מחוון לבודקים- תרגיל סוקטים מוצפנים

הבדיקה מורכבת משלב ראשון של מעבר על הקוד ווידוא שכל החלקים ישנם, יש לתת ניקוד לפי הפירוט הבא.

בשלב השני הרצת הקוד ובדיקות, כאשר על כשלון מורידים ניקוד לפי הפירוט.

1. יצירת הצפנה סימטרית מבוססת מפתח- 20 נקודות
   1. הפונקציה protocol.symetric\_encryption ממומשת ללא שגיאות
   2. נעשה בה שימוש הן בשרת והן בלקוח, הן בשליחה והן בקבלה
2. מימוש החלפת מפתח סימטרי באמצעות דיפי הלמן – 30 נקודות
   1. מימוש 3 הפונקציות שמחשבות את דיפי הלמן בפרוטוקול
   2. יישום חישוב סוד משותף הן בשרת והן בלקוח
3. מימוש פונקציית גיבוב – 20 נקודות
   1. מימוש פונקציית גיבוב של 16 ביט
4. מימוש חתימה ו-MAC באמצעות שילוב גיבוב ומפתח פרטי – 30 נקודות
   1. מימוש אלגוריתם RSA ומציאת שני צמדים של מפתח ציבורי+פרטי- אקבל גם פתרונות שהשתמשו במודולים חיצוניים כדי ליצור צמד מפתחות
   2. החלפת המפתחות הציבוריים בין הצדדים
   3. שימוש בפונקציה שמחשבת את ה-MAC ובודקת שהמסר מתאים ל-MAC גם בשרת וגם בלקוח

בדיקות

1. תקינות- לשלוח מספר הודעות ולראות שעובר תקין. אם יש קריסה או שהשרת לא עונה על כולן– מינוס 30
2. סגירת הלקוח באמצעות EXIT, השרת צריך לסיים פעולה בלי לקרוס – מינוס 10
3. לשנות את ה-MAC רק בצד אחד ולראות שיש שגיאה – אם אין הודעה על אי התאמה – מינוס 10 (הבדיקה תתבצע רק בהנחה שבדיקת התקינות הרגילה עברה בהצלחה)