עמוס ביימל
המחלקה למדעי המחשב
אוניברסיטת בן-גוריון בנגב
Ben-Gurion University of the Negev

קריפטוגרפיה – מועד ב'

202-1-5351
סמסטר א' תשס"ט
24.4.2009

הנחיות:

1. בטופס הבחינה 3 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 [35 נקודות]

בשאלה זו נעסוק בגרסה של מערכת הצפנה דמוית AES עם שני סיבובים. ליתר דיוק, נעסוק במערכת הקריפטוגרפית המתוארת לעיל.

Simple AES

Input:

in: Message (128 bits)

k_1, k_2: keys (each key – 128 bits)

Begin

state = in

For i=1 to 2 do

state = SubBytes(state)

state = ShiftRows(state)

state = MixColumns(state)

state = AddRoundKey(state, k_i)

Endfor

Output:

state

סעיף א (17 נקודות)

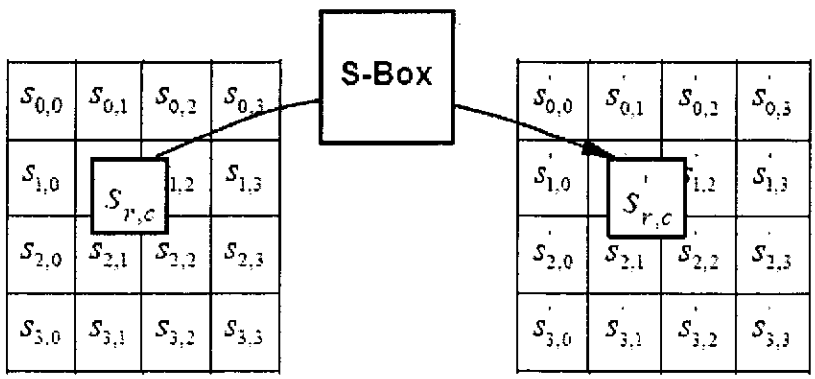
הראו כי לכל הודעה M וקריפטוגרמה C קיימים בדיוק 2^{128} מפתחות k_1, k_2 המעתיקים את M ל- C.

סעיף ב (18 נקודות)

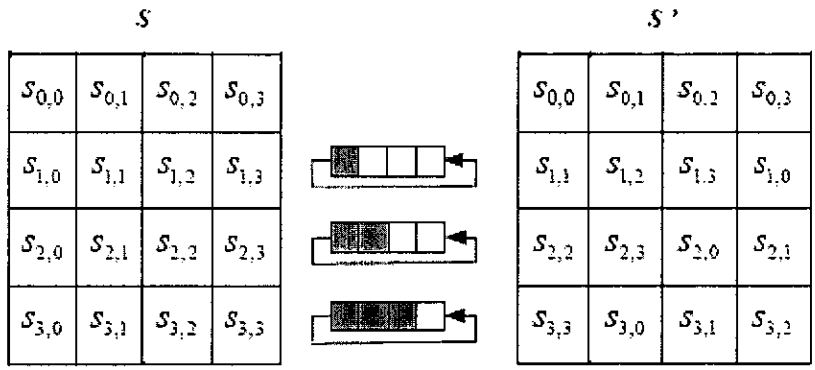
הניחו כי אם הודעות M_1, M_2, M_3 הוצפנו לקריפטוגרמות C_1, C_2, C_3 ע"י מפתחות k_1, k_2, אזי ההסתברות שקיימים מפתחות אחרים המעתיקים את M_1, M_2, M_3 ל- C_1, C_2, C_3 היא זניחה. הראו התקפה על המערכת בסיבוכיות 2^{128} שבהינתן הודעות M_1, M_2, M_3 וההצפנות שלהם C_1, C_2, C_3 מוצאת את המפתחות k_1, k_2.

<u>תזכורת:</u>

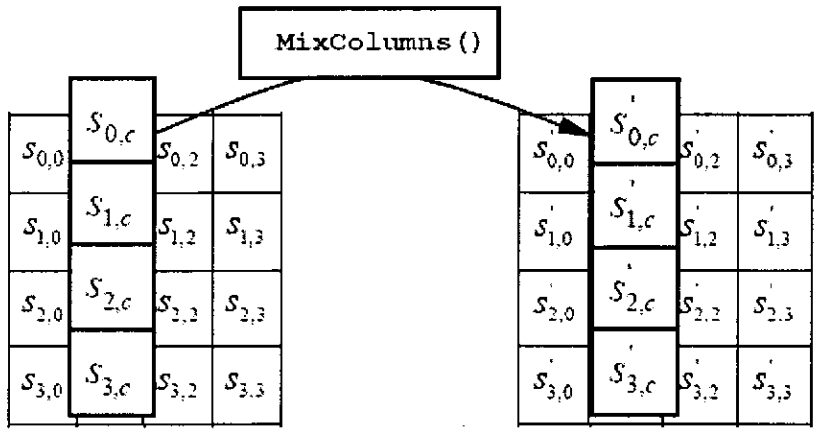
SubBytes מפעילה את קופסת ה-S על כל byte במצב



ShiftRows מפעילה את הטרנספורמציה הבאה:



MixColumns מפעילה טרנספורמציה לינארית הפיכה על כל עמודה



ו- AddRoundKey מבצעת XOR עם המפתח.

שאלה 2 [30 נקודות]

תהי (γ,δ) חתימה חוקית בשיטת ElGamal על מסמך m עם מפתח ציבורי (p,g,B).

סעיף א [10 נקודות]

נתון כי $\gamma g < p-1$. יהיו $\gamma' = \gamma g$ ו- $\delta' = \delta g \bmod (p-1)$. הראו כי (γ',δ') היא חתימה חוקית על המסמך

$$m' = (m+\delta)g \bmod (p-1).$$

סעיף ב [20 נקודות]

יהי ℓ מספר טבעי כך ש- $\gamma g^{\ell} < p-1$. הראו איך מתקיף היודע את המפתח הציבורי (p,g,B), את ההודעה m ואת החתימה שלה (γ,δ), יכול לחשב בצורה יעילה חתימה למסמך

$$m' = (m+\ell\delta)g^{\ell} \bmod (p-1).$$

שאלה 3 [35 נקודות]

בשאלה זו נדון בשימוש בפרוטוקולי Oblivious Transfer (OT). בפרוטוקול 1-מתוך-2 OT עבור מחרוזות באורך ℓ, הקלט של אליס הוא אינדקס $i\in\{1,2\}$ והקלט של בוב הוא שני מחרוזות $b_1,b_2\in\{0,1\}^{\ell}$. בסוף הפרוטוקול אליס צריכה ללמוד את המחרוזת b_i ולא ללמוד מידע נוסף. בנוסף, בוב לא ילמד שום מידע במהלך הפרוטוקול.

סעיף א [15 נקודות]

נניח כי יש לנו פרוטוקול 1-מתוך-2 OT עבור מחרוזות באורך 1. הראו איך להשתמש בפרוטוקול זה כדי לבנות פרוטוקול 1-מתוך-2 OT עבור מחרוזות באורך ℓ, כך שאליס ובוב סקרנים לא ילמדו מידע (כלומר, אליס ובוב ישלחו הודעות על פי הפרוטוקול).

סעיף ב [20 נקודות]

נניח כעת כי הקלט של אליס הוא n ביטים $x_1, x_2, \ldots, x_n$ והקלט של בוב הוא n ביטים $y_1, y_2, \ldots, y_n$. אליס ובוב רוצים לחשב בצורה פרטית את הפונקציה $x_1y_1 + x_2y_2 + \ldots + x_ny_n$. תארו פרוטוקול לפונקציה בו בוב אינו לומד כל מידע ואליס לא לומדת מידע פרט לפלט הפונקציה. אתם רשאים להשתמש בפרוטוקול 1-מתוך-2 OT עבור מחרוזות באורך $\ell\approx\log n$. הוכיחו כי הפרוטוקול שתיארתם נכון, בוב לא לומד מידע בפרוטוקול ואליס לא לומדת מידע פרט לפלט הפונקציה.

הדרכה: הפרוטוקול בוחר ראשוני $p>n$ ומחשב את הפונקציה $x_1y_1 + x_2y_2 + \ldots + x_ny_n \bmod p$.