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

קריפטוגרפיה - מועד ב'

202-1-5351
סמסטר א' תשס"ה
18.2.2005

הנחיות:

1. בטופס הבחינה שלושה דפים מלבד דף זה. ודאו כי כולם נמצאים בידכם.
2. בבחינה 3 שאלות שמשקלן איננו 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 [35 נקודות]

נסמן $\mathrm{DES}_k(M)=\mathrm{DES}(M,k)$. בהרצאה הגדרנו את מערכת DES-משולש המוגדרת בצורה הבאה:

$$\mathrm{TDES}(M,\langle k_1,k_2,k_3\rangle)=\mathrm{DES}_{k_3}(\mathrm{DES}_{k_2}(\mathrm{DES}_{k_1}(M))),$$

כאשר $M\in\{0,1\}^{64}$ ו-$k_1,k_2,k_3\in\{0,1\}^{56}$. נניח כי עבור זוג $\langle M,C\rangle$ קיימת שלשה אחת k_1,k_2,k_3 לכל היותר המקיימת $\mathrm{TDES}(M,\langle k_1,k_2,k_3\rangle)=C$ (הנחה זו היא פישוט של המציאות).

סעיף א [8 נקודות]

הראו כי קיימת התקפת הודעה נתונה על TDES הדורשת $2^{56}+2^{112}$ הפעלות של DES, זיכרון $64\cdot(2^{56}+2^{112})$ ביטים, וזמן חישוב נוסף בסדר גודל של 2^{112}.

סעיף ב [9 נקודות]

בשלושת הסעיפים הבאים נתייחס למערכת TDES בה $k_1=k_3$, כלומר למערכת 'TDES הבאה:

$$\mathrm{TDES}'(M,\langle k_1,k_2\rangle)=\mathrm{DES}_{k_1}(\mathrm{DES}_{k_2}(\mathrm{DES}_{k_1}(M))).$$

מאזין יודע מהו k_1. הראו איך ע"י התקפת <u>הודעה נבחרת</u> המאזין יכול למצוא זוג $\langle M,C\rangle$ המקיים $\mathrm{DES}_{k_1}(M)=0^{64}$ ו-$\mathrm{TDES}'(M,\langle k_1,k_2\rangle)=C$.

סעיף ג [9 נקודות]

מאזין יודע מהו k_1 ובידו זוג $\langle M,C\rangle$ המקיים $\mathrm{DES}_{k_1}(M)=0^{64}$ ו-$\mathrm{TDES}'(M,\langle k_1,k_2\rangle)=C$. הראו איך ע"י $2\cdot2^{56}$ הפעלות של DES, המאזין יכול למצוא את k_2.

סעיף ד [9 נקודות]

הראו התקפת הודעה נבחרת על 'TDES הדורשת 2^{56} הצפנות 'TDES של הודעות נבחרות, $3\cdot2^{56}$ הפעלות של DES, זיכרון $2\cdot64\cdot2^{56}$ ביטים וזמן חישוב נוסף בסדר גודל של 2^{56}.

שאלה 2 [35 נקודות]

בשאלה זו נראה אלגוריתם אקראי הבודק אם מספר k כך ש- $k \equiv 3 \pmod 4$ הוא ראשוני. רעיון האלגוריתם הוא להגריל מספר $a \in \mathbb{Z}_k^*$, לעלות אותו בריבוע מודולו k ולהוציא שורש מודולו k. אם קיבלנו מספר ששונה מ- $\pm a$ אזי k פריק, אחרת כנראה k ראשוני.

סעיף א [9 נקודות]

יהי $k = k_1 k_2$ מספר אי-זוגי כך ש- $\gcd(k_1, k_2) = 1$ ו- $k_1, k_2 > 1$. הראו כי לכל $b \in \mathrm{QR}_k$ יש לפחות 4 שורשים שונים זה מזה.

סעיף ב [9 נקודות]

יהי $k = k_1 k_2$ מספר אי-זוגי כך ש- $\gcd(k_1, k_2) = 1$ ו- $k_1, k_2 > 1$. עבור i טבעי נגדיר את הפונקציה $f(a) = a^{2i} \bmod k$.

הראו כי

$$\left|\{a \in \mathbb{Z}_k^* : f(a) \equiv \pm a \pmod k\}\right| \le \frac{\left|\mathbb{Z}_k^*\right|}{2}.$$

סעיף ג [9 נקודות]

נסתכל על האלגוריתם הבא:

קלט: מספר k כך ש- $k \equiv 3 \pmod 4$.

1. אם קיים m טבעי ו- $i > 1$ כך ש- $k = m^i$ החזירו k פריק ועצרו (ניתן לממש שלב זה ביעילות).
2. הגרילו $a \in \mathbb{Z}_k$ כך ש- $a \neq 0$. אם $\gcd(a, k) \neq 1$ החזירו k פריק ועצרו.
3. חשבו $b \leftarrow a^2 \bmod k$ ו- $c \leftarrow b^{(k+1)/4} \bmod k$.
4. אם $c \not\equiv \pm a \pmod k$ החזירו k פריק ועצרו.
5. החזירו k ראשוני ועצרו.

הוכיחו כי אם k הוא ראשוני כך ש- $k \equiv 3 \pmod 4$, אזי האלגוריתם יחזיר תמיד כי k ראשוני.

סעיף ד [8 נקודות]

הוכיחו כי אם k הוא פריק, אזי האלגוריתם יחזיר בהסתברות לפחות $1/2$ כי k פריק.

שאלה 3 [30 נקודות]

סעיף א [6 נקודות]

נסתכל על הפרוטוקול PIR שתואר בכיתה עם 2 שרתים וסיבוכיות תקשורת $O\left(n^{1/2}\right)$. הראו כי אם שני השרתים משתפים פעולה אזי הם יכולים ללמוד מידע על הביט שהמשתמש מבקש. הסבירו תשובתכם בקצרה.

סעיף ב [8 נקודות]

נאמר כי פרוטוקול PIR עם k שרתים הוא t–פרטי אם כל t שרתים שמשתפים פעולה לא ילמדו מידע על הביט שהמשתמש מבקש. בסעיפים הבאים נתכנן פרוטוקול PIR 2–פרטי עם 3 שרתים.

תחילה נתכנן פרוטוקול בו סיבוכיות התקשורת מהמשתמש לשרתים היא $O(n)$ וסיבוכיות התקשורת מכל שרת למשתמש היא 1. נתאר כיצד המשתמש מכין את השאילתות שלו.

המשתמש רוצה הביט ה- i מתוך מסד נתונים בגודל n.
המשתמש מגריל שתי קבוצות אקראיות $A_1, A_2 \subseteq \{1,...,n\}$.
המשתמש מחשב את הקבוצה $A_3 \subseteq \{1,...,n\}$ הבאה:

1. לכל $j \neq i$ אם j שייך <u>בדיוק</u> לקבוצה אחת מבין A_1, A_2 אזי $j \in A_3$. אחרת, $j \notin A_3$.
2. אם i שייך <u>בדיוק</u> לקבוצה אחת מבין A_1, A_2 אזי $i \notin A_3$. אחרת, $i \in A_3$.
3. המשתמש שולח את הקבוצה A_ℓ לשרת ℓ.

הסבירו מדוע כל שני שרתים שישתפו פעולה לא ילמדו מידע על הביט שהמשתמש מבקש.

סעיף ג [8 נקודות]

הראו כיצד כל שרת יכול לשלוח ביט אחד למשתמש כך שהמשתמש יכול לשחזר את הביט ה- i. הסבירו כיצד המשתמש מחשב את הביט ה- i, והוכיחו כי חישוב זה נכון.

סעיף ד [8 נקודות]

תכננו פרוטוקול PIR 2–פרטי עם 3 שרתים כך שסיבוכיות התקשורת הכללית היא $O\left(n^{1/2}\right)$. תארו את הפרוטוקול והסבירו מדוע הוא נכון, למה הוא שומר על פרטיות ומדוע סיבוכיות התקשורת היא כמבוקש.