עמוס ביימל
אורי שטמר

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

המחלקה
למדעי המחשב

קריפטוגרפיה – מועד ב'

202-2-5871

סמסטר א' תשע"ה

16.2.2015

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 (35 נקודות)

בשאלה זו תראו מתקפה על מערכת הצפנה AES עם 3 סיבובים. ליתר דיוק, נעסוק במערכת הקריפטוגרפית הבאה, בה k_1, k_2, k_3 נבחרים באופן בלתי תלוי.

3-Rounds 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 = ShiftRows(state)
    state = MixColumns(state)
    state = AddRoundKey(state, k_i)
Endfor
out = state
```

End

סעיף א (10 נקודות)

בהינתן זוג (in, out), הראו כי מספר המפתחות k_1, k_2, k_3 המעתיקים את in ל- out הוא בדיוק 2^{256}. הוכיחו את תשובתכם.

סעיף ב (25 נקודות)

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) 2^{256} וסיבוכיות זיכרון $O(1)$ המקבלת 4 זוגות של קלטים ופלטים מתאימים ומוצאת את המפתחות k_1, k_2, k_3. הסבירו מדוע זמן הריצה והזיכרון של ההתקפה שלכם עונים לדרישות.

שאלה 2 (40 נקודות)

נסתכל על מערכת עם m משתתפים $P_1, \dots, P_m$ בה כל P_i מחזיק בביט x_i. נתאר כעת פרוטוקול המחשב את הפונקציה $x_1 \vee x_2 \vee \cdots \vee x_m$.

משתתף P_1:

1. מוצא q ראשוני גדול כך ש- $p = 2q + 1$ ראשוני, מוצא g יוצר של $\mathbb{Z}_p^*$ ומחשב $h = g^2 \bmod p$.
2. מגריל $b \in \mathbb{Z}_q$ ומחשב $B = h^b \bmod p$.
3. מגדיר $y_0 = A_0 = 1$.

עבור $i = 1$ עד m משתתף P_i מבצע:

1. מגריל $a_i \in \mathbb{Z}_q$ ומחשב $A_i = A_{i-1} \cdot h^{a_i} \bmod p$.
2. אם $x_i = 0$ אזי מחשב $y_i = (y_{i-1} \cdot B^{a_i}) \bmod p$,
3. אם $x_i = 1$ אזי מגריל $c \in \mathrm{QR}_p$ ומחשב $y_i = (y_{i-1} \cdot B^{a_i} \cdot \mathrm{c}) \bmod p$,
4. שולח ל- P_{i+1} את ההודעה p, h, B, A_i, y_i (כאשר P_m שולח את ההודעה ל- P_1).

סעיף א (14 נקודות)

הסבירו כיצד P_1 יכול (בהסתברות גבוהה) לחשב את $x_1 \vee x_2 \vee \cdots \vee x_m$.

סעיף ב (13 נקודות)

הסבירו מדוע כאשר $x_2 \vee \cdots \vee x_m = 1$, משתתף P_1 (המחזיק ב- $q, p, g, h, b, B, y_1, a_1, x_1$ ומקבל את ההודעה A_m, y_m) איננו לומד מידע נוסף על $x_2, \dots, x_m$.
האם הסתמכתם על הנחת קושי חישובי? האם הטענה נכונה גם כאשר ל- P_1 יש כח חישוב לא מוגבל?

סעיף ג (13 נקודות)

הסבירו מדוע מאזין ששומע את כל התקשורת לא לומד מידע על $x_1, \dots, x_m$.
האם הסתמכתם על הנחת קושי חישובי? האם הטענה נכונה גם כאשר למאזין יש כח חישוב לא מוגבל?

שאלה 3 (25 נקודות)

היזכרו בהגדרת הבטיחות שניתנה בכיתה עבור מערכת הצפנה במפתח פומבי $\pi = (\mathrm{Gen}, \mathrm{Enc}, \mathrm{Dec})$.

משחק הבחנה א (עם פרמטר n):

1. $(PK, SK) \leftarrow \mathrm{Gen}(1^n)$.
2. בהינתן קלט PK, היריב $\mathcal{A}$ פולט זוג מסרים m_0, m_1 ממרחב המסרים של מערכת ההצפנה.
3. מגרילים בהתפלגות אחידה $b \in \{0,1\}$, ומחשבים קריפטוגרמה $c \leftarrow \mathrm{Enc}(m_b, PK)$.
