אוניברסיטת בן-גוריון בנגב
Ben-Gurion University of the Negev

קריפטוגרפיה - מועד א'

202-1-5351
סמסטר א' תשס"ה
4.2.2005

הנחיות:

1. בטופס הבחינה שלושה דפים מלבד דף זה. ודאו כי כולם נמצאים בידכם.
2. בבחינה 4 שאלות שמשקלן שווה. יש לענות על כולן.
3. הבחינה עם חומר פתוח.
4. נמקו את כל תשובותיכם. פתרון ללא הוכחה לא יתקבל.
5. משך הבחינה 3 שעות.
6. מומלץ לא להתעכב זמן רב מדי על שום סעיף.
7. הנכם רשאים להסתמך על סעיפים קודמים, גם אם לא השבתם עליהם.
8. מותר להסתמך על משפטים שהוכחו בהרצאות, אך יש לצטט אותם במדויק.
9. אם אתם מסתמכים על טענות שהוכחו בתרגילי בית יש להוכיח אותם.
10. **במידה ואינכם יודעים את התשובה לסעיף כלשהו, רשמו "לא יודעים" ותזכו ב- 20% מניקוד הסעיף.**

בהצלחה!

שאלה 1 [25 נקודות]

בהרצאה הגדרנו את מערכת DES -כפול המוגדרת בצורה הבאה:

$$\mathrm{DDES}(M,k_1,k_2)=\mathrm{DES}(\mathrm{DES}(M,k_1),k_2),$$

כאשר $M\in\{0,1\}^{64}$ ו- $k_1,k_2\in\{0,1\}^{56}$. הראינו כי קיימת התקפת הודעה נתונה על המערכת הדורשת $2\cdot 2^{56}$ הפעלות של DES, זיכרון $2\cdot 64\cdot 2^{56}$ ביטים וזמן חישוב נוסף בסדר גודל של 2^{56}. בשאלה זו נראה איך לחסוך בזיכרון הנדרש תוך תשלום במספר ההפעלות של DES.

סעיף א [4 נקודות]

נניח כי ידוע שהביט הראשון של k_1 והביט הראשון של k_2 הם 0. הראו כי במקרה זה קיימת התקפת הודעה נתונה על המערכת הדורשת $2\cdot 2^{55}$ הפעלות של DES, זיכרון $2\cdot 64\cdot 2^{55}$ ביטים, וזמן חישוב נוסף בסדר גודל של 2^{56}.

סעיף ב [12 נקודות]

יהי $0<s<56$. נניח כי ידועים s הביטים הראשונים של k_1. הראו כי במקרה זה קיימת התקפת הודעה נתונה על המערכת הדורשת $2^{56}+2^{56-s}$ הפעלות של DES, זיכרון $2\cdot 64\cdot 2^{56-s}$ ביטים וזמן חישוב נוסף בסדר גודל של 2^{56}.
<u>הערה</u>: ניתן להשתמש באותו זיכרון מספר פעמים.

סעיף ג [9 נקודות]

יהי $0<s<56$. הראו כי קיימת התקפת הודעה נתונה על המערכת הדורשת $2^{56}+2^{56+s}$ הפעלות של DES, זיכרון $2\cdot 64\cdot 2^{56-s}$ ביטים וזמן חישוב נוסף בסדר גודל של 2^{56+s}.

שאלה 2 [25 נקודות]

בשאלה זו נראה כי אם מאזין מצליח להשיג את המפתח הפרטי במערכת RSA, אזי הוא יכול לפרק את N. פורמאלית, יהיו p ו- q מספרים ראשוניים גדולים מ-2 ושונים זה מזה, $N=pq$, ויהיו $e,d\in\mathbb{Z}^*_{\varphi(N)}$ כך ש- $ed\equiv 1 \pmod{\varphi(N)}$ ו- $e,d>1$. נניח כי המאזין מחזיק ב- N,e,d.

סעיף א [5 נקודות]

הראו איך המאזין יכול בצורה יעילה למצוא מספר $k\neq 0$ שהוא כפולה של $\varphi(N)$.

סעיף ב [2 נקודות]

הוכיחו כי אם $k\neq 0$ הוא כפולה של $\varphi(N)$, אזי קיימים $t\geq 1$ ו- r אי-זוגי כך ש- $k=2^t r$.

סעיף ג [9 נקודות]

נניח כי המאזין מחזיק ב- N,e,d ו- מספר $k=2^t r$ שהוא כפולה של $\varphi(N)$. הראו איך לכל $a\in\mathbb{Z}^*_N$ כך ש- $a^r\not\equiv 1 \pmod N$ מאזין יכול למצוא בצורה יעילה מספר T כך ש- $a^{2T}\equiv 1 \pmod N$ אולם $a^T\not\equiv 1 \pmod N$.

סעיף ד [9 נקודות]

נניח כי התמזל מזלנו ו- a מסעיף ג מקיים בנוסף $a^T\not\equiv -1 \pmod N$. הראו איך המאזין יכול במקרה זה לפרק את N בזמן פולינומי.
הערת אגב: אם נגריל $a\in\mathbb{Z}^*_N$ באקראי, אז בהסתברות לפחות $1/2$ יתמזל מזלנו.

שאלה 3 [25 נקודות]

תהי $h:\{1,...,N^2\}\to\{1,...,N\}$ פונקציה hash. נסמן ב- s_a, עבור $a\in\{1,...,N\}$, את **גודל** הקבוצה $\{x:h(x)=a\}$. בהרצאה הראינו כי אם $s_a=N$ לכל $a\in\{1,...,N\}$, אזי צריך $O(\sqrt{N})$ הפעלות של הפונקציה h כדי למצוא התנגשות. בשאלה זו נראה זהו המקרה עבורו בדרש המספר הגדול ביותר של הפעלות של הפונקציה h על מנת למצוא התנגשות.

סעיף א [6 נקודות]

נניח כי $s_1=N^2/4$, כלומר אם נגריל $x\in\{1,...,N^2\}$ באקראי אזי $h(x)=1$ בהסתברות $1/4$. מהי במקרה זה ההסתברות שאם נגריל t איברים באקראי מתוך $\{1,...,N^2\}$ ונחשב את ערך הפונקציה h עבורם, נמצא לפחות שני איברים x_1 ו- x_2 כך ש- $h(x_1)=h(x_2)=1$?

סעיף ב [11 נקודות]

תהי $h':\{1,...,N^2\}\to\{1,...,N\}$ פונקציה hash כך ש- $s_1>s_2+1$ ויהי x_1 כך ש- $h'(x_1)=1$. נגדיר h בצורה הבאה:

$$h(x)=\begin{cases}2 & \text{if } x=x_1\\ h'(x) & \text{otherwise}\end{cases}.$$

כלומר, שינינו את h' בדיוק בנקודה אחת.

נסתכל על שני ניסויים. בניסוי הראשון נגריל t איברים באקראי מתוך $\{1,...,N^2\}$ ונחשב את ערך הפונקציה h עבורם. הניסוי יצליח אם הגרלנו לפחות שני איברים x_1 ו- x_2 כך ש- $h(x_1)=h(x_2)$. בניסוי השני נגריל t איברים באקראי מתוך $\{1,...,N^2\}$ ונחשב את ערך הפונקציה h' עבורם. הניסוי יצליח אם הגרלנו לפחות שני איברים x_1 ו- x_2 כך ש- $h'(x_1)=h'(x_2)$. הראו כי סיכויי ההצלחה בניסוי השני גבוהים יותר.

<u>הדרכה</u>: השוו בין מספר הסדרות באורך t בהם יש התנגשות ב- h לבין מספר הסדרות בהם יש התנגשות ב- h'. שימו לב כי בשני המקרים מספיק להסתכל על סדרות בהם x_1 מופיע.

סעיף ג [8 נקודות]

יהיו $h,h':\{1,...,N^2\}\to\{1,...,N\}$ פונקציות hash כך שעבור h מתקיים $s_1=s_2=\ldots=s_N=N$ ועבור h' לא מתקיים שוויון זה. נסתכל על שני ניסויים כמו בסעיף הקודם. כלומר, בניסוי הראשון נגריל t איברים באקראי מתוך $\{1,...,N^2\}$ ונחשב את ערך הפונקציה h עבורם. הניסוי יצליח אם הגרלנו לפחות שני איברים x_1 ו- x_2 כך ש- $h(x_1)=h(x_2)$. בניסוי השני נגריל t איברים באקראי מתוך $\{1,...,N^2\}$ ונחשב את ערך הפונקציה h' עבורם. הניסוי יצליח אם הגרלנו לפחות שני איברים x_1 ו- x_2 כך ש- $h'(x_1)=h'(x_2)$. הראו כי סיכויי ההצלחה בניסוי השני גבוהים יותר.

שאלה 4 [25 נקודות]

בשאלה זו נתכנן פרוטוקול Private Information Retrieval (PIR) עבור 4 שרתים בו סיבוכיות התקשורת היא $O\left(n^{1/3}\right)$.

סעיף א [10 נקודות]

יהי $0<\alpha<1$. תכננו פרוטוקול PIR עבור 2 שרתים בו סיבוכיות התקשורת מהמשתמש לשרתים היא $O\left(n^{\alpha}\right)$ וסיבוכיות התקשורת מהשרתים למשתמש היא $O\left(n^{1-\alpha}\right)$, כך שהמשתמש זקוק לביט אחד בלבד מהתשובה של כל שרת.

סעיף ב [15 נקודות]

תכננו פרוטוקול PIR עבור 4 שרתים בו סיבוכיות התקשורת הכוללת היא $O\left(n^{1/3}\right)$. הקפידו על תיאור מדויק של הפרוטוקול והוכיחו את תכונותיו.

הדרכה: השתמשו בפרוטוקול מהסעיף הקודם באופן רקורסיבי.