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"ה

25.1.2015

הנחיות:

1. בטופס הבחינה 3 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)

בסעיף זה תראו איך לשבור מערכת הצפנה דמוית AES עם 3 סיבובים כאשר הורדנו את הפונקציה ShiftRows. ליתר דיוק, נעסוק במערכת הקריפטוגרפית הבאה, בה k_1, k_2, k_3 נבחרים באופן בלתי תלוי.

Simple AES

Input:

in: Message (128bit)

k_1, k_2, k_3: keys (128bit each)

Begin

state = in

For *i* = 1 **to** 3

state = SubBytes(state)

state = MixColumns(state)

state = AddRoundKey(state, k_i)

Endfor

out = state

End

הניחו כי בהינתן 4 זוגות של קלטים ופלטים $(in_1, out_1), (in_2, out_2), (in_3, out_3), (in_4, out_4)$ קיימת לכל היותר שלשת מפתחות k_1, k_2, k_3 אחת המעתיקה את הקלטים הנ"ל לפלטים המתאימים. תארו מתקפה בסיבוכיות זמן (בערך) $4 \cdot 2^{96}$ וסיבוכיות זיכרון $O(1)$ המקבלת 4 זוגות של קלטים ופלטים מתאימים ומוצאת את המפתחות k_1, k_2, k_3.

סעיף ב (15נקודות)

בהינתן זוג (in, out), מהו מספר המפתחות k_1, k_2, k_3 המעתיקים את in ל- out?
הוכיחו את תשובתכם.

שאלה 2 (35 נקודות)

יהי p ראשוני גדול, ויהיו g_1, g_2 שני יוצרים אקראיים (ב"ת) של $\mathbb{Z}_p^*$.
נגדיר את הפונקציה $h: \mathbb{Z}_p^* \times \mathbb{Z}_p^* \to \mathbb{Z}_p^*$ הבאה:
$$h(x,y) = g_1^x \cdot g_2^y \pmod p.$$
הפרמטרים p, g_1, g_2 הם פומביים.

סעיף א (10נקודות)

נתון z כך ש- $g_2 = g_1^z \pmod p$. בהינתן z הנ"ל, הראו כי לכל $x, y \in \mathbb{Z}_p^*$ ניתן לחשב ביעילות $x', y' \in \mathbb{Z}_p^*$ כך ש- $(x,y) \neq (x',y')$ ומתקיים $h(x,y) = h(x',y')$.

סעיף ב (12נקודות)

נתונים $(x,y) \neq (x',y')$ כך ש- $h(x,y) = h(x',y')$ וכך ש- $\gcd(y-y', p-1) = 1$. הראו כי ניתן לחשב ביעילות z כך ש- $g_2 = g_1^z \pmod p$.

סעיף ג (13נקודות)

עבור $2 \leq r \in \mathbb{N}$, תארו פונקצייה h_r הממפה r איברים מ- $\mathbb{Z}_p^*$ לאיבר אחד ב- $\mathbb{Z}_p^*$ כך שמציאת התנגשות עבור h_r גוררת מציאת התנגשות עבור h. תארו אלגוריתם יעיל המתרגם התנגשות עבור h_r להתנגשות עבור h.

שאלה 3 (35 נקודות)

נתון פרוטוקול ה PIR הבא:
ישנם 4 שרתים. כל שרת מחזיק את מאגר נתונים X בן n ביטים, שנתייחס אליו כמערך דו-מיימדי $X = \begin{pmatrix} x_{1,1} & \cdots & x_{1,\sqrt{n}} \\ \vdots & \ddots & \vdots \\ x_{\sqrt{n},1} & \cdots & x_{\sqrt{n},\sqrt{n}} \end{pmatrix}$ בגודל $\sqrt{n} \times \sqrt{n}$. המשתמש מעוניין בערך התא (i,j).

<u>המשתמש</u>:

- מגריל 2 תתי קבוצות אקראית $A, B \subseteq \{1, \ldots, \sqrt{n}\}$ באופן ב"ת.
- מחשב:

$$\begin{aligned} S_1 &= A & T_1 &= B \\ S_2 &= A \oplus \{i\} & T_2 &= B \\ S_3 &= A & T_3 &= B \oplus \{j\} \\ S_4 &= A \oplus \{i\} & T_4 &= B \oplus \{j\} \end{aligned}$$

- עבור $1 \leq \ell \leq 4$: שולח לשרת ℓ את S_ℓ, T_ℓ.

<u>שרת ℓ</u>:

- מחשב ושולח:

$$a_\ell = \bigoplus_{s \in S_\ell, t \in T_\ell} x_{s,t}.$$

סעיף א (3 נקודות)
מהי סיבוכיות התקשורת של השאילתות והתשובות בפרוטוקול הנ"ל?

סעיף ב (7 נקודות)
הסבירו מדוע כל שרת איננו לומד מידע על (i,j).

סעיף ג (12 נקודות)
הסבירו כיצד המשתמש משחזר את ערך התא ה- (i,j) מהתשובות שהוא מקבל. הוכיחו את תשובתכם.

סעיף ד (13 נקודות)
הראו כיצד ניתן בעזרת פרוטוקול זה ליצור פרוטוקול עם סיבוכיות תקשורת של השאילתות ותשובות $O\left(n^{1/3}\right)$.

בהצלחה!