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

מרכז הוראה: ד"ר יהודה לינדל

סמסטר א' תשס"ז, מועד א'1

<u>הערות</u>:

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

שאלה 1 (20 נקודות)

הוכיחו או הפריכו:

נתונה הצפנת בלוק שבה גודל המפתח שווה לגודל הבלוק והמפתח נבחר בהסתברות אחידה מתוך מרחב המפתחות. אז להצפנה זו יש סודיות מושלמת אם המפתח משמש להצפנת בלוק אחד בלבד.

שאלה 2 (20 נקודות)

בסכימת הצפנה מסוג SPN (רשת החלפה-תמורה) יש Nr שלבים. בכל שלב מבצעים XOR של התת-מפתח המתאים לשלב זה עם ערך הביניים המהווה את הקלט לשלב הזה, אחר כך מבצעים פעולת החלפה ולבסוף תמורה.

נציע כעת גרסה אחרת של רשת החלפה-תמורה: בשיטה המוצעת אנו ראשית עושים XOR של הטקסט הגלוי עם Nr תת-מפתחות (כלומר, Nr פעולות XOR בזו אחר זו), לאחר מכן עושים Nr פעולות החלפה בזו אחר זו, ולבסוף מבצעים Nr תמורות בזו אחר זו.

א. נתחו את בטיחות שיטת ההצפנה המוצעת כאשר כל Nr פעולות ההחלפה הן זהות וכל Nr התמורות הן זהות.

ב. נתחו את בטיחות שיטת ההצפנה המוצעת כאשר יש Nr פעולות החלפה שונות ו- Nr תמורות שונות.

בכל אחד משני הסעיפים לעיל, הצדיקו את תשובתכם אם אתם טוענים שהשיטה בטוחה, או תארו בפרוטרוט התקפה מוצלחת אם אתם טוענים שהשיטה איננה בטוחה.

שאלה 3 (20 נקודות)

נגדיר פונקצית דחיסה $c:\{0,1\}^{112}\to\{0,1\}^{64}$ על ידי Double-DES באופן הבא:

$$c(x_1,x_2)=DES_{x_2}(DES_{x_1}(0)).$$

א. תארו התנגשות עבור פונקצית דחיסה זו (רמז: מפתחות חלשים של DES).

ב. בכמה זמן ניתן למצוא מקור (preimage) עבור פונקצית דחיסה זו. כלומר, בהינתן $y\in\{0,1\}^{64}$, בכמה זמן ניתן למצוא $(x_1,x_2)\in\{0,1\}^{112}$ כך ש: $c(x_1,x_2)=y$? האם ניתן למצוא מקור y שכזה שהוא "בעל משמעות" (למשל, מילה באנגלית) ולא סתם רצף ביטים חסרי-פשר?

ג. נניח שנשתמש בפונקצית הדחיסה c שתוארה לעיל במסגרת בניית מרקל-דמגרד של פונקציות תמצות. מה תהיינה ההשלכות על בטיחותה של פונקצית התמצות שתתקבל?

שאלה 4 (20 נקודות)

מוצע להשתמש ב- RSA להצפנת כל תו באנגלית בנפרד. נתחו את בטיחות השיטה המוצעת בכל אחד משלושה המימושים הבאים של השיטה:

א. הצפנת RSA פשוטה: כל תו x (שהוא אחד מ- 26 אותיות האלפבית האנגלי) מוצפן כ- $x^e \bmod N$.

ב. בוחרים 26 מחרוזות אקראיות ארוכות, $r_A, r_B, \ldots, r_Z$, ואז מצפינים את התו x על ידי כך שקודם משרשרים אליו את המחרוזת r_x ורק אז מפעילים את הצפנת RSA. (למשל, בהצפנת האות A תמיד נשרשר אל הערך x שמייצג אות זו את המחרוזת r_A ואז נפעיל על התוצאה המתקבלת את הצפנת RSA.)

ג. כמו במימוש הקודם, רק שבכל הצפנה של תו חדש משתמשים במחרוזת אקראית r חדשה ובלתי תלויה במחרוזות בהן השתמשנו להצפנת התווים הקודמים.

שאלה 5 (20 נקודות)

א. הראו שבחתימות RSA (שיטה 7.1 בספר, עמוד 276), אם נתונות חתימות על שתי הודעות x_1 ו- x_2 אז ניתן למצוא חתימה על $\left(x_1^j \cdot x_2^k\right) \bmod N$ לכל שני מספרים טבעיים j, k. רשמו אלגוריתם מדויק לביצוע החישוב לעיל ונתחו את זמן הריצה שלו.

ב. הראו שבהינתן הצפנת אל-גמאל של ערך x **שאיננו ידוע** ניתן לחשב את הצפנת אל-גמאל של $10x$ (הכוונה ב- $10x$ היא לכפל ב- 10 בתוך החבורה המתאימה. למשל, בהצפנת אל-גמאל מודולו ראשוני p אז הכוונה היא ל- $10x \bmod p$).

ג. נדון בחתימת RSA (המשולבת עם hash) שבה במקום לחתום עם (a, N) ולוודא חתימה עם (b, N), נחתום עם (b, N) ונוודא חתימה עם (a, N). האם זה רעיון טוב? הצדיקו את תשובותיכם.

בהצלחה !