**עבודה מס׳ 1, חלק ב׳**

שאלה 3:

שאלה 4:

1. במקרה זה, איב יכולה לגרום לאליס לחשוב שהיא בוֹב וּלבוֹב לחשוב שהיא אליס, כלומר ליירט את העברת המפתחות הפומביים. אם נלך לפי התרשים המצורף לעבודה וסימוניו, איב תיירט מאליס את ומבוב את . כתשובה לכל אחד מהם היא תשלח את כך שכתוצאה מכך לאליס ולאיב יהיה מפתח סימטרי , ולאליס ולבוב יהיה מפתח סימטרי . כתוצאה מכך, איב תוכל ליירט מאליס ובוב את ההודעות בצורה ב״ת ולעשות כרצונה.
2. בהתבסס על הסעיף הקודם, איב מבצעת את אותה התחבולה במהלך שלב 1 של התהליך. לכן למעשה כאשר שלב 1 מסתיים איב כולה לראות כל הודעה מוצפנת שעוברת בין אליס לבוב ולהפך. כל מה שנשאר לאיב הוא להמשיך להעביר את ההודעות מאליס לבוב ובחזרה כאילו היא לא שם, כלומר, **מבלי לשנות דבר** (חוץ מההצפנה, איב תפענח את ותצפין מחדש את ההודעה עם ולהפך) וכאשר אליס ובוב השתכנעו בסוף התהליך שהשיחה ביניהם אכן פרטית ושמדובר בזהות האמיתית של כל אחד מהם איב תוכל להיכנס לפעולה ולבצע ככל הועלה על רוחה.
3. השינויים הם כאלה:  
   נסמן: , משלבים 2 ו-3 בהתאמה.  
   השינוי שצריך להתבצע הוא שבשלב 2 ההודעה תהיה: ובשלב 3 ההודעה תהיה: . שינוי זה יימנע מאיב לשנות את ההודעה (כלומר, לפענח את ההצפנה לפי המפתח הפרטי של אליס בעזרת המפתח הפומבי שהיא חולקת עם אליס, להצפין את ההודעה מחדש ע״י המפתח שהיא חולקת עם בוב ולשלוח לבוב) ולהשאיר את נוכחותה מוסתרת כי הרי יצירת החתימה מתבצעת ע״י המפתחות הפרטיים של אליס ובוב אשר לא ידועים לאיב ולכן איב לא יכולה לגעת ולשנות את החתימה כנדרש כדי למנוע את גילויה.

שאלה 5:

1. השרת יודע שמרצה אכן שלח לו בקשה ולא סטודנט ע״י ההודעה השלישית. רק מרצה יוכל לפענח את ההודעה השנייה כראוי, לראות את RANDS ולשלוח אותו בהודעה השלישית (זה בעצן סוג של אתגר של השרת שהמרצה צריך לענות עליו).
2. הוא יכול ליירט את ההודעה הראשונה, השניה וגם את השלישית ובעזרת ברוט פורס למצוא מפתח שיתאים להודעת RSA מוצפנת מהפורמט הבא (RANDS|RANDL|StudentID|Grade) וגם להודעה (RANDS|RANDL) וגם (RANDL) את הסייפר של שניהם יש לו ולכן הוא יכול להשוות, מכיוון שתעודת זהותו וציונו ידוע המשתנים הם: RANDS+RANDL

ולכן כדי לנחש את קבוצת הפתרונות שמתאימים ל RANDL ייקח לו 228 ניסיונות שכל ניסיון יארך כזמן ריצת RSA. נקרא לגודל קבוצת הפתרונות הנכונים X.

כדי למצוא את RANDL אנו צריכים גם לרוץ על כל הקומבינציות וזה יארך כפול זמן חישוב של RSA.

לאחר מכן את קבוצת הפתרונות הנכונים נשמור כ Y.

לבסוף ישרש הסטודנט עבור כל קומבינציה ב-Y עם הת.ז והציון ויצפין עם המפתח המתאים לקומבינציה ולכל היותר ייקח לו Y ריצות RSA מרחב הפתרונות הינו Z.  
הזיכרון הדרוש הינו X+Y.  
הערה : לאחר שהצליח בחישוב קיים סיכוי להתנגשות (2 מפתחות או 2 מספרים מקריים שההצפנה שלהם יצאה זהה למרות שהם שונים) הסיכוי שדבר כזה יקרה הוא אחד חלקי Z שכן זה נדיר מאוד ובמקרה שכזה השרת לא יקבל את הבקשה.  
ובסיכוי1-P(Z) השרת יקבל את הבקשה.

שאלה 6:

1. ראשית, חישבנו באופן ידני את השפעת AES3\* על המטריצה המייצגת את המידע. לאחר מכן, מיפינו את מיקום המפתחות מכל אחד משלוש המפתחות בפלט הסופי כפי שנלמד בתרגול. לאחר מכן, עשינו את הפעולה ההפוכה, כלומר, ביטלנו את התוכן המקורי מהסייפר כך שהשארנו בכל תא את הערך השווה ל-xor(k1, k2, k3). לכל ערך שכזה מצאנו שלושה מס׳ שה-xor ביניהם שווה לערך ע״י פ׳ הזהות.