ΕΝΔΕΙΚΤΙΚΑ ΘΕΜΑΤΑ ΑΣΦΑΛΕΙΑΣ ΔΙΚΤΥΩΝ

1. Τι είναι η συμμετρική και τι η ασύμμετρη κρυπτογράφηση;

2. Παραθέστε ονομαστικά τουλάχιστον έναν αλγόριθμο συμμετρικής και έναν ασύμμετρης κρυπτογράφησης

3. Σε τι αναφέρονται οι όροι Μυστικότητα, Ακεραιότητα και Πιστοποίηση αυθεντικότητας;

4. Τι ονομάζουμε modulus στον αλγόριθμο RSA; Ποια η σχέση του με το μήκος του ιδιωτικού κλειδιού;

5. Σε τι εξυπηρετεί ο αλγόριθμος Diffie-Hellman;

6. Δώστε παράδειγμα χρήσης των αλγορίθμων κατακερματισμού για τη λειτουργία ταυτοποίησης κωδικού πρόσβασης σε μια βάση δεδομένων.

7. Ο MD5 θεωρείται ασφαλής αλγόριθμος κατακερματισμού; Ποιοι εναλλακτικοί αλγόριθμοι κατακερματισμού υπάρχουν;

8. Αναπαραστήστε σε σχήμα ένα παράδειγμα προσθήκης ψηφιακής υπογραφής σε ένα ψηφιακό έγγραφο. Στη συνέχεια, δώστε ένα δεύτερο σχήμα που αναπαριστά τη διαδικασία επιβεβαίωσης της ψηφιακής υπογραφής.

9. Τι είναι το ψηφιακό πιστοποιητικό και ποια η χρησιμότητά του;

10. Ποιος ο ρόλος της Αρχής Πιστοποίησης (CA) σε μια υποδομή δημοσίου κλειδιού (PKI);

11. Στο TLS, πότε χρησιμοποιείται η ασύμμετρη και πότε η συμμετρική κρυπτογράφηση;

12. Από ποιο κλειδί εξαρτάται η ασφάλεια μιας συνεδρίας TLS;

13. Ποιους αλγορίθμους αναγνωρίζετε στο εξής cipher suite; Πόσο ασφαλές θεωρείτε το εν λόγω cipher; TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256

14. Τι είναι ο πληρεξούσιος εξυπηρετητής (proxy server) και ποια η χρησιμότητά του σε ένα εργασιακό περιβάλλον;

15. Σχεδιάστε ένα διάγραμμα που απεικονίζει ένα υποδίκτυο διαλογής. Ποια είναι η χρησιμότητα του DMZ;

16. Σε ένα υποδίκτυο διαλογής (Screened Subnet), σε ποιο δίκτυο θα τοποθετούσατε έναν Web server, ο οποίος θα θέλατε να ήταν προσβάσιμος από εξωτερικούς χρήστες;

17. Αναφέρετε τουλάχιστον ένα λογισμικό προστασίας από κακόβουλο λογισμικό για Windows και τουλάχιστον ένα λογισμικό για Linux.