σενάρια ασφαλείας. Συχνά, η καλύτερη πρακτική είναι να συνδυάζονται για την επίτευξη βέλτιστης ασφάλειας και απόδοσης. Συνοψίζοντας, η συμμετρική κρυπτογράφηση είναι γρηγορότερη, αλλά απαιτεί την ασφαλή διανομή του κλειδιού, ενώ η ασύμμετρη κρυπτογράφηση είναι πιο ασφαλής και επιτρέπει την ανώνυμη ασφάλεια, αλλά είναι πιο αργή και απαιτεί περισσότερους υπολογιστικούς πόρους. Η επιλογή μεταξύ των δύο εξαρτάται από τις απαιτήσεις ασφάλειας, την απόδοση και το περιβάλλον εφαρμογής. Συχνά χρησιμοποιούνται και οι δύο τύποι κρυπτογράφησης σε συνδυασμό, για να επιτευχθεί ισορροπία μεταξύ ασφάλειας και απόδοσης.

3.7 Κρυπταλγόριθμος δημοσίου και ιδιωτικού κλειδιού

Η κρυπτογράφηση είναι το κύριο στοιχείο αυτής της εργασίας, η πιο σημαντική λειτουργία και ο σκοπός της. Ο αλγόριθμος που χρησιμοποιήθηκε είναι ο RSA, ένας κρυπταλγόριθμος ασύμμετρου κλειδιού για κρυπτογράφηση και άλλες λειτουργίες, το όνομα του οποίου προέρχεται από τους δημιουργούς του *Ron Rivest*, *Adi Shamir* και *Len Adleman* του πανεπιστημίου MIT. Επιλέχθηκε

έπειτα από αρκετό διάβασμα και σύγκριση διαφόρων πηγών κυρίως στο *internet,* γνώμες προγραμματιστών και όχι, και το αποτέλεσμα οδήγησε σε αυτόν λόγω της ασφάλειας που προσφέρει, της εμπιστευτικότητας, της ακεραιότητας και της αυθεντικοποίησης σε υψηλότερο βαθμό από τους υπόλοιπους που υπάρχουν αυτή την στιγμή διαθέσιμοι. Ο κρυπταλγόριθμος RSA βασίζεται στην δυσκολία παραγοντοποίησης μεγάλων αριθμών, χρησιμοποιεί δύο κλειδιά για την λειτουργία του, ένα κατα της την διάρκεια της κρυπτογράφηση, το δημόσιο κλειδί (κρυπτογράφηση των μηνυμάτων και κωδικών του αποστολέα στην περίπτωση της παρούσας εργασίας), και ένα για την αποκρυπτογράφηση, το ιδιωτικό (αποκρυπτογράφηση των μηνυμάτων του αποστολέα στην πλευρά του δέκτη)

Οι πρώτοι αριθμοί παίζουν πολύ σημαντικό ρόλο στον αλγόριθμο RSA και αυτός είναι ένας από τους λόγους που οι μαθηματικοί συνεχώς ψάχνουν όλο και μεγαλύτερους πρώτους αριθμούς. Πρώτοι αριθμοί ονομάζονται οι φυσικοί αριθμοί που διαιρούνται με τον εαυτό τους και την μονάδα. Αν ένας αριθμός δεν είναι πρώτος τότε ονομάζεται σύνθετος. Δύο αριθμοί που δεν έχουν κοινούς διαιρέτες (εκτός από το 1) ονομάζονται πρώτοι, για παράδειγμα το 4 δεν είναι πρώτος (αφου διαιρείται με το 2) ούτε το 9 (αφού διαιρείται με το 3), ωστόσο είναι μεταξύ τους πρώτοι αφου ο μοναδικός αριθμός που διαιρεί και τους δυο είναι το 1. Ο μεγαλύτερος πρώτος αριθμός που γνωρίζουμε, ανακαλύφθηκε το 2016 ωστόσο δεν έχει κάποια πρακτική αξία μιας και στην πράξη οι πρώτοι αριθμοί που χρειάζονται στην κρυπτογράφηση είναι πολύ μικρότεροι, μερικές εκατοντάδες ψηφία.

Ο αλγόριθμος δημόσιου και ιδιωτικού κλειδιού, γνωστός επίσης ως κρυπτογράφηση δημοσίου κλειδιού, είναι μια μέθοδος κρυπτογράφησης δεδομένων που βασίζεται σε δύο διαφορετικά κλειδιά: ένα δημόσιο και ένα ιδιωτικό. Το δημόσιο κλειδί είναι προσβάσιμο σε όλους και χρησιμοποιείται για την κρυπτογράφηση των δεδομένων. Το ιδιωτικό κλειδί είναι μυστικό και γνωρίζεται μόνο από τον κάτοχό του, και χρησιμοποιείται για την αποκρυπτογράφηση των δεδομένων. Στη διαδικασία κρυπτογράφησης, ο αποστολέας χρησιμοποιεί το δημόσιο κλειδί του παραλήπτη για να κρυπτογραφήσει το μήνυμα. Στη συνέχεια, το κρυπτογραφημένο μήνυμα αποστέλλεται στον παραλήπτη και ο αυτός χρησιμοποιεί το ιδιωτικό του κλειδί για να το αποκρυπτογραφήσει. Η δημιουργία των δύο κλειδιών γίνεται μέσω ενός μαθηματικού αλγορίθμου, που βασίζεται στην δυσκολία του υπολογισμού του αντίστροφου ενός μεγάλου αριθμού. Ο αλγόριθμος δημοσίου κλειδιού/ιδιωτικού κλειδιού χρησιμοποιείται ευρέως για την ασφαλή ανταλλαγή μηνυμάτων στο διαδίκτυο και σε άλλες εφαρμογές κρυπτογραφίας. Οι πιο γνωστοί αλγόριθμοι δημοσίου κλειδιού/ιδιωτικού κλειδιού είναι οι RSA (*Rivest-Shamir-Adleman*), Diffie-Hellman και Elliptic Curve Cryptography (ECC), όπως στις συναλλαγές ηλεκτρονικού εμπορίου, τις τραπεζικές συναλλαγές και την αποστολή ηλεκτρονικού ταχυδρομείου. Ο αλγόριθμος δημόσιου κλειδιού RSA και ο αλγόριθμος ιδιωτικού κλειδιού AES (Advanced Encryption Standard) είναι δύο από τους πιο δημοφιλείς αλγορίθμους κρυπτογράφησης. Ο αλγόριθμος RSA χρησιμοποιεί ένα ζεύγος κλειδιών, ένα δημόσιο κλειδί και ένα ιδιωτικό κλειδί, για την κρυπτογράφηση και αποκρυπτογράφηση μηνυμάτων. Ο αλγόριθμος AES από την άλλη, χρησιμοποιεί ένα κλειδί για την κρυπτογράφηση και αποκρυπτογράφηση των δεδομένων. Αυτό σημαίνει ότι η ασφάλεια του RSA βασίζεται στην αδυναμία ενός επιτιθέμενου να αποκτήσει πρόσβαση στο ιδιωτικό κλειδί, ενώ η ασφάλεια του AES βασίζεται στην ανθεκτικότητά του κλειδιού σε εξαντλητικές επιθέσεις (brutal force attack).

Οι κρυπταλγόριθμοι δημοσίου κλειδιού και ιδιωτικού κλειδιού είναι δύο διαφορετικές κατηγορίες αλγορίθμων κρυπτογράφησης. Και οι δύο κατηγορίες χρησιμοποιούνται για την προστασία των δεδομένων και της επικοινωνίας, αλλά λειτουργούν με διαφορετικό τρόπο.

Ο RSA είναι ένας από τους πιο αξιόπιστους κρυπταλγορίθμους γιατί βασίζεται στη δυσκολία του προβλήματος του πολλαπλασιασμού μεγάλων πρώτων αριθμών. Αυτό σημαίνει ότι είναι πολύ δύσκολο να λυθεί ένα κρυπτογραφημένο μήνυμα αν δεν έχεις την ιδιωτική κλειδοθήκη του αποστολέα. Αυτό οφείλεται στο γεγονός ότι η αποκρυπτογράφηση του μηνύματος απαιτεί τον υπολογισμό του ιδιωτικού κλειδιού, το οποίο μπορεί να πάρει πάρα πολύ χρόνο και πόρους.

Δημιουργία των κλειδιών

1. Επιλογή δυο τυχαίων (μεγάλων) πρώτων αριθμών p και q έτσι ώστε $p \neq q$
2. Υπολογίζουμε $n = p.q$
3. Υπολογίζουμε την συνάρτηση του Όιλερ, $\phi(n) = (p-1)(q-1)$.
4. Επιλογή ενός αριθμού $e > 1$ έτσι ώστε $e^{\phi(n)} \equiv 1 \pmod{n}$.
5. Υπολογίζουμε τον αριθμό d έτσι ώστε $d \equiv e^{-1} \pmod{\varphi(n)}$.

- Για την εύρεση πρώτων αριθμών χρησιμοποιούνται πιθανολογικοί αλγόριθμοι.
- Συνηθισμένες επιλογές για το e είναι το 3, 7 και $2^{16} + 1$. Μικροί αριθμοί οδηγούν σε ταχύτερους υπολογισμούς αλλά και σε πιο αδύνατη ασφάλεια.

Τα κλειδιά είναι τα εξής:

- δημόσιο: (n, e)
- ιδιωτικό: (n, d)

Μπορούμε τώρα να δημοσιεύσουμε το πρώτο κλειδί, δίνοντας έτσι τη δυνατότητα σε οποιονδήποτε να μας στείλει κρυπτογραφημένα μηνύματα που μόνο εμείς (χάρη στο ιδιωτικό κλειδί) μπορούμε να αποκρυπτογραφήσουμε.

Κρυπτογράφηση

Το μήνυμα μπορεί να αντιπροσωπευθεί από έναν αριθμό m (π.χ. "RSA" → 0x525341, όπου *0x52* είναι ο δεκαεξαδικός κωδικός ASCII του χαρακτήρα *R*, *0x53* του *S* και τέλος *0x41* του *A*). Το κρυπτογραφημένο μήνυμα c υπολογίζεται με τον εξής τρόπο:

$$c = m^e \mod n$$

Αποκρυπτογράφηση

Αφού ληφθεί ένα κρυπτογραφημένο μήνυμα c, για να διαβάσουμε το αρχικό μήνυμα προβαίνουμε στον ακόλουθο υπολογισμό:

$$m = c^d \mod n \equiv (m^e)^d \mod n \equiv m^{e.d} \mod n$$

Ξέρουμε πως *e.d* ≡ 1 (mod *p-1*) και *e.d* ≡ 1 (mod *q-1*), όποτε με το μικρό θεώρημα του Φερμά, έχουμε:

$$m^{e.d} \equiv m^1 \equiv m \mod p-1$$

και

$$m^{e.d} \equiv m^1 \equiv m \mod q-1$$

Οι αριθμοί *p* και *q* είναι πρώτοι μεταξύ τους, χρησιμοποιώντας λοιπόν το Κινέζικο Θεώρημα Υπολοίπων, έχουμε:

$$m^{e.d} \equiv m \mod n$$

Εικόνα 13, γενική αναφορά για την δημιουργία των κλειδιών.

Ο αλγόριθμος RSA είναι ένας από τους πιο ασφαλείς κρυπταλγορίθμους που χρησιμοποιούνται σήμερα, καθώς βασίζεται σε δύο δύσκολα προβλήματα της αριθμοθεωρίας: την παραγοντοποίηση αριθμών και το πρόβλημα του διακριτού λογαρίθμου. Η δυσκολία στην επίλυση αυτών των προβλημάτων καθιστά τον RSA ασφαλή και αποτελεσματικό για την κρυπτογράφηση και αποκρυπτογράφηση των δεδομένων. Αντίθετα, άλλοι κρυπταλγόριθμοι, όπως οι κρυπτογραφικοί αλγόριθμοι DES και AES, είναι βασισμένοι σε περιστροφές και αντιστροφές στα δεδομένα και δεν παρέχουν το ίδιο επίπεδο ασφάλειας με τον RSA. Συνεπώς, ο RSA θεωρείται ως ένας από τους πιο αξιόπιστους κρυπταλγορίθμους και χρησιμοποιείται ευρέως σε πολλές εφαρμογές ασφαλείας των δεδομένων, όπως οι ψηφιακές υπογραφές, η κρυπτογράφηση μηνυμάτων και η απομακρυσμένη πρόσβαση σε συστήματα.

Επιπλέον, ο RSA χρησιμοποιείται ευρέως γιατί είναι ανθεκτικός σε επιθέσεις brute-force (δοκιμή όλων των πιθανών κλειδιών) εξαιτίας του μεγέθους των κλειδιών που χρησιμοποιούνται. Αυτό το καθιστά ιδανικό για την ασφάλεια στην εποχή των υπολογιστών με μεγάλη υπολογιστική ισχύ. Τέλος, ο RSA είναι αξιόπιστος γιατί έχει χρησιμοποιηθεί επιτυχώς σε πολλές εφαρμογές ασφαλείας, όπως η προστασία των δεδομένων πιστωτικών καρτών και η κρυπτογράφηση επικοινωνιών.

Η ασφάλεια του αλγορίθμου RSA έγκειται στο γεγονός ότι η ανάλυση ενός αριθμού σε γινόμενο πρώτων παραγόντων είναι μια ιδιαίτερα χρονοβόρα διαδικασία για τους υπολογιστές. Για παράδειγμα ο RSA-768 (μήκος κλειδιού 768 bits) έχει πρώτους αριθμούς που αποτελούνται από 232 ψηφία και

τον Δεκέμβριο του 2009 ερευνητές κατάφεραν να τον σπάσουν δηλαδή να παραγοντοποιήσουν τον πρώτο αριθμό. Χρειάστηκαν 2 χρόνια για να το καταφέρουν με μια συστοιχία υπερυπολογιστών. Ο αντίστοιχος χρόνος αν το προσπαθούσαν σε έναν απλό υπολογιστή αντιστοιχεί σε 2000 χρόνια. Όσο μεγαλύτερες είναι οι παράμετροι που χρησιμοποιούνται τόσο μεγαλύτερη είναι και η ασφάλεια που προσφέρει ο αλγόριθμος. Παρόλα αυτά η κακή του χρήση μπορεί να οδηγήσει σε μεγάλες αδυναμίες ασφαλείας. Επίσης δεν αποτελεί τον μοναδικό παράγοντα υπολογισμό της ασφάλειας, έτσι σύμφωνα με έρευνες που έχουν γίνει μία μέση τιμή παραμέτρων οδηγεί σε ένα αρκετά καλό επίπεδο ασφάλειας μειώνοντας τις αδυναμίες κακής χρήσης που οδηγούν σε παραβίαση του αλγορίθμου και άρα σε κενά ασφαλείας.

Η βασική ιδέα του συγκεκριμένου τρόπου κρυπτογράφησης είναι ότι ο αποστολέας και ο παραλήπτης δεν μοιράζονται ένα κοινό μυστικό (όπως στην κρυπτογράφηση συμμετρικού κλειδιού) αλλά διαθέτουν διαφορετικά κλειδιά για διαφορετικές λειτουργίες. Κάθε χρήστης διαθέτει δύο κλειδιά κρυπτογράφησης, ένα ιδιωτικό κλειδί, private key, και ένα δημόσιο κλειδί, public key. Το πρώτο θα πρέπει κάθε χρήστης να το κρατάει κρυφό, ασφαλή, να είναι ο μόνος που το γνωρίζει. Αντιθέτως το δεύτερο θα πρέπει θα πρέπει να το γνωστοποιήσει σε όποιον/ους θέλει πιθανώς να επικοινωνήσει ή ακόμα να το έχει διαθέσιμο σε όλη την διαδικτυακή κοινότητα ώστε ανα πάσα στιγμή όποιος θέλει να έχει πρόσβαση σε αυτό. Τα δύο αυτά κλειδιά συνδέονται μεταξύ τους παρολο την παραπάνω ευαίσθητη διαφορά τους. Το ένα χρησιμοποιείται για την κρυπτογράφηση (μηνύματος ή κωδικών στην περίπτωση μας) και το δεύτερο για την αποκρυπτογράφηση. Ο αποστολέας θα πρέπει να χρησιμοποιήσει το δημόσιο κλειδί του παραλήπτη για να κρυπτογραφήσει το μήνυμα. Στη συνέχεια στέλνει το κρυπτογραφημένο μήνυμα στον παραλήπτη και ο τελευταίος μπορεί να το αποκρυπτογραφήσει με το ιδιωτικό κλειδί του. Για να έχει επιτυχία η παραπάνω συνεργασία των δύο αυτών κλειδιών θα πρέπει το δημόσιο κλειδί, γνωστό στην διαδικτυακή κοινότητα να μην οδηγεί με κανέναν τρόπο στον υπολογισμό του ιδιωτικού κλειδιού.

Εικόνα 14, παράδειγμα δημοσίου κλειδιού.

Η δημιουργία του δημόσιου και του ιδιωτικού κλειδιού γίνεται από ειδικές συναρτήσεις οι οποίες δέχονται ως είσοδο έναν μεγάλο τυχαίο αριθμό και στην έξοδο παράγουν το ζεύγος των κλειδιών. Όσο πιο τυχαίος είναι ο αριθμός που παρέχεται ως είσοδος στη γεννήτρια κλειδιών τόσο πιο ασφαλή είναι τα κλειδιά που παράγονται. Σε σύγχρονα προγράμματα κρυπτογράφησης ο τυχαίος αριθμός παράγεται ως εξής: Κατά τη διαδικασία κατασκευής των κλειδιών, το πρόγραμμα σταματάει για 5

λεπτά και καλεί τον χρήστη να συνεχίσει να εργάζεται με τον υπολογιστή. Στη συνέχεια για να παραγάγει τον τυχαίο αριθμό συλλέγει στα 5 αυτά λεπτά τυχαία δεδομένα που εξαρτώνται από τη συμπεριφορά του χρήστη (κινήσεις ποντικιού, πλήκτρα του πληκτρολογίου που πατήθηκαν, κύκλοι μηχανής που καταναλώθηκαν κοκ). Με βάση αυτά τα πραγματικά τυχαία δεδομένα υπολογίζεται ο τυχαίος αριθμός και εισάγεται στη γεννήτρια κλειδιών για να κατασκευαστεί το δημόσιο και το ιδιωτικό κλειδί του χρήστη.

Η κρυπτογράφηση δημοσίου κλειδιού λύνει ένα σημαντικότατο πρόβλημα που υπήρχε στους κρυπτογραφικούς αλγόριθμους συμμετρικού κλειδιού. Συγκεκριμένα, οι κρυπτογραφικοί αλγόριθμοι συμμετρικού κλειδιού χρησιμοποιούν ένα κοινό μυστικό κλειδί, το οποίο το γνωρίζουν τόσο ο αποστολέας του κρυπτογραφημένου περιεχομένου όσο και ο παραλήπτης. Αυτό το κοινό μυστικό κλειδί χρησιμοποιείται κατά τη διαδικασία κρυπτογράφησης και αποκρυπτογράφησης του μηνύματος.

Προκύπτει όμως το εξής πρόβλημα:

Εάν υποθέσουμε ότι το κανάλι επικοινωνίας δεν είναι ασφαλές, τότε πως γίνεται ο αποστολέας να στείλει το κλειδί κρυπτογράφησης στον παραλήπτη για να μπορέσει αυτός με τη σειρά του να αποκρυπτογραφήσει το μήνυμα. Αυτό το πρόβλημα είναι ιδιαίτερα έντονο στις σύγχρονες ψηφιακές επικοινωνίες όπου σε πολλές περιπτώσεις ο αποστολέας δεν γνωρίζει καν τον παραλήπτη και απέχει από αυτόν αρκετές χιλιάδες χιλιόμετρα. Οι κρυπτογραφικοί αλγόριθμοι δημόσιου κλειδιού λύνουν αυτό το πρόβλημα και ανοίγουν νέους δρόμους για εφαρμογές της κρυπτογράφησης όπως την παρούσα (εφαρμογές επικοινωνιας) αλλά και οποιαδήποτε άλλη εφαρμογή που πραγματεύεται προσωπικά δεδομένα.

3.8 Εμπιστευτικότητα, ακεραιότητα και διαθεσιμότητα

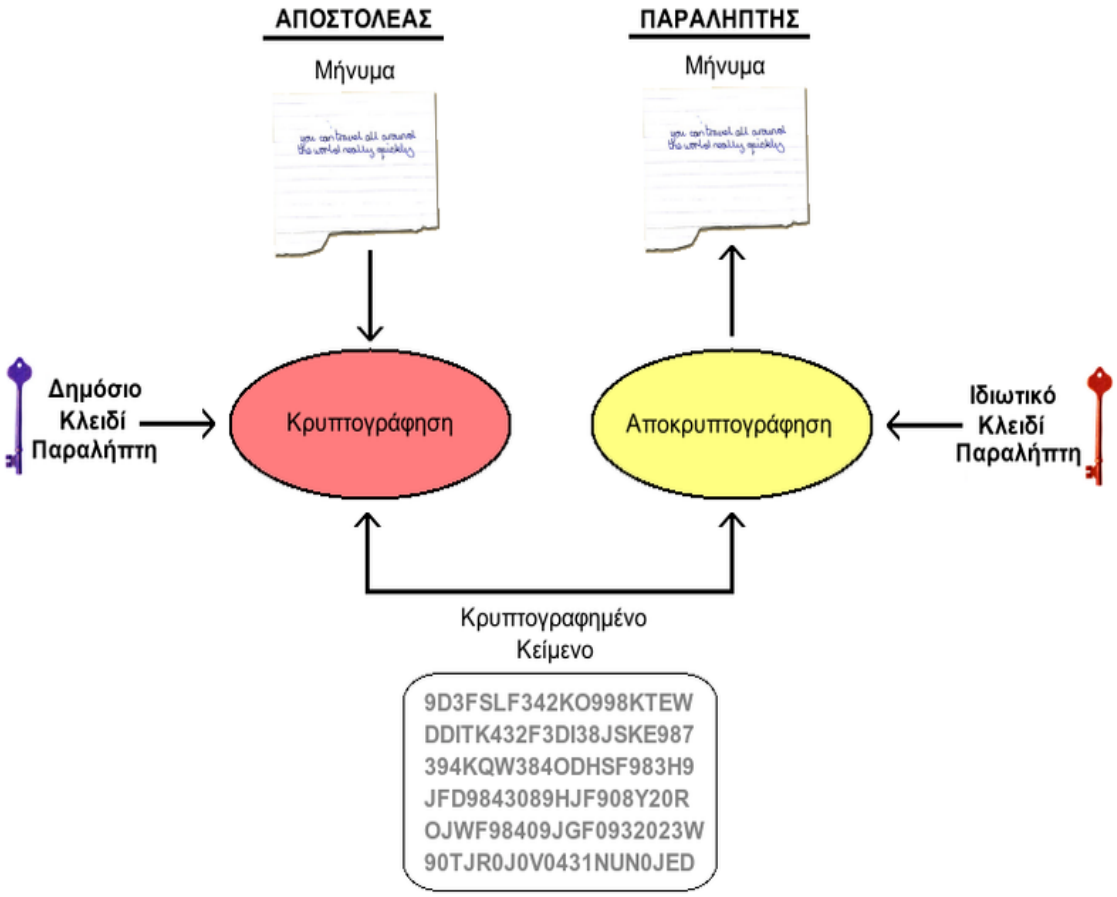
Οι συναρτήσεις hash χρησιμοποιούνται ευρέως για την επαλήθευση της ακεραιότητας ενός μηνύματος. Η ακεραιότητα είναι η μία πτυχή του τρίπτυχου CIA (Confidentiality Integrity & Availability). Η συνάρτηση hash μπορεί να χρησιμοποιηθεί για την επαλήθευση της ακεραιότητας με τον ίδιο τρόπο που μπορεί να προστατευθεί ένας κωδικός πρόσβασης. Μια συνάρτηση hash μπορεί να χρησιμοποιηθεί για τον υπολογισμό μιας τιμής για ολόκληρο το περιεχόμενο ενός μηνύματος και να σταλεί μαζί με το αρχικό μήνυμα. Ο παραλήπτης του κρυπτογραφημένου κωδικού πρόσβασης μπορεί στη συνέχεια να επαληθεύσει ότι η τιμή hash (η λεγόμενη «σύνοψη μηνύματος») αντιστοιχεί στην υπολογισμένη τιμή όταν την παραλαμβάνει. Ορισμένες κρυπτογραφικές συναρτήσεις hash ενσωματώνουν την ταυτότητα στη συνάρτηση, η οποία μπορεί να ελεγχθεί από τον παραλήπτη. Αυτές οι συναρτήσεις δημιουργούν αυτό που ονομάζεται Message Authentication Code (κωδικός ελέγχου ταυτότητας μηνύματος – MAC).

Η σύγχρονη κρυπτογραφία βασίζεται στη μυστικότητα του κλειδιού και χρησιμοποιεί γνωστούς και ευρέως μελετημένους κώδικες. Οι κώδικες μπορούν να είναι γνωστοί καθώς η μυστικότητα εξαρτάται από το κλειδί αντί για τον τρόπο που χρησιμοποιείται. Για παράδειγμα, όταν επισκέπτεστε διαδικτυακά την τράπεζά σας, το πρόγραμμα περιήγησής σας και ο διακομιστής web της τράπεζας ανταλλάσσουν με ασφάλεια ένα μυστικό συμμετρικό κλειδί μιας χρήσης που χρησιμοποιείται για την κρυπτογράφηση της κυκλοφορίας μεταξύ του προγράμματος περιήγησής σας και του διακομιστή της τράπεζας. Επιπλέον, η κρυπτογράφηση δημόσιου κλειδιού συνήθως χρησιμοποιείται για την επαλήθευση της ταυτότητας του άλλου μέρους. Το κάθε μήνυμα είναι επίσης επαληθεύσιμο από ένα MAC. Αυτή η διαδικασία ανταλλαγής κλειδιών, επαλήθευσης και ελέγχου ταυτότητας μεταξύ προγράμματος περιήγησης και διακομιστή ονομάζεται Transport Layer Security(ασφάλεια επιπέδου

μεταφοράς). Οι προηγούμενες εκδόσεις χρησιμοποιούσαν μια πλέον ξεπερασμένη μέθοδο που ονομάζεται SSL- secure socket layer (SSL - ασφαλές επίπεδο υποδοχής).

Όπως αναφέρθηκε και προηγουμένως ένα από τα βασικότερα χαρακτηριστικά του κρυπταλγόριθμου RSA είναι η εμπιστευτικότητα. Οι κρυπτογραφικοί αλγόριθμοι δημόσιου κλειδιού μπορούν να εγγυηθούν εμπιστευτικότητα (confidentiality), δηλαδή ότι το κρυπτογραφημένο μήνυμα που θα στείλει ο αποστολέας μέσω του διαδικτύου στον παραλήπτη θα είναι αναγνώσιμο από αυτόν και μόνο. Για να επιτευχθεί η εμπιστευτικότητα, ο αποστολέας θα πρέπει να χρησιμοποιήσει το δημόσιο κλειδί του παραλήπτη για να κρυπτογραφήσει το μήνυμα. Στη συνέχεια στέλνει το κρυπτογραφημένο μήνυμα στον παραλήπτη και ο τελευταίος μπορεί να το αποκρυπτογραφήσει με το ιδιωτικό κλειδί του. Δεδομένου ότι το ιδιωτικό κλειδί του παραλήπτη είναι γνωστό μονάχα στον ίδιο και σε κανέναν άλλον, μόνο παραλήπτης μπορεί να αποκρυπτογραφήσει το μήνυμα και να το διαβάσει. Άρα λοιπόν με αυτόν τον τρόπο ο αποστολέας γνωρίζει ότι το κρυπτογραφημένο μήνυμα μπορεί να αποκρυπτογραφηθεί μόνο από τον παραλήπτη και έτσι διασφαλίζεται η εμπιστευτικότητα του μηνύματος.

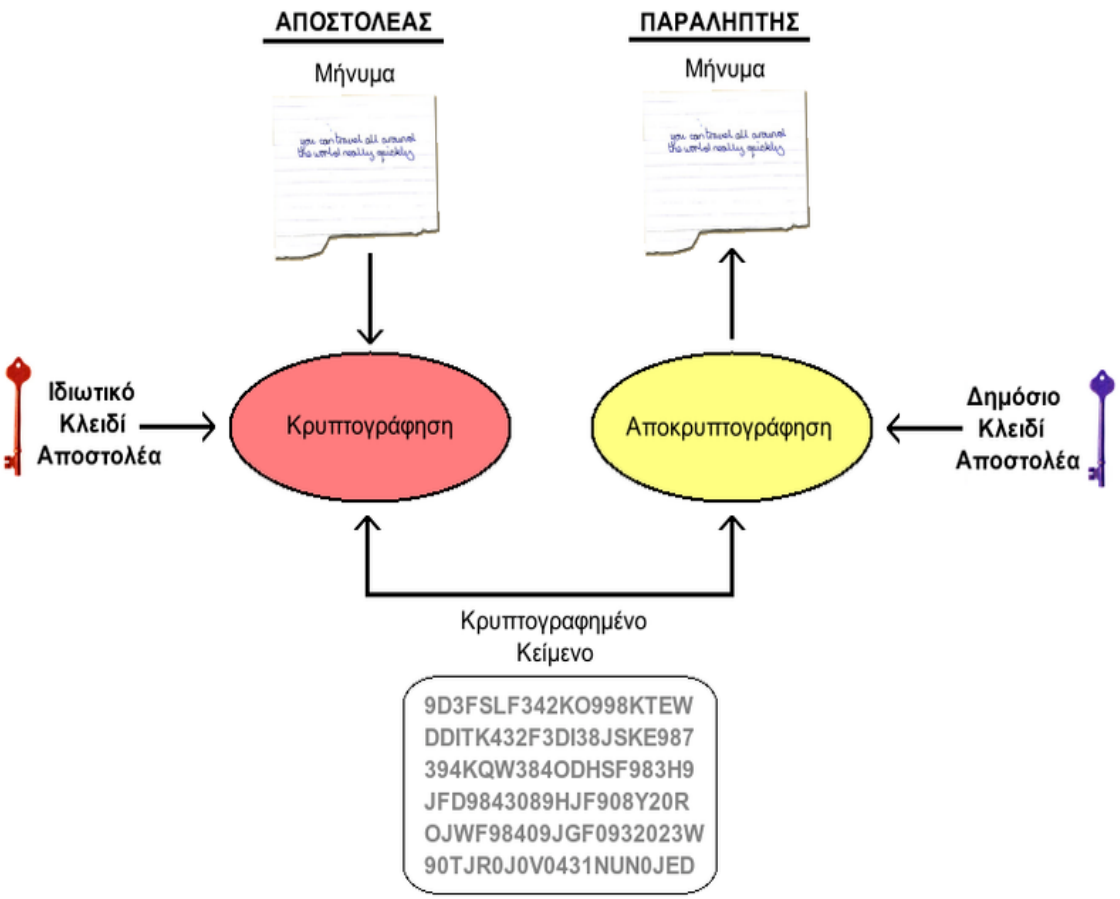
Η αυθεντικοποίηση και η εμπιστευτικότητα είναι δύο διαφορετικά χαρακτηριστικά της κρυπτογραφίας μηνυμάτων. Η εμπιστευτικότητα αφορά την προστασία του περιεχομένου ενός μηνύματος από την πρόσβαση ανεπιθύμητων τρίτων, ενώ η αυθεντικοποίηση αφορά την επιβεβαίωση της ταυτότητας του αποστολέα ενός μηνύματος.



Εικόνα 15, εμπιστευτικότητας αλλά όχι πιστοποίηση.

Χρησιμοποιώντας κατάλληλα τους κρυπτογραφικούς αλγόριθμους δημοσίου κλειδιού μπορεί να επιτευχθεί πιστοποίηση (authentication), δηλαδή ο παραλήπτης να γνωρίζει με ασφάλεια την

ταυτότητα του αποστολέα. Για να επιτευχθεί αυτό θα πρέπει ο αποστολέας να χρησιμοποιήσει το ιδιωτικό του κλειδί για την κρυπτογράφηση του μηνύματος. Στη συνέχεια στέλνει το μήνυμα στον παραλήπτη και ο τελευταίος χρησιμοποιεί το δημόσιο κλειδί του αποστολέα για την αποκρυπτογράφησή του. Δεδομένου ότι το ιδιωτικό κλειδί του αποστολέα είναι γνωστό μονάχα στον ίδιο, ο παραλήπτης μπορεί να είναι σίγουρος για την ταυτότητα του αποστολέα.



Εικόνα 16, αυθεντικοποίηση αλλά όχι εμπιστευτικότητα.

Παρόλο που η παραπάνω μέθοδος εγγυάται την ταυτοποίηση του αποστολέα, δεν δύναται να εγγυηθεί την εμπιστευτικότητα του μηνύματος. Πράγματι, το μήνυμα μπορεί να το αποκρυπτογραφήσει οποιοσδήποτε διαθέτει το δημόσιο κλειδί του αποστολέα. Όπως έχει ήδη ειπωθεί, το δημόσιο κλειδί είναι γνωστό σε όλη τη διαδικτυακή κοινότητα, άρα πρακτικά ο οποιοσδήποτε μπορεί να διαβάσει το περιεχόμενο του μηνύματος.

Το στοίχημα επομένως είναι να πετύχουμε το καλύτερο αποτέλεσμα, συνδυάζοντας φυσικά τις δύο προηγούμενες τεχνικές που αναφέρθηκαν. Με αυτό τον τρόπο είναι εφικτό να επιτύχουμε εμπιστευτικότητα του μηνύματος και πιστοποίηση του αποστολέα. Δηλαδή αφενός το μήνυμα παραμένει γνωστό μονάχα στον αποστολέα και τον παραλήπτη και αφετέρου ο παραλήπτης γνωρίζει με ασφάλεια ποιος του έστειλε το μήνυμα. Για να επιτευχθεί αυτό ο αποστολέας μπορεί να κρυπτογραφήσει το μήνυμα πρώτα με το δικό του ιδιωτικό κλειδί και στη συνέχεια με το δημόσιο κλειδί του παραλήπτη. Όταν ο παραλήπτης λάβει το μήνυμα θα πρέπει να χρησιμοποιήσει το ιδιωτικό του κλειδί για να το αποκρυπτογραφήσει (εμπιστευτικότητα) και στη συνέχεια να αποκρυπτογραφήσει το αποτέλεσμα χρησιμοποιώντας το δημόσιο κλειδί του αποστολέα (πιστοποίηση).

Η κρυπτογραφία με συμμετρικά κλειδιά παρέχει μόνο εμπιστευτικότητα στο μήνυμα, καθώς το κλειδί που χρησιμοποιείται για την κρυπτογράφηση και αποκρυπτογράφηση του μηνύματος είναι το ίδιο και πρέπει να είναι γνωστό στον αποστολέα και τον παραλήπτη.

Η κρυπτογραφία με δημόσιο κλειδί (όπως ο RSA) παρέχει και αυθεντικοποίηση και εμπιστευτικότητα. Ο παραλήπτης μπορεί να επιβεβαιώσει την ταυτότητα του αποστολέα μέσω της δημιουργίας μιας ψηφιακής υπογραφής με το ιδιωτικό κλειδί του αποστολέα, ενώ το μήνυμα παραμένει κρυπτογραφημένο για να διασφαλιστεί η εμπιστευτικότητα του.

Οι δύο αυτές έννοιες είναι στενά συνδεδεμένες στην κρυπτογραφία, αλλά έχουν διαφορετικούς σκοπούς και μηχανισμούς. Η αυθεντικοποίηση αναφέρεται στη διασφάλιση της προέλευσης των δεδομένων και της ακεραιότητάς τους, ενώ η εμπιστευτικότητα αναφέρεται στη διατήρηση του μυστικού χαρακτήρα των δεδομένων και της απόκρυψής τους από μη εξουσιοδοτημένα μέρη.

Για παράδειγμα, στην κρυπτογραφία κλειδί δημοσίου-ιδιωτικού κλειδιού, το κλειδί δημοσίου κρυπτογραφεί το μήνυμα και το κλειδί ιδιωτικού αυθεντικοποιεί το μήνυμα. Αντίθετα, στην κρυπτογραφία κλειδί-κλειδί, τα ίδια κλειδιά χρησιμοποιούνται και για την εμπιστευτικότητα και για την αυθεντικότητα.

Συνολικά, η αυθεντικοποίηση και η εμπιστευτικότητα είναι σημαντικά στοιχεία της κρυπτογραφίας και συνήθως χρησιμοποιούνται μαζί για να διασφαλιστεί η ασφάλεια των δεδομένων.

3.9 Θύρες επικοινωνίας και Sockets

Οι θύρες επικοινωνίας είναι φυσικές ή λογικές συνδέσεις σε ένα δίκτυο που επιτρέπουν την ανταλλαγή δεδομένων μεταξύ δύο ή περισσότερων συσκευών. Οι φυσικές θύρες είναι το φυσικό σημείο στο οποίο μια συσκευή συνδέεται με το δίκτυο, όπως μια θύρα Ethernet σε έναν υπολογιστή ή μια θύρα RJ45 σε ένα δρομολογητή. Από την άλλη πλευρά, οι λογικές θύρες είναι τμήματα του λογισμικού που ελέγχουν την κίνηση των δεδομένων μέσα στο δίκτυο. Μια λογική θύρα μπορεί να αποτελείται από πολλές φυσικές θύρες που συνδέονται μεταξύ τους και λειτουργούν ως ένα ενιαίο σημείο εισόδου και εξόδου στο δίκτυο. Κάθε θύρα έχει έναν αριθμό καθορισμένο από το πρωτόκολλο επικοινωνίας που χρησιμοποιείται στο δίκτυο, όπως τον αριθμό θύρας TCP (*Transmission Control Protocol*) ή τον αριθμό θύρας UDP (User Datagram Protocol). Αυτές παρέχουν έναν τρόπο για τα δεδομένα ώστε να προσδιοριστούν στη σωστή εφαρμογή που τα αποδέχεται και τα επεξεργάζεται. Αποτελούν τους συνδετήρες που χρησιμοποιούνται για την σύνδεση διαφορετικών συσκευών σε ένα δίκτυο επικοινωνιών. Κάθε συσκευή που συνδέεται σε ένα δίκτυο έχει μια συγκεκριμένη θύρα επικοινωνίας που χρησιμοποιεί για να ανταλλάσσει δεδομένα με άλλες συσκευές και μπορεί να διαφέρουν ανάλογα με το είδος της συσκευής και τον τύπο του δικτύου. Για παράδειγμα, οι θύρες ενός δρομολογητή δικτύου θα διαφέρουν από τις θύρες ενός διακομιστή ή ενός ενσύρματου δικτύου συνδέσμου.

Οι γνωστές θύρες επικοινωνίας αναφέρονται σε συγκεκριμένους αριθμούς θυρών που χρησιμοποιούνται για διάφορες επικοινωνιακές διεργασίες σε ένα δίκτυο. Οι πιο γνωστές θύρες επικοινωνίας είναι οι εξής:

1. Θύρα 80 (HTTP): Χρησιμοποιείται για την επικοινωνία με διαδικτυακές σελίδες μέσω του πρωτοκόλλου HTTP (Hypertext Transfer Protocol). Είναι η προκαθορισμένη θύρα για την περιήγηση στον Παγκόσμιο Ιστό.
2. Θύρα 443 (HTTPS): Χρησιμοποιείται για την ασφαλή επικοινωνία με διαδικτυακές σελίδες μέσω του πρωτοκόλλου HTTPS (Hypertext Transfer Protocol Secure). Η επικοινωνία μέσω της θύρας 443 είναι κρυπτογραφημένη για επιπλέον ασφάλεια.

3. Θύρα 25 (SMTP): Χρησιμοποιείται για την αποστολή ηλεκτρονικού ταχυδρομείου μέσω του πρωτοκόλλου SMTP (Simple Mail Transfer Protocol).
4. Θύρα 110 (POP3): Χρησιμοποιείται για τη λήψη ηλεκτρονικού ταχυδρομείου από έναν διακομιστή μέσω του πρωτοκόλλου POP3 (Post Office Protocol version 3).
5. Θύρα 143 (IMAP): Χρησιμοποιείται για την ανάκτηση και διαχείριση ηλεκτρονικού ταχυδρομείου από έναν διακομιστή μέσω του πρωτοκόλλου IMAP (Internet Message Access Protocol).

Αυτές είναι μερικές από τις γνωστές θύρες επικοινωνίας και οι κύριες χρήσεις τους. Κάθε θύρα έχει αντιστοιχημένο ένα πρωτόκολλο ή μια υπηρεσία που ορίζει την επικοινωνία και τη λειτουργία που πραγματοποιείται μέσω αυτής.

Η σύνδεση μεταξύ μιας θύρας και μιας διεύθυνσης Internet Protocol (IP) σχετίζεται με τον τρόπο που ένα πακέτο δεδομένων προορίζεται για τη σωστή διεύθυνση στο δίκτυο. Οι θύρες χρησιμοποιούνται για να προσδιορίσουν συγκεκριμένες εφαρμογές ή υπηρεσίες που λειτουργούν σε μια συσκευή, ενώ οι διευθύνσεις IP αναγνωρίζουν μοναδικά τις συσκευές στο δίκτυο. Η σύνδεση μεταξύ της θύρας και της διεύθυνσης IP γίνεται με τη χρήση του πρωτοκόλλου μεταφοράς (TCP) στο OSI μοντέλο. Κάθε συσκευή σε ένα δίκτυο έχει μια μοναδική διεύθυνση IP, η οποία αποτελείται από μια σειρά αριθμών που χωρίζονται μεταξύ τους με τη χρήση τελείας. Παράδειγμα μιας διεύθυνσης IP είναι η 192.168.0.1. Η διεύθυνση IP προσδιορίζει τη συσκευή στο δίκτυο και τον υπολογιστή με τον οποίο θα επικοινωνήσει. Από την άλλη πλευρά, οι θύρες προσδιορίζουν τις συγκεκριμένες εφαρμογές ή υπηρεσίες που εκτελούνται σε μια συσκευή. Οι θύρες αναπαριστούνται με αριθμούς, και οι γνωστές θύρες έχουν καθορισμένους αριθμούς για συγκεκριμένες υπηρεσίες. Για παράδειγμα, η θύρα 80 χρησιμοποιείται για την υπηρεσία HTTP, ενώ η θύρα 443 χρησιμοποιείται για την υπηρεσία HTTPS. Η σύνδεση μεταξύ μιας θύρας και μιας διεύθυνσης IP σημαίνει ότι ένα πακέτο δεδομένων που προορίζεται για μια συγκεκριμένη υπηρεσία ή εφαρμογή, όπως ένα αίτημα για μια ιστοσελίδα, θα πρέπει να προωθηθεί στη σωστή θύρα στην αντίστοιχη συσκευή με βάση τη διεύθυνση IP του παραλήπτη. Αυτό γίνεται για να εξασφαλιστεί ότι η επικοινωνία γίνεται με τη σωστή υπηρεσία που λειτουργεί στην προορισμένη συσκευή.

Ο συνδυασμός της διεύθυνσης IP και του αριθμού θύρας μας παρέχει ένα σημείο πρόσβασης σε μια εφαρμογή. Αυτός ο συνδυασμός ονομάζεται socket. Ένα socket είναι ένα μοναδικό αναγνωριστικό που χρησιμοποιείται για να ανοίξει κανάλι επικοινωνίας μεταξύ δύο προγραμμάτων σε ένα δίκτυο. Κατά την επικοινωνία μέσω δικτύου, ένα πρόγραμμα που λειτουργεί σε έναν υπολογιστή ορίζει ένα socket για να περιμένει συνδέσεις ή να επικοινωνήσει με ένα άλλο πρόγραμμα σε έναν απομακρυσμένο υπολογιστή. Το socket αναγνωρίζεται μέσω του συνδυασμού της διεύθυνσης IP (π.χ. 192.168.1.1) και του αριθμού θύρας (π.χ. 80 για HTTP). Με τη χρήση sockets, οι προγραμματιστές μπορούν να δημιουργήσουν δικτυακές εφαρμογές που ανταλλάσσουν δεδομένα μεταξύ τους μέσω του δικτύου, επιτρέποντας την αποστολή και λήψη πακέτων δεδομένων. Ο συνδυασμός IP και θύρας μεταφέρει τα δεδομένα στο σωστό πρόγραμμα προορισμού με βάση την εφαρμογή και τη λειτουργία που εκτελείται σε αυτήν τη θύρα.

Τα sockets χρησιμοποιούν ένα σύνολο κανόνων για την επικοινωνία στο δίκτυο και χρησιμοποιούνται κυρίως για τη μεταφορά δεδομένων μεταξύ των διαφορετικών συστημάτων. Κάθε ένα αντιστοιχεί σε έναν αριθμό θύρας και ένα πρωτόκολλο επικοινωνίας. Η χρήση sockets επιτρέπει την ανάπτυξη εφαρμογών δικτύου που μπορούν να λειτουργούν σε διάφορα λειτουργικά συστήματα και να επικοινωνούν με διαφορετικούς τύπους συστημάτων. Είναι ένας μηχανισμός που επιτρέπει τη δημιουργία διεπαφής επικοινωνίας μεταξύ δύο διαφορετικών υπολογιστών σε ένα δίκτυο και

χρησιμοποιούνται σε πολλές εφαρμογές δικτύου, όπως παιχνίδια δικτύου, συνομιλίες σε πραγματικό χρόνο, αποστολή και λήψη αρχείων και πρόσβαση σε απομακρυσμένους υπολογιστές.

3.10 Επίλογος

Στη σημερινή εποχή της ψηφιακής επικοινωνίας, η ασφάλεια είναι ένα θέμα μείζονος σημασίας. Η απειλή από κυβερνοεπιθέσεις και την κλοπή προσωπικών δεδομένων έχει αυξηθεί δραματικά, καθιστώντας την ασφαλή επικοινωνία αναγκαία για τη διατήρηση της ιδιωτικότητας και της ακεραιότητας των δεδομένων μας. Οι τεχνολογίες ασφαλείας στην επικοινωνία σήμερα περιλαμβάνουν την κρυπτογράφηση, τους πιστοποιητικούς φορείς, την πιστοποίηση ταυτότητας και άλλα μέτρα ασφαλείας που εξασφαλίζουν την εμπιστευτικότητα και ακεραιότητα των δεδομένων που ανταλλάσσονται μέσω δικτύων επικοινωνίας.

Η ανάπτυξη μιας εφαρμογής ασφαλούς επικοινωνίας θα βοηθήσει στην αποτροπή όλων των προβλημάτων διέρευσεις δεδομένων που αναφέρθηκαν ώστε να διασφαλίσει την εμπιστοσύνη ανάμεσα στους χρήστες που επικοινωνούν. Είναι μια σύνθετη διαδικασία που περιλαμβάνει πολλούς παράγοντες. Η ασφάλεια της επικοινωνίας πρέπει να είναι εξασφαλισμένη σε όλα τα επίπεδα του μοντέλου OSI, χρησιμοποιώντας κατάλληλους κρυπτογραφικούς αλγόριθμους και πρωτόκολλα ασφαλείας. Επίσης, η εφαρμογή πρέπει να είναι σχεδιασμένη έτσι ώστε να προσφέρει τον απαιτούμενο βαθμό ασφάλειας για το είδος της επικοινωνίας που πραγματοποιείται, καθώς και να λαμβάνει υπόψη τις απαιτήσεις προστασίας δεδομένων και προσωπικής απορρήτου. Επιπλέον, είναι σημαντικό να γίνεται συνεχής αναβάθμιση της εφαρμογής και των κρυπτογραφικών της αλγορίθμων, καθώς και να προσαρμόζεται στις αλλαγές των πρωτοκόλλων ασφαλείας και των πρακτικών ασφαλείας.

Παρόλα αυτά, η τεχνολογία συνεχίζει να εξελίσσεται και οι επιθέσεις καθίστανται ολοένα και πιο εξειδικευμένες και επικίνδυνες. Για αυτόν το λόγο, είναι σημαντικό να διατηρούμε επίσης την επίγνωση και την προσοχή μας στην ασφάλεια της επικοινωνίας μας, και να χρησιμοποιούμε μόνο αξιόπιστες και ασφαλείς εφαρμογές για την ανταλλαγή πληροφοριών και δεδομένων.

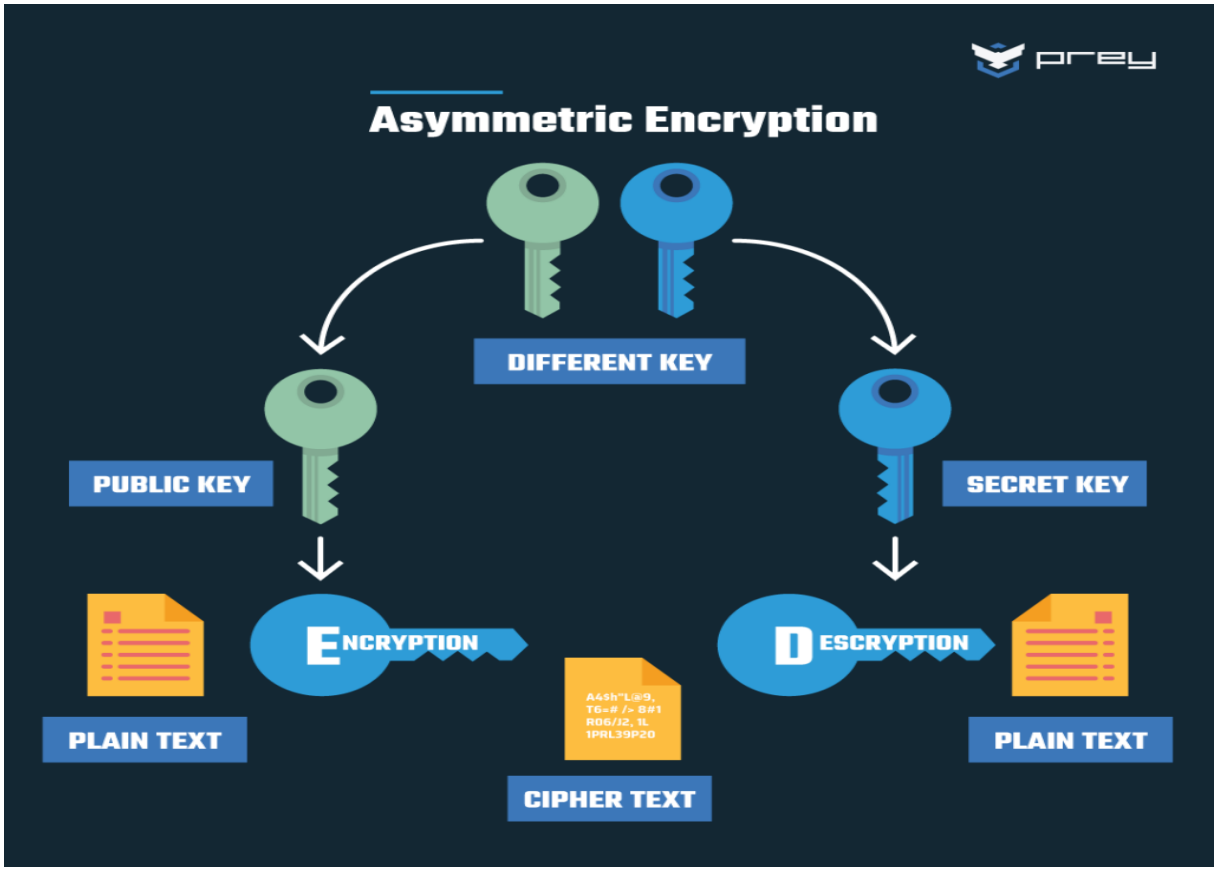
Κεφάλαιο 4ο: Πλαίσιο ανάπτυξης πτυχιακής εργασίας

4.1 Εισαγωγή

Στα πλαίσια της παρούσας πτυχιακής εργασίας, έχει σχεδιαστεί η ανάπτυξη μιας εφαρμογής ανταλλαγής μηνυμάτων με χρήση κρυπτογράφησης. Η εφαρμογή θα επιτρέπει στους χρήστες να ανταλλάσσουν μηνύματα μεταξύ τους με ασφάλεια, εξασφαλίζοντας την εμπιστευτικότητα και την ακεραιότητα των δεδομένων.

4.2 Πραγμάτευση πτυχιακής εργασίας

Στην υλοποίηση της εφαρμογής θα χρησιμοποιηθεί ο αλγόριθμους κρυπτογράφησης για την κρυπτογράφηση των μηνυμάτων πριν από την αποστολή τους και για την αποκρυπτογράφηση των μηνυμάτων κατά την παραλαβή τους από τον παραλήπτη. Ο αλγόριθμος που χρησιμοποιήθηκε είναι ο RSA-768 ο οποίος έπειτα από αρκετή έρευνα στο διαδίκτυο, σε συγγράμματα αφιερωμένα στην αξιοποίηση αλλά και στο έλεγχο της ασφάλειας του, αλλά και σε συγκρίσεις μεταξύ των τελευταίων εφαρμογών της αγοράς που λειτουργούν με παρόμοιο τρόπο αξιοποιώντας την κρυπτογράφηση και την αποκρυπτογράφηση, θεωρείται ο πιο αξιόπιστος.



Εικόνα 17, ασύμμετρη κρυπτογράφηση.

Ο αλγόριθμος εφαρμόζει μια συνάρτηση κρυπτογράφησης στο περιεχόμενο του μηνύματος, χρησιμοποιώντας ζεύγη κλειδιών, ένα δημόσιο κλειδί και ένα ιδιωτικό κλειδί. Ο αποστολέας θα κρυπτογραφεί το μήνυμα χρησιμοποιώντας το δημόσιο κλειδί του παραλήπτη, ενώ ο παραλήπτης θα αποκρυπτογραφεί το μήνυμα χρησιμοποιώντας το ιδιωτικό κλειδί του. Η ασύμμετρη κρυπτογραφία

προσφέρει το πλεονέκτημα της εξασφάλισης της εμπιστευτικότητας των δεδομένων χωρίς την ανάγκη κοινής γνώσης του κλειδιού. Η ανάπτυξη της εφαρμογής περιλαμβάνει την υλοποίηση των αλγορίθμων κρυπτογράφησης, τη διαχείριση των κλειδιών, την ασφαλή αποθήκευση των κλειδιών και την ανάπτυξη του περιβάλλοντος ανταλλαγής μηνυμάτων.

Η γλώσσα προγραμματισμού με την οποία υλοποιήθηκε ο κώδικας για την εφαρμογή είναι η Java. Η Java είναι μια πανίσχυρη, αντικειμενοστραφής γλώσσα προγραμματισμού που χρησιμοποιείται ευρέως για την ανάπτυξη εφαρμογών σε διάφορους τομείς, όπως ο ιστός (web), οι κινητές συσκευές (mobile), οι ενσωματωμένοι συστήματα (embedded systems) και πολλοί άλλοι. Η Java παρέχει ένα ισχυρό περιβάλλον εκτέλεσης που ονομάζεται Java Virtual Machine (JVM), το οποίο επιτρέπει την εκτέλεση του κώδικα σε διάφορες πλατφόρμες χωρίς να απαιτείται η μεταγλώττισή του για κάθε πλατφόρμα ξεχωριστά. Αυτό το χαρακτηριστικό της Java την καθιστά πολύ ευέλικτη και φορητή. Η Java προσφέρει επίσης ένα ευρύ φάσμα βιβλιοθηκών και πλαισίων ανάπτυξης που διευκολύνουν την υλοποίηση διάφορων λειτουργιών και λύσεων. Είναι μια γλώσσα με ισχυρές δυνατότητες ασφαλείας, σταθερότητας και αποδοτικότητας. Ο κώδικας που γράφεται σε Java είναι αναγνώσιμος και κατανοητός, καθώς η γλώσσα έχει σχεδιαστεί με έμφαση στην απλότητα και τη συνοχή. Επιπλέον, η Java υποστηρίζει την ανάπτυξη μεγάλων εφαρμογών μέσω της δυνατότητας αντικατάστασης και επαναχρησιμοποίησης κώδικα μέσω των αντικειμενοστραφών αρχών. Συνολικά, η Java είναι μια ισχυρή γλώσσα προγραμματισμού που προσφέρει αξιόπιστες λύσεις για την ανάπτυξη πολλών είδων εφαρμογών.

Εικόνα 18, η γλώσσα προγραμματισμού java.

Το κύριο αποτέλεσμα της πτυχιακής εργασίας θα είναι η υλοποίηση μιας λειτουργικής εφαρμογής ανταλλαγής μηνυμάτων με κρυπτογράφηση, η οποία θα παρέχει ασφάλεια και προστασία των δεδομένων για τους χρήστες της. Επιπλέον, η εργασία θα προσφέρει μια αναλυτική αξιολόγηση της απόδοσης της εφαρμογής και των αλγορίθμων κρυπτογράφησης, καθώς και προτάσεις για περαιτέρω

βελτιώσεις και επεκτάσεις. Με αυτόν τον τρόπο, θα συνδυαστούν θεωρητική ανάλυση της κρυπτογραφίας με την πρακτική υλοποίηση μιας ασφαλούς εφαρμογής ανταλλαγής μηνυμάτων.

4.3 Επίλογος

Η χρήση των παραπάνω δυνατοτήτων της γλώσσας προγραμματισμού αλλά και του κρυπτογραφικού αλγορίθμου RSA προσφέρει πολλές δυνατότητες, εύκολες για επαναχρησιοποίηση και κατανόηση. Οι δυνατότητες της Java σε συνδυασμό με τον αλγόριθμο RSA παρέχουν μεγάλη ευελιξία και δυνατότητες προσαρμογής. Μπορεί ο προγραμματιστής να προσθέσετε επιπλέον λειτουργίες στην εφαρμογή, να βελτιώσει την απόδοση ή να επεκτείνετε τις λειτουργίες κρυπτογράφησης και αποκρυπτογράφησης με βάση τις ανάγκες του. Ο συνδυασμός αυτό αφήνει ανοιχτές πιθανότητες για περαιτέρω ανάπτυξη, βελτιώσεις και προσαρμογές στο μέλλον. Μπορεί να εξερευνήσει νέες τεχνολογίες, πρότυπα κρυπτογράφησης και προηγμένες λειτουργίες της Java για να δημιουργήσει ακόμα πιο ασφαλείς και αποδοτικές εφαρμογές.

Κεφάλαιο 5ο: Ανάλυση της εφαρμογής

5.1 Εισαγωγή

Η κρυπτογράφηση αποτελεί ένα σημαντικό μέσο για τη διασφάλιση της ασφάλειας των επικοινωνιών στο διαδίκτυο. Μια εφαρμογή επικοινωνίας με κρυπτογράφηση επιτρέπει στους χρήστες να ανταλλάσσουν πληροφορίες μεταξύ τους με ασφάλεια, χωρίς να ανησυχούν για τον κίνδυνο της παραβίασης της απόρρητης πληροφορίας τους.

Για την ανάπτυξη μιας εφαρμογής επικοινωνίας με κρυπτογράφηση, πρέπει να ληφθούν υπόψη διάφοροι παράγοντες, όπως ο αλγόριθμος κρυπτογράφησης που θα χρησιμοποιηθεί, η διαχείριση των κλειδιών κρυπτογράφησης, οι μέθοδοι πιστοποίησης και αυθεντικοποίησης των χρηστών και η διαχείριση των πιστοποιητικών ασφαλείας.

5.2 Έναρξη της εφαρμογής

5.2.1 Αρχικοποίηση της θύρας επικοινωνίας

Η πρώτη δουλειά, μετά την εκτέλεση του προγράμματος, για να μπει σε λειτουργία την εφαρμογή και να δώσουμε τις υπηρεσίες που παρέχουμε στους χρήστες, είναι να αρχικοποιηθεί η θύρα στην οποία θα “μιλάει” η εφαρμογή μας. Ο αριθμός θύρας είναι ένας τρόπος για τον προσδιορισμό μιας συγκεκριμένης διαδικασίας στην οποία πρόκειται να προωθηθεί ένα μήνυμα Διαδικτύου ή άλλου δικτύου, κάποιο τοπικό δίκτυο για παράδειγμα μια εταιρείας που θα χρησιμοποιήσει την εφαρμογή ως εσωτερική επικοινωνία για τα μέλη της. Αυτή η ενέργεια προσφέρει την επιλογή στον υπεύθυνο διαχείρισης, να αρχικοποιήσει την θύρα που θα επικοινωνούν οι χρήστες της ομάδας του αλλά είναι αρκετά χαμηλού επιπέδου διαδικασία. Έτσι αν και προσφέρει μία επιπλέον εξειδίκευση, και κατ’ επέκταση ασφάλεια, αφού η επιλογή της θύρας βρίσκεται αποκλειστικά στα χέρια του υπεύθυνου και είναι γνωστή μόνο στους χρήστες που αυτός έχει επιλέξει, η συγκεκριμένη ενέργεια μπορεί να αυτοματοποιηθεί σε μελλοντικές αναπτύξεις έτσι ώστε να αποδεσμευτεί από το ανθρώπινο δυναμικό, επιλέγοντας την βέλτιστη θύρα επικοινωνίας για το εκάστοτε δίκτυο.

```
package com.alex.server;

public class ServerMain {
    public static void main(String[] args) {
        int port = 3389;
        Server server = new Server(port);
        server.start();
        try {
            server.join();
        } catch (InterruptedException e) {
            e.printStackTrace();
        }
    }
}
```

Εικόνα 19, αρχικοποίηση θύρας προώθησης μηνυμάτων.

Για το συγκεκριμένο παράδειγμα που φαίνεται στις παρακάτω εικόνες θα χρησιμοποιηθεί η βοήθεια του Telnet το οποίο παρέχεται από τα windows και είναι αρκετά εύκολο στην χρήση του. Το Telnet είναι ένα πρωτόκολλο εφαρμογής που χρησιμοποιείται στο διαδίκτυο ή στο τοπικό δίκτυο για την παροχή μιας αμφίδρομης διαδραστικής δυνατότητας επικοινωνίας προσανατολισμένης σε κείμενο χρησιμοποιώντας μια σύνδεση εικονικού τερματικού. Ανοίγοντας ένα παράθυρο CMD, ένα παράθυρο

επεξεργαστή εντολών που παρέχεται στα περισσότερα λειτουργικά συστήματα windows εκτελούμε την εντολή telnet localhost <port number> και αρχικοποιείται η θύρα επικοινωνίας.

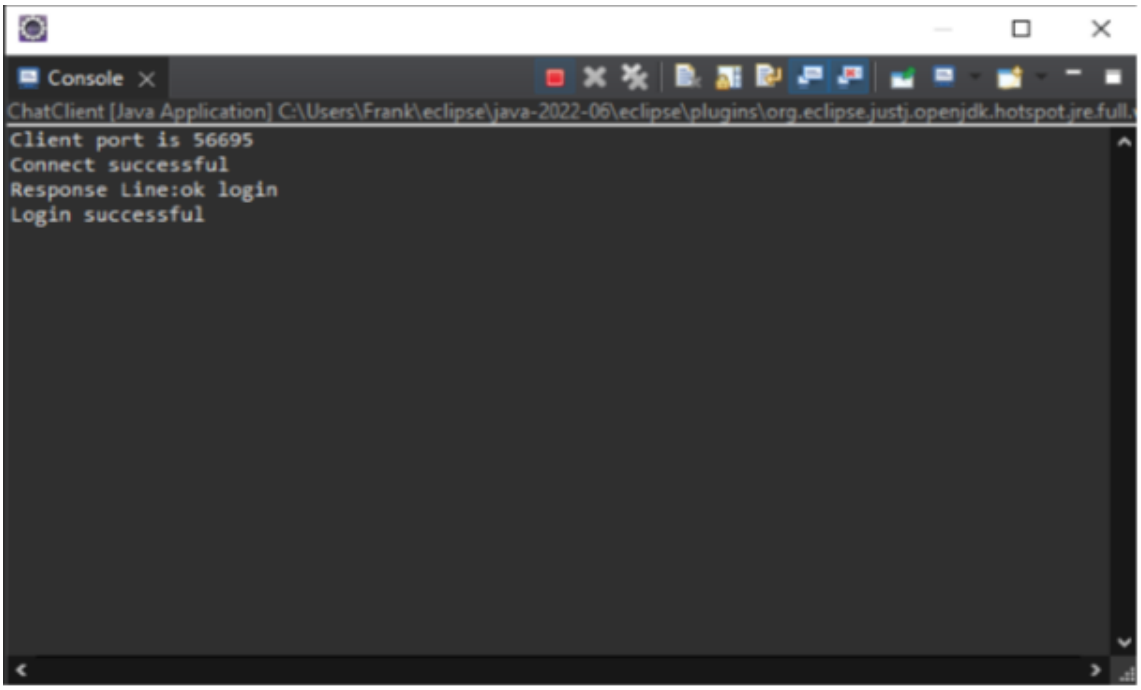
Το παράθυρο εντολών χρησιμοποιεί το κελύφος της γραμμής εντολών (command-line shell) για την επικοινωνία με το λειτουργικό σύστημα. Η γραμμή εντολών είναι ένας τρόπος για να αλληλεπιδράσετε με το λειτουργικό σύστημα χρησιμοποιώντας εντολές κειμένου, αντί για τη χρήση γραφικού περιβάλλοντος χρήστη.

Το παράθυρο εντολών (Command Prompt) είναι ένα παράθυρο που εμφανίζεται στον υπολογιστή και παρέχει ένα περιβάλλον εντολών για την επικοινωνία με το σύστημα. Στο παράθυρο αυτό μπορείτε να εκτελέσετε εντολές και να προγραμματίσετε διάφορες λειτουργίες στον υπολογιστή σας.

Στο παράθυρο εντολών, μπορούν να πληκτρολογηθούν εντολές για να αλληλεπιδράσετε με το σύστημα και να εκτελέσετε διάφορες εργασίες, όπως τον έλεγχο των αρχείων και των φακέλων, την εγκατάσταση προγραμμάτων, την αναζήτηση πληροφοριών για το σύστημα σας, την προβολή διαθέσιμων συσκευών και πολλά άλλα.

5.2.2 Ενημέρωση έκβασης μέσω εσωτερικών μηνυμάτων

Εκτελώντας το main κομμάτι του κώδικα για την αρχικοποίηση του server μας, ως αποτέλεσμα έχουμε τα παρακάτω μηνύματα τα οποία διευκολύνουν και ενημερώνουν τον προγραμματιστή / διαχειριστή. Υπάρχει ένα σύντομο μήνυμα επιτυχίας σε συνδυασμό με την θύρα επικοινωνίας στην οποία ορίστηκε ότι θα γίνει η ανταλλαγή των μηνυμάτων.

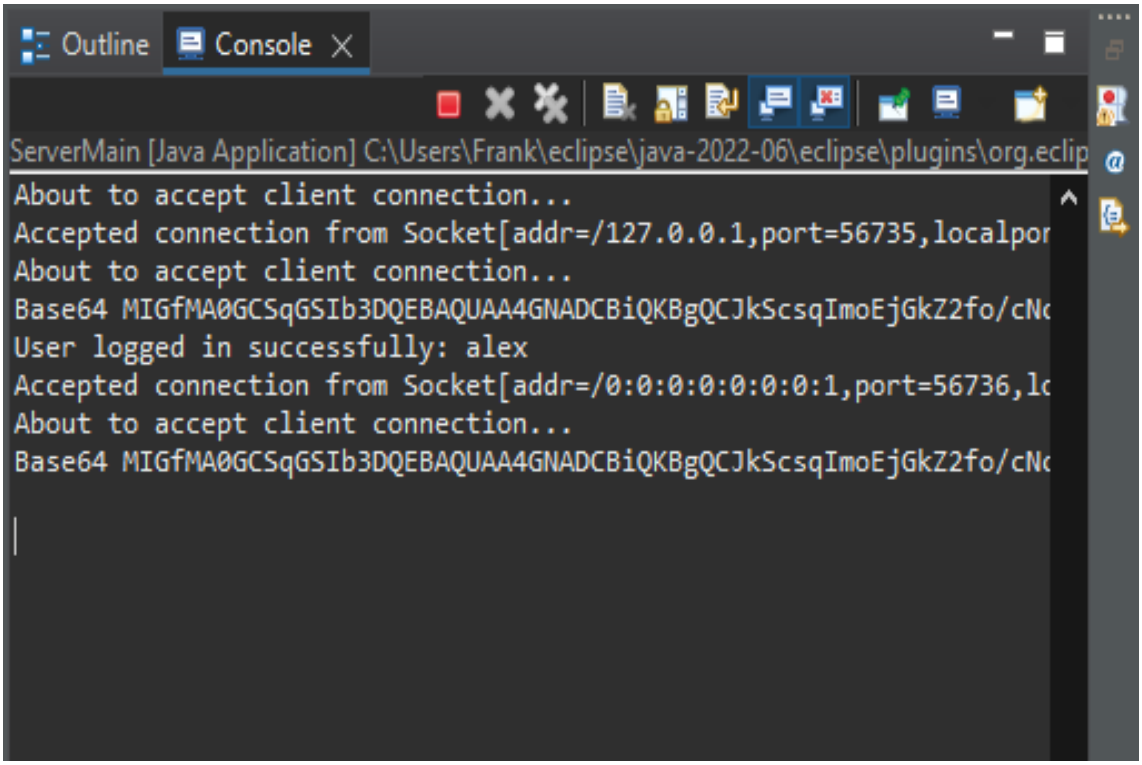


Εικόνα 20, successful LogIn message, with port.

Στην συνέχεια με τη λειτουργία του εκτελέσιμου αρχείου για τον server εμφανίζεται το παράθυρο της παρακάτω εικόνας, ως διαχειριστές της εφαρμογής αυτή την φορά είναι ορατό μόνο σε εμάς και όχι στον απλό χρήστη για λόγους διευκόλυνσης του προγραμματιστή. Το πρώτο μήνυμα αφού αρχικοποιηθεί η θύρα σωστά, ενημερώνει ότι η εφαρμογή είναι έτοιμη να δεχθεί συνδέσεις δηλαδή οι χρήστες μπορούν να εισέλθουν με τα προσωπικά του στοιχεία.

Ένα δεύτερο μήνυμα είναι η ενημέρωση για το socket το οποίο θα χρησιμοποιηθεί για την ανταλλαγή μηνυμάτων. Με αυτόν τον τρόπο ο προγραμματιστής γνωρίζει σε ποιό στάδιο βρίσκεται η εφαρμογή και ακόμη εάν όλα πήγαν όπως θα έπρεπε, κάνοντας τον εντοπισμό προβλημάτων πιό εύκολο σε περίπτωση που συμβεί ένα πρόβλημα.

Στην συνέχεια υπάρχει ένα νέο μήνυμα το οποίο αναφέρει ότι ο χρήστης συνδέθηκε επιτυχώς και ταυτόχρονα και το userName του χρήστη. Παρακάτω θα δούμε ένα παρόμοιο μήνυμα που ενημερώνει του ενεργούς χρήστες για τον νέο χρήστη μόλις εισέρχεται στην εφαρμογή. Το τελευταίο αν και σε εμφάνιση είναι παρόμοιο με αυτό στην ουσία διαφέρει διότι το ένα είναι στην πλευρά του backend το οποίο είναι το κομμάτι που αφορά τον προγραμματιστή / διαχειριστή ενώ το μήνυμα της παρακάτω ενότητας αναφέρεται καθαρά στο, User interface (UI) στην αλληλεπίδραση του χρήστη με το σύστημα με σκοπό την βελτίωση και την καλύτερη χρήση του.



Εικόνα 21, response message from console.

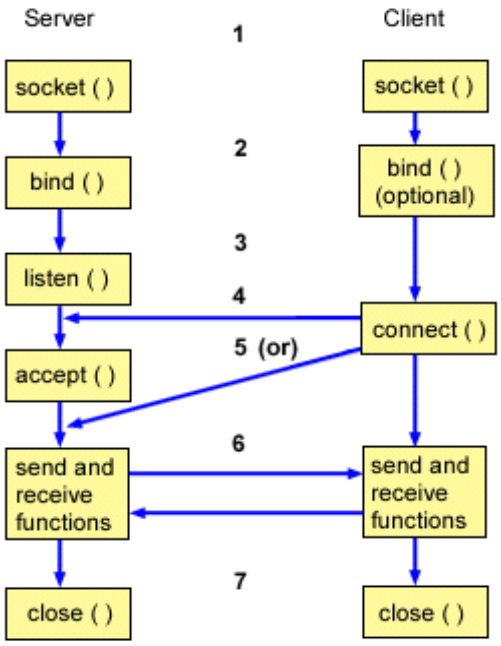
5.2.3 Η κύρια μέθοδος *run*

Στο παράρτημα ένα, στο πρώτο κομμάτι κώδικα, μπορείται να δείτε πως δημιουργούνται τα αντίστοιχα κλειδιά κρυπτογράφησης και αποκρυπτογράφησης κάθε χρήστη αλλά και το κύριο *Socket*, στο οποίο θα επικοινωνούν οι χρήστες, το οποίο βρίσκεται μέσα σε βρόχο επανάληψης ώστε να υποστηρίξει πολλαπλές συνδέσεις χρηστών καθόλη την διάρκεια ζωής της εφαρμογής.

5.2.4 Αναπαράσταση ροής γεγονότων

Τα Sockets χρησιμοποιούνται συνήθως για αλληλεπίδραση πελάτη και διακομιστή. Η τυπική διαμόρφωση συστήματος τοποθετεί τον διακομιστή σε ένα μηχάνημα, με τους πελάτες σε άλλα μηχανήματα. Οι πελάτες συνδέονται στον διακομιστή, ανταλλάσσουν πληροφορίες και στη συνέχεια αποσυνδέονται. Ένα Socket έχει μια τυπική ροή γεγονότων. Σε ένα μοντέλο πελάτη-προς-διακομιστή, το αντίστοιχο Socket περιμένει αιτήματα από έναν πελάτη. Για να γίνει αυτό, ο διακομιστής πρώτα

δημιουργεί (δεσμεύει) μια διεύθυνση που μπορούν να χρησιμοποιήσουν οι πελάτες για να βρουν τον διακομιστή. Όταν δημιουργηθεί η διεύθυνση, ο διακομιστής περιμένει τους πελάτες να ζητήσουν μια υπηρεσία. Η ανταλλαγή δεδομένων πελάτη-προς-διακομιστή πραγματοποιείται όταν ένας πελάτης συνδέεται στον διακομιστή μέσω ενός Socket. Ο διακομιστής εκτελεί το αίτημα του πελάτη και στέλνει την απάντηση πίσω στον πελάτη.



Εικόνα 22, παράδειγμα τυπικής ροής γεγονότων.

5.2.5 Η μέθοδος εισόδου *handleLogin & login*

Το επόμενο βήμα και το πρώτο από την πλευρά του χρήστη είναι η είσοδος του, η διαδικασία του *Log in* ή της εγγραφής *Sign up στην περίπτωση νέου χρήστη.* Η είσοδος στην εφαρμογή είναι αρκετά απλή και παρόμοια με τις περισσότερες εφαρμογές ανταλλαγής μηνυμάτων που υπάρχουν διαθέσιμες αυτή την στιγμή στην αγορά. Ανάμεσά τους είναι οι εξής:

- Ηλεκτρονικό ταχυδρομείο (Email): Οι πάροχοι ηλεκτρονικού ταχυδρομείου χρησιμοποιούν κρυπτογράφηση για την ασφαλή μετάδοση και αποθήκευση email. Παραδείγματα περιλαμβάνουν το Gmail της Google και το Outlook της Microsoft, που χρησιμοποιούν κρυπτογράφηση TLS/SSL για την προστασία των μηνυμάτων κατά τη μετάδοση και τον αποθηκευτικό χώρο.
- Εφαρμογές ανταλλαγής μηνυμάτων και συνομιλίας: Εφαρμογές όπως το Signal, το WhatsApp και το Telegram χρησιμοποιούν κρυπτογράφηση για την ασφαλή ανταλλαγή μηνυμάτων και την προστασία των προσωπικών δεδομένων των χρηστών. Αυτές οι εφαρμογές χρησιμοποιούν πρωτόκολλα όπως το Signal Protocol για την κρυπτογράφηση των μηνυμάτων.
- Ηλεκτρονικές τραπεζικές συναλλαγές: Οι υπηρεσίες ηλεκτρονικής τραπεζικής και πληρωμών, όπως το PayPal και οι τράπεζες, χρησιμοποιούν κρυπτογράφηση για την ασφαλή μετάδοση προσωπικών και οικονομικών δεδομένων των χρηστών. Το πρωτόκολλο SSL/TLS χρησιμοποιείται συχνά για την κρυπτογράφηση των επικοινωνιών.
- Εφαρμογές ανταλλαγής αρχείων: Εφαρμογές όπως το Dropbox και το Google Drive χρησιμοποιούν κρυπτογράφηση για την ασφαλή μετάδοση και αποθήκευση αρχείων στον υπολογιστικό τους νέφος (cloud). Η κρυπτογράφηση εξασφαλίζει ότι τα αρχεία παραμένουν ιδιωτικά και μη προσβάσιμα από άλλους.

Αυτά είναι μερικά παραδείγματα εφαρμογών της αγοράς που χρησιμοποιούν κρυπτογράφηση για την ασφαλή ανταλλαγή μηνυμάτων. Οι προαναφερθείσες εφαρμογές επιδεικνύουν την σημασία της κρυπτογράφησης στη διατήρηση της ιδιωτικότητας και της ασφάλειας των επικοινωνιών στον ψηφιακό κόσμο.

Ο χρήστης αρχικά θα πρέπει να δημιουργήσει έναν λογαριασμό δίνοντας ένα έγκυρο email και έναν κωδικό πρόσβασης σύμφωνο με τους όρους δημιουργίας λογαριασμού, ώστε να συνάδει με τους κανόνες ασφαλείας. Έπειτα από την επιβεβαίωση, ο νέος λογαριασμός, ως χρήστης της εφαρμογής πλέον, πληκτρολογώντας το email και τον κωδικό πρόσβαση μπορεί να εισέλθει στην εφαρμογή αντικρίζοντας έτσι την πρώτη οθόνη καλωσορίσματος - μικρής ενημέρωσης.

Στο δεύτερο παράρτημα, το κομμάτι κώδικα το οποίο είναι υπεύθυνο για την διαχείριση της εισόδου του χρήστη στην εφαρμογή είναι ημέθοδος ονομάζεται handleLogin, αποτελείται από έναν αρχικό έλεγχο στις πρώτες γραμμές του σώματος της, ο οποίος ελέγχει το κείμενο που έχει δώσει ο χρήστης.

Αφού το χωρίσει σε 3 token κομμάτια :

- το πρώτο αντιστοιχεί στην αναγνώριση της εντολής ώστε να προετοιμάσουμε τον worker (υπεύθυνο για διαχείριση των λειτουργιων),
- το δεύτερο στο userName / όνομα του χρήστη
- και το τρίτο και τελευταίο token, στον κωδικό που έχει πληκτρολογήσει ο χρήστης σε ασφαλή μορφή.

Στις επόμενες γραμμές υπάρχει ο επόμενος έλεγχος των στοιχείων που έχει δώσει ώστε να επιβεβαιωθεί ότι ο συγκεκριμένος ανήκει στην λίστα εγγεγραμμένων. Εφόσον ο παραπάνω βρόγχος περάσει από το κομμάτι επιτυχίας που σημαίνει ότι τα στοιχεία αντιστοιχούν σε κάποιον εγγεγραμμένο χρήστη, γίνεται είσοδος στην εφαρμογή. Τα παραπάνω σε επίπεδο κώδικα σημαίνουν ότι το συγκεκριμένο αντικείμενο, ο χρήστης, προστίθεται σε μια λίστα από workers, χρήστες που έχουν εισέλθει και μπορούν να επικοινωνήσουν μεταξύ τους.

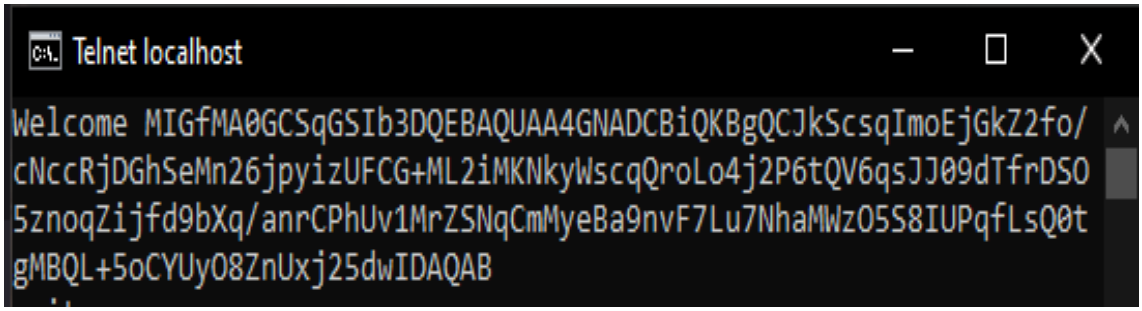
Τέλος για την διευκόλυνση των χρηστών και για να γίνει πιο απλή και εύκολη η περιήγηση τους και η διαχείριση της εφαρμογής, αποστέλλεται αυτόματα ένα μήνυμα με το όνομα του χρήστη μόλις ολοκληρωθεί η παραπάνω διαδικασία, μόλις πραγματοποιήσει τη διαδικασία του LogIn δηλαδη, σε όλους του υπόλοιπους χρήστες που ανήκουν στην λίστα με τους workers, ενεργούς χρήστες ενημερώνοντας τους ότι εισήλθε, αλλά αποστέλλεται και στον ίδιο χρήστη που μόλις εισήλθε ώστε να ενημερωθεί ποιοί είναι ενεργοί και μπορεί να ξεκινήσει την επικοινωνία.

```
// Expose the login to others users
public String getLogin() {
    return login;
}
```

Εικόνα 23, μέθοδος getLogIn, ενημέρωση ενεργών χρηστών.

Η παρακάτω εικόνα δείχνει ένα μήνυμα καλωσορίσματος πρός τον χρήστη κατά την είσοδό του στην εφαρμογή. Το συγκεκριμένο στιγμιότυπο έχει αποτυπωθεί από παράθυρο cmd για λόγους παρουσίασης και όπως φαίνεται το κομμάτι που έπρεπε να αναφέρεται το όνομα του χρήστη έχει

αντικατασταθεί από μία αλληλουχία χαρακτήρων οι οποίο θα λέγαμε ότι δεν βγάζουν κάποιο νόημα σε αυτή την μορφή. Κάτι τέτοιο θεωρείται δυσνόητο και μη αναγνωρίσιμου στα μάτια ενός απλού χρήστη. Ο λόγος είναι η κρυπτογράφηση που έχει υποστεί το userName του χρήστη. Φυσικά και σε κανονική ροή ο χρήστης βλέπει το userName του και όχι κάτι τέτοιο, κάτι που θα αναλυθεί παρακάτω.

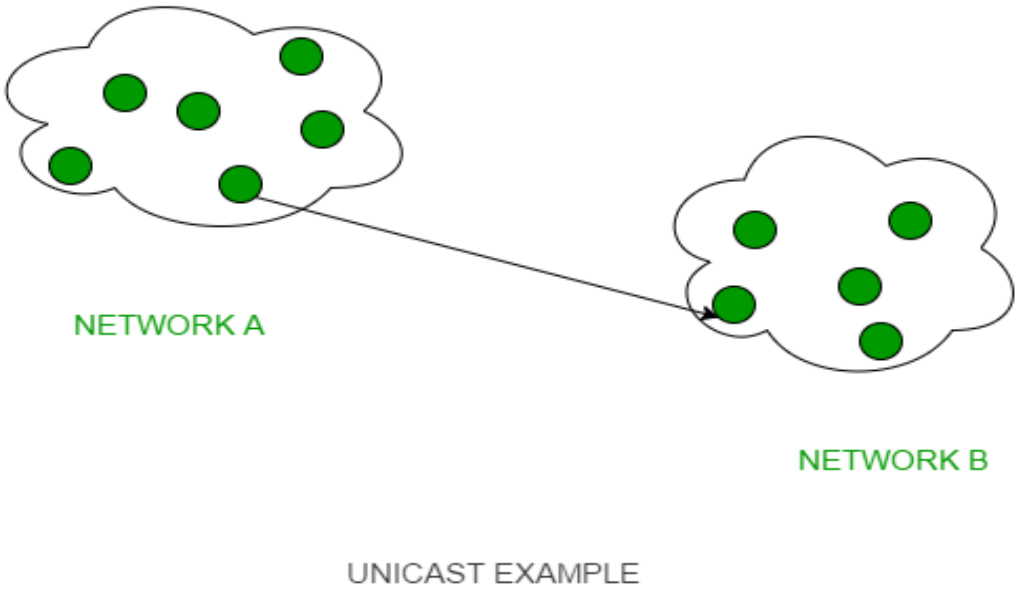


Εικόνα 24, response message from cmd, encrypted userName.

5.3 Παραλήπτης/ες τύπου unicast, multicast & broadcast

5.3.1 Unicast

Ο τύπος μεταφοράς πληροφοριών unicast είναι χρήσιμος όταν υπάρχει συμμετοχή ενός μόνο αποστολέα και ενός μόνο παραλήπτη. Έτσι, εν συντομία, μπορούμε να χαρακτηριστεί ως μετάδοση ένα προς ένα. Για παράδειγμα, εάν μια συσκευή με συγκεκριμένη διεύθυνση IP σε ένα δίκτυο θέλει να στείλει τη ροή κίνησης (πακέτα δεδομένων) στη συσκευή με μια άλλη διεύθυνση IP στο άλλο δίκτυο, τότε το *unicast* εμφανίζεται στην εικόνα. Αυτή είναι η πιο κοινή μορφή μεταφοράς δεδομένων μέσω των δικτύων.



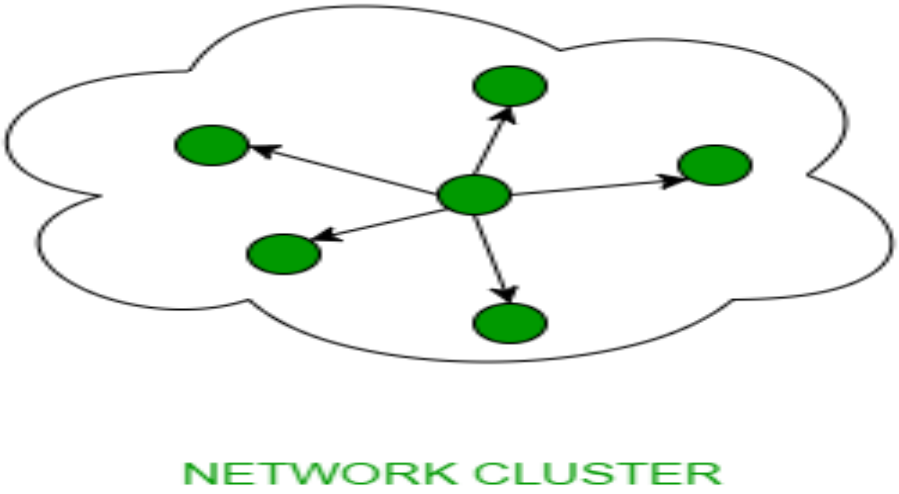
Εικόνα 25, unicast.

5.3.2 Broadcast

Οι τεχνικές μεταφοράς μετάδοσης (ένας προς όλους) μπορούν να ταξινομηθούν σε δύο τύπους:

- Limited Broadcasting (Περιορισμένη εκπομπή). Σε αυτόν τον τύπο, ένα μήνυμα αποστέλλεται σε μια προκαθορισμένη ομάδα παραληπτών. Αντί να αποστέλλεται σε όλες τις συσκευές του δικτύου, το μήνυμα προωθείται μόνο σε μια επιλεγμένη ομάδα συσκευών που έχουν συγκεκριμένες ρυθμίσεις ή παραμέτρους. Η περιορισμένη εκπομπή επιτρέπει την αποστολή μηνυμάτων σε ορισμένες ομάδες παραληπτών, εξοικονομώντας εύρος ζώνης και πόρους στο δίκτυο.
- Broadcast (Ευρεία εκπομπή). Στον τύπο αυτό, ένα μήνυμα αποστέλλεται σε όλες τις συσκευές του δικτύου. Το μήνυμα διαβιβάζεται σε όλες τις συσκευές που βρίσκονται στο ίδιο δίκτυο, ανεξαρτήτως του παραλήπτη. Αυτό επιτυγχάνεται με τη χρήση της διεύθυνσης ευρείας εκπομπής (broadcast address) στο πακέτο δεδομένων. Όλες οι συσκευές που λαμβάνουν το μήνυμα αποκρίνονται σε αυτό. Οι διευθύνσεις IP που χρησιμοποιούνται για την ευρεία εκπομπή έχουν τη μορφή 255.255.255.255.

Σε αυτό το σενάριο πρέπει να στείλουμε μια ροή πακέτων σε όλες τις συσκευές μέσω του δικτύου που βρισκόμαστε, σε αυτή την περίπτωση η περιορισμένη εκπομπή limited broadcasting είναι η κατάλληλη.



Εικόνα 26, limited broadcasting.

Αυτή η λειτουργία χρησιμοποιείται κυρίως από τηλεοπτικά δίκτυα για διανομή βίντεο και ήχου.Ένα σημαντικό πρωτόκολλο αυτής της κατηγορίας στα Δίκτυα Υπολογιστών είναι το Πρωτόκολλο Ανάλυσης Διεύθυνσης (ARP) το οποίο χρησιμοποιείται για την επίλυση μιας διεύθυνσης IP σε μια φυσική διεύθυνση που είναι απαραίτητη για την υποκείμενη επικοινωνία.

5.3.3 Multicast

Στο multicasting, ένας προς περισσότερους παραλήπτες συμμετέχουν στην κίνηση μεταφοράς δεδομένων. Σε αυτή τη μέθοδο η κυκλοφορία γίνεται μεταξύ των ορίων του unicast (ένας προς έναν) και του broadcast (ένας προς όλους). Το Multicast επιτρέπει στους διακομιστές να κατευθύνουν μεμονωμένα αντίγραφα ροών δεδομένων που στη συνέχεια προσομοιώνονται και δρομολογούνται σε κεντρικούς υπολογιστές που το ζητούν. Το IP multicast απαιτεί την υποστήριξη ορισμένων άλλων

πρωτοκόλλων όπως το IGMP (Internet Group Management Protocol) και τη δρομολόγηση Multicast για να λειτουργήσει με επιτυχία.

5.4 Ενέργειες διαχείρισης μηνυμάτων

Η αποστολή μηνυμάτων αντιπροσωπεύει μια σημαντική διαδικασία επικοινωνίας σε πολλές εφαρμογές, όπως εφαρμογές κοινωνικής δικτύωσης, εφαρμογές συνομιλίας, ηλεκτρονικό ταχυδρομείο και άλλες. Η αποστολή μηνυμάτων μέσω μιας συγκεκριμένης εφαρμογής μπορεί να παρέχει πολλά πλεονεκτήματα, όπως η δυνατότητα πρόσβασης σε επαφές, η διαχείριση μηνυμάτων και η ασφάλεια των επικοινωνιών. Η ανάπτυξη μιας εφαρμογής αποστολής μηνυμάτων προσφέρει μια ευκαιρία να ενώσουν οι άνθρωποι της κοινωνίας, να επικοινωνούν εύκολα και να δημιουργούν νέες σχέσεις

5.4.1 Αποστολή μηνυμάτων

Μετά την εισαγωγή του, ο χρήστης, είναι σε θέση πλέον να αποστείλει μηνύματα και να λάβει και γενικά να επικοινωνήσει με τους υπόλοιπους ενεργούς χρήστες που αυτός επιθυμεί.

Στο κομμάτι κώδικα του παραρτήματος 3 (*3ο κομμάτι κώδικα - μέθοδος handleMessage, διαχείριση αποστολής μηνύματος*) εικόνα αντιστοιχεί στο κομμάτι του κώδικα το οποίο είναι υπεύθυνο για την σύνταξη και την αποστολή του μηνύματος. Ο χρήστης (στην απλούστερη μορφή της εφαρμογής, έπειτα από την ένταξη του ui interface, γραφικού περιβάλλοντος η διαδικασία γίνεται αυτοματοποιημένα) θα πρέπει να ακολουθήσει την προκαθορισμένη σύνταξη έτσι ώστε η εντολή να αναγνωριστεί από το σύστημα και να δημιουργηθεί το μήνυμα. Όπως φαίνεται στις πρώτες γραμμές της εικόνας, η είσοδος που έχει δοθεί από τον χρήστη κατα της πληκτρολόγηση του μηνύματος, χωρίζεται και πάλι σε 3 μέρη, 3 token. Το πρώτο token αντιστοιχεί σε ένα String, κομμάτι χαρακτήρων προκαθορισμένο για να καταλάβει ο Controller ότι πρόκειται για την συγκεκριμένη λειτουργία αποστολής μηνύματος. Το δεύτερο token, αντιστοιχεί στο κομμάτι το οποίο αναφέρεται το όνομα userName, του παραλήπτη του μηνυματος, το άτομο / ομάδα που θέλουμε να επικοινωνήσουμε. Με αυτή τη διαδικασία συντάσσεται το μήνυμα, η οποία περικλείεται μέσα σε ένα βρόγχο ο οποίος είναι υπεύθυνος για να αναγνωρίζει ανάλογα με την σύνταξη του μηνύματος και συγκεκριμένα με τον έλεγχο του δεύτερου token, εάν το μήνυμα προορίζεται σε κάποιο μεμονωμένο άτομο ή σε μία ομάδα ατόμων. Αυτός έλεγχος γίνεται ώστε το μήνυμα να είναι ορατό μόνο στο επιθυμητό εύρος του αποστολέα και όχι σε όλους τους χρήστες.

Παρόλα αυτά, για να γίνει η αποστολή του μηνύματος σε κάποια ομάδα ο χρήστης θα πρέπει πριν από την παραπάνω διαδικασία να είναι και ο ίδιος του μέλος αυτής. Η παρακάτω εικόνα αποτελεί το κομμάτι του κώδικα υπεύθυνο για την ένταξη ενός χρήστη σε κάποια ομάδα.

```
// A method for joining user to a group
private void handleJoin(String[] tokens) {
    if (tokens.length > 1) {
        String topic = tokens[1];
        topicSet.add(topic);
    }
}
```

Εικόνα 27, μέθοδος handleJoin, διαχείριση ένταξης χρήστη σε ομάδα ατόμων.

Όπως και σε κάθε ενέργεια η εντολή έχει προκαθορισμένο τρόπο σύνταξης ώστε να ξεχωρίζει η κάθε ενέργεια. Έτσι ο χρήστης, ενεργός πλέον, έχοντας στην οθόνη του την λίστα των ενεργών χρηστών αλλά και σε δεύτερη οθόνη μια ακόμη λίστα με το ιστορικό των συνομιλιών του, μπορεί να ξεκινήσει μία νέα συνομιλία ή να συνεχίσει να στέλνει μηνύματα σε κάποια από αυτές στο ιστορικό του.

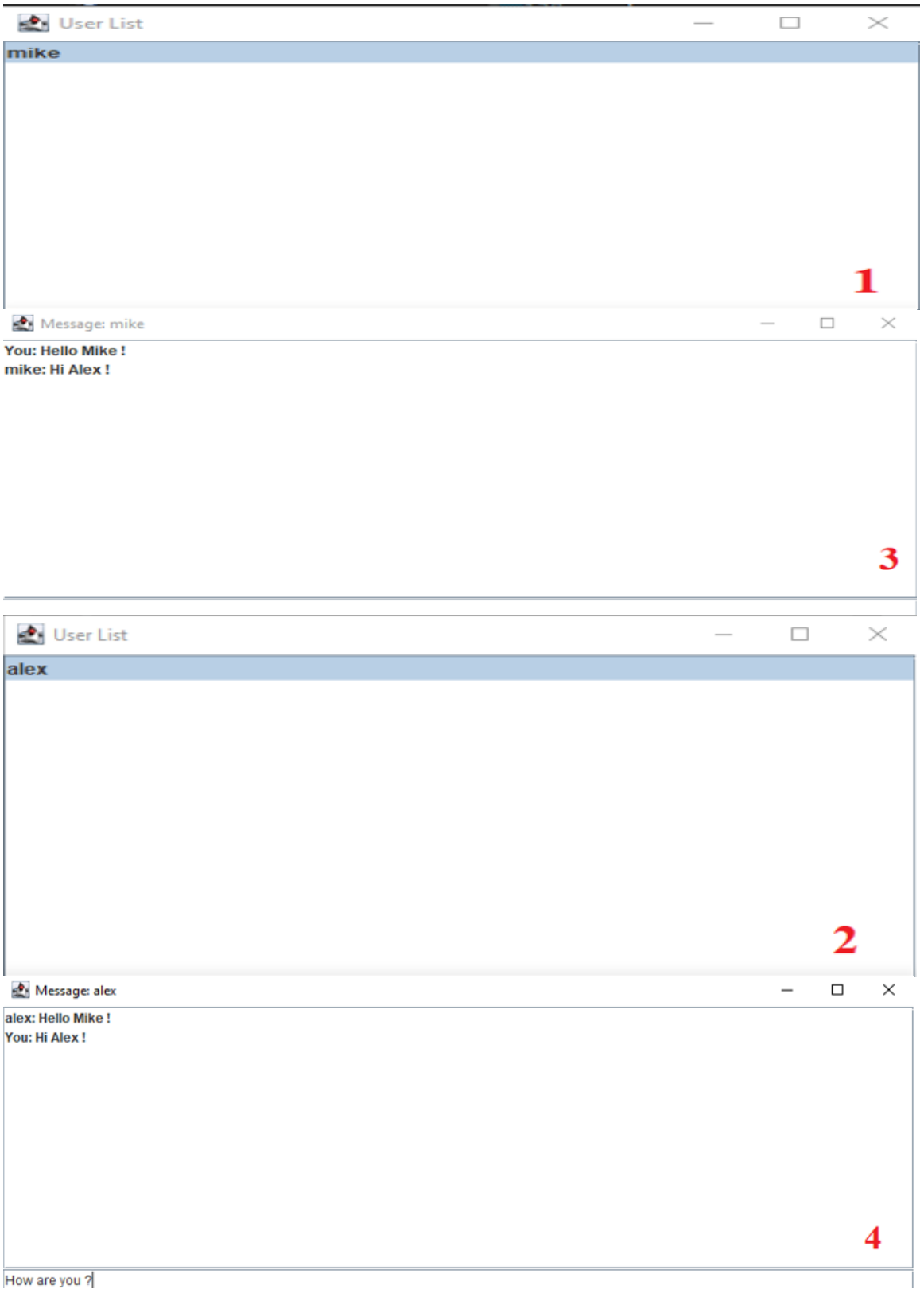
Το broadcast είναι μια μέθοδος αποστολής μηνυμάτων σε όλους τους υπολογιστές σε ένα δίκτυο. Παρόλο που αυτή η μέθοδος μπορεί να φαίνεται χρήσιμη για την αποστολή ενός μηνύματος σε πολλούς παραλήπτες ταυτόχρονα, δεν χρησιμοποιείται στην συγκεκριμένη εφαρμογή λόγω των κινδύνων ασφαλείας και των επιπτώσεων στην απόδοση του δικτύου. Από τη στιγμή που ένα broadcast μήνυμα αποστέλλεται σε όλους τους υπολογιστές στο δίκτυο, μπορεί να προκαλέσει περιττή κυκλοφορία δεδομένων και να επιβαρύνει την επίδοση του δικτύου. Επιπλέον, η χρήση broadcast μπορεί να ανοίξει την πόρτα για επιθέσεις διακινδυνευτικών πακέτων και κακόβουλου λογισμικού. Έτσι, συνήθως προτιμάται η αποστολή μηνυμάτων σε ειδικές διευθύνσεις παραλήπτη, αντί για τη χρήση του broadcast.

Στην μετάδοση δεδομένων ο όρος εκπομπή *unicast* ορίζεται ως η αποστολή δεδομένων από ένα αποστολέα σε ένα και μόνο παραλήπτη δικτύου. Ο όρος *Unicast* είναι παραπλήσιος του όρου *broadcast* που σημαίνει την μεταφορά των ίδιων δεδομένων σε όλους τους δυνατούς σταθμούς - παραλήπτες. Μιά άλλη μέθοδος αποστολής σε συγκεκριμένους παραλήπτες είναι η αποστολή *multicasting*, η οποία στέλνει δεδομένα σε ενδιαφερόμενους μόνο παραλήπτες χρησιμοποιώντας ειδικές τεχνικές απόδοσης διευθύνσεων.

Τα μηνύματα Unicast χρησιμοποιούνται για όλες τις λειτουργίες του δικτύου όπου απαιτείται μοναδική ή αποκλειστική χρήση ενός πόρου. Σε πολλές περιπτώσεις οι εφαρμογές δικτύων που απαιτούν μαζική διανομή δεδομένων έχουν μεγάλο κόστος αν υλοποιηθούν με μεταφορές unicast διότι κάθε σύνδεση απαιτεί την χρήση πόρων του αποστολές και ξεχωριστό εύρος ζώνης για κάθε μεταφορά δεδομένων.

Ο όρος *cast* σημαίνει ότι ορισμένα δεδομένα (ροή πακέτων) μεταδίδονται στον παραλήπτη από την πλευρά του πελάτη μέσω του καναλιού επικοινωνίας που τους βοηθά να επικοινωνούν

Όλη η παραπάνω διαδικασία φυσικά θα ήταν περίπλοκη, δύσκολη και τελικά θα αποθάρρυνε τους χρήστες να επιλέξουν την συγκεκριμένη εφαρμογή αλλά και όποια άλλη εφαρμογή που απευθύνεται σε απλούς χρήστες. Το command line μπορεί να αποτελεί ένα εξαιρετικά χρήσιμο και απαραίτητο εργαλείο στα χέρια των προγραμματιστών αλλά όταν περνάμε στο κομμάτι της χρηστικότητας και της αλληλεπίδρασης των λειτουργιών με τον χρήστη θεωρείται χαμηλού επιπέδου και μη αποδεκτό για τον απλο χρήστη. Έτσι όλη η παραπάνω διαδικασία αλλά και ότι αφορά τον χρήστη προσαρμόστηκε σε γραφικό περιβάλλον, αρκετά απλό για την παρούσα φάση αφήνοντας ιδέες για μελλοντικές αναπτύξεις.



Εικόνα 28, προσομοίωση επικοινωνίας δύο χρηστών.

Στο κομμάτι κώδικα του παραρτήματος 4 (*4ο κομμάτι κώδικα - προσομοίωση επικοινωνίας δύο χρηστών*) φαίνονται δύο χρήστες, εγγεγραμμένοι που έχουν πραγματοποιήσει το 1ο βήμα και έχουν εισέλθει στην εφαρμογή. Ας θεωρήσουμε την παραπάνω εικόνα σαν δύο τελείως διαφορετικά άτομα σε δύο διαφορετικούς υπολογιστές. Αριστερά ο πρώτος χρήστης Alex βλέπει στο πρώτο παράθυρο

(περιοχή 1) την λίστα με τους ενεργούς χρήστες την παρούσα στιγμή που είναι και ο ίδιος ενεργός χρήστης. Παρόμοια και ο δεύτερος χρήστης Mike στα δεξιά βλέπει την δική του αντίστοιχη λίστα (περιοχή 2). Αυτό το παράθυρο στον υπολογιστή του κάθε χρήστη αντιπροσωπεύει τους ενεργούς χρήστες, κάθε είσοδος ή έξοδος ενός χρήστη ανανεώνει την λίστα για όλους αφού για την δημιουργία της το κομμάτι κώδικα διαβάζει διαρκώς την λίστα των worker ώστε να ξέρει πως είναι συμπληρωμένη και να κρατάει ενημερωμένο τον χρήστη με σωστά δεδομένα. Επιλέγοντας έναν χρήστη που θέλουμε να ανταλλάξουμε μηνύματα από την παραπάνω λίστα ανοίγει ένα δεύτερο παράθυρο (περιοχή 2 & περιοχή 4) αντίστοιχα για κάθε χρήστη, όπου έχουμε στο κάτω μέρος την περιοχή σύνταξης του μηνύματος (στην περιοχή 4 φαίνεται το μήνυμα που πληκτρολόγησε ο χρήστης Mike προς τον χρήστη Alex αλλά ακόμα δεν το έχει στείλει) και στο κυρίως μέρος αυτού του παραθύρου εμφανίζονται τα απεσταλμένα μηνύματα των δύο χρηστών με το αντίστοιχο πρόθεμα για την καλύτερη κατανόηση από την πλευρά του χρήστη.

Ένα επιπλέον στοιχείο που αξίζει να επισημανθεί είναι η περιοχή των μηνυμάτων στο παράθυρο console που φαίνεται στο παρασκήνιο. Μηνύματα που όπως έχουμε πει είναι βοηθητικά προς τον προγραμματιστή και μη ορατά στον χρήστη. Προσπερνώντας τα πρώτα που έχουν αναλυθεί, σε αυτή την φάση της αποστολής μηνυμάτων βλέπουμε και μία επιπλέον ενημέρωση στην τελευταία γραμμή “Chat Client calling decrypt method of Encryption class” με απλά λόγια δηλαδή καλείται η μέθοδος του κρυπταλγορίθμου που είναι υπεύθυνη για την αποκρυπτογράφηση των μηνυμάτων. Εδώ παρατηρούμε ένα πρώτο κύριο στοιχείο της παρούσας εργασίας αυτό την αποκρυπτογράφησης. Το μήνυμα έχει φτάσει στον χρήστη αλλά πρίν εμφανιστεί στην οθόνη του παραλήπτη καλείται μία μέθοδος την οποία έχουμε ονομάσει Decrypt της τάξης Encryption η οποία αποκρυπτογραφεί το μήνυμα έτσι ώστε να μετατραπεί σε μορφή κατανοητή από τον χρήστη. Η αντίστοιχη διαδικασία συμβαίνει και στην πλευρά του αποστολέα καλώντας μία άλλη μέθοδο Encrypt η οποία αυτή την φορά κρυπτογραφεί το μήνυμα σε δυσνόητη μορφή αποτρέποντας με αυτες τις 2 μεθόδους την αξιοποίηση των μηνυμάτων σε περίπτωση κακόβουλης ενέργειας.

5.4.2 Αποδοχή μηνυμάτων

Αποδοχή μηνυμάτων είναι μια κρίσιμη διαδικασία για κάθε επικοινωνία, είτε πρόκειται για επαγγελματικό περιβάλλον είτε για προσωπική χρήση. Η αποδοχή ενός μηνύματος συνήθως απαιτεί την κατανόηση του περιεχομένου του, την αξιολόγηση της εγκυρότητάς του και τη λήψη κατάλληλων μέτρων ανάλογα με το περιεχόμενο και τον αποστολέα του μηνύματος. Επομένως, η διαδικασία αποδοχής μηνυμάτων πρέπει να είναι ασφαλής και αξιόπιστη, ενώ παράλληλα να επιτρέπει την ευχρηστία και την αποτελεσματικότητα στην επικοινωνία.

Η αποδοχή κρυπτογραφημένων μηνυμάτων είναι ένας κρίσιμος παράγοντας για την ασφαλή επικοινωνία σε διάφορες εφαρμογές. Μέσω της κρυπτογραφίας, οι αποστολείς μπορούν να προστατεύσουν τα μηνύματά τους από τυχόν παρείσακτους ή κακόβουλους αναγνώστες. Ωστόσο, η επιτυχημένη αποδοχή κρυπτογραφημένων μηνυμάτων απαιτεί τη σωστή εφαρμογή και αποκρυπτογράφηση τους από τον παραλήπτη. Αυτό περιλαμβάνει τη χρήση σωστών κλειδιών κρυπτογραφίας και την αξιόπιστη επαλήθευση της ταυτότητας του αποστολέα. Η αποδοχή κρυπτογραφημένων μηνυμάτων είναι, συνεπώς, κρίσιμη για την εξασφάλιση της απορρήτου και της ακεραιότητας των επικοινωνιών και εφαρμογών που τα χρησιμοποιούν.

Όπως και κάθε άλλη ενέργεια της εφαρμογής έτσι και η αποδοχή μηνυμάτων απαιτεί από τον χρήστη να είναι εγγεγραμμένος, να ανήκει δηλαδή στη ομάδα κάτω από την εφαρμογή. Έτσι ο χρήστης, ενεργός πλέον, έχοντας στην οθόνη του την λίστα των χρηστών αλλά και σε δεύτερη οθόνη μια ακόμη

λίστα με το ιστορικό των συνομιλιών του, όπως αναφέρθηκε και παραπάνω από την πλευρά του αποστολέα μπορεί να επιλέξει μία συνομιλία ή ένα όνομα και σε μία δεύτερη οθόνη αφού ανοίξει η συνομιλία με αυτο το συγκεκριμένο άτομο να συνεχίσει την επικοινωνία του.

Τα μηνύματα που έχουν φτάσει πλέον στο επιλεγμένο άτομο / δέκτη μηνυμάτων, έχουν περάσει από όλες τις απαραίτητες ενέργειες ασφαλείας και ελέγχου ώστε να βλέπει το σωστό μήνυμα ο σωστός χρήστης. Κάθε μήνυμα έχει περάσει από την διαδικασία της κρυπτογράφησης, της αποκρυπτογράφησης αλλά και από τον έλεγχο για την ταυτοποίηση των δύο χρηστών που ανταλλάσουν μηνύματα, αφού τα δύο μεμονωμένα άτομα και μόνο αυτά πρέπει να έχουν πρόσβαση στα μηνύματα του ή η ομάδα στην περίπτωση του group, και να αποκλειστεί η παρέμβαση κάποιου άλλου.

Η παρακάτω εικόνα είναι μία μέθοδος υπεύθυνη για τον έλεγχο του μηνύματος και την αντιστοίχιση του στον αποστολέα, ώστε να εξασφαλιστεί ο παραπάνω έλεγχος.

```
@Override
public void onMessage(String fromLogin, String msgBody) {
    // Filters the message to make sure that the message are from the panel of current login
    if (login.equalsIgnoreCase(fromLogin)) {
        String text;
        try {
            text = RSAUtils.decrypt(msgBody, client.getPrivateKey());
        } catch (InvalidKeyException | IllegalBlockSizeException | BadPaddingException | NoSuchAlgorithmException
                | NoSuchPaddingException e) {
            JOptionPane.showMessageDialog(MessagePane.this, "Can not decrypt message", "Error",
                    JOptionPane.ERROR_MESSAGE);
            e.printStackTrace();
            return;
        }
        String line = fromLogin + ": " + text;
        listModel.addElement(line);
    }
}
```

Εικόνα 29, μέθοδος onMessage, έλεγχος μηνύματος - αποστολέα.

Σε αυτό αυτό το σημείο, την θέση του δέκτη μηνυμάτων, στην οποία ουσιαστικά βρίσκεται κάθε ενεργός χρήστης αφού μπορεί ανα πάσα στιγμή να λάβει μηνύματα, βρίσκεται και η μέθοδος της παρακάτω εικόνας. Ένα ξεχωριστό thread, ομάδα εντολών σε κάποιες περιπτώσεις όπως αυτή σε αναμονή για να εκτελεστούν, έχει ανοίξει το οποίο τρέχει συνέχεια, μέσα σε ένα επαναληπτικό βρόγχο / loop, ένα set εντολών οι οποίες διαβάζουν από τον server μηνύματα, έτσι ώστε ο δέκτης μηνυμάτων, κάθε χρήστης δηλαδή, να έχει ενημερωμένη την οθόνη μηνυμάτων του χωρίς καθυστέρηση επιτυγχάνοντας έτσι την άμεση επικοινωνία.

5.4.3 Συνεχής ανάγνωση δεδομένων

Όταν σχεδιάζουμε μια εφαρμογή επικοινωνίας, είναι σημαντικό να λάβουμε υπόψη την ανάγκη για συνεχή ανάγνωση μηνυμάτων από τους χρήστες. Για να επιτευχθεί αυτό, μπορούμε να χρησιμοποιήσουμε μια πολλαπλασιαστική διεργασία ή ένα νήμα στην εφαρμογή μας, που θα αναλάβει την ανάγνωση μηνυμάτων σε κάθε χρονικό διάστημα. Μπορούμε να χρησιμοποιήσουμε επίσης έναν κατάλληλο αλγόριθμο για τη διαχείριση των μηνυμάτων, ώστε να εξασφαλίσουμε τη

σωστή σειρά εμφάνισής τους στους χρήστες και την αποφυγή απώλειας μηνυμάτων. Επιπλέον, μπορούμε να εμφανίζουμε μια ειδοποίηση στον χρήστη για νέα μηνύματα, ώστε να μη χρειάζεται να ελέγχει συνεχώς την εφαρμογή για να δει αν έχει νέα μηνύματα. Με αυτόν τον τρόπο, μπορούμε να δημιουργήσουμε μια ομαλή και αποτελεσματική εμπειρία επικοινωνίας για τους χρήστες μας.

Η συνεχής ανάγνωση μηνυμάτων σε μια εφαρμογή επικοινωνίας μπορεί να επιτευχθεί μέσα σε ένα επαναληπτικό βρόγχο / loop που θα ελέγχει συνεχώς για την ύπαρξη νέων μηνυμάτων και θα τα εμφανίζει στο χρήστη. Αυτή η διαδικασία μπορεί να είναι χρονοβόρα και επιβαρύνει την επεξεργαστική ισχύ του υπολογιστή.

```
// A method  that reading responses from the server
private void startMessageReader() {
      Thread t = new Thread() {
          @Override
          public void run() {
             readMessageLoop();
           }
          };
            t.start();
   }
       /* This method is an infinity loop that read line by line
           from the server output which is the client input
       */
        private void readMessageLoop(){
           try{
              String line;
              while ((line = bufferedIn.readLine()) != null){
                  String[] tokens = StringUtils.split (line);
                  if (tokens != null && tokens.length > 0) {
                      String cmd = tokens[0];
                      if ("online".equalsIgnoreCase(cmd)){
                          handleOnline(tokens);
                      }
                      else if ("offline".equalsIgnoreCase(cmd)){
                          handleOffline(tokens);
                      }
                      else if ("msg".equalsIgnoreCase(cmd)){
                          String[] tokensMsg = StringUtils.split(line, null, 3);
                          handleMessage(tokensMsg);
                      }
                  }
              }
           }
           catch (Exception ex) {
               ex.printStackTrace();
               try {
                   socket.close();
               }
               catch (IOException e){
                   e.printStackTrace();
               }
           }
       }
```

Εικόνα 30, μέθοδος startMessageReader, συνεχής διαβασμα μηνυμάτων.

5.4.4 Κρυπτογράφηση και αποκρυπτογράφηση μηνυμάτων

Στις παρακάτω εικόνες φαίνεται το κομμάτι κώδικα παραγωγής των δύο κλειδιών, υπεύθυνων για τις διαδικασίες της κρυπτογράφησης και της αποκρυπτογράφησης σύμφωνα με τον κρυπταλγόριθμο RSA-768 που περιγράφηκε παραπάνω και χρησιμοποιήθηκε στην συγκεκριμένη εφαρμογή.

```java
package com.alex.common;

import java.security.InvalidKeyException;

public class RSAUtils {

    public static class PrivatePublicKeys {
        private PrivateKey privateKey;
        private PublicKey publicKey;

        //Constructor
        public PrivatePublicKeys(PrivateKey privateKey, PublicKey publicKey) {
            this.privateKey = privateKey;
            this.publicKey = publicKey;
        }

        public PrivateKey getPrivateKey() {
            return privateKey;
        }

        public PublicKey getPublicKey() {
            return publicKey;
        }

    }
```

Εικόνα 31.1, γεννήτρια κλειδιών, public / private keys.

```java
    //Genarate a pair of keys private & public
    public static PrivatePublicKeys generateKeys() throws NoSuchAlgorithmException {
        KeyPairGenerator keyGen = KeyPairGenerator.getInstance("RSA");
        keyGen.initialize(1024);
        KeyPair pair = keyGen.generateKeyPair();

        return new PrivatePublicKeys(pair.getPrivate(), pair.getPublic());

    }

    public static String publicKeyToBase64(PublicKey publicKey) {

        return Base64.getEncoder().encodeToString(publicKey.getEncoded());
    }

    public static PublicKey constructPublicKeyFromBase64(String publicKeyBase64)
            throws InvalidKeySpecException, NoSuchAlgorithmException {
        X509EncodedKeySpec keySpec = new X509EncodedKeySpec(Base64.getDecoder().decode(publicKeyBase64.getBytes()));
        KeyFactory keyFactory = KeyFactory.getInstance("RSA");
        return keyFactory.generatePublic(keySpec);
    }
```

Εικόνα 31.2, γεννήτρια κλειδιών, public / private keys.

```
63    public static String encrypt(String data, PublicKey publicKey)
64            throws BadPaddingException, IllegalBlockSizeException, InvalidKeyException, NoSuchPaddingException,
65            NoSuchAlgorithmException, InvalidKeySpecException {
66        Cipher cipher = Cipher.getInstance("RSA/ECB/PKCS1Padding");
67        cipher.init(Cipher.ENCRYPT_MODE, publicKey);
68        byte[] encryptedBytes = cipher.doFinal(data.getBytes());
69        return Base64.getEncoder().encodeToString(encryptedBytes);
70    }
71
72    public static String decrypt(String encryptedBase64, PrivateKey privateKey) throws InvalidKeyException,
73            IllegalBlockSizeException, BadPaddingException, NoSuchAlgorithmException, NoSuchPaddingException {
74
75        Cipher cipher = Cipher.getInstance("RSA/ECB/PKCS1Padding");
76        cipher.init(Cipher.DECRYPT_MODE, privateKey);
77        return new String(cipher.doFinal(Base64.getDecoder().decode(encryptedBase64)));
78    }
```

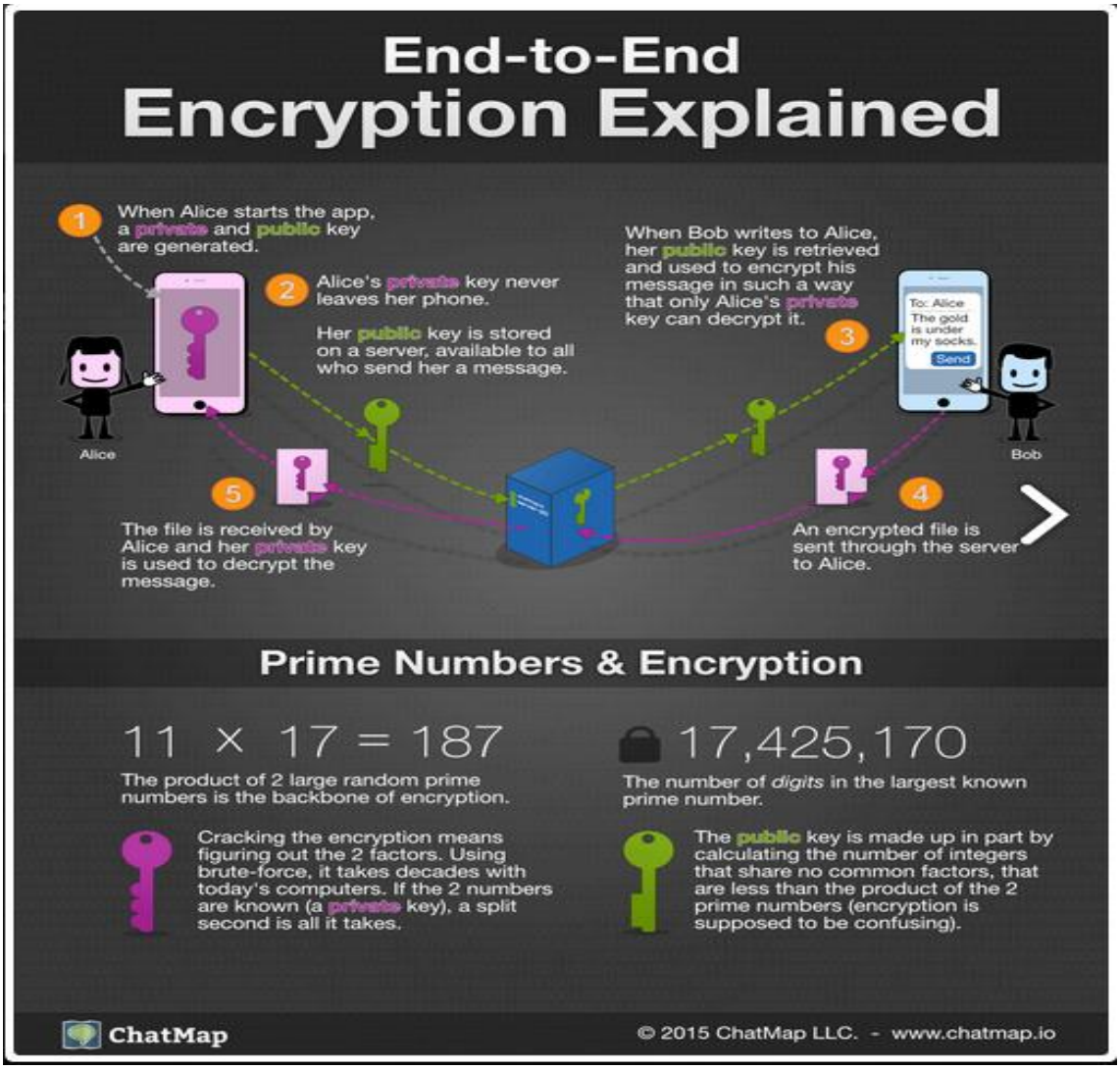
Εικόνα 31.3, γεννήτρια κλειδιών, public / private keys.

Παρακάτω παρουσιάζεται ένα απλό παράδειγμα ώστε να γίνει κατανοητή η παραπάνω διαδικασίας και ο τρόπος λειτουργίας της αναπαριστώντας ένα σενάριο της πραούσας εφαρμογής.

Έστω η Alice και ο Bob, θέλουν να επικοινωνήσουν με ασφάλεια χρησιμοποιώντας το δημόσιο ταχυδρομείο. Η Alice θέλει να στείλει ένα κρυφό μήνυμα στον Bob και περιμένει μια κρυφή απάντηση από αυτόν. Σύμφωνα με την κρυπτογράφηση συμμετρικού κλειδιού η Alice θα βάλει το μήνυμά της μέσα σε ένα κουτί με λουκέτο για το οποίο έχει το κλειδί. Στέλνει το κλειδωμένο κουτί με το δημόσιο ταχυδρομείο στον Bob. Ο Bob έχει ένα ίδιο κλειδί (το οποίο έχει πάρει από την Alice στο παρελθόν, σε προσωπική συνάντηση που είχαν) και μόλις λαμβάνει το κουτί, ανοίγει το λουκέτο και διαβάζει το μήνυμα. Ο Bob βάζει το μήνυμά του στο κουτί, το κλειδώνει και το στέλνει με δημόσιο ταχυδρομείο στην Alice. Το πρόβλημα εδώ είναι ότι το κλειδί για το λουκέτο είναι κοινό και για την Alice και για τον Bob και για να δώσει αντίγραφο του κλειδιού ο ένας με τον άλλον θα πρέπει να συναντηθούν γιατί δεν είναι ασφαλές να το στείλουν με το δημόσιο ταχυδρομείο (ίσως τότε κάποιος θα μπορούσε να υποκλέψει το κλειδί και να δημιουργήσει ένα αντίγραφο ώστε στο μέλλον να υποκλέπτει ή να παραποιεί τα μηνύματα που ανταλλάσσονται). Στην πράξη της ασυμμετρικής κρυπτογραφίας, ο Bob και η Alice έχουν ξεχωριστές κλειδαριές. Πρώτα η Alice βάζει το μυστικό μήνυμα στο κουτί, το κλειδώνει με το λουκέτο που έχει μόνο αυτή κλειδί. Το στέλνει το κουτί στον Bob με απλό δημόσιο ταχυδρομείο. Όταν ο Bob λαμβάνει το κουτί, προσθέτει το δικό του λουκέτο στο κουτί και στο στέλνει πίσω στην Alice. Η Alice λαμβάνει το κουτί με δύο λουκέτα, αφαιρεί το δικό της λουκέτο και το στέλνει πίσω στον Bob. Όταν ο Bob λαμβάνει το κουτί έχει πάνω μόνο το δικό του λουκέτο, το οποίο μπορεί να ξεκλειδώσει και να δει το μήνυμα της Alice. Σε αυτό το παράδειγμα η διαδικασία της αποκρυπτογράφησης είναι ίδια με τη διαδικασία της κρυπτογράφησης.

Η κρίσιμη διαφορά στο κλειδί ασυμμετρικής κρυπτογράφησης είναι ότι η Alice και ο Bob ποτέ δεν χρειάζεται να στείλουν αντίγραφο του κλειδιού ο ένας στον άλλον. Σε αυτήν την περίπτωση αποφεύγουμε την περίπτωση της κλοπής του κλειδιού κατά τη μεταφορά. Σε αυτή την περίπτωση η

Alice και ο Bob δεν χρειάζεται να εμπιστευτούν το δημόσιο ταχυδρομείο. Επιπρόσθετα ο Bob επιτρέπει σε όποιον επιθυμεί να αντιγράψει το κλειδί του και τα μηνύματα της Alice προς τον Bob θα είναι εκτεθειμένα σε κίνδυνο υποκλοπής. Όμως όλα τα μηνύματα της Alice προς άλλους θα είναι μυστικά, αφού οι υπόλοιποι θα παρέχουν διαφορετικά λουκέτα για να κλειδώσει η Alice το μήνυμα στο κουτί πριν το στείλει σε αυτούς.



Εικόνα 32, παράδειγμα Alice - Bob, public / private keys.

Η κρυπτογραφία και αποκρυπτογραφία μηνυμάτων είναι μια σημαντική τεχνολογία που χρησιμοποιείται σε πολλούς τομείς της κοινωνίας μας, όπως στις επικοινωνίες, την τραπεζική, την υγεία, την επιχειρηματικότητα και πολλούς άλλους. Η κρυπτογραφία επιτρέπει την ασφαλή αποστολή και λήψη μηνυμάτων από δύο ή περισσότερα μέρη που θέλουν να διατηρήσουν την επικοινωνία τους μακριά από προβλήματα ασφαλείας.

Η κρυπτογραφία μπορεί να είναι συμμετρική ή δημόσιο-ιδιωτικό κλειδί. Η συμμετρική κρυπτογραφία χρησιμοποιεί το ίδιο κλειδί για την κρυπτογράφηση και αποκρυπτογράφηση του μηνύματος, ενώ η δημόσιο-ιδιωτικό κλειδί χρησιμοποιεί διαφορετικά κλειδιά για την κρυπτογράφηση και αποκρυπτογράφηση του μηνύματος.

Στην αυθεντικοποίηση, το μήνυμα επαληθεύεται ότι είναι πράγματι από τον αποστολέα που υποτίθεται ότι είναι. Στην εμπιστευτικότητα, το μήνυμα προστατεύεται από τρίτους.

Με βάση τα παραπάνω, μπορούμε να συμπεράνουμε ότι η κρυπτογραφία και αποκρυπτογραφία μηνυμάτων είναι σημαντικές διαδικασίες για τη διατήρηση της ασφάλειας και της ιδιωτικότητας στις επικοινωνίες. Αποτελούν βασικά εργαλεία για την προστασία των δεδομένων από ανεπιθύμητη παρακολούθηση ή διαρροή.

Ωστόσο, η κρυπτογραφία δεν είναι απόλυτα ασφαλής και υπάρχουν διάφοροι τρόποι για να παραβιαστεί ένα κρυπτογραφημένο μήνυμα. Οι κρυπτογράφοι πρέπει να συνεχώς αναβαθμίζουν τις μεθόδους κρυπτογράφησης και να διατηρούνται ενημερωμένοι για τις τελευταίες εξελίξεις στον τομέα της κρυπτογραφίας.

Συνολικά, η κρυπτογραφία και αποκρυπτογραφία μηνυμάτων αποτελούν βασικά εργαλεία για τη διασφάλιση της ιδιωτικότητας και της ασφάλειας στις επικοινωνίες, αλλά απαιτούν προσοχή και συνεχή ενημέρωση για να παραμείνουν αποτελεσματικά.

5.5 Αποχώρηση από μία ομάδα χρηστών

Η δυνατότητα εξόδου από μια ομάδα χρηστών σε μια εφαρμογή επικοινωνίας είναι ένα σημαντικό χαρακτηριστικό που επιτρέπει στους χρήστες να διαχειρίζονται τις συμμετοχές τους σε διάφορες ομάδες. Αυτό επιτρέπει στους χρήστες να ελέγχουν την προσωπική τους συμμετοχή σε συγκεκριμένες συζητήσεις ή ομάδες και να αποφασίζουν πότε θα αποχωρήσουν από αυτές. Αυτή η δυνατότητα εξόδου δίνει στους χρήστες την ελευθερία και τον έλεγχο των επικοινωνιακών τους επιλογών και επιτρέπει στην εφαρμογή να λειτουργεί με πιο αποτελεσματικό τρόπο.

Η επικοινωνία με την συγκεκριμένη εφαρμογή μπορεί να γίνει σε δύο διαφορετικά επίπεδα, μεμονωμένα άτομο προς άτομο, ή και ανάμεσα σε μία ομάδα / group ατόμων. Κάθε χρήστης έχει την δυνατότητα να ενταχθεί σε μία ή / και περισσότερες ομάδες επικοινωνίας ανάλογα με την οργάνωση που έχει γίνει στους χρήστες της εφαρμογής. Ως συνέχεια αυτής την δυνατότητας όπως είναι λογικό, ο χρήστης θα πρέπει και μπορεί να αποχωρήσει από την / τις ομάδες όπου είναι μέλος για δικούς του λόγους.

Στην παρακάτω εικόνα απεικονίζεται αυτή η δυνατότητα με το αντίστοιχο κομμάτι κώδικα που εκτελεί την ενέργεια αυτή. Έτσι με την σύνταξη της κατάλληλης εντολής για την έξοδο από κάποιο group, καλείται η συγκεκριμένη μέθοδος όπου αφού ελεγχθεί η εντολή που έδωσε χρήστης, αφαιρεί από το topicSet, την λίστα των χρηστών της ομάδας τον συγκεκριμένο χρήστη. Έτσι ο χρήστης πλέον δεν μπορεί να επικοινωνεί με την συγκεκριμένη ομάδα, ούτε στέλνει ούτε λαμβάνει μηνύματα. Παρόλα αυτά μεμονωμένα με τα άτομα αυτής εξακολουθεί να έχει αυτή την δυνατότητα επικοινωνίας, αφού έχει αποχωρήσει από την συγκεκριμένη ομάδα αποκλειστικά και όχι από την εφαρμογή, εξακολουθώντας να έχει την δυνατίτητα επικοινωνίας.

```
// A method for leaving user from a group
private void handleLeave(String[] tokens) {
    if (tokens.length > 1) {
        String topic = tokens[1];
        topicSet.remove(topic);
    }
}
```

Εικόνα 33, γενική αναφορά για την δημιουργία των κλειδιών.

Η έξοδος από μια ομάδα χρηστών σε μια εφαρμογή επικοινωνίας είναι εξίσου σημαντική με την είσοδο σε αυτήν. Όταν αποφασίζετε να αποχωρήσετε από μια ομάδα, πρέπει να σκεφτείτε την επίπτωση στην επικοινωνία και τη συνεργασία μεταξύ των μελών της ομάδας. Είναι σημαντικό να ενημερώσετε τα μέλη της ομάδας για την απόφασή σας και να εξηγήσετε τους λόγους για τους οποίους αποχωρείτε.

Παράλληλα, πρέπει να είστε βέβαιοι ότι έχετε ολοκληρώσει οποιαδήποτε εργασία ή συζήτηση στην οποία συμμετέχατε με την ομάδα πριν αποχωρήσετε. Αν έχετε ανοιχτά θέματα ή διαφωνίες, πρέπει να τις επιλύσετε πριν αποχωρήσετε από την ομάδα.

5.6 Αποσύνδεσε από την εφαρμογή

Εξοδος από μια εφαρμογή επικοινωνίας: Ο σωστός τρόπος κλεισίματος και έξοδος από μια εφαρμογή επικοινωνίας είναι εξίσου σημαντικός με τον τρόπο εισόδου σε αυτήν. Καθώς η ασφάλεια είναι κρίσιμη στην επικοινωνία, η εξοδος από μια εφαρμογή επικοινωνίας πρέπει να γίνεται με προσοχή και να περιλαμβάνει το κλείσιμο όλων των συνδέσεων, το καθαρισμό των πόρων και τη διαγραφή τυχόν ευαίσθητων πληροφοριών από τη μνήμη. Επιπλέον, πρέπει να διασφαλίζεται ότι όλα τα κρυπτογραφημένα δεδομένα έχουν αποκρυπτογραφηθεί και διαγραφεί πριν από την έξοδο από την εφαρμογή.

Μία ακόμα λειτουργία είναι αυτή της αποσύνδεσης από την εφαρμογή. Η αντίθετη αυτής της εισόδου, LogIn, που αποτελεί την βασικότερη για ένα χρήστη ώστε να μπορέσει να χρησιμοποιήσει τις υπηρεσίες της εφαρμογής.

Στην παρακάτω εικόνα απεικονίζεται αυτή η δυνατότητα με το αντίστοιχο κομμάτι κώδικα που εκτελεί την αποσύνδεση του χρήστη και κατ' επέκταση τον αποκλεισμό του από την εφαρμογή έως ότου συνδεθεί και πάλι όπως αναφέρθηκε στο πρώτο κεφάλαιο.

```
private void handleLogoff() throws IOException {
    // Remove a user from the list once he logs off
    server.removeWorker(this);
    List<ServerWorker> workerList = server.getWorkerList();

    // send other online users current user's status
    String onlineMsg = "offline " + login;
    for (ServerWorker worker : workerList) {
        // Prevent the login message to myself
        if (!login.equals(worker.getLogin())) {
            worker.send(onlineMsg);
        }
    }
    clientSocket.close();
}
```

Εικόνα 34, γενική αναφορά για την δημιουργία των κλειδιών.

5.7 Επίλογος

Όταν τελειώνει η χρήση μιας εφαρμογής επικοινωνίας, είναι σημαντικό να κλείσετε τη σύνδεσή σας και να βγείτε από την εφαρμογή. Αυτό βοηθά στη διατήρηση της ασφάλειας και της ιδιωτικότητάς σας, καθώς αποτρέπει την πρόσβαση στα δεδομένα σας από άλλους. Επίσης, επιτρέπει στην εφαρμογή να απελευθερώσει τους πόρους που χρησιμοποιεί, όπως το δίκτυο και τη μνήμη, για άλλες εφαρμογές και χρήστες. Συνεπώς, είναι σημαντικό να έχετε προσοχή κατά την έξοδό σας από μια εφαρμογή επικοινωνίας και να ακολουθείτε τις οδηγίες της εφαρμογής σχετικά με το πώς να αποσυνδεθείτε και να βγείτε από αυτήν.

Κεφάλαιο 6ο: Συμπεράσματα και προτάσεις βελτίωσης

6.1 Εισαγωγή

Η οπτική κατανόηση των δεδομένων είναι ένα σημαντικό εργαλείο στην ανάλυση και επεξεργασία δεδομένων. Με την ανάπτυξη της τεχνολογίας και της πολυπλοκότητας των δεδομένων, η οπτικοποίηση έχει γίνει ακόμα πιο σημαντική. Συμπεράσματα και βελτιώσεις οπτικής ανάλυσης μπορούν να βοηθήσουν στην αύξηση της αποτελεσματικότητας και της ακρίβειας της ανάλυσης δεδομένων.

Μέσω της οπτικής ανάλυσης, μπορούν να ανακαλυφθούν τάσεις, πρότυπα και ανωμαλίες στα δεδομένα. Μπορεί επίσης να βοηθήσει στην κατανόηση των δεδομένων και της σχέσης μεταξύ τους. Επιπλέον, η οπτική ανάλυση μπορεί να βοηθήσει στην ανάπτυξη προγραμμάτων μηχανικής μάθησης και τη βελτίωση της πρόβλεψης των αποτελεσμάτων.

Παράλληλα, η βελτίωση της οπτικής ανάλυσης μπορεί να γίνει μέσω της ανάπτυξης πιο αποτελεσματικών και φιλικών προς τον χρήστη εργαλείων αναλυτικής αναφοράς.

6.2 Μελλοντικές προτάσεις βελτίωσης

Στην παρούσα πτυχιακή εργασία περιγράφηκε μια εφαρμογή η οποία προσφέρει την δυνατότητα της επικοινωνίας στους χρήστες της με το επιπλέον χαρακτηριστικό της ασφάλειας των δεδομένων των χρηστών και των μηνυμάτων αυτών. Αυτό το χαρακτηριστικό που ξεχωρίζει την παρούσα εφαρμογή επιτυγχάνεται με την βοήθεια ενός κρυπταλγόριθμου ο οποίος κρυπτογραφεί και αποκρυπτογραφεί ευαίσθητα προσωπικά δεδομένα τα οποία αποτελούν πανίσχυρο εργαλείο στις μέρες μας. Αυτός ο κρυπταλγόριθμος είναι ο RSA. Πολλές παρόμοιες εφαρμογές υπάρχουν στην αγορά και η διαφορά της παρούσης από αυτές είναι και ταυτόχρονα το σημαντικότερο χαρακτηριστικο της, ο κρυπταλγόριθμος της.

Η απλότητα στις εφαρμογές μπορεί να αποτελέσει θετικό στοιχείο στο αποτέλεσμα, αφού όσο λιγότερες είναι οι λειτουργίες τόσο πιο εύστοχα και καλοστημένα υλοποιούνται από τον προγραμματιστή, εφόσον οι αλληλεπιδράσεις μεταξύ των λειτουργιών αυτών, είναι λιγότερες και άρα τα προβλήματα που δημιουργούνται, η θα δημιουργηθούν για την χρήση της εφαρμογής, είναι λιγότερα. Παρόλα αυτά δεν θα πρέπει να υπεραπλουστευουσουμε μία εφαρμογή, γιατί για παράδειγμα μπορεί να στερήσουμε από τον χρήστη υπηρεσίες που θα του κάνουν την χρήση της ευκολότερη, γρηγορότερη αλλά και αποτελεσματικότερη. Έτσι και η παρούσα εργασία πραγματεύεται μία εφαρμογή σε αρκετά απλή μορφή με ελάχιστες λειτουργίες, οι οποίες παρόλο την επίτευξη του κύριου στόχου την εφαρμογής μπορούν να βελτιωθούν αλλά και να στελεχωθούν από επιπλέον κώδικα που θα δώσει κι άλλες δυνατότητες στον χρηστη. Αρκετές ιδέες δημιουργήθηκαν από αρχικό στάδιο, από τον σχεδιασμό της εφαρμογής αλλά οι περισσότερες δημιουργήθηκαν κατά την υλοποίηση της. Η μετάφραση των ιδεών σε κώδικα δημιουργούσε και εξακολουθεί να δημιουργεί, ιδέες βελτίωσης αλλά και προτάσεις για το μέλλον της.

1. Προσθήκη της δυνατότητας αποστολής διαφορετικών τύπων μηνυμάτων όπως ψηφιακών αρχείων(εικόνων, ήχων κλπ) Μία μελλοντική ανάπτυξη είναι η παραπάνω, καθώς οι χρήστες έχουν την ανάγκη εκτός των γραπτών παραδοσιακών μηνυμάτων να αποστέλλουν και άλλα που διευκολύνουν την δουλειά αλλά και την καθημερινότητα τους.
2. Ευκαιρίας να επεξεργαστούν ή ακόμα και να διαγράψουν τα μηνύματα που έχουν αποστείλει, και γιατί όχι και την δυνατότητα να διαγράψουν ολόκληρη την συνομιλία.

3. Επιπλέον ευχαρίστηση κατά την χρήσης της εφαρμογής θα δώσουν αντιδράσεις μηνυμάτων, λειτουργια που παρέχουν οι περισσότερες παρόμοιες εφαρμογές και έχουν αποδείξει ότι προτιμούνται από τους χρήστες καθώς βελτιώνουν εμφανισιακά τις οθόνες τους.
4. Δυνατότητα λειτουργία της εφαρμογής στο διαδίκτυο για απομακρυσμένη επικοινωνία. Η αρχική ιδέα της εφαρμογής ήταν το εύρος δράσης της να είναι περιορισμένο σε κάποιο τοπικό δίκτυο, για παράδειγμα μια εταιρεία στο χώρο εργασίας της για την επικοινωνία των εργαζομένων της. Αυτός ο τρόπος μειώνει τους κινδύνους κακόβουλων επιθέσεων αλλά μειώνει και τις δυνατότητες της εφαρμογής αφού με την ανάπτυξη το remote εργασιών στις μέρες μας θα ήταν αδύνατο κάποιος από διαφορετικό μέρος να επικοινωνήσει με τους συναδέλφους του.

6.3 Πλεονεκτήματα εφαρμογής

Όλα αυτά τα στοιχεία οδήγησαν στην δημιουργία αυτής της εφαρμογής με αρκετά πλεονεκτήματα, μερικά από αυτά είναι :

1. Μεγαλύτερη ασφάλεια μέσω του αλγορίθμου RSA, ο οποίος θεωρείται μέχρι σήμερα ο καταλληλότερος, λόγω πολυπλοκότητας των κλειδιών του, αφού η παράκαμψη του είναι αρκετά δύσκολη, σχεδόν αδύνατη.
2. Απλότητα στην χρήστη της. Η δημιουργία ενος λογαριασμού, email & password, είναι αρκετό για την χρήση της, εφόσον προσφέρει καθαρή και ασφαλή δυνατότητα επικοινωνίας και όχι άλλες λιγότερο σημαντικές λειτουργίες απομακρύνοντας την από τον κύριο σκοπό της.
3. Δυνατότητα μεμονωμένης επικοινωνίας, άτομο προς άτομο, αλλά και ομαδικής επικοινωνίας εκπέμποντας μηνύματα σε πολλά άτομα ταυτόχρονα αλλά και δέχοντας από αυτά, αντίστοιχα.

6.4 Επίλογος

Η πτυχιακή εργασία ανταλλαγής κρυπτογραφημένων μηνυμάτων αναδεικνύει τη σημασία της κρυπτογραφίας στη σύγχρονη εποχή της ψηφιακής επικοινωνίας. Μέσω της εφαρμογής αλγορίθμων κρυπτογράφησης και αποκρυπτογράφησης, οι χρήστες μπορούν να επικοινωνήσουν με ασφάλεια, προστατεύοντας την εμπιστευτικότητα και την ακεραιότητα των μηνυμάτων τους.

Η εφαρμογή της κρυπτογραφίας στην ανταλλαγή μηνυμάτων πρέπει να γίνεται με προσοχή και επαρκή γνώση των αλγορίθμων, καθώς μια αδύναμη κρυπτογράφηση μπορεί να επιτρέψει σε εξωτερικούς επιτιθέμενους να αποκτήσουν πρόσβαση στα μηνύματα. Επιπλέον, η ανταλλαγή κρυπτογραφημένων μηνυμάτων πρέπει να συνοδεύεται από τη χρήση αυθεντικοποίησης, προκειμένου να εξασφαλίζεται η ταυτότητα των αποστολέων και η προστασία από επιθέσεις ψευδο-αποστολής.

Ωστόσο, η κρυπτογραφία δεν αποτελεί από μόνη της λύση σε όλα τα προβλήματα ασφαλεία.

Στο μέλλον, μπορούν να γίνουν πολλές βελτιώσεις στην ανταλλαγή κρυπτογραφημένων μηνυμάτων, εξαρτώμενες από τις ανάγκες και τις απαιτήσεις των χρηστών. Μία βελτίωση θα μπορούσε να είναι η αύξηση της ασφάλειας των κρυπτογραφημένων μηνυμάτων μέσω της χρήσης δυνατότερων κρυπτογραφικών αλγορίθμων ή μέσω της χρήσης διαφορετικών μεθόδων κρυπτογράφησης, όπως η κρυπτογράφηση με βάση το έλεγχο πρόσβασης ή η κρυπτογράφηση με χρήση της τεχνολογίας blockchain.

Επιπλέον, μπορούν να προστεθούν περισσότερες δυνατότητες στην επικοινωνία μεταξύ των χρηστών, όπως η δυνατότητα αποστολής κρυπτογραφημένων αρχείων και η δυνατότητα ανταλλαγής κρυπτογραφημένων φωτογραφιών και βίντεο.

Επιπλέον, η βελτίωση της οπτικής εμπειρίας του χρήστη μπορεί να είναι ένας σημαντικός παράγοντας για την επιτυχία μιας εφαρμογής ανταλλαγής κρυπτογραφημένων μηνυμάτων.

ΒΙΒΛΙΟΓΡΑΦΙΑ

- Smith, J. (2018). "Introduction to Cryptography: Principles and Applications." Εκδόσεις ABC.
- Diffie, W., & Hellman, M. (1976). "New directions in cryptography." IEEE Transactions on Information Theory, 22(6), 644-654.
- Stallings, W. (2017). "Cryptography and Network Security: Principles and Practice." Pearson Education.
- Menezes, A. J., van Oorschot, P. C., & Vanstone, S. A. (1996). "Handbook of Applied Cryptography." CRC Press.
- Schneier, B. (1996). "Applied Cryptography: Protocols, Algorithms, and Source Code in C." John Wiley & Sons.
- Katz, J., & Lindell, Y. (2014). "Introduction to Modern Cryptography." Chapman and Hall/CRC.
- Paar, C., & Pelzl, J. (2010). "Understanding Cryptography: A Textbook for Students and Practitioners." Springer.
- Ferguson, N., Schneier, B., & Kohno, T. (2010). "Cryptography Engineering: Design Principles and Practical Applications." Wiley.
- Boneh, D., & Shoup, V. (2017). "A Graduate Course in Applied Cryptography." Free Online Version.
- Katz, J., & Lindell, Y. (2015). "Introduction to Modern Cryptography." Chapman and Hall/CRC.
- Housley, R., Polk, W., Ford, W., & Solo, D. (2020). "Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile." RFC 5280

ΠΑΡΑΡΤΗΜΑ

1ο κομμάτι κώδικα

```
@Override
    public void run() {
      try {
       keys = RSAUtils.generateKeys();
      } catch (NoSuchAlgorithmException e1) {
         e1.printStackTrace();
         System.exit(1);
         }
         try (ServerSocket serverSocket = new ServerSocket(serverPort)) {
           //Needs to be in a loop because continuously accepts the connections of clients
           while (true) {
            try {
            System.out.println("About to accept client connection...");
//accept method creates the connection between server and the client this socket represents the  connection to the client
             Socket clientSocket = serverSocket.accept();
               System.out.println("Accepted connection from " + clientSocket);
           // Create an instance (object) of worker
           ServerWorker worker = new ServerWorker(this, clientSocket);
            workerList.add(worker);
             worker.start();
//Create new different Threads for every connection in order to run multiple connections concurrently,
//and keep the main Thread free to accept other connections
             } catch (Exception e) {
       System.err.println("Error accepting connnection");
             e.printStackTrace();
     }
   }
         } catch (IOException e) {
         System.err.println("Can not start server");
        e.printStackTrace();
       }
```

2ο κομμάτι κώδικα

```
private void handleLogin(String[] tokens) throws IOException, InvalidKeyException, IllegalBlockSizeException,
 BadPaddingException, NoSuchAlgorithmException, NoSuchPaddingException {
        if (tokens.length == 3) {
         String login = tokens[1];
          String encryptedPassword = tokens[2];
 String password = RSAUtils.decrypt(encryptedPassword, server.getPrivateKey());
            //Three example of users who can login
 if ((login.equals("alex") && password.equals("alex")) || (login.equals("jim") && password.equals("jim")) || (login.equals("mike") && password.equals("mike"))) {
            String msg = "ok login";
         writer.println(msg);
           this.login = login;
        System.out.println("User logged in successfully: " + login);
            publicKeyBase64 = reader.readLine();
           writer.println("ok");
     List<ServerWorker> workerList = server.getWorkerList();
                    // send current user all other online logins
       for (ServerWorker worker : workerList) {
        if (worker.getLogin() != null) {
         if (!login.equals(worker.getLogin())) {
           String msg2 = "online " + worker.getLogin() + " " + worker.publicKeyBase64;
           send(msg2);
         }
     }
 }
          // send other online users current user's status
     String onlineMsg = "online " + login + " " + publicKeyBase64;
        for (ServerWorker worker : workerList) {
           if (!login.equals(worker.getLogin())) {
              worker.send(onlineMsg);
            }
         }
```

```
            } else {
           String msg = "error login";
            writer.println(msg);
           System.err.println("Login failed for " + login);
       }
     }
   }
```

3ο κομμάτι κώδικα

```
 private void handleMessage(String[] tokens) throws IOException {
         String sendTo = tokens[1];
         String body = tokens[2];
          boolean isTopic = sendTo.charAt(0) == '#';
    List<ServerWorker> workerList = server.getWorkerList();
         for (ServerWorker worker : workerList) {
           if (isTopic) {
             if (worker.isMemberOfTopic(sendTo)) {
               String outMsg = "msg " + sendTo + ":" + login + " " + body;
             worker.send(outMsg);
         }
           } else {
        if (sendTo.equalsIgnoreCase(worker.getLogin())) {
      String outMsg = "msg " + login + " " + body;
       worker.send(outMsg);
        }
      }
    }
}
```

4ο κομμάτι κώδικα

```
private void handleMessage(String[] tokens) throws IOException {
   String sendTo = tokens[1];
   String body = tokens[2];
   boolean isTopic = sendTo.charAt(0) == '#';
   List<ServerWorker> worker List = server.getWorkerList();
     for (ServerWorker worker : workerList) {
       if (isTopic) {
           if (worker.isMemberOfTopic(sendTo)) {
             String outMsg = "msg " + sendTo + ":" + login + " " + body;
              worker.send(outMsg);
              }
       } else {
      if (sendTo.equalsIgnoreCase(worker.getLogin())) {
          String outMsg = "msg " + login + " " + body;
           worker.send(outMsg);
       }
     }
  }
}
```