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

קריפטוגרפיה - מועד א'

202-1-5351
סמסטר א' תשס"ט
26.3.2009

הנחיות:

1. בטופס הבחינה 4 דפים מלבד דף 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 [40 נקודות]

נסתכל על הפרוטוקול הבא להחלפת מפתחות. יהי q ראשוני כך ש- $p=2q+1$ הוא ראשוני. אנו מניחים כי q ידוע לכל המשתתפים במערכת.

פרוטוקול להחלפת המפתחות:

1. אליס מגרילה מפתח $k \in QR_p$ כך ש- $k \neq 1$. הגרל
2. אליס מגרילה $a \in Z_q^*$, מחשבת $A = k^a \bmod p$ ושולחת A לבוב.
3. בוב מגריל $b \in Z_q^*$, מחשב $B = A^b \bmod p$ ושולח B לאליס.
4. אליס מחשבת את $C = k^b \bmod p$ מתוך B ו- a ושולחת C לבוב.
5. בוב מחשב את k מתוך C ו- b.

סעיף א [12 נקודות]

הסבירו כיצד אליס יכולה לחשב בצורה יעילה את $\boldsymbol{C = k^b \bmod p}$ מתוך B ו- a (ללא ידיעת b), וכיצד בוב יכול לחשב בצורה יעילה את $\boldsymbol{k}$ מתוך C ו- b (ללא ידיעת a).

סעיף ב [16 נקודות]

הסבירו מדוע איב ששומעת רק את ההודעה הראשונה A ויודעת מהו q לא לומדת כל מידע על k גם אם יש לה כוח חישובי לא מוגבל.

סעיף ג [12 נקודות]

הסבירו מדוע איב ששומעת רק את ההודעות A ו- B ויודעת מהו q לא לומדת כל מידע על k גם אם יש לה כוח חישובי לא מוגבל.

רמז: אתם יכולים להניח כי איב יודעת גם את b.

שאלה 2 [40 נקודות]

בשאלה זו נדון בפרוטוקולי Oblivious Transfer (OT). תזכורת, בפרוטוקול OT *n*-מתוך-1 הקלט של אליס הוא אינדקס $i \in \{1, \dots, n\}$ והקלט של בוב הוא *n* ביטים $b_1, \dots, b_n$. בסוף הפרוטוקול אליס צריכה ללמוד את b_i ולא ללמוד מידע נוסף. בנוסף, בוב לא ילמד שום מידע במהלך הפרוטוקול. בשאלה זו נניח כי יש לנו פרוטוקול OT 1-מתוך-*2* ונבנה ממנו פרוטוקול OT *n*-מתוך-1.

<u>ניסיון ראשון</u>: אליס ובוב יריצו *n* הרצות של פרוטוקול OT 2-מתוך-1. בריצה ה- *j* (כאשר $\mathbf{1 \le j \le n}$) הקלט של אליס הוא 1 אם $i = j$ והוא 2 אם $i \neq j$, הקלט של בוב הוא $\boldsymbol{b_j}, \mathbf{0}$.

סעיף א [6 נקודות]

הסבירו מדוע בוב לא ילמד שום מידע במהלך הפרוטוקול.

סעיף ב [7 נקודות]

הראו כיצד אליס רמאית יכולה ללמוד את כל הביטים של בוב.

נראה כעת פרוטוקול בטוח.

בתחילת הפרוטוקול בוב מגריל *n* ביטים אקראיים $r_1, \dots, r_n$. כעת אליס ובוב יריצו *n* הרצות של פרוטוקול OT 2-מתוך-1. בריצה ה- *j* (כאשר $1 \le j \le n$):

- הקלט של אליס הוא 1 אם $i = j$ והוא 2 אם $i \neq j$.
- הקלט של בוב הוא $b_j \oplus r_1 \oplus \dots \oplus r_{j-1}, r_j$.

סעיף ג [7 נקודות]

הסבירו כיצד אליס הגונה יכולה לחשב את $\boldsymbol{b_i}$.

סעיף ד [20 נקודות]

הראו כעת כי גם אם אליס רמאית, היא אינה יכולה ללמוד יותר מביט אחד בוב.

הדרכה: הראו כי לכל סדרה של אינדקסים $i_1, \dots, i_n$ שאליס משתמשת בהם בפרוטוקולי ה- OT קיימים לפחות *n*-1 אינדקסים שאליס לא לומדת דבר אליהם.

