Πανεπιστήμιο Κύπρου – Τμήμα Πληροφορικής
(Εαρινό Εξάμηνο 2010-2011)

ΕΠΛ 674: Ασφάλεια Συστημάτων και Δικτύων

Εργαστήριο 4

ΕΝΤΟΛΗ: openssl (Linux)
Το **OpenSSL** είναι μια βιβλιοθήκη κρυπτογράφησης για την υλοποίηση των πρωτοκόλλων **SSL** (Secure Sockets Layer) και **TLS** (Transport Layer Security). Το πρόγραμμα **openssl** χρησιμοποιεί συναρτήσεις της βιβλιοθήκης **OpenSSL** για τη δημιουργία κλειδιών τόσο συμμετρικής όσο και ασύμμετρης κρυπτογράφησης, για την υλοποίηση διαδικασιών κρυπτογράφησης και αποκρυπτογράφησης καθώς και για τις διαδικασίες υπογραφής και επαλήθευσης.

Γενική μορφή σύνταξης: **openssl command <command_options> <command_args>**

1) Αφού συνδεθείτε μέσω στο εργαστήριο των Linux (μέσω nxclient), δημιουργείστε μέσα στον προσωπικό σας φάκελο (folder) το φάκελο **openSSL**. Εν συνεχεία ανοίξτε ένα παράθυρο στο οποίο να βλέπετε τα περιεχόμενα του φακέλου **openSSL**.

a. Στον παραπάνω φάκελο δημιουργείστε το αρχείο lab4.txt στο οποίο θα γράψετε μέσα το όνομα, το επίθετο και το ID σας (π.χ. Pavlos Antoniou 817651). Αποθηκεύστε και κλείστε το αρχείο.

b. Στο terminal πληκτρολογείστε την εντολή:
openssl des3 –e –in lab4.txt –out testDES3.txt
Θα σας ζητηθεί συνθηματικό και επιβεβαίωσή του (επιλέγετε κατά βούληση). Η παραπάνω εντολή χρησιμοποιεί το **συμμετρικό** αλγόριθμο κρυπτογράφησης TripleDES (**des3**) προκειμένου να κρυπτογραφήσει (**-e**) το αρχείο που δηλώνετε ως είσοδος (**-in lab4.txt**) και να παράγει έξοδο το αρχείο testDES3.txt **(–out testDES3.txt).**

c. Ανοίξτε το αρχείο testDES3.txt με ένα editor (emacs ή gedit).

d. Για την αποκρυπτογράφηση (**-d**) του testDES3.txt στο testDES3Dec.txt πληκτρολογείστε την εντολή:
openssl des3 –d –in testDES3.txt –out testDES3Dec.txt
Το αρχείο **testDES3Dec.txt** θα πρέπει να περιέχει ότι και το αρχείο **lab4.txt**.

e. Δοκιμάστε τις εντολές:
openssl des3 –e –a –in lab4.txt –out testDES3b.txt και
openssl des3 –d –a –in testDES3b.txt –out testDES3bDec.txt
και συγκρίνετε τα αρχεία **testDES3.txt** και **testDES3b.txt**. Το αρχείο **testDES3bDec.txt** θα πρέπει να περιέχει ότι και το αρχείο **lab4.txt**. Η επιλογή της παραμέτρου –a μαζί με το –e επιτρέπει την κωδικοποίηση του περιεχομένου του lab4.txt σε **base64 encoding** (χρησιμοποιείται για κωδικοποίηση δυαδικών αρχείων – binary files – που πρέπει να σταλούν πάνω από μέσα τα οποία είναι σχεδιασμένα να επεξεργάζονται αρχεία κειμένου – textual data – βλέπε μεταφορά εικόνων σαν attachments μέσω μηνυμάτων ηλεκτρονικού ταχυδρομείου).

2) Μεταφερθείτε στο terminal:

a. πληκτρολογείστε την εντολή:
openssl enc –help
και θα δείτε τις επιλογές που έχετε για χρήση κρυπτογραφικών αλγορίθμων.

b. Κρυπτογραφείστε και αποκρυπτογραφείστε το αρχείο **lab4.txt** με τον συμμετρικό αλγόριθμο **Blowfish**. Ονομάστε το κρυπτογραφημένο αρχείο **testBF.txt** και το αποκρυπτογραφημένο **testBFDec.txt**.

3) Ο RSA είναι αλγόριθμος **ασύμμετρης κρυπτογράφησης**. Κατά την κρυπτογράφηση απαιτεί τη χρήση δημοσίου κλειδιού, ενώ κατά την αποκρυπτογράφηση τη χρήση ιδιωτικού κλειδιού.

a. Με την εντολή:
   openssl genrsa –out private.key 1024
   θα δημιουργηθεί το ιδιωτικό κλειδί **private.key** του **RSA** μήκους **1024 bits**.

b. Για τη δημιουργία του δημόσιου κλειδιού **public.pem** από το ιδιωτικό κλειδί **private.key** που φτιάξαμε στο προηγούμενο βήμα θα πρέπει να δώσετε την εντολή:
   openssl rsa –in private.key –pubout –out public.pem

c. Κατασκευάστε και ένα 2° δημόσιο κλειδί **public2.pem** από το ίδιο ιδιωτικό **private.key.**

d. Ανοίξτε με το WordPad τα αρχεία **private.key, public.pem** και **public2.pem.** Τί παρατηρείτε για τα **public.pem** και **public2.pem**, είναι αναμενόμενο;

e. Για να κρυπτογραφήσουμε το **lab4.txt** θα χρησιμοποιήσουμε το **public.pem**. Η εντολή είναι:
   openssl rsautl –encrypt –inkey public.pem –pubin –in lab4.txt –out testRSA.txt

f. Για να αποκρυπτογραφήσουμε το **testRSA.txt** θα χρησιμοποιήσουμε το **private.key**. Η εντολή είναι:
   openssl rsautl –decrypt –inkey private.key –in testRSA.txt –out testRSADec.txt

4) Ανταλλάξτε σε ζεύγη μέσω mail με τον διπλανό σας τα δημόσια κλειδιά σας. Για να γίνει αυτό αντιγράψτε, επικολλείστε και μετονομάστε το **public.pem** σε **publicID.pem,** όπου ID ο αριθμός ταυτότητάς σας, για παράδειγμα **public811765.pem.** Στη συνέχεια στείλτε στο διπλανό σας, του οποίου το δημόσιου κλειδί έχετε, ένα επισυναπτόμενο κρυπτογραφημένο αρχείο με το δικό του δημόσιο κλειδί. Αντίστοιχα θα παραλάβει ο καθένας σας ένα κρυπτογραφημένο αρχείο με το δικό σας δημόσιο κλειδί. Αποκρυπτογραφείστε το με το **private.key** σας.

5) Χρησιμοποιώντας το **private.key** μπορείτε να **υπογράψετε ψηφιακά** ένα αρχείο.

a. Με την εντολή:
   openssl rsautl –sign –inkey private.key –in lab4.txt –out testSigned.txt
   θα παραχθεί από το αρχείο **lab4.txt** το υπογεγραμμένο **testSigned.txt**.

b. Με την εντολή:
   openssl rsautl –verify –inkey public.pem –pubin –in testSigned.txt –out testVerified.txt
   κάνετε επαλήθευση της ψηφιακής υπογραφής.

6) Υπογράψτε ένα αρχείο και στείλτε το μέσω mail στον διπλανό σας ο οποίος έχει το δικό σας δημόσιο κλειδί. Αντίστοιχα θα παραλάβει ο καθένας σας ένα υπογεγραμμένο αρχείο με το ιδιωτικό κλειδί του διπλανού του. Επαληθεύστε την υπογραφή με το δημόσιο κλειδί του διπλανού σας.