ת.ז.: _____ מס' מחברת: _____

מבחן בקורס "מבוא לקריפטוגרפיה מודרנית"

סמסטר א' התשע"ד, מועד א'

תאריך: 21.1.2014

מרצה: פרופ' בני שור

מתרגל: ניר ביטנסקי

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.
- מומלץ לא להתעכב יתר על המידה על שום סעיף.

בהצלחה!

א1		ב1		ג1		
א2		ב2				
א3		ב3		ג4		
א4		ב4				

ת.ז.: _____ מס' מחברת: _____

שאלה 1 (סה"כ 30 נק')

יהיו p, q ראשוניים כך ש-$p = 2q + 1$ ו-g יוצר כפלי של $\mathbb{Z}_p^*$. (כולם ידועים בפומבי).

סעיף א' (10 נק')

תהי $\mathbb{QR}$ חבורת השאריות הריבועיות ב-$\mathbb{Z}_p^*$. מהו הסדר של $\mathbb{QR}$? ומהי דוגמא לאיבר היוצר את $\mathbb{QR}$?

תשובה (אין צורך לנמק בסעיף זה):
סדר החבורה הנו q. g^2 הנו יוצר. למעשה, $\mathbb{QR} \setminus \{1\} = \{g^{2k} : k \neq 0 \mod q\}$ כולם יוצרים.

סעיף ב' (10 נק')

יהי f יוצר של $\mathbb{QR}$, יהי $x \in \mathbb{Z}_q$, ו-$h = f^x \mod p$. נגדיר פונקציית האש $H_{f,h} : \mathbb{Z}_q \times \mathbb{Z}_q \to \mathbb{Z}_p^*$:

$$.(a, b) \mapsto f^a h^b \mod p$$

נתון אלגוריתם (דטרמיניסטי) יעיל A שבהנתן כל h, f כנ"ל מוצא התנגשות ב-$H_{f,h}$, כלומר $(a, b), (a', b') \in \mathbb{Z}_q \times \mathbb{Z}_q$ כך ש- $(a, b) \neq (a', b')$ וכן $H_{f,h}(a, b) = H_{f,h}(a', b')$.

הראו כיצד להשתמש ב-A על-מנת לפתור ביעילות את בעיית הלוגריתם הדיסקרטי בבסיס f ב-$\mathbb{QR}$. כלומר, בהנתן $f, f^x \mod p$ עבור כל $x \in \mathbb{Z}_q$, למצוא את x.

תשובה:
בהנתן קלט f, f^x כנ"ל, נריץ את A על-מנת למצוא התנגשות $(a, b), (a', b') \in \mathbb{Z}_q \times \mathbb{Z}_q$. ההתנגשות מקיימת $ax + b = a'x + b' \mod q$. ראשית נשים לב כי $a \neq a' \mod q$, אחרת נובע כי $b = b' \mod q$ ו-$(a, b) = (a', b')$. מאחר ו-q ראשוני נוכל לחשב $x = (b' - b)(a - a')^{-1} \mod q$.

סעיף ג' (10 נק')

בני נזף בניר על־כך שהפונקציה $H_{f,h}$ אינה מכווצת דיה. בהתאם, ניר הציע להגדיר, לכל $x_1, \ldots, x_k \in \mathbb{Z}_q$, ו-$h_i = f^{x_i} \mod p$, פונ' האש $H_{h_1,\ldots,h_k} : (\mathbb{Z}_q)^k \to \mathbb{Z}_p^*$:

$$(a_1, \ldots, a_k) \mapsto h_1^{a_1} \cdot h_2^{a_2} \cdots h_k^{a_k} \mod p.$$

נתון אלגוריתם (דטרמיניסטי) יעיל A שבהנתן $h_1, \ldots, h_k$ כנ"ל, עבור $x_1, \ldots, x_k \in \mathbb{Z}_q$ אקראיים, מוצא התנגשות ב-$H_{h_1,\ldots,h_k}$ בהסתברות $\frac{1}{10}$ על פני בחירת הערכים x_i.

הראו כיצד להשתמש ב־A על־מנת לפתור ביעילות את בעיית הלוגריתם הדיסקרטי בבסיס f ב-$\mathbb{QR}$ בהסתברות $\frac{1}{10k}$. כלומר, בהנתן $f, f^x \mod p$ עבור $x \in \mathbb{Z}_q$ אקראי, למצוא את x בהסתברות $\frac{1}{10k}$, על פני בחירת x ועל־פני בחירותיו האקראיות של האלגוריתם (במידה ואתם מראים אלגוריתם הסתברותי).

תשובה:
בהנתן קלט f, f^x נדגום באקראי $i \leftarrow [k]$ וכן נדגום באקראי $x_1, \ldots, x_{i-1}x_{i+1}, \ldots, x_k$. נסמן $x_i = x$ (זהו הערך אותו אנו מנסים למצוא). כעת נריץ את A על

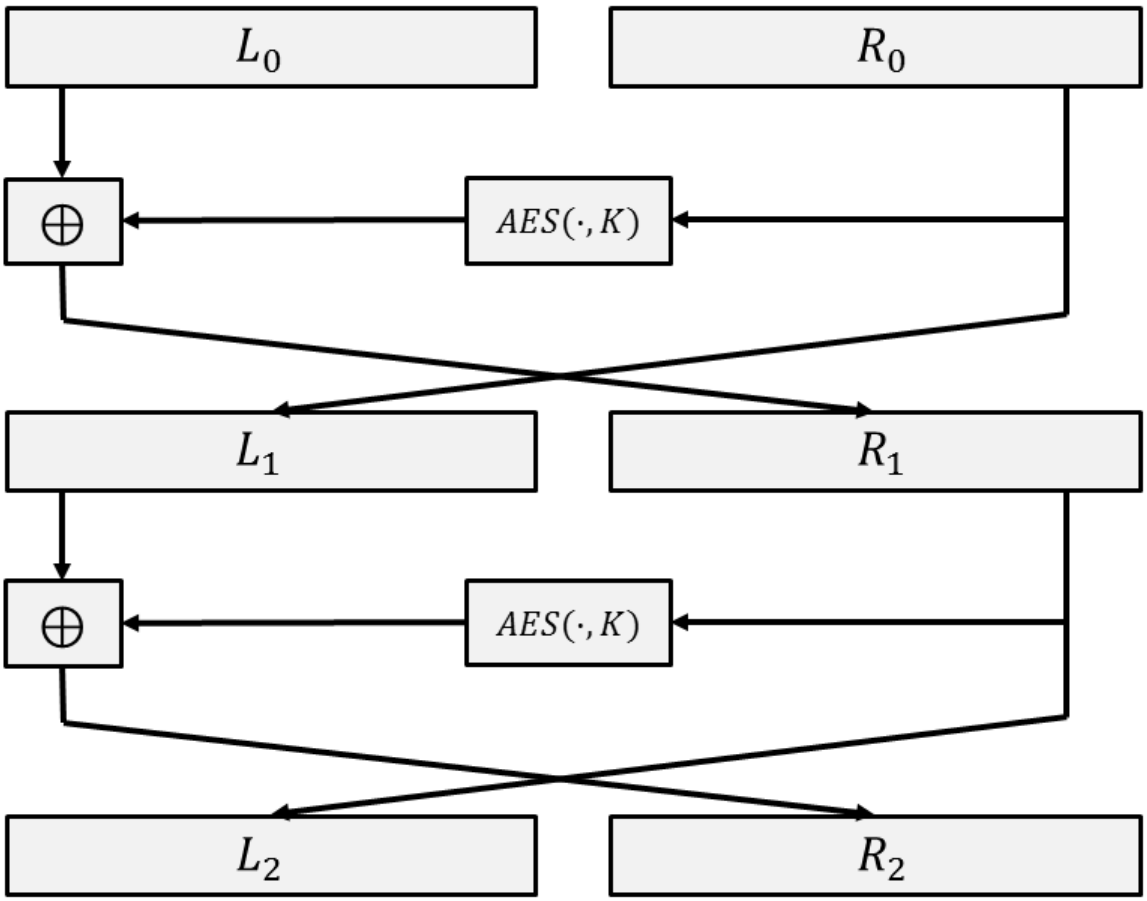
$$(h_1, \ldots, h_k) := (f^{x_1}, \ldots, f^{x_{i-1}}, f^x, f^{i+1_1} \ldots f^{x_k})$$

$\{x_i\}_{i\in[k]}$ מתפלגים יוניפורמית ועל־כן בהסתברות $1/10$ נקבל התנגשות $(a_1, \ldots, a_k) \neq (a'_1, \ldots, a'_k)$. בפרט קיים $\ell \in [k]$ כך ש $a'_\ell \neq a_\ell$. מאחר וההתנגשות מקיימת $\sum_{j\in[k]} a_j x_j = \sum_{j\in[k]} a'_j x_j \mod q$, אם $i = \ell$ נוכל לחשב $x = (a_i - a'_i)^{-1} \sum_{j\neq i}(a'_j - a_j)x_j$ כנדרש. ההסתברות כי זה אכן יקרה (בהנתן התנגשות) הנה $1/k$. אכן בחירת i הנה בלתי תלויה בבחירת $x_1, \ldots, x_k$. סה"כ נצליח למצוא את x בהסתברות $1/10k$ כנדרש.

שאלה 2 (סה"כ 20 נק')

נציע סכמת אימות $MAC : \{0,1\}^{2n} \times \{0,1\}^k \to \{0,1\}^{2n}$ **המוגדרת באופן הבא.**

- **המפתח** $K \in \{0,1\}^k$ **הנו מפתח עבור** $AES : \{0,1\}^n \times \{0,1\}^k \to \{0,1\}^n$.
- **על מנת לתייג הודעה** $M \in \{0,1\}^{2n}$ **מפעילים שני סיבובי פייסטל עם אותו המפתח** K**:**
  - **הקלט** M **מחולק לשני חצאים** L_0, R_0.
  - **בסיבוב הראשון** $L_1 = R_0, R_1 = AES(R_0, K) \oplus L_0$.
  - **בסיבוב השני** $L_2 = R_1, R_2 = AES(R_1, K) \oplus L_1$.
  - **הפלט הנו** L_2, R_2.
- **הניחו לאורך השאלה כי בהנתן** K **הפונ'** $MAC(\cdot, K)$ **הנה דטרמיניסטית.**
- **אין צורך להניח דבר על המימוש והתכונות של** AES.



סעיף א' (10 נק')

הראו כי יריב היכול לבקש תג על הודעה אחת M לבחירתו יכול לייצר תג חוקי על הודעה חדשה $M^* \neq M$ בהסתברות $1 - O(2^{-n})$.

תשובה:
נשים לב כי הפונקציה מוגדרת ע"י

$$L_2 = AES_K(R_0) \oplus L_0 \quad R_2 = AES_K(AES_K(R_0) \oplus L_0) \oplus R_0$$

נבקש תג על $M, 0^n$ עבור M אקראית, ונקבל

$$L_2 = AES_K(0^n) \oplus M \quad R_2 = AES_K(AES_K(0^n) \oplus M)$$

כעת נקבע $M^* = AES_K(0^n), 0^n$, ונחשב

$$MAC_K(M^*) = \begin{array}{rcccc} L_2 & = & AES_K(0^n) \oplus AES_K(0^n) & = & 0^n \\ R_2 & = & AES_K(AES_K(0^n) + AES_K(0^n)) + 0^n & = & AES_K(0^n) \end{array}$$

ואת המידע הזה אנו כבר יודעים מהשאילתא שביצענו.
נותר לשים לב כי $AES_K(0^n) \neq M$ בהסתברות $1 - 2^{-n}$, כי M נבחרה באקראי.

סעיף ב' (10 נק')

בנסיון לתקן את הסכמה נרכיב אותה עם פונקציה פסאודו אקראית $F : \{0,1\}^{2n} \times \{0,1\}^k \to \{0,1\}^{2n}$.
כלומר הסכמה החדשה נתונה ע"י ההרכבה

$$MAC'(M, K, K') = F(MAC(M, K), K')$$

הראו כי בהנתן אלגוריתם (דטרמיניסטי) יעיל A, המקבל תג על הודעה M לבחירתו ומייצר תמיד תג חוקי $MAC'(M^*, K, K')$ על הודעה חדשה $M^* \neq M$, ניתן לבנות אלגוריתם יעיל A' המבחין בין גישת אורקל (אוב) לפונקציה אקראית $R : \{0,1\}^{2n} \to \{0,1\}^{2n}$ לגישת אורקל לפונקציה $F(\cdot, K)$, עבור K אקראי. אין צורך לנתח את הסתברות האבחנה של A'.

