שאלון בקורס "**מבוא לקריפטוגרפיה**" – 20580

מרכז הוראה: ד"ר יהודה לינדל

סמסטר א' תשס"ז, מועד א'2

<u>הערות</u>:

1. המבחן עם חומר פתוח, מותר להשתמש בכל כלי עזר.
2. משך הבחינה: שלש שעות.
3. ענו על כל השאלות.

שאלה 1 (20 נקודות)

נסתכל על הגרסה הבאה של הצופן האפיני (Affine): לפני הצפנת הטקסט הגלוי נסלק ממנו את כל מופעי האותיות a,e,i ואז נעבוד מודולו 23 (כיוון שנותרו רק 23 אותיות בטקסט הגלוי) במקום מודולו 26 כמקובל. (ההנחה היא שטקסט באנגלית ניתן להבנה ולשחזור מלא גם אם מסלקים ממנו את התנועות a,e,i).

האם שינוי זה מעלה או מוריד את בטיחות הצופן האפיני המקורי? התייחסו גם להתקפות על ידי חיפוש בכל מרחב המפתחות וגם להתקפות קריפטאנליטיות מתוחכמות יותר (הכוונה היא להתקפות "ידניות" ללא שימוש במחשב).

שאלה 2 (20 נקודות)

א. בצופן החד-פעמי (One Time Pad או Vernam's cipher), אם מצפינים באמצעות המפתח המורכב כולו מאפסים, $K = 0^n$, אז $e_K(x) = x$. לפיכך, מוצע לשפר את הצופן החד-פעמי על ידי כך שתמיד נצפין באמצעותו על ידי שימוש במפתחות $K \neq 0^n$. (כלומר, נגריל מפתח אקראי ממרחב המפתחות $\{0,1\}^n$ ואם יוצא המפתח המורכב כולו מאפסים, נגריל שוב עד שנקבל מפתח $K \neq 0^n$.) האם גרסה זו של הצופן החד-פעמי מהווה שיפור? בפרט, האם היא עדיין בעלת סודיות מושלמת? הוכיחו את טענותיכם. אם טענתכם היא שגם הגרסה הזו עדיין בעלת בטיחות מושלמת - הסבירו מדוע הצופן החד-פעמי איננו מתואר כך. אם טענתכם היא שגרסה זו פחות בטוחה מהצופן החד-פעמי, כיצד ניתן ליישב זאת עם העובדה שבצופן החד-פעמי יש מקרים בהם ההצפנה איננה משנה את הטקסט הגלוי.

ב. הצפנת Double-DES איננה בטוחה מספיק, אך הצפנת Triple-DES עם שני מפתחות היא בעלת בטיחות מספקת. נציע כעת שתי שיטות של Triple-2DES המשתמשות בשני מפתחות. זכרו ש:

$$2DES_{k_1,k_2}(x) = DES_{k_2}\left(DES_{k_1}(x)\right)$$

השיטה האחת היא:

$$6DES_{k_1,k_2}(x) = 2DES_{k_1,k_2}\left(2DES^{-1}_{k_1,k_2}\left(2DES_{k_1,k_2}(x)\right)\right)$$

השיטה השנייה היא:

$$6DES_{k_1,k_2}(x) = 2DES_{k_1,k_2}\left(2DES_{k_1,k_2}\left(2DES_{k_1,k_2}(x)\right)\right)$$

נתחו את בטיחותן של שתי השיטות האלה.

שאלה 3 (20 נקודות)

א. מה תהיה בטיחות שיטת AES אם נדלג בה על כל פעולות ה- ShiftRows ו- MixColumns?
(כלומר, כל יתר מרכיבי הצופן יישארו, רק שבכל מקום בו היינו צריכים לעשות פעולת ShiftRows או MixColumns לא נעשה זאת).

ב. מהי תהיה בטיחות שיטת AES אם נדלג בה על כל פעולות ה-AddRoundKey?

הצדיקו את תשובותיכם בפרוטרוט.

שאלה 4 (20 נקודות)

בגישה המקובלת לחתימה, מפעילים על ההודעה המיועדת לחתימה פונקצית תמצות (hash) חסינת-התנגשויות ואחר כך מחשבים את החתימה על ערך התמצות שמתקבל. נניח שבחרנו להשתמש בפונקצית תמצות חלשה. תארו "התקפות מעניינות" (דהיינו - יעילות, מעשיות ומזיקות ככל האפשר) בכל אחד משלושה המקרים הבאים:

א. פונקצית התמצות איננה חסינת-התנגשויות (collision resistant) אך חסינה כנגד מציאת מקור שני (second preimage resistant).

ב. פונקצית התמצות איננה חסינה כנגד מציאת מקור שני אך היא חסינה כנגד מציאת מקור (preimage resistant).

ג. פונקצית התמצות איננה אפילו חסינה כנגד מציאת מקור.

אתם רשאים להניח שפונקצית החתימה היא RSA (אך הנחה זו איננה חיונית).

שאלה 5 (20 נקודות)

במקום להשתמש בסכמת הסף של שמיר לשיתוף סודות, מוצע לנקוט בגישה הבאה: כל אחד מ- w המשתתפים מקבל זוג מפתחות פומבי ופרטי של RSA. כלומר, המשתתף P_i מקבל מפתח פומבי pk_i ומפתח פרטי (סודי) sk_i. כעת, על מנת לשתף סוד s בין w המשתתפים כך שכל קבוצה של t (או יותר) משתתפים תוכל לשחזרו אך קבוצה קטנה יותר לא תוכל, אנו מבצעים את הפעולות הבאות: לכל תת-קבוצה של t משתתפים, אנו מצפינים את הסוד s על ידי המפתחות של כל t המשתתפים (כלומר, הסוד s מוצפן t פעמים בזו אחר זו לכל תת-קבוצה נתונה בגודל t). לבסוף, אנו מפיצים לכל המשתתפים את כל ה- $\binom{w}{t}$ ערכים מוצפנים שקיבלנו.

המשך השאלה בעמוד הבא

א. האם לשיטה זו יש אותה בטיחות כמו לסכמת הסף של שמיר (הכוונה היא לבטיחות ערכו של הסוד מפני תת-קבוצות שגודלן פחות מ- t)?

ב. האם שיטה זו בטוחה דיה (גם כאן הכוונה היא לבטיחות ערכו של הסוד מפני תת-קבוצות שגודלן פחות מ- t)?

ג. האם יש יתרונות לשיטה זו? רמז: חשבו על מצב של משתתף לא הגון בסכמת הסף המקורית של שמיר המשקר ביחס לערך של המנה (share) שלו.

ד. מדוע שיטה זו איננה מומלצת בדרך כלל לשימוש?

בהצלחה !