Εργαστήριο Δικτύων
Τμήμα Μηχανικών Η/Υ & Πληροφορικής Πανεπιστήμιο Πατρών

Ερωτήσεις κατανόησης και Εργασία για το μάθημα:
Σύγχρονες Εφαρμογές Ασφάλειας Δικτύων

5η Εργασία - Κρυπτογράφηση αρχείου.

Μέρος Α

1) Εγκαταστήστε το πακέτο openssl.
   - Ποιες εντολές χρησιμοποιήσατε?
   - Με ποια εντολή ελέγχετε η έκδοση που έχει εγκατασταθεί?

2) Με ποια εντολή βρίσκω όλους τους κώδικες κρυπτογράφησης που υποστηρίζονται?

3) Με ποια εντολή βρίσκω βρίσκω μόνο τους κώδικες κρυπτογράφησης που υποστηρίζουν TLSv1-3?

Για κάθε ένα από αυτούς δώστε πληροφορίες για:
- τρόπο authentication
- αλγόριθμό κρυπτογράφηση, μέγεθος κλειδιού και mode λειτουργίας
- Hash

4) Ανατρέξτε στην σελίδα https://ciphersuite.info/ και ελέγξτε ποιοι από αυτούς είναι ευπαθείς αλγόριθμοι (weak) και ποιοι όχι. Από την ίδια σελίδα βρείτε ποιοι είναι οι πιο ισχυροί αλγόριθμοι κρυπτογράφησης (recommended και strong) που υποστηρίζουν TLSv1-3 ή/και TLSv1-2.

5) Αναλύστε τον κώδικα κρυπτογράφησης **“**ECDHE-ECDSA-AES128-GCM-SHA256” και ειδικότερα τον τρόπο δημιουργίας και ανταλλαγής κλειδιών.

6) Ανατρέξτε στην ιστοσελίδα: https://www.javainuse.com/aesgenerator και κρυπτογραφήστε τον αριθμό μητρώου σας. Επιλέξτε CBC mode, 256 μέγεθος κλειδιού και τυχαίο κλειδί Secret και Initialization Vector. Ποια η έξοδος?
   - Επαληθεύστε από άλλη ιστοσελίδα: https://www.devglan.com/online-tools/aes-encryption-decryption
   - Τι είναι κωδικοποίηση base64? Πως μετατρέπεται σε αναγνώσιμη μορφή?

7) Τι είναι οι κρυπτογραφικές λειτουργίες hash (cryptographic hash functions) και που/πως χρησιμοποιείτε?
   - Με ποια εντολή βρίσκω ποιοι hash αλγόριθμοι υποστηρίζονται από το openssl?
   - Δημιουργείστε το SHA512 hash του αριθμού μητρώου σας χρησιμοποιώντας την ιστοσελίδα: https://emn178.github.io/online-tools/sha512.html

Μέρος Β

1) Ακολουθήστε **όλες** τις οδηγίες από το παρακάτω σύνδεσμο: https://gist.github.com/kebman/f02fe0b1dbebc9ee1a56a7885c30f014 και κρυπτογραφήστε ένα απλό αρχείο, χρησιμοποιώντας τον αριθμό μητρώου σε κάθε αρχείο και πιο συγκεκριμένα:

- Δημιουργία private/public κλειδιών μεγέθους 4096:
  1044545_private.pem 1044545_public.pem

- Δημιουργία μηνύματος προς κρυπτογράφηση:
  1044545_msg.txt με περιεχόμενο: Hello world: 1044545

- Δημιουργία Hash Digest (1044545_msg.digest.txt)

- Κρυπτογραφημένη υπογραφή (1044545_msg.signature.bin)

➔ Χρησιμοποιείστε ως έτερο public κλειδί το *kvlachos_public.pem* που είναι στο φάκελο των εγγράφων στο eclass, στον φάκελο "**7. Advanced Encryption Standard**" (σε zip αρχείο).

➔ Υποβάλλετε σε zip ή tar αρχείο τα ακόλουθα στο eclass:
- `1044545_msg.b64`
- `1044545_msg.digest.b64`
- `1044545_msg.signature.b64`
- `1044545_randomkey.enc.b64`
- `1044545_public.pem (το δικό σας δημόσιο κλειδί)`

➔ Κάνετε upload τα ίδια αρχεία (όχι zip!! όπως είναι) εδώ:
https://upatrasgr-my.sharepoint.com/:f:/g/personal/kvlachos_upatras_gr/Eg8eC1LOpJlIt3VSAVqr9JsB1QO6IZdLCLm_hahnIZ6UoQ

Μετά το πέρας της καταληκτικής ημερομηνίας θα γίνει αυτόματη διόρθωση των αρχείων που υποβάλλατε και θα λάβετε αυτόματο εμαιλ που θα αναφέρει είτε τα αρχεία που λείπουν είτε εάν εάν τα αρχεία αποκρυπτογραφήθηκαν επιτυχώς.

Για όσους φοιτητές τα αρχεία αποκρυπτογραφήθηκαν σωστά, θα λάβουν 2ο εμαιλ με οδηγίες για τη 2η φάση της εργασίας (αποστολή μηνύματος και κλειδιού για να αποκωδικοποιηθούν). Οδηγίες θα υπάρχουν στο εμαιλ που θα σταλεί.

➔ Μην χάσετε το private κλειδί σας.