שאלה 3 [20 נקודות]

בשאלה זו נראה איך לשבור גירסה של מערכת הצפנה דמוית AES עם סיבוב אחד. ליתר דיוק, נעסוק במערכת הקריפטוגרפית המתוארת לעיל.

Simple AES

Input:

in: Message

k_1: key

Begin

state = in

state = SubBytes(state)

state = ShiftRows(state)

state = MixColumns(state)

state = AddRoundKey(state, k_1)

Output:

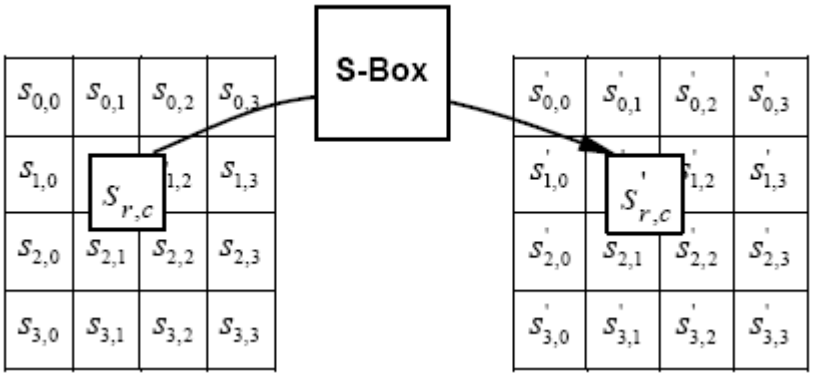
state

End

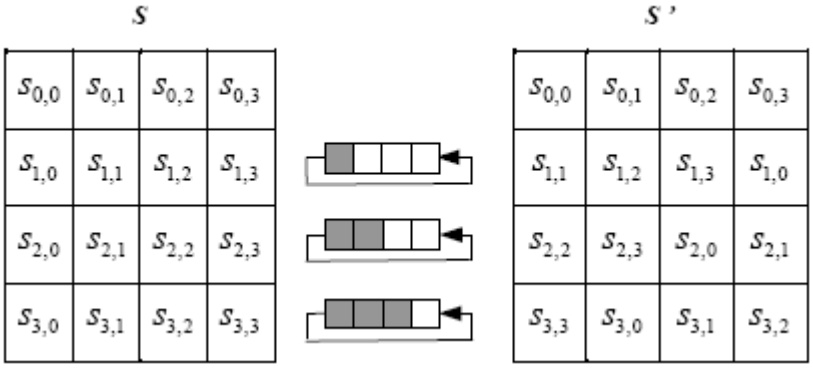
הראו איך במערכת זאת בהינתן הודעה M כלשהי והצפנה שלה C, ניתן בצורה יעילה לחשב את המפתח k_1.

<u>תזכורת</u>:

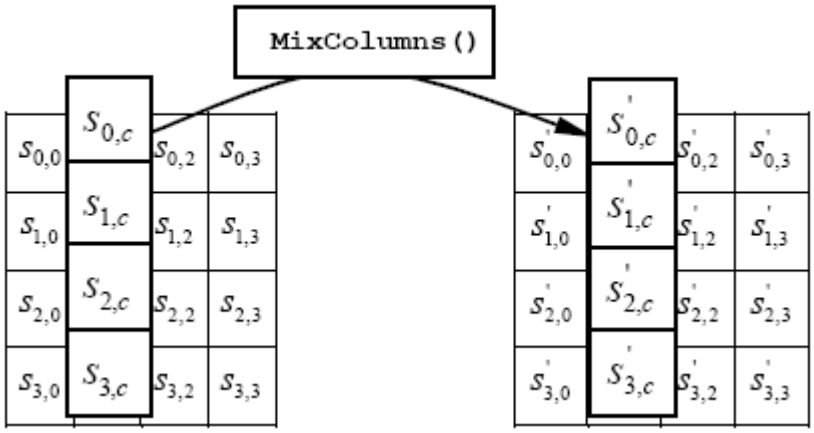
SubBytes מפעילה את קופסת ה-S על כל byte במצב



ShiftRows מפעילה את הטרנספורמציה הבאה:



MixColumns מפעילה טרנספורמציה לינארית הפיכה על כל עמודה



ו- AddRoundKey מבצעת XOR עם המפתח.