Εξεταστική Περιόδου Ιουνίου 2022

φοιτητές του ΠΣ Διηρκούς Πληροφορικής ΤΕ που έχουν παρακολουθήσει - εξεταστεί στο εργαστήριο του μαθήματος καλούνται να επιλέξουν ή από τα 10 διαφορετικά θέματα και να απαντήσουν σε αυτά ανάς 90'. Στη προκειμένη περίπτωση όλα τα θέματα βαθμολογούνται με 2 μονάδες.

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

Θέματα (Επιστρέφονται)

Μέρος Α [Θεωρία]: Επιλέξτε από τις παρακάτω ερωτήσεις (μέγιστο άθροισμα επιλεγόμενων μονάδων = 2,5 μονάδες)

1. Ποιες οι βασικές έννοιες ασφάλειας και τι γνωρίζετε επιγραμματικά γι αυτές; **[0,5]**
2. Τι γνωρίζετε συνοπτικά για τις ευπάθειες, απειλές και επιθέσεις; **[1]**
3. Ποιες παθητικές και ποιες ενεργητικές επιθέσεις γνωρίζετε; **[0,5]**
4. Τι είναι η συμμετρική κρυπτογράφηση (συνοπτικά); Αποτυπώστε το μοντέλο λειτουργίας της **[1]**
5. Συγκρίνετε τα χαρακτηριστικά των αλγορίθμων ασύμμετρης κρυπτογράφησης; **[0,5]**
6. Αναπτύξτε και εξηγήστε συνοπτικά τους (4) τρόπους που αφορούν «επίσιμο» κωδικών πρόσβασης **[1]**
7. Αναπτύξτε τι γνωρίζετε σχετικά με τα υποκείμενα, αντικείμενα και δικαιώματα πρόσβασης **[1]**
8. Τι γνωρίζετε για τις περιπτώσεις κρυπτογράφησης σε βάσεις δεδομένων; **[0,5]**
9. Τι γνωρίζετε για τους τύπους του κακόβουλου λογισμικού; **[1]**
10. Αναπτύξτε και σχολιάστε τις (4) γενιές λογισμικού προστασίας από ιούς **[1]**

Μέρος Β [Ασκήσεις]: Επιλέξτε από τις παρακάτω ερωτήσεις (μέγιστο άθροισμα επιλεγόμενων μονάδων = 10 μονάδες)

1. Για **k = 7** και εφαρμογή του αλγορίθμου **Caesar Cipher**, πως κρυπτογραφείται η φράση «**TEST**»; **[1]**
2. Για **k = MATH** και εφαρμογή του αλγορίθμου **Vigenere**, κρυπτογραφήστε η φράση «**HAPPY HOLIDAY**»; **[1,5]**
3. Για **k = BACK UP** και εφαρμογή του αλγορίθμου **HILL**, πως κρυπτογραφείται η φράση «**SAFE COMMS**» ; **[2,5]**
   *(Σημείωση: Για τον πίνακα του κλειδιού συμπληρώστε ανά γραμμή και βάλτε dummy στοιχεία **A B C** και δημιουργήστε πίνακα 3x3 και 3x1 για τα μηνύματα)*
4. Έστω ότι διαθέτετε το Cipher = **HDS IOE YQO CAA** και θέλετε να το αποκρυπτογραφήσετε εφαρμόζοντας τον αλγόριθμο **HILL**. Έχετε επίσης στη διάθεσή σας το κλειδί **k = CIP HER ING**. Ποιο μήνυμα προκύπτει; **[3]**
   (Σημείωση: Για τον πίνακα κλειδιού συμπληρώστε ανά γραμμή και δημιουργήστε 3x3 και 3x1 για τα ciphers)
5. α) Εφαρμόζοντας τον αλγόριθμο **Playfair** και θέλοντας να κρυπτογραφήσετε το μήνυμα « **FRIDAY**», ποιο cipher προκύπτει; (χρήση πίνακα 5x5) **[0,5]**
   β) Κάντε το ίδιο με το (α), αλλά έχοντας και το κλειδί «**EXAMS**» **[0,5]** *(Σημείωση: 1 γραμμή του πίνακα 5x5)*
6. Έστω ότι θέλετε να εφαρμόσετε τον αλγόριθμο **Affine** για να κρυπτογραφήσετε τη φράση «**TELEÇOMS**» και έχετε στη διάθεσή σας το ζεύγος κλειδιού: **k -> (x,y)** όπου **x** = το **τελευταίο ψηφίο** του αριθμού μητρώου σας και **y = 10**.
   α) Ποια η συνθήκη για να μπορεί να εφαρμοστεί ο Affine; Σύμφωνα με το x που έχετε, μπορείτε να το εκτελέσετε; Αιτιολογήστε την απάντησή σας **[0,5]**
   β) Αν από το (α) ερώτημα μπορείτε να τον εκτελέσετε, τότε βρείτε το κρυπτογράφημα. Αν **δεν** μπορείτε, τότε αλλάξτε κατάλληλα το x (έστω x=3), ώστε να μπορείτε και προχωρήστε στην κρυπτογράφηση του αρχικού μηνύματος **[1]**
7. Υπολογίστε τα ακόλουθα: α) 17^{-1} **mod 43 [0,5]** β) 27^{-1} **mod 392 [0,5]** γ) **ΜΚΔ(36,60,84) [0,5]**
8. Έστω ότι θέλουμε να ελέγξουμε ένα κρυπτοσύστημα ως προς την **απόλυτη ασφάλειά του**. Ο σύνολο των μηνυμάτων του είναι τα: **M = {x,y,z}**, τα οποία επιλέγονται με πιθανότητες: ¾, 0, ¼ αντίστοιχα. Το σύνολο των κλειδιών **K = {k1,k2,k3}** έχει πιθανότητες επιλογής **1/8, 1/8, ¾** αντίστοιχα. Οι αντιστοιχίσεις κλειδιού -> μηνύματος, μέσω των συναρτήσεων κρυπτογράφησης, δίνονται από τον παρακάτω πίνακα **[2,5]**:

	x	y	z
k1	1	2	3
k2	2	3	1
k3	3	4	2

   *(Σημείωση: Ελέγξτε ως προς την απόλυτη ασφάλεια **μόνο για cipher = 1 και 2**)*
9. Υπολογίστε τα: α) 5^{80} **mod 19** με τη χρήση μεθόδου δυνάμεων **[0,5]** β) 15^{30} **mod 19** με εκθετοποίηση/πίνακα **[0,5]**
10. 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; **[1]**
11. Έστω ένα ζεύγος sender/receiver ανταλλάσσει μηνύματα μέσω **RSA**. Το σύστημα κάνει χρήση των στοιχείων: **(p,q)=(3,11)** και δημόσιο κλειδί το γράμμα **H**. Να προσδιορίσετε το ιδιωτικό κλειδί ώστε να σταλθεί κρυπτογραφημένη η αλληλουχία **{2,5,3}** **[2]**

Σημείωση: Το σύνολο των επιλεγόμενων μονάδων να είναι το μέγιστο 10.