ת.ז.: _____ מס' מחברת: _____

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 *"אינני 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						
2						
3א		3ב				
4א		4ב		4ג		

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** $0 \leq x < p-1$ **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:

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:

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:

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 בתוחלת?

תשובה:

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

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 את הסוד כקומבינציה לינארית של $f(i)$ ו-$f(4)$ עבור $i = 1, 2, 3$. נמקו בקיצור.

תשובה:

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]

תשובה:

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:

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

מסגרת "חירום" לשאלה מספר _____, סעיף _____:

מסגרת "חירום" לשאלה מספר _____, סעיף _____: