Ονοματεπώνυμο:

Μάθημα: ΔΙΚΤΑ

Υλη: Εφ όλης της ύλης

Επιμέλεια διαγωνίσματος:

ΛΑΜΠΡΑΚΗΣ ΜΑΝΩΛΗΣ

Αξιολόγηση :……

……..

ΘΕΜΑ Α

1) Ερωτήσεις Σωστό/Λάθος **(Μανάδες 10)**

1.1) Η διαχείριση σφαλμάτων έχει ως στόχο εκτός από την αντιμετώπιση σφαλμάτων και την πρόβλεψη μελλοντικών προβλημάτων
1.2) Η μέθοδος κρυπτογράφησης με μυστικό κλειδί χρησιμοποιείται από την ασυμμετρική κρυπτογράφηση
1.3) Έμπιστο θεωρείται το δίκτυο οι κανόνες ασφαλείας του διαχειρίζονται και καθορίζονται από την επιχείρηση που κατέχει το δίκτυο
1.4) Το πρωτόκολλο IPSec παρέχει υπηρεσίες αυθεντικοποίησης μόνο της επικεφαλίδας των πακέτων
1.5) Το επίπεδο εφαρμογών δεν αποτελεί στόχο παραβίασης της ασφάλειας ενός δικτύου, καθώς τα πρωτόκολλα εφαρμογών δεν παρουσιάζουν αδυναμίες στην σχεδίασή τους

2) Να αντιστοιχίσετε τα στοιχεία της στήλης Α με αυτά της στήλης Β **(Μονάδες 10)**

Στήλη Α: Βασικά χαρακτηριστικά	**Στήλη Β:** Είδος δικτύου
1. Διαχείριση κόστους 2. Μη άρνηση ταυτότητας 3. Μεταμφίεση 4. Firewall 5. Μέθοδος παραβίασης	Α. Απόδοση πράξεων σε συγκεκριμένο χρήστη Β. Επίθεση στους κωδικούς πρόσβασης Γ. Απαιτεί αλλαγές στους πίνακες δρομολόγησης του δικτύου Δ. Παρακολούθηση πόρων του δικτύου Ε. Προγράμματα και φίλτρα σε σημεία εισόδου του δικτύου

3) Στην παρακάτω ερώτηση να επιλέξετε την απάντηση που θεωρείτε σωστή (μία σωστή απάντηση) **(Μονάδες 5)**

«Η χρήση συμμετρικής κρυπτογράφησης χρησιμοποιείται κυρίως για εξασφάλιση»

Α) Ακεραιότητας Β) Αυθεντικότητας Γ) Εγκυρότητας Δ) Εμπιστευτικότητας

καινοτόμος Μάθηση

ΘΕΜΑ Β

1) Εξηγήστε τους όρους «Ανάκαμψη», «Σχέδιο Συνέχειας» και «Εφεδρικό Αντίγραφο πληροφοριών» για την αποφυγή καταστροφών σε ένα πληροφοριακό σύστημα **(Μονάδες 9)**
2) Παρουσιάστε την μέθοδο παραβίασης «Άρνηση Παροχής Υπηρεσίας**» (Μονάδες 5)**
3) Να περιγράψετε τους όρους «απειλές» και «αδυναμίες» σε ένα πληροφοριακό σύστημα **(Μονάδες 6)**
4) Ποια είναι η λειτουργία του αλγορίθμου Diffie – Hellman στην ασφάλεια δικτύων ; **(Μονάδες 5)**

ΘΕΜΑ Γ

1) Να συμπληρώσετε τα παρακάτω κενά με τις διαθέσιμες λέξεις/προτάσεις, ώστε να παρουσιάζεται η λειτουργία της ασυμμετρικής κρυπτογράφησης με χρήση ψηφιακής υπογραφής **(Μονάδες 10)**

Διαθέσιμες λέξεις/προτάσεις: 1) Δημόσιο κλειδί του χρήστη Α **2)** Δημόσιο κλειδί του χρήστη Β, **3)** Ιδιωτικό κλειδί του χρήστη Α **4)** Ιδιωτικό κλειδί του χρήστη Β **5)** σύνοψη **6)** συνάρτηση κατατεμαχισμού **7)** αρχικού μηνύματος που έστειλε ο χρήστης Α **8)** ψηφιακή υπογραφή **9)** σύνοψη **10)** αποκρυπτογραφημένου μηνύματος

Παρατηρήσεις: η λέξη «σύνοψη» υπάρχει και θα χρησιμοποιηθεί δύο φορές

«Υποθέτουμε ότι ο χρήστης Α θέλει να στείλει ένα κρυπτογραφημένο μήνυμα στον χρήστη Β με χρήση Ψηφιακής Υπογραφής σε συνδυασμό με ασυμμετρική κρυπτογράφηση. Η γενική περιγραφή των βημάτων είναι η ακόλουθη »

- **Από την πλευρά του χρήστη Α γίνονται οι ακόλουθες ενέργειες:**

Βήμα 1: Ο χρήστης Α εφαρμόζει _____ στο μήνυμα και προκύπτει η σύνοψη του μηνύματος
Βήμα 2: Στη συνέχεια κρυπτογραφείται η _____ με το _____ και προκύπτει η ψηφιακή υπογραφή.
Βήμα 3: Τέλος, κρυπτογραφείται το αρχικό κείμενο με το _____. Στο κρυπτογραφημένο κείμενο προστίθεται η ψηφιακή υπογραφή, και αποστέλλεται στον χρήστη Β

- **Από την πλευρά του χρήστη Β γίνονται οι ακόλουθες ενέργειες:**

Βήμα 1: Από την στιγμή που ο χρήστης Β λαμβάνει το μήνυμα που έστειλε ο Α, αποσπάει την _____ από το κρυπτογραφημένο μήνυμα
Βήμα 2: Αποκρυπτογραφεί την ψηφιακή υπογραφή με το _____, και προκύπτει η σύνοψη του μηνύματος που έστειλε ο χρήστης Α
Βήμα 3: Αποκρυπτογραφεί το κρυπτογραφημένο μήνυμα με το _____ και προκύπτει το αρχικό μήνυμα του χρήστη Α
Βήμα 4: Εφαρμόζει συνάρτηση κατατεμαχισμού στο αποκρυπτογραφημένο μήνυμα, και προκύπτει η _____ του αποκρυπτογραφημένου μηνύματος
Βήμα 5: Τέλος συγκρίνει την σύνοψη _____ με την σύνοψη του _____.

Κοινότητα Νίκαιας

2) Σε ποιο συμπέρασμα οδηγείται ο χρήστης Β, στην περίπτωση που οι δύο συνόψεις που σύγκρινε στο Βήμα 5 είναι οι ίδιες; **(Μονάδες 10)**

3) Με ποιες από τις ενέργειες που περιγράφονται εξασφαλίζουν την εμπιστευτικότητα μεταξύ του χρήστη Α και του χρήστη Β; **(Μονάδες 5)**

ΘΕΜΑ Δ

1) Ένα αυτοδύναμο πακέτο «σπάει» σε πέντε κομμάτια. Θεωρούμε ότι σε κάθε κομμάτι η επικεφαλίδα αποτελείται μόνο από το σταθερό τμήμα της. Το τέταρτο κομμάτι έχει ΔΕΤ=300 και το πέμπτο κομμάτι έχει συνολικό μήκος=200 **Ζητούνται:**

- **a.** Ποιο είναι το μέγεθος του αρχικού αυτοδύναμου πακέτου, καθώς και καθενός από τα πέντε πακέτα; Να αιτιολογήσετε την απάντησή σας **(Μονάδες 9)**;
- **b.** Από τις τιμές ποιων δεικτών της επικεφαλίδας του πακέτου καταλαβαίνουμε ποιο είναι το πρώτο και το τελευταίο κομμάτι; **(Μονάδες 3);**

2) Δίνεται η IP 160.20.2.17 και η Μάσκα Υποδικτύου 255.255.255.240. Να απαντήσετε στις παρακάτω ερωτήσεις

- **a.** Πόσα Bits είναι διαθέσιμα για το μέρος δικτύου και πόσα για τους υπολογιστές; Να αιτιολογήσετε την απάντησή σας **(Μονάδες 3)**
- **b.** Ποια είναι η διεύθυνση υποδικτύου; Να αιτιολογήσετε την απάντησή σας **(Μονάδες 3)**
- **c.** Ποια είναι η multicast διεύθυνση του υποδικτύου; Να αιτιολογήσετε την απάντησή σας **(Μονάδες 4)**
- **d.** Ποια είναι η πρώτη και η τελευταία διαθέσιμη IP διεύθυνση για τους υπολογιστές**; (Μονάδες 3)**

ΚΑΛΗ ΕΠΙΤΥΧΙΑ !!!!!!!!

Καινοτόμος Μάθηση