תשובה:
בהנתן אלג' המצליח לזייף תג לאחר שאילתא אחת, נבנה מבחין A' באופן הבא. המבחין ידגום מפתח K עבור AES נסמן ב־P את הפרמוטציה המתקבלת ע"י שני סיבובי פייסטל עם AES_K. המבחין A' יריץ את A אשר יפיק שאילתא M. A' ישאל את האוב על $P(M)$ ויחזיר את התשובה T ל-A. במידה והאוב הנו פונ' פסאודו־אקראית $F_{K'}$, A בהכרח יפיק הודעה חדשה M^* ביחד עם $F_{K'}(P(M^*))$, אם האוב הנו פונקציה אקראית R, הסיכוי של A לחשב את $R(P(M^*))$ הנו זניח (לכל היותר 2^{-2n}), שכן $P(M^*) \neq P(M)$. לכן A' יוכל להבחין ע"י שישאל את האוב על $P(M^*)$ וישווה לתג T^* ש-A הפיק.

שאלה 3 (סה"כ 30 נק')

בפרוטוקול OR-Oblivious Transfer (OR-OT) ל-S קלטים $m_0, m_1, s \in \{0,1\}$ ול-R קלט $r \in \{0,1\}$. בסוף הפרוטוקול R אמור ללמוד את m_b ולא ללמוד דבר על m_{1-b} עבור $b = OR(r,s)$.

נציע פרוטוקול לחישוב שער $OR-OT$ עבור S, R ישרים אך סקרנים:

1. S דוגם ארבעה מפתחות אקראיים $K_S^0, K_S^1, K_R^0, K_R^1$.
2. S שולח ל-R שער OR "יאו-מקושקש", המורכב מהצפנות

$$E_{K_S^0}(E_{K_R^0}(m_0)) \quad E_{K_S^0}(E_{K_R^1}(m_1)) \quad E_{K_S^1}(E_{K_R^0}(m_1)) \quad E_{K_S^1}(E_{K_R^1}(m_1))$$

בסדר אקראי.

3. S שולח ל-R את K_S^s.
4. בעזרת Oblivious Transfer "רגיל", S שולח גם את K_R^r.

סעיף א' (10 נק')

ניר הציע לממש את סכמת ההצפנה על-ידי One-Time Pad, כלומר המפתח הנו ביט יחיד $K \in \{0,1\}$ והצפנה של ביט $m \in \{0,1\}$ מחושבת על-ידי $E_K(m) = m \oplus K$.

הסבירו מדוע במימוש זה יתקשה R ללמוד את הפלט הנכון m_b, עבור $b = OR(r,s)$.

תשובה:
שני המפתחות ש-R מחזיק הנם ביטים יחידים וכך גם כל אחת מההצפנות. אלג' הפענוח על-כן יחזיר ביט כלשהו לכל אחת מהשורות ואין דרך לדעת איזו מבין השורות שסודרו באקראי מייצגת את התוצאה (אכן, בהס' קבועה לא כל הערכים זהים).

סעיף ב' (10 נק')

בני הציע לתקן את הבעיה ע"י שימוש ב-One-Time Pad עם מפתחות ארוכים, כלומר $K \in \{0,1\}^n$, עבור $n \in \mathbb{N}$ גדול, ו-$E_K(m) = \begin{cases} m^n \oplus K & |m| = 1 \\ m \oplus K & |m| = n \end{cases}$.

הראו כיצד במימוש זה יכול R ללמוד את הפלט הנכון m_b בהסתברות $1 - O(2^{-n})$, כאשר ההסתברות הינה על פני בחירת המפתחות $K_S^0, K_S^1, K_R^0, K_R^1 \in \{0,1\}^n$ באקראי.

תשובה:
R ישתמש במפתחות העומדים לרשותו על־מנת לפתוח כל אחת מההצפנות. בשורה הנכונה המתאימה לפלט m_b הוא יראה m_b^n. נראה כי למעט בהסתברות $O(2^{-n})$ בשורות האחרות המחרוזות אינן מהצורה m^n עבור $m \in \{0,1\}$. בכל אחת מהשורות האחרות הערך הנו סכום של מפתחות אקראיים ב"ת ומחרוזת בת ביט יחיד ב"ת. סכום מפתחות זה מתפלג יוניפורמית ופוגע במחרוזת בת ביט יחיד בהסתברות לכל היותר 2^{-n+1} וסה"כ ההתסברות לשגיאה באחת משלושת השורות הנה לכל היותר $3 \cdot 2^{-n+1}$.

סעיף ג' (10 נק')

ניר התלונן כי על־אף הנכונות, הפרוטוקול אינו בטוח. הראו כי כאשר $(s,r) = (0,0)$, R ישר אך סקרן יכול ללמוד, בהסתברות $1 - O(2^{-n})$, לא רק את m_0 אלא גם את m_1.

תשובה:
נתבונן בהצפנות (נניח לפני הפרמוטציה האקראית):

$$\begin{array}{ccccc} K_S^0 & \oplus & K_R^0 & \oplus & m_0^n \\ K_S^0 & \oplus & K_R^1 & \oplus & m_1^n \\ K_S^1 & \oplus & K_R^0 & \oplus & m_1^n \\ K_S^1 & \oplus & K_R^1 & \oplus & m_1^n \end{array}$$

נשים לב עי ע"י סכימה (מודולו 2) של השורות נקבל $m_0^n \oplus m_1^n$. מאחר ואת m_0^n אנו לומדים בהסתברות $1 - O(2^{-n})$ (בהתאם לסעיף הקודם), נוכל ללמוד את m_1 כנדרש.

שאלה 4 (סה"כ 20 נק')

עבור $N = pq$, כאשר p, q ראשוניים, נסמן ב-$\mathbb{QR}$ את חבורת השאריות הריבועיות ב- $\mathbb{Z}_N^*$.
נציע פרוטוקול אינטרקטיבי (P, V) להוכחה כי קלט נתון $y \in \mathbb{Z}_N^*$ הנו ב־$\mathbb{QR}$:

- קלט משותף: $y \in \mathbb{QR}$.
- קלט פרטי של P: $x \in \mathbb{Z}_N^*$ המקיים $y = x^2 \mod N$.

1. $P \to V$: P דוגם $r_1, r_2 \in \mathbb{Z}_N^*$ באקראי תחת האילוץ $r_1 \cdot r_2 = 17 \mod N$, קובע $r_3 := x \cdot r_1 \cdot r_2$, ושולח ל־$V$ את $\{a_j = r_j^2 \mod N\}_{j \in [3]}$.
2. $P \leftarrow V$: V דוגם $1 \le i \le 3$ באקראי ושולח ל־P את i.
3. $P \to V$: P שולח ל־V את $r = r_i$.
4. V: V מקבל אמ"מ $r^2 = a_i \mod N$ וכן $a_3 = y \cdot a_1 \cdot a_2 \mod N$.

סעיף א' (10 נק')

הראו כי עבור קלט משותף $y \notin \mathbb{QR}$, ולכל מוכיח רשע P^*, המוודא V דוחה בהסתברות לפחות $1/3$.

תשובה:
אם $a_3 \neq y \cdot a_1 \cdot a_2$ V דוחה. אחרת, קיים $i \in [3]$ כך ש-$a_i \notin \mathbb{QR}$. אכן במידה ו־a_1, a_2 שאריות ריבועיות אזי $y \cdot a_1 \cdot a_2$ אינו. V יבקש שורש של a_i בהסתברות $1/3$ והמוכיח לא יכול לספק שורש שכזה.

סעיף ב' (10 נק')

הראו כי הפרוטוקול אינו "אפס־ידע" (ניתן להניח כי קשה למצוא שורשים ב-$\mathbb{Z}_N^*$ מבלי לדעת את p, q).

תשובה:
מוודא (אפילו ישר) מקבל את $r_3 = x \cdot r_1 \cdot r_2 = x \cdot 17 \mod N$ **בהס' 1/3, ויכול ללמוד את השורש** x **של** y **ע"י הכפלה ב-**$17^{-1} \mod N$ **(וכאמור הנחנו שקשה למצוא כזה שורש בהנתן** y **בלבד).**

מסגרת "חירום" לשאלה מספר _____, סעיף _____:

מסגרת "חירום" לשאלה מספר _____, סעיף _____: