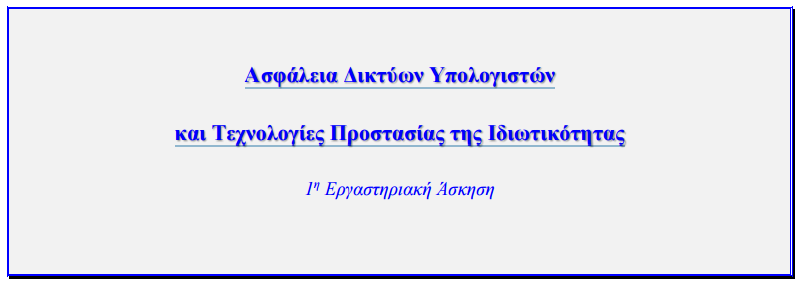
ΠΑΝΕΠΙΣΤΗΜΙΟ ΑΙΓΑΙΟΥ

ΣΧΟΛΗ ΘΕΤΙΚΩΝ ΕΠΙΣΤΗΜΩΝ

ΤΜΗΜΑ ΜΗΧΑΝΙΚΩΝ ΠΛΗΡΟΦΟΡΙΑΚΩΝ ΚΑΙ ΕΠΙΚΟΙΝΩΝΙΑΚΩΝ ΣΥΣΤΗΜΑΤΩΝ

Διδάσκων: Επίκουρος Καθηγητής Γεώργιος Καμπουράκης

Εργαστηριακοί Συνεργάτες: Δημήτρης Παπαμαρτζιβάνος (ΥΔ), Αλέξανδρος Φακής (ΥΔ)

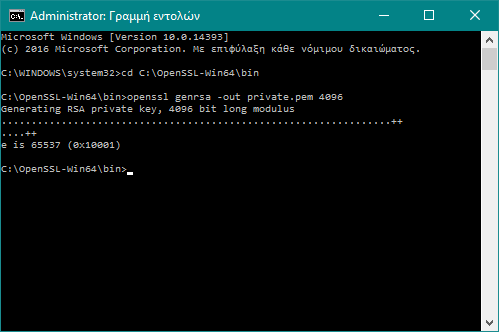


# Δημιουργία Πιστοποιητικών

Όλες οι εντολές για τη δημιουργία του πιστοποιητικού γίνοτ

Αρχικά παράγουμε το private key του server με την παρακάτω εντολή:

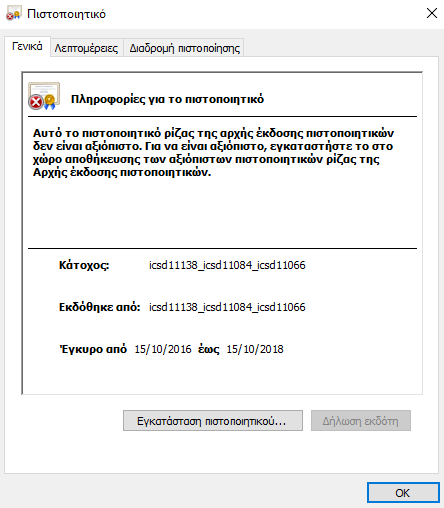
openssl genrsa –out private.pem 4096

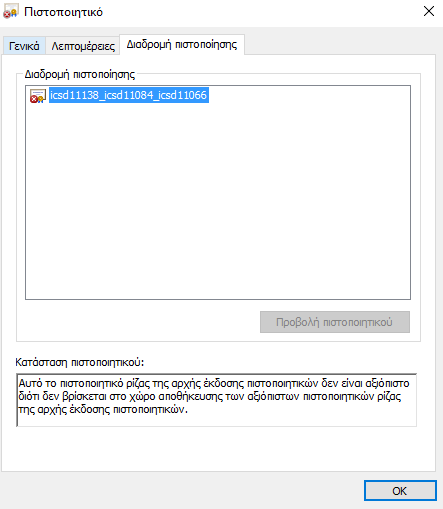


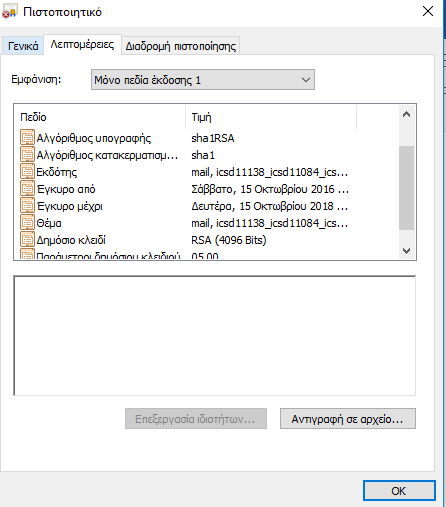
Παράγει ένα 4096-bit RSA κλειδί για τον server και το αποθηκεύει.

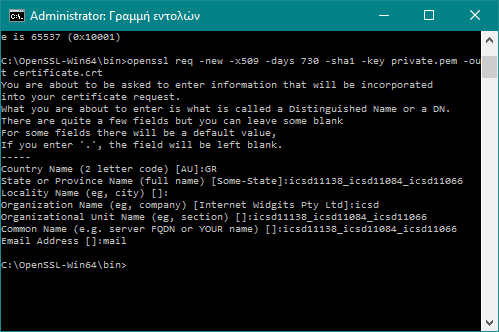
Με την παρακάτω εντολή δημιουργέιται το πιστοποιητικό. (αρχειο πιστοποιητικό)

openssl req -new -x509 -days 730 -sha1 -key private.pem -out certificate.crt





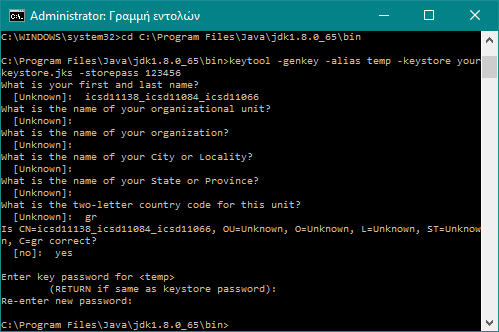




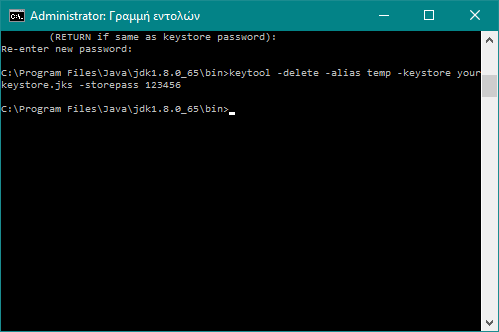
Επειδή η java δεν μπορεί να διαβάσει τα αρχεία .crt τα μετατρέπουμε μέσω των παρακάτω keytool εντολών σε .jks.  
-yourkeystore: όνομα αρχείου

-123456: κωδικός συστήματος

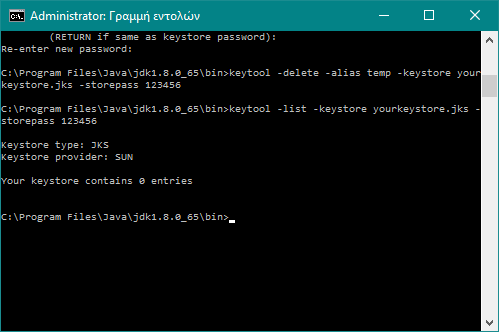
keytool -genkey -alias temp -keystore yourkeystore.jks -storepass 123456



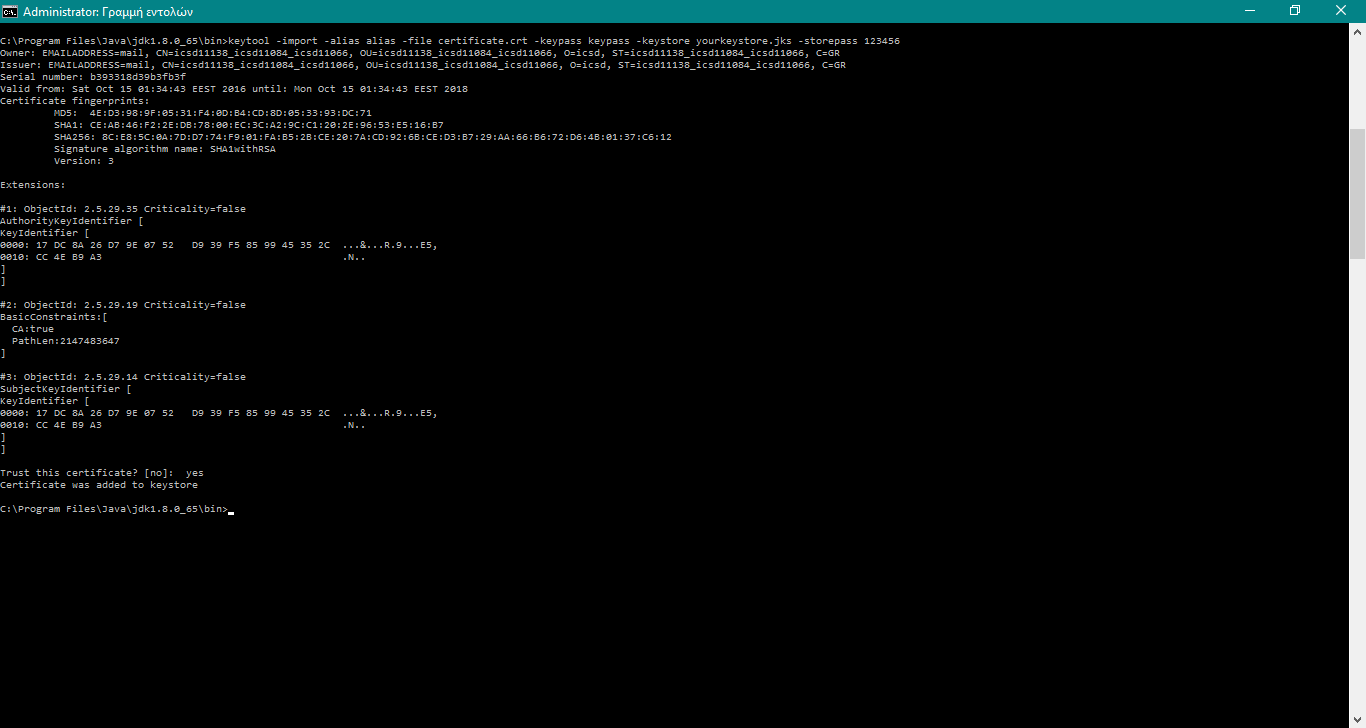
keytool -delete -alias temp -keystore yourkeystore.jks -storepass 123456



keytool -list -keystore yourkeystore.jks -storepass 123456



keytool -import -alias alias -file certificate.crt -keypass keypass -keystore yourkeystore.jks -storepass 123456

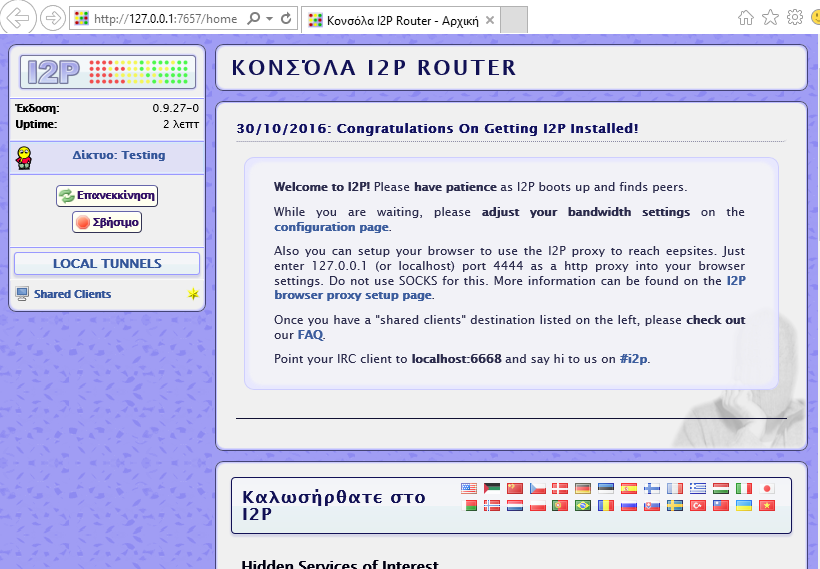


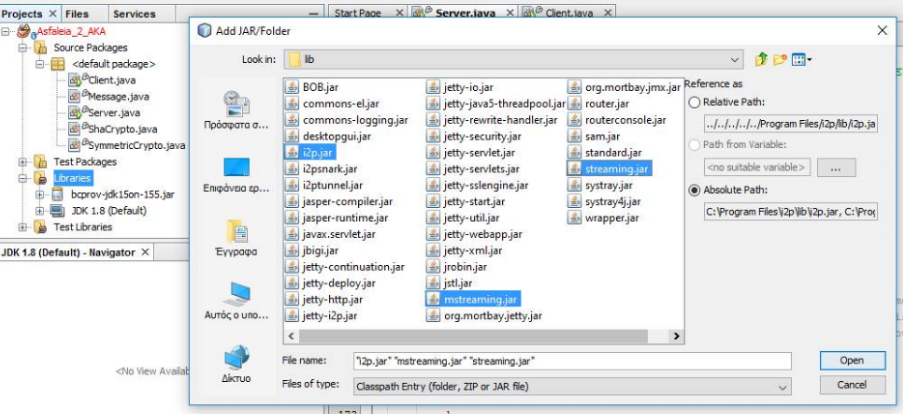
Πηγή: http://stackoverflow.com/questions/4022604/java-how-to-obtain-keystore-file-for-a-certification-crt-file

# Για το Ι2Ρ:

Έπρεπε να κατεβάσουμε τις παρακάτω βιβλιοθήκες.

Πηγή: https://geti2p.net/tr/get-involved/develop/applications





# Θεωρητικές

1. **Το ΑΚΑ πρωτόκολλο εξασφαλίζει από επιθέσεις τύπου spoofing και security downgrade; Αν ναι, με ποιόν τρόπο; Αν όχι, πως θα μπορούσαν να αποφευχθούν τέτοιου είδους επιθέσεις; Αναπτύξτε με συντομία.**

Αρχικά, spoofing είναι η τεχνική όπου αποκτούμε πρόσβαση σε υπολογιστές με την δημιουργία πακέτων TCP/IP, χρησιμοποιώντας τη διεύθυνση και τα στοιχεία κάποιου άλλου αξιόπιστου. Τα routers χρησιμοποιούν την διεύθυνση της IP προορισμού ώστε να διαδώσουν τα πακέτα μέσω διαδικτύου αλλάζοντας εικονικά την διεύθυνση της IP πηγής. Αυτή η διεύθυνση χρησιμοποιείται μόνο από το μηχάνημα προορισμού όταν απαντά πίσω στη πηγή.

Το πρωτοκολλο ΑΚΑ εξασφαλίζει από επιθέσεις spoofing διότι ο server στελνει ένα τυχαίο αλφαριθμητικό ως cookie στον client και περιμένει να το πάρει πίσω στο επόμενο μήνυμα του client.

Downgrade: Σε αυτή την κατηγορία επιθέσεων (επιθέσεις υποβίβασης) ο επιτιθέμενος προσπαθεί να αναγκάσει τα δύο μέρη να επιλέξουν αδύναμες κρυπτογραφικές σουίτες.

Στην περιπτωσή μας αν η Alice επιλέξει π.χ. 2 αλγόριθμους και ο ένας από τους δύο είναι αδύναμος τότε ο επιτιθέμενος μπορεί να ‘’κόψει’’ το δυνατό κ να σταλθεί έτσι ο αδύναμος στο server.

Συνεπώς, δεν εξασφαλίζεται πλήρως από το security downgrade, παρόλο που όπως βλέπουμε στο σχήμα της εκφώνησης (βήμα 5) ότι υπάρχει εν μέρη security downgrade.

1. **Το πρωτόκολλο εξασφαλίζει την επικαιρότητα (freshness) της συνόδου; Αν ναι, με ποιόν τρόπο; Αν όχι, πως μπορεί να εξασφαλιστεί αυτή η ιδιότητα;**

Στο πρωτόκολλο ΑΚΑ υπάρχει η επικαιρότητα (freshness) διότι χρησιμοποιεί συνεχώς διαφορετικό κλειδί και όχι το ίδιο

1. **Μπορείτε να βελτιώσετε τη λειτουργία του πρωτοκόλλου; Ποια θεωρείτε ότι είναι τα αδύναμα χαρακτηριστικά του και τι θα προτείνατε για τη βελτίωση του;**

Για τη βελτίωση του πρωτοκόλλου θα μπορούσαμε να αλλάξουμε τον τρόπο όπου στέλνουμε τις σουίτες. Αν οι σουίτες στέλνονταν κρυπτογραφημμένες δεν θα υπήρχε ο κίνδυνος του downgrade.

1. **Μελετήστε τη λειτουργία του δικτύου ανωνυμίας I2P και του δικτύου ανωνυμίας TOR. Ποιες διαφορές παρουσιάζουν; Ποιο είναι ασφαλέστερο και γιατί;**

* Στον Τοr όταν θέλουμε να επισκεφτούμε το ίντερνετ μπορούμε ελεύθερα ενώ σε αντίθεση στον I2P χρειαζόμαστε έναν outbound proxy.
* Στον Ι2Ρ σπάει η διαδρομή σε 2 κομμάτια ενώ στο tor γίνεται με το ίδιο κανάλι.
* O Tor έχει σχεδιαστεί με μεγάλους κόμβους εξόδου σε αντίθεση με τον Ι2Ρ.
* Ο Tor υποστηρίζει C ενώ ο Ι2Ρ Java.
* Στο Ι2Ρ τα δεδομένα στέλνονται σε πακέτα ενώ οι clients του Tor καθορίζουν τυχαία το μονοπάτι της σύνδεσης.
* Το Tor κάνει πιο αποτελεσματική χρήση μνήμης.
* Οι κόμβοι του Tor έχουν χαμηλό εύρος ζώνης.
* Ο κεντρικό έλεγχος στο Tor μειώνει την πολυπλοκότητα σε κάθε κόμβο και μπορεί να αντιμετωπίσει αποτελεσματικά τις επιθέσεις Sybil
* Στο Tor ένας πυρήνας υψηλής χωρητικότητας κόμβου παρέχει υψηλότερη απόδοση και χαμηλότερη αφάνεια.
* Το Ι2P έχει σχεδιαστεί για κρυφές υπηρεσίες οι οποίες είναι πιο γρήγορες έναντι του Tor.
* Στο Ι2Ρ υπάρχει πλήρης κατανομής και αυτο οργάνωση.
* Οι διαδρομές (tunnels) στο Ι2Ρ έχουν μικρή διάρκεια ζωής σε αντίθεση με του Tor.
* To I2P έχει ενσωματωμένο μηχανισμό αυτόματης ενημέρωσης ενώ το Tor όχι.

H πιο βασική διαφορά του Tor από τον Ι2Ρ είναι πως στο Tor το πακέτο κρυπτογραφείται επανειλημμένα σε κάθε κόμβο που διέρχεται μέχρι να φτάσει στο τελικό κόμβο όπου αποκρυπτογραφείται και προωθείται στον τελικό χρήστη. Αυτό αποτρέπει τους ενδιάμεσους κόμβους να μάθουν την προέλευση, τον προορισμό και το περιεχόμενο του μηνύματος. Συνεπώς αυτό το κάνει ασφαλέστερο έναντι του Ι2Ρ.

# Printscreen Εκτέλεσης Προγράμματος:

