עמוס ביימל
אורי שטמר

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

המחלקה
למדעי המחשב

קריפטוגרפיה – מועד א'

202-2-5871

סמסטר א' תשע"ו

24.1.2016

הנחיות:

1. בטופס הבחינה 2 עמודים מלבד עמוד זה. ודאו כי כולם נמצאים בידכם.
2. בבחינה 3 שאלות שמשקלן אינו 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 (30 נקודות)

סעיף א [15 נקודות]
בהינתן מפתח k בן 56 ביטים והודעה m בת 64 ביטים, נסמן ב- $L_i(m,k)\,,R_i(m,k)$ את המחרוזות L_i,R_i לאחר הסיבוב ה- i בהרצה של DES על ההודעה m עם המפתח k.
הוכיחו כי לכל מפתח k קיימות לפחות 2^{32} הודעות m כך ש- $L_8(m,k)=R_8(m,k)$.

סעיף ב [15 נקודות]
נגדיר כ 'DES מערכת הצפנה זהה ל DES פרט לכך שהיא מקבלת מפתח אחד k בן 48 ביטים ומשתמשת בו בכל הסיבובים.
הוכיחו כי לכל מפתח k קיימות לפחות 2^{32} הודעות m כך ש- $\mathrm{DES}'(m,k)=m$.

שאלה 2 (40 נקודות)

כפי שראינו בכיתה, בגלל תכונת הכפליות של מערכת ההצפנה RSA, היא אינה עמידה להתקפת הודעה נבחרת. כדי להתגבר על חולשה זו הוצע לשנות את אלגוריתם ההצפנה באופן הבא:

$$\mathrm{RSA}'\big(m,(N,e)\big)=(2m)^e \bmod N\,.$$

אלגוריתם יצור המפתחות ללא שינויי.

סעיף א [5 נקודות]
הראו איך ניתן לפענח צפנים בעזרת המפתח הסודי.

סעיף ב [11 נקודות]
גם מערכת זו אינה עמידה להתקפת הודעה נבחרת: הראו אלגוריתם יעיל אשר בהינתן צופן c מבקש פענוח של שני צפנים (שונים מ- c) ולאחר מכן מסוגל לפענח את c.

סעיף ג [11 נקודות]
הראו מתקפה כנ"ל עבור

$$\mathrm{RSA}''\big(m,(N,e)\big)=(m+1)^e \bmod N\,.$$

סעיף ג [13 נקודות]
הראו מתקפה כנ"ל עבור

$$\mathrm{RSA}'''\big(m,(N,e)\big)=(5m+7)^e \bmod N\,.$$

שאלה 3 (30 נקודות)

יהי $T > 0$ שלם, ויהי $X = (x_1, x_2, \dots, x_n) \in \{1,2, \dots, T\}^n$ דטהבייס המכיל n מספרים בין 1 ל- T.
בשאלה זו ניתן להניח כי המספרים בדטהבייס שונים זה מזה. לכל $1 \le j \le T$ נסמן את מספר האיברים בדטהבייס הגדולים שווים j כ- $f_j(X) = |\{i : x_i \ge j\}|$.

בשאלה זו אנו מעוניינים לחשב (בצורה פרטית) מספר $1 \le t \le T$ כך ש- $f_t(X) \approx n/2$. לדוגמה, אם $T = 200$ ו- $X = (2,4,6,8, \dots, 198,200)$ אזי $t = 103$ הוא פלט אפשרי טוב.

סעיף א [10 נקודות]
סטודנט בקורס הציע את האלגוריתם הבא:
קלט: דטהבייס $X \in \{1,2, \dots, T\}^n$
1. מיין את האיברים בדטהבייס, וסמנם כ- $z_1 \le z_2 \le \cdots \le z_n$.
2. הגרל $Y \sim Lap\left(\frac{1}{\epsilon}\right)$, וסמן $j = \left\lfloor \frac{n}{2} + Y \right\rfloor$.
3. החזר את z_j (אם $j < 1$ או $j > n$ אז הפלט הוא z_1 או z_n בהתאמה).

הוכיחו כי האלגוריתם הנ"ל איננו משמר ϵ-פרטיות דיפרנציאלית (לאף ערך של ϵ).

סעיף ב [10 נקודות]
תכננו אלגוריתם $\mathcal{A}_j$ המשמר $\varepsilon/\log T$ פרטיות דיפרנציאלית אשר על קלט X מחזיר הערכה רועשת a_j ל- $f_j(X)$. חשבו את גודל הדהבייס n הדרוש על מנת ש-

$$\Pr\left[\left|a_j - f_j(X)\right| \le \frac{n}{100}\right] \ge 1 - \frac{1}{100 \log T}$$

סעיף ג [10 נקודות]
תכננו אלגוריתם המשמר ε פרטיות דיפרנציאלית אשר על קלט X מחזיר מספר $1 \le t \le T$ כך ש-

$$\Pr\left[\frac{n}{2} - \frac{n}{50} \le f_t(X) \le \frac{n}{2} + \frac{n}{50}\right] \ge 1 - \frac{1}{100}$$

חשבו את גודל הדהבייס n הדרוש.
עליכם להציג אלגוריתם הפועל על דטהבייס בגודל

$$n = O\left(\frac{1}{\epsilon} \cdot \operatorname{polylog} T\right).$$

בהצלחה!