המכללה
הטכנולוגית
באר שבע
בשיתוף WORLD ORT
קדימה מדע

שאלה 1: (20 נק')

מרגל מצליח לשים את ידו על ההודעה המוצפנת (ciphertext) הבאה:

TBBQNSGREABBAFGHQRAGF!

אין ברשותו של המרגל מפתח כדי לפענח את ההודעה, אך הוא יודע שההודעה הוצפנה באמצאות צופן הזזה.

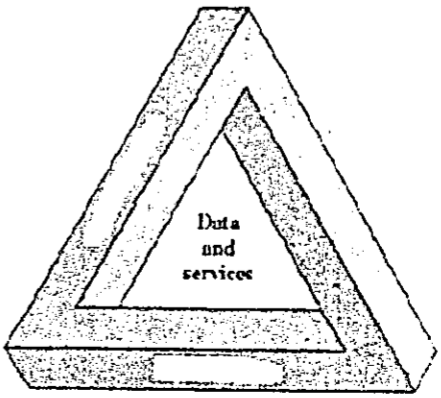
מהי ההודעה שהוצפנה (plaintext) ומהו המפתח בו היא הוצפנה?

בסוף לשתובה, יש להסביר במילים (לא יותר מ-2 שורות) כיצד שברתם את הצופן.

תשובה:

שאלה 2: (20 נק')

באיור הבא מופיע משולש דרישת אבטחה.



The Security Requirements Triad

מהן שלושת הדרישות האבטחה?

נא להסביר בקצרה למה הן חשובות. האם ייתכן שבתוכנה כלשהי תחסור אחת מהדרישות (או כמה מהן)? יש לתת דוגמא לכך.

תשובה:

שאלה 3: (20 נק')

התקפות בטיחות מתחלקות להתקפות אקטיביות (active attacks) והתקפות פסיביות (passive attacks).

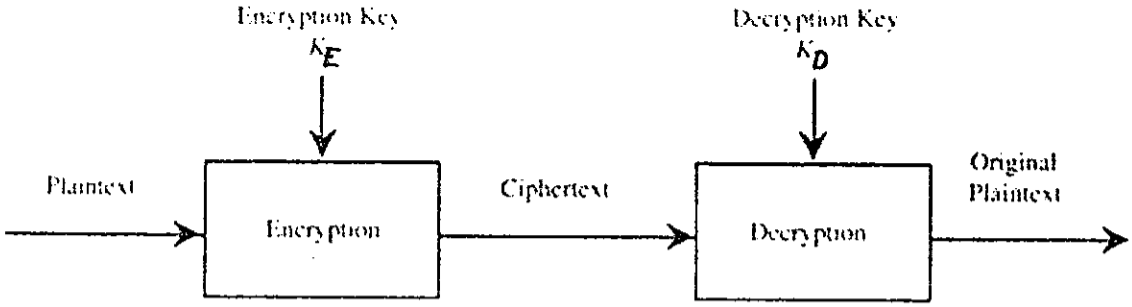
המכללה
הטכנולוגית
באר שבע
בשיתוף WORLD ORT
קדימה מדע

נא להסביר בקצרה מהי התקפת Denial of Service (DoS), ולאיזה סוג ההתקפה היא שייכת.

תשובה:

שאלה 4: (20 נק')

נא להסביר איזה סוג קריפטוגרפיה (סימטרית / אסימטרית) מתוארת באיור הבא:



נא לתת דוגמא להצפנה זו (אילו אלגוריתמים קיימים). נא להסביר מהם יתרונות בשימוש בהצפנה זו.

תשובה:

שאלה 5: (20 נק')

באיזה אלגוריתם הצפנה משתמשים על מנת לשמור סיסמא של המשתמש בבסיס נתונים?

מה יתרון של האלגוריתם הזה לאומת אלגוריתמם הצפנה אחר?

מה חסרון של האלגוריתם הזה לאומת אלגוריתמם הצפנה אחר?

תשובה: