Ασφάλεια Ψηφιακών Συστημάτων
Εξεταστική Περιόδου Ιουνίου 2024
Διάρκεια εξέτασης: 2 ώρες

Ονοματεπώνυμο: ..... **Αριθμός Μητρώου:** .....

Θέματα (Επιστρέφονται)

ΘΕΩΡΙΑ: [*Επιλέξτε 4 ερωτήσεις*]. **Σύνολο μονάδων 3**

1. Αναφέρατε την ορολογία που αφορά τον RSA και φτιάξτε (2) σχήματα όπου θα δείχνετε την κρυπτογράφηση με δημόσιο κλειδί και την κρυπτογράφηση με ιδιωτικό κλειδί.
2. Τι είναι η συμμετρική κρυπτογράφηση (συνοπτικά); Αποτυπώστε το μοντέλο λειτουργίας της
3. Παραδείγματα απειλών υπολογιστικών και διαδικτυακών πόρων. Αναφέρατε συνοπτικά τι συμβαίνει σε κάθε περίπτωση
4. Αναφέρατε και εξηγήστε συνοπτικά τους (4) τρόπους που αφορούν «σπάσιμο» κωδικών πρόσβασης
5. Τι γνωρίζετε για τους τύπους του κακόβουλου λογισμικού;
6. Αναφέρατε και σχολιάστε κλασσικές επιθέσεις DoS
7. Επιθέσεις επιπέδου ζεύξης: Τι γνωρίζετε για την επίθεση sniffing και MAC spoofing;
8. Αναφέρατε και σχολιάστε σύντομα τις τοπολογίες τείχους προστασίας

ΑΣΚΗΣΗ: **Επιλέξτε** ασκήσεις ώστε να **αθροίζουν στις 7 μονάδες**

Άσκηση 1: (Α) Εφαρμόζοντας τον **OTP** με δεδομένα σύνολο κλειδιών (k) = σύνολο μηνυμάτων (m) = συνδυασμοί στο σύνολο $(0,1)^8$, βρείτε το cipher που προκύπτει εάν κάνουμε χρήση του **(m1,k1) = (75,81)** και έπειτα **(m2,k2) = (178,168)**.Τι παρατηρείτε ως προς το cipher που προκύπτει στις δύο περιπτώσεις; (Β) Εάν (k) και (m) ανήκουν στο σύνολο $(0,1)^7$, και από όλα τα διαθέσιμα κλειδιά, εμείς λαμβάνουμε το 3^{19} **mod 22** τότε ποιο cipher προκύπτει; (2 μονάδες)

Άσκηση 2: Έστω ένα ζεύγος (S)ender – (R)eceiver. Ο S στέλνει στον R το δημόσιο κλειδί RSA (n,e) = (33,7). Ποια η ψηφιακή υπογραφή για το μήνυμα m = 15; Πώς ο R επιβεβαιώνει την αυθεντικότητα του μηνύματος; (2 μονάδες)

Άσκηση 3: Έστω το κρυπτογράφημα y = QDZTG. Αποκρυπτογραφήστε το με τη χρήση του ομοπαραλληλικού αλγορίθμου Affine, για το ζεύγος κλειδιού k = (3,11). Κάντε εφαρμογή των απεικονίσεων γραμμάτων – αριθμών από το Z_{26}. (2 μονάδες)

Άσκηση 4: Έστω ένα κρυπτοσύστημα {P,C,K}, όπου P = messages, C = ciphers, K = keys, με τα εξής χαρακτηριστικά: P = {0,1} με P(0) = ¼, P(1) = ¾. K = {A,B} με P(A) = ¼, P(B) = ¾ και C = {a,b}. Δίνονται επίσης οι απεικονίσεις κρυπτογράφησης: $E_A(0) = a$, $E_A(1) = b$, $E_B(0) = b$, $E_B(1) = a$. Να ελέγξετε εάν υπάογει τέλεια μυστικότητα για το message P = 0 στην περίπτωση του C = a. Θεωρήστε επίσης στατιστικά ανεξάρτητες τις τυχαίες μεταβλητές P,K. (2,5 μονάδες)

Άσκηση 5: Έστω (2) χρήστες, ο (S)ender και ο (R)eceiver, οι οποίοι θέλουν να ανταλλάξουν κρυπτογραφημένο μήνυμα. Δύο υπολογιστές του ίδιου τοπικού δικτύου PC1, PC2, συνδέονται στο ίδιο switch. Συγκεκριμένα, ο PC1 έχει **IP = 210.93.105.10/24** και ο PC2 έχει **IP = 210.93.105.133/24**. Έχει ρυθμιστεί μία ACL στον Router ως εξής:

Access list 1 permit 210.93.105.0 0.0.0.127

Access list 1 deny any

Το δημόσιο κλειδί του PC1 είναι $(\mathbf{n,e_1}) = (\mathbf{3,55})$ και του PC2 είναι $(\mathbf{n,e_2} = \mathbf{119,5})$. Και οι δύο κρυπτογραφούν το μήνυμα m = 'P' (τιμή 80 δεκαδικού στον ASCII), όμως λόγω της ACL, μόνο ένα κρυπτογράφημα περνά από τον Router. Ζητείται:

1. Ποιο περνά και γιατί;
2. Ποιο το cipher που λαμβάνει ο Receiver;

(2,5 μονάδες)