ρος Α: Επιλέξτε από τις παρακάτω ερωτήσεις ώστε το (Σύνολο Μονάδων = 2)

. Ποιες οι βασικές έννοιες ασφάλειας και τι γνωρίζετε επιγραμματικά για αυτές; **[1]**
. Τί είναι η συμμετρική κρυπτογράφηση (συνοπτικά); Αποτυπώστε το μοντέλο λειτουργίας της **[1]**
. Αναφέρατε την ορολογία του RSA και φτιάξτε (2) σχήματα όπου θα δείχνετε την κρυπτογράφηση με δημόσιο κλειδί και την κρυπτογράφηση με ιδιωτικό κλειδί; **[0,5]**
Αναφέρατε και σχολιάστε κλασσικές επιθέσεις DoS **[1]**
Ποιες κατηγορίες κυβερνοεγκλημάτων γνωρίζετε **[0,5]**
Σχετικά με τη συμπεριφορά των χάκερ, αναφέρατε επιγραμματικά τις βασικές τους επιδιώξεις **[0,5]**
Ποιες επιθέσεις αφορούν βασικά ζητήματα ασφάλειας του Διαδικτύου και τι γνωρίζετε (συνοπτικά) για κάθε μία; **[1]**
Ποιος ο ορισμός και η χρήση ενός τείχους προστασίας (firewall) και ποιες οι δύο βασικές κατηγορίες στις οποίες διαχωρίζονται; **[1]**
Ποιες τεχνικές εφαρμόζει ο κρυπταναλυτής για την εύρεση ενός κλειδιού αποκρυπτογράφησης και τι γνωρίζετε γι' αυτές; **[1]**

ς Β: Υποχρεωτικές ασκήσεις ώστε το (**Σύνολο μονάδων = 6**)

Για **k = τελευταίο ψηφίο του Α.Μ.** σας και εφαρμογή του αλγορίθμου **Caesar Cipher**, πως κρυπτογραφείται η φράση «**GREAT**»; *Σημείωση: Εάν το τελευταίο ψηφίο του Α.Μ. σας είναι ίσο με 0, τότε χρησιμοποιήστε k = 3* **[1]**
Για **k = PATH** και εφαρμογή του αλγορίθμου **Vigenere**, κρυπτογραφήστε η φράση «**HAPPY HOLIDAY**»; **[1,5]**
Υπολογίστε τα ακόλουθα (να φαίνονται όλες οι πράξεις): α) $17^{-1} \bmod 43$ **[0,5]** , β) $5^{80} \bmod 19$ με τη χρήση μεθόδου δυνάμεων **[0,5]**, γ) **ΜΚΔ(36,60,84) [0,5],** δ) $15^{20} \bmod 19$ με εκθετοποίηση/πίνακα **[0,5]**
Έστω ότι θέλετε να εφαρμόσετε τον αλγόριθμο **Affine** για να κρυπτογραφήσετε τη φράση «**TELECOMS**» 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, κατά την αποκρυπτογράφηση; Σύμφωνα με το x που έχετε, μπορείτε να το εκτελέσετε πλήρως (κρυπτογράφηση και αποκρυπτογράφηση); Δικαιολογήστε 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, ώστε να προκύψει το κρυπτογράφημα **[1]**

Γ: Ασκήσεις επιλογής ώστε το (**Σύνολο μονάδων = 2**) **Εστιάζετε μόνο σε 1 άσκηση**

α) Για **k = BACK UP** και εφαρμογή του αλγορίθμου **HILL**, πως κρυπτογραφείται η φράση «**SAFE COMMS**» *(Σημείωση: Για τον πίνακα του κλειδιού συμπληρώστε ανά γραμμή και βάλτε dummy στοιχεία **A B C** και δημιουργήστε πίνακα 3x* *και 3x1 για τα μηνύματα)* **[1] και β)** Δίνεται το κρυπτογράφημα y = **QDZTG**. Αποκρυπτογραφήστε το με Affine κα ζεύγος κλειδιού (3,11). Ποιο το μήνυμα που προκύπτει; **[1]**
α) Εφαρμόζοντας τον **OTP** με δεδομένα σύνολο κλειδιών (k) = σύνολο μηνυμάτων (m) = συνδυασμοί στο σύνολ **(0,1)^8**, βρείτε το cipher που προκύπτει εάν κάνουμε χρήση του **(m1,k1) = (75,81)** και έπειτα **(m2,k2) = (178,168)**. παρατηρείτε ως προς το cipher που προκύπτει στις δύο περιπτώσεις; **[1] και β)** Να γράψετε τις ACLs που προκύπτο όταν: i) Επιτρέπουμε όλους τους χρήστες του δικτύου **192.168.3.0/24** ii) Επιτρέπουμε μόνο τους χρήστες με περιτ IP από το δίκτυο **192.168.3.32/28** iii) Επιτρέπουμε μόνο τον χρήστη **192.168.1.5** του δικτύου **192.168.1.0/24** **[1]**
Έστω ένα ζεύγος sender/receiver ανταλλάσσει μηνύματα μέσω **RSA**. Το σύστημα κάνει χρήση των στοιχείω **(p,q)=(3,11)** και δημόσιο κλειδί το γράμμα **H** στην κλίματα αντιστοίχισης Z_{26}. Μπορεί να προκύψει ιδιωτικό κλειδ (δικαιολογήστε). Να προσδιορίσετε το ιδιωτικό κλειδί και στη συνέχεια να βρεθεί η κρυπτογραφημένη ακολουθ **{2,5,3,9}** **[2]**

ΚΑΛΗ ΕΠΙΤΥΧΙΑ!

☺