4. היריב $\mathcal{A}$ מקבל את הקריפטוגרמה c ופולט $\hat{b} \in \{0,1\}$. היריב $\mathcal{A}$ מנצח אם $\hat{b} = b$.

הגדרה א:

מערכת π היא בטוחה אם לכל יריב פולינומי הסתברותי $\mathcal{A}$ קיימת פונקציה זניחה $\mathrm{negl}(\cdot)$ כך ש-

$$\Pr\left[\begin{matrix}\text{מנצח } \mathcal{A} \\ \text{במשחק א}\end{matrix}\right] \leq \frac{1}{2} + \mathrm{negl}(n)$$

סעיף א (13 נקודות)

סטודנט בקורס טען שאפשר לפשט את משחק ההבחנה באופן הבא:
במקום לאפשר ליריב לבחור זוג מסרים m_0, m_1, נאפשר לו לבחור רק מסר אחד m. על מנת לנצח במשחק היריב יידרש להבחין בין הצפנה של m לבין הצפנה של 1 (הניחו כי 1 נמצא במרחב המסרים של המערכת). באופן פורמלי:

משחק הבחנה ב (עם פרמטר n):

1. $(PK, SK) \leftarrow \mathrm{Gen}(1^n)$.
2. בהינתן קלט PK, היריב $\mathcal{B}$ פולט מסר m ממרחב המסרים של מערכת ההצפנה.
3. מגרילים בהתפלגות אחידה $b \in \{0,1\}$.
   אם $b = 0$ אז מחשבים קריפטוגרמה $c \leftarrow \mathrm{Enc}(m, PK)$.
   אם $b = 1$ אז מחשבים קריפטוגרמה $c \leftarrow \mathrm{Enc}(1, PK)$.
4. היריב $\mathcal{B}$ מקבל את הקריפטוגרמה c ופולט $\hat{b} \in \{0,1\}$. היריב $\mathcal{B}$ מנצח אם $\hat{b} = b$.

הגדרה ב:
מערכת π היא בטוחה אם לכל יריב פולינומי הסתברותי $\mathcal{B}$ קיימת פונקציה זניחה $\mathrm{negl}(\cdot)$ כך ש-

$$\Pr\left[\begin{matrix}\text{מנצח } \mathcal{B} \\ \text{במשחק ב}\end{matrix}\right] \leq \frac{1}{2} + \mathrm{negl}(n).$$

הוכיחו כי אם π אינה בטוחה לפי הגדרה ב אזי π אינה בטוחה לפי הגדרה א.
הדרכה: הניחו כי קיים יריב $\mathcal{B}$ המנצח במשחק ב בהסת' $\frac{1}{2} + \epsilon(n)$ והראו בעזרתו יריב $\mathcal{A}$ למשחק א.

סעיף ב (12 נקודות)

סטודנט אחר בקורס טען שאפשר לפשט עוד יותר את משחק ההבחנה:
לא נאפשר ליריב לבחור מסרים כלל, ועל מנת לנצח במשחק היריב יידרש להבחין בין הצפנה של 1 לבין הצפנה של 2 (הניחו כי 1 ו- 2 נמצאים במרחב המסרים של המערכת). באופן פורמלי:

משחק הבחנה ג (עם פרמטר n):

1. $(PK, SK) \leftarrow \mathrm{Gen}(1^n)$.
2. מגרילים בהתפלגות אחידה $b \in \{0,1\}$.
   אם $b = 0$ אז מחשבים קריפטוגרמה $c \leftarrow \mathrm{Enc}(1, PK)$.
   אם $b = 1$ אז מחשבים קריפטוגרמה $c \leftarrow \mathrm{Enc}(2, PK)$.
3. היריב $\mathcal{B}$ מקבל את PK ואת הקריפטוגרמה c ופולט $\hat{b} \in \{0,1\}$. היריב $\mathcal{B}$ מנצח אם $\hat{b} = b$.

הגדרה ג:
מערכת π היא בטוחה אם לכל יריב פולינומי הסתברותי $\mathcal{B}$ קיימת פונקציה זניחה $\mathrm{negl}(\cdot)$ כך ש-

$$\Pr\left[\begin{matrix}\text{מנצח } \mathcal{B} \\ \text{במשחק ג}\end{matrix}\right] \leq \frac{1}{2} + \mathrm{negl}(n).$$

הראו כי קיימת מערכת הצפנה במפתח פומבי אשר בטוחה לפי הגדרה ג <u>ולא</u> בטוחה לפי הגדרה א. ניתן להסתמך על הנחות הקושי שנלמדו בכיתה.
<u>רמז</u>: ניתן להתחיל ממערכת הצפנה כלשהי הבטוחה לפי הגדרה א ולשנות אותה בהתאם.