מס' מחברת: 27

מבחן בקורס "מבוא לקריפטוגרפיה מודרנית"

סמסטר א' התש"ע, מועד א'

תאריך: 24.1.2010

מרצה: פרופ' בני שור

מתרגל: רני הוד

מומלץ לקרוא את כל ההנחיות והשאלות בתחילת המבחן, לפני תחילת כתיבת התשובות.

- משך הבחינה שלוש שעות.
- חומר עזר מותר: שני דפי A4, כתובים משני הצדדים.
- בראש כל עמוד בטופס המבחן יש למלא מספר ת"ז ומספר מחברת.
- במבחן ארבע שאלות פתוחות ולחלקן סעיפי משנה. כדי לקבל ציון 100 בבחינה יש לענות נכונה על כל השאלות. ניקוד כל סעיף מצוין לידו. אין בהכרח קשר בין ניקוד הסעיף ובין קושיו.
  - על התשובה לכל שאלה להופיע במסגרת המתאימה בטופס המבחן (טופס זה). יש לענות תשובות ברורות ותמציתיות. תשובות מסורבלות או לא ניתנות פיזית לקריאה יזכו לניקוד חלקי בלבד.
  - ודא/י היטב את תשובתך לפני כתיבתה בטופס המבחן. בסוף הטופס מצורפת מסגרת לשימוש במקרי "חירום".
  - מחברת הבחינה משמשת כטיוטא בלבד ולא תיבדק, אך יש להגישה עם המבחן.
- על סעיף של שאלה פתוחה ניתן לענות *"איני יודע/ת"* כתשובה; על סעיף זה יינתנו 20% מהנקודות. במקרה זה אין להוסיף שום הסבר.
- מותר להשתמש בכל טענה שהוכחה בכיתה (בהרצאה, בתירגול או בתרגיל הבית) בתנאי שמצטטים אותה באופן מדויק. טענות שהוכחו במקום אחר (כגון: בספר הלימוד, בויקיפדיה, ב־MIT, בסמסטר קודם) יש להוכיח מחדש. בפתרון סעיף בשאלה מותר להשתמש בתוצאות הסעיפים הקודמים, גם אם לא פתרתם אותם.

בהצלחה!

1						4
2						20
3א	15	3ב	15			30
4א	5	4ב	10	4ג	15	30

מס' מחברת: 27

שאלה 1 (20 נק')

בעית הלוגריתם הדיסקרטי: נקבע p ראשוני ו־g יוצר כפלי של $\mathbb{Z}_p^*$. בהנתן $y \in \mathbb{Z}_p^*$, מצאו $0 \le x < p-1$ כך ש־$y = g^x$.

ידוע ש־p הוא מהצורה $p = 10^n + 1$. תארו אלגוריתם יעיל הפותר את בעית הלוגריתם הדיסקרטי ב־$\mathbb{Z}_p^*$ והוכיחו את נכונותו.

תשובה:

לצערי הרב אינני יודע.

$\frac{4}{20}$

מס' מחברת: 27

שאלה 2 (20 נק')

משרד התקשורת הציע להפעיל *שירות לתיאום מפתחות הצפנה* (להלן *שלמה*) שיפעל בצורה הבאה. שלמה בוחר זוג ראשוניים גדולים מאד p, q ומפרסם את מכפלתם $N = pq$. כשאליס ובוב רוצים לתאם מפתח משותף, כל אחד מהם מגריל מספר $1 < r < N$ מקרי — אליס את r_A ובוב את r_B — מעלה אותו בחזקת $e = 3$ מודולו n ושולח לשלמה. שלמה מקבל את $r_A^3 \bmod N$ ואת $r_B^3 \bmod N$, מפענח אותם, ושולח לאליס ולבוב את $r_A + r_B \bmod N$. כעת אליס ובוב יודעים שניהם גם את r_A וגם את r_B ויכולים לחשב מפתח משותף $K = \mathrm{AES}_{r_A}(r_B)$.

כדי להבטיח הגנה מלאה למשתמשים, שלמה שומר אצלו מאגר ביומטרי עם כל השאילתות שנשלחו אליו אי פעם ומסרב לענות פעמיים על אותה שאילתה (כלומר: אם, למשל, שולחים אליו את $r_A^3 \bmod N$ פעם נוספת, הוא מחזיר שגיאה).

מנחם המאזין שמע את r_A^3 ואת r_B^3 ורוצה לחשב את K. הסבירו כיצד הוא ושותפתו למזימה, שפרה, יכולים לנצל את שלמה למטרה זו.

תשובה:

רעיון התשובה הוא לקבל משלמה 2 משוואות עם 2 נעלמים (r_A, r_B) ומהן למצוא את K.
תחילה r_A: שולחים לשלמה עבור $m \in \mathbb{Z}_N^*$ את $m^3 r_A^3 \bmod N$ ועבור $i \in \mathbb{Z}_N$ כלשהו את $i^3 \bmod N$.
אם קיבלנו שגיאה אזי ננסה (שוב) את m או i אחרים מהתחום המבוקש לעיל. בקבלת התשובה X משלמה, ידוע: $mr_A + i = X \pmod N$ וכיוון ש-m הפיך ניתן לחשב מיד את r_A.
באופן דומה נמצא את r_B, כאשר נבחר $n \in \mathbb{Z}_N^*$ ו-$j \in \mathbb{Z}_N$ שלא נבחרו קודם ונבקש משלמה את $n^3 r_B^3 \bmod N$, $j^3 \bmod N$ ונקבל Y כך ש-$nr_B + j = Y \pmod N$.
כעת יש ברשותנו את r_A ו-r_B ולכן ניתן לחשב את $K = AES_{r_A}(r_B)$.
הערה: נשאר רק ש-m, n נבחרו כך שהם הפיכים ב-$\mathbb{Z}_N^*$ ולכן ניתן לבודד את r_A ו-r_B ולחלצם מהמשוואות.
ניתן לוותר ... ע"י שליחת $l^3 r_A^3 r_B^3 \bmod N$ ו-$z^3 \bmod N$ כאשר $(l \in \mathbb{Z}_N^*, z \in \mathbb{Z}_N)$ ... לקבל $r_A r_B$ (מודולו N) ... לתשובה ... .

בסיכוי גבוה, $1 - \frac{1}{\sqrt{N}}$.

ואם לא (קיים) הביטוי, פירקנו את N.

מס' מחברת: 27

שאלה 3 (סה"כ 30 נק')

דני סנדרסון מצפין את מילות השירים של כוורת באמצעות מצפין בלוקים של 128 ביט בשם "פוגי".

לפוגי שני מפתחות, נסמנם K_0 ו-K_1, בגודל 64 ביט כ"א.

פוגי משתמש בפרמוטציה $f : \{0,1\}^{64} \to \{0,1\}^{64}$ המוגדרת ע"י $f(x) = \mathrm{DES}_{baruch}(x)$, קרי הצפנה של הבלוק x ב-DES עם המפתח הקבוע "ברוך".

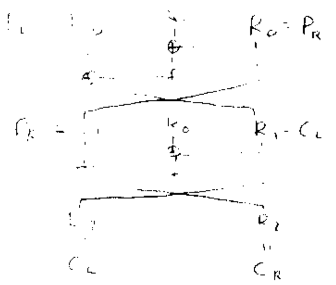
פוגי מורכב מ-1000 ~~כבאים~~ סיבובים של רשת פייסטל. בלוק הקלט P מחולק לשני חצאים L_0, R_0 בגודל 64 ביט כ"א; בסיבוב ה-t מייצרים את $L_t = R_{t-1}$ ואת $R_t = L_{t-1} \oplus f\left(R_{t-1} \oplus K_{(t \bmod 2)}\right)$. בלוק הפלט C הוא השרשור של החצאים L_{1000}, R_{1000}.

סעיף א' (15 נק')

מאיר פניגשטיין הוא סוכן סמוי של כוחותינו ולבקשתנו חיבל במצפין כך שיבצע שני סיבובים במקום 1000.

הראו כיצד ניתן לשחזר במהירות את המפתחות K_0 ו-K_1 באמצעות זוג בודד (P, C) שהוצפן ע"י פוגי המוחלש.

תשובה: [illegible] (P, C) [illegible]



[illegible]

$f^{-1}(x) = \mathrm{DES}^{-1}_{baruch}(x)$

[illegible]

[illegible] $L_1 = R_0 = P_R$ [illegible] $R_1 = L_2 = C_L$ [illegible]

• $C_R = P_R \oplus f(K_0 \oplus C_L) \Rightarrow f(K_0 \oplus C_L) = C_R \oplus P_R \Rightarrow K_0 \oplus C_L = f^{-1}(C_R \oplus P_R) \Rightarrow$
$K_0 = f^{-1}(C_R \oplus P_R) \oplus C_L$ [illegible]

[illegible]

• [illegible] $P_L \oplus f(K_1 \oplus C_L)$ [illegible] $\Rightarrow K_1 \oplus P_R = f^{-1}(C_L \oplus P_L) \Rightarrow$
$K_1 = f^{-1}(C_L \oplus P_L) \oplus P_R = \mathrm{DES}^{-1}_{baruch}(C_L \oplus P_L) \oplus P_R$

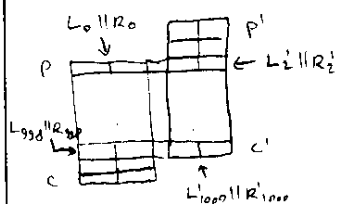
סעיף ב' (15 נק')

לאחר שגילה את מה שאירע, תיקן דני את המצפין, טען בו מפתחות K_0 ו-K_1 אקראיים, פירק את כוורת והקים להקה חדשה בשם גזוז.

נאמר ששני זוגות (P,C) ו-(P',C') הם *כפתור ופרח* אם הם מקיימים את התכונה $L_0 = L'_2, R_0 = R'_2$, כאשר L_t, R_t ו-L'_t, R'_t הם חצאי הבלוקים של פוגי בסיבוב ה-t, כאשר משתמשים בו להצפנת P ו-P' (בהתאמה).

- תארו אלגוריתם הבודק במהירות[1] האם שני זוגות נתונים (P,C) ו-(P',C') הם כפתור ופרח. לאלגוריתם מותר לטעות בסיכוי קטן, וכמובן אין לו גישה למפתחות K_0 ו-K_1.
- מזי כהן העמידה לרשותנו מאגר גדול של זוגות (P_i,C_i) שהוצפנו ע"י פוגי. הראו כיצד ניתן לשחזר את K_0 ו-K_1. לכמה זוגות האלגוריתם זקוק בתחילה?

תשובה: (נסמן את הבלוקים השונים וההצפנות על (P,C) ו-(P',C') בצורה הבאה: $P = L_0\|R_0$, $C = L_{1000}\|R_{1000}$, $P' = L'_0\|R'_0$ ו-$C' = L'_{1000}\|R'_{1000}$ ושים לב [illegible]



ש-(P,C) ו-(P',C') יהיו כפתור ופרח צריך להתקיים: $L_0 = L'_2$ ו-$R_0 = R'_2$ אך הנוסף לשני גם צריך להתקיים

אם רק ש- $L_{998} = L'_{1000}$ ו- $R_{998} = R'_{1000}$. משוויונות אלו

ומהידע על סיבוב feistel ומספר ה-DES שבסיבוב (נסמני b) נגיע לכך

שאם הזוג הם כפתור ופרח ניתן לחשב מהם את k_0 ו-k_1 בשני מקומות - בהתחלה ובסוף, ע"י השוויונות: בהתחלה: סוף:

- $k_0 = DES_b^{-1}(R'_0 \oplus R_0) \oplus L_0$
- $k_1 = DES_b^{-1}(L_0 \oplus L'_0) \oplus R'_0$

- $k_0 = DES_b^{-1}(R'_{1000} \oplus R_{1000}) \oplus L_{1000}$
- $k_1 = DES_b^{-1}(L_{1000} \oplus L'_{1000}) \oplus R'_{1000}$

(ניתן להגיע לכך בקלות, חסרתי כאן את המשוואה). כל שנותר לנו רק הוא לחשב את k_0 ו-k_1 רק ולבדוק (האם k_0,k_1 בהתחלה שווים ל-k_0,k_1 בסוף)

אם כן, הזוג הוא כפתור ופרח. [illegible] הוא לא.

אחרת כן ואומר כי לא ידוע לי למה האלגוריתם יכול לטעות בסיכוי קטן.

ייתכן שבטעות זה קרה. 2^{-128}

אם לרשותינו מאגר גדול של זוגות (P_i,C_i), ברור כי צריך לנו למצוא שני זוגות $(P_1,C_1),(P_2,C_2)$ שהם כפתור ופרח ניתן לחשב מהם את k_0,k_1 בעזרת הנ"ל לעיל.

התנאים של כל זוג עם הפעלה 2 סיבובי Feistel של הזוג השני להיות בסיכוי להתנגשות 2 בלוקים (או בעצם 2 הודעות) מתאימות. [illegible] $O(\sqrt{2^{[illegible]}})$ (גודל מרחב המפתחות - c). [illegible]

[1] לצורך סעיף זה, 1000 הפעלות של DES זה סביר, ויזכה בניקוד חלקי. לידיעתכם, יש פתרון יעיל יותר.

מס' מחברת: 27

שאלה 4 (סה"כ 30 נק')

נתונה לנו סכימת שמיר לחלוקת סוד $b \in \mathbb{Z}_5$ בין ארבעה משתתפים, כך שכל זוג מהם יכול לשחזר את הסוד יחדיו אך כל אחד לחוד אינו יכול לשחזר.

ספציפית, $a \in \mathbb{Z}_5$ נבחר באקראי והחלק שמקבל משתתף i הוא $f(i) = ai + b$ עבור $(i = 1, 2, 3, 4)$.

סעיף א' (5 נק')

למדנו בהרצאה שזוג המשתתפים i ו-j משחזרים את הסוד ע"י חישוב קומבינציה לינארית של $f(i)$ ו-$f(j)$. אצלנו, למשל, ניתן לשחזר את הסוד $b = f(0)$ ע"י הקומבינציות הבאות ב-$\mathbb{Z}_5$:

$$\begin{aligned} b &= 2f(1) - f(2) \\ &= 3f(2) - 2f(3) \\ &= 2f(3) - f(1) \end{aligned}$$

השלימו את רשימת הקומבינציות, קרי: הציגו את הסוד כקומבינציה לינארית של $f(i)$ ו-$f(4)$ עבור $i = 1, 2, 3$. נמקו בקיצור.

תשובה:

$\mathbb{Z}_5$ [illegible]

[illegible] 1,4:

$f_1(x) = y_1 \cdot \frac{x-4}{1-4} = y_1 \cdot (-\frac{1}{3})(x-4) = y_1 \cdot 4 \cdot 2(x-4) = y_1(3x+3)$

$\Rightarrow f_1(0) = 3y_1 = 3f(1)$

$f_4(x) = y_4 \cdot \frac{x-1}{4-1} = y_4 \cdot \frac{1}{3}(x-1) = y_4 \cdot 2(x+4) = y_4(2x+3)$

$\Rightarrow f_4(0) = 3y_4 = 3f(4) = -2f(4)$

[illegible]

$b = f(0) = f_1(0) + f_4(0) = \boxed{3f(1) - 2f(4)}$

[illegible]

[illegible] $f(x) = f_1(x) + f_4(x)$ [illegible]

[illegible] $b = f(0)$ [illegible]

[illegible] 2,4: $f_2(0) = y_2 \cdot \frac{-4}{2-4} = y_2 \cdot 2 = 2f(2)$, $f_4(0) = [illegible] \frac{-2}{4-2}$ [illegible] $4f(4)$

$\Leftarrow$ $\boxed{b = f(0) = 2f(2) - f(4)}$

[illegible] 3,4: $f_3(0) = y_3 \cdot \frac{-4}{3-4} = 4y_3 = 4f(3)$, $f_4(0) = y_4 \cdot \frac{-3}{4-3}$ [illegible] $= 2f(4)$.

$\Leftarrow$ $b = f(0) = 4f(3) - 3f(4)$

5/5

מס' מחברת: 27

סעיף ב' (10 נק')

נניח כי חלה תקלה בקו התקשורת בעת שיחתו של המחלק (dealer) עם משתתף i ולפיכך משתתף i קיבל בטעות את $f(i)+c$ במקום את $f(i)$, עבור $c \neq 0$ כלשהו (c אינו תלוי בסוד b). שאר המשתתפים קיבלו את חלקם ללא שגיאות ואף אחד אינו מודע לתקלה.

הראו כי כל שלושת הערכים המתקבלים כאשר משתתף i ומשתתף נוסף $j \in \{1,2,3,4\} \setminus \{i\}$ משחזרים את הסוד שונים זה מזה. כדי לחסוך לכם עבודה, הראו זאת רק עבור i שהוא מספר מחברת הבחינה שלכם מודולו 4, ועוד 1.[2]

על זה...

תשובה: במקרה שלי ובדוק עבור $i = 4$ (וגם כאילו החישוב, בלי ל.)

$1,4$: $f_1(0) \overset{\text{כמו קודם}}{=} 3f(1)$, $f_4(0) = 3y_4 \overset{\text{בגלל השגיאה}}{=} 3[f(4)+c] = 3f(4)+3c \Rightarrow f(0) = \overbrace{3f(1)+3f(4)}^{X_1 :=} + 3c$

$2,4$: $f_2(0) = 2f(2)$, $f_4(0) = 4y_4 = 4[f(4)+c] = 4f(4)+4c \Rightarrow f(0) = \overbrace{2f(2)+4f(4)}^{X_2 :=} + 4c$

$3,4$: $f_3(0) = 4f(3)$, $f_4(0) = 2y_4 = 2[f(4)+c] = 2f(4)+2c \Rightarrow f(0) = \overbrace{4f(3)+2f(4)}^{X_3 :=} + 2c$

כיון שידוע שכל החלקים ללא השגיאה הם ה-c שונים (כלומר $X_1 = X_2 = X_3$ כי הסוד לא)) אז ודאי שנקבל תוצאות שונות, שכן לכל $c \neq 0$: $3c \neq 4c \neq 2c \pmod 5$

10/10

סעיף ג' (15 נק')

כעת כל ארבעת המשתתפים משתפים פעולה כדי לשחזר את הסוד. הראו כיצד ניתן לשחזר את הסוד מתוך ארבעת החלקים גם במקרה שאחד החלקים השתבש. שימו לב שאף אחד מהמשתתפים לא יודע היכן חל השיבוש (אם בכלל).

תשובה: עבור משתתף i כלשהו, נשחזר את הסוד עם כל 3 המשתתפים האחרים. אם כל השחזורים (אולי רק רב ב-2) קיבלו תשובות שונות, אזי יש שגיאה אצל המשתתף i. אם השחזור עם משתתף $j \neq i$ שונה מ-2 השחזורים האחרים (שהם שווים ביניהם), השגיאה אצל המשתתף j. אם כולם שווים אזי אין שגיאה.

במידה ומצאנו השגיאה, ניקח (ללא הגבלה) 2 שחזורים של הסוד של המשתתף עם השגיאה עם 2 משתתפים שונים אחרים. נניח המשתתף עם השגיאה הוא i. אנו יודעים שהוא מתנהג כ- $f_i(0) = m \cdot y_i$ כאשר m יכול להיות (חישבנו אותו) עבור השחזור עם המשתתף הראשון ושונה עבור השחזור עם השני. לכן שהשחזורים נקבל:

$f(0) = X + m_1 \cdot c$

$f(0) = X + m_2 \cdot c$

כאשר m_1, m_2 ידועים (וגם X) ויש לנו 2 משוואות ב-2 נעלמים מודולו 5; ניתן להשתמש אם כך בשחזור שלנו (כמו בשחזור ואותו כל לגלות את X)

כמו כן ניתן לשחזר מתוך המשוואות את $f(i)$ האמיתי.

15/15

[2] צוות הקורס יסייע לכם בחישוב זה, אם יש צורך.

מס' מחברת: 27

מסגרת "חירום" לשאלה מספר 3, סעיף ג':

המסק. לפי הבדיקה [illegible] זה ניתן לבחור את צומת e (v,u)

(למה [illegible] של צומת) ולבדוק לפי [illegible] המעגל הוא [illegible].

[illegible] ובדוק [illegible].

(תחת הנחה [illegible] [illegible] סיבוב [illegible] – גם [illegible])

מסגרת "חירום" לשאלה מספר ____, סעיף ____: