ת.ז.: _____ מס' מחברת: _____

מבחן בקורס "מבוא לקריפטוגרפיה מודרנית"

סמסטר א' התשע"ד, מועד ב'

תאריך: 21.2.2014

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!

1					
2א		2ב			
3א		3ב		4ג	
4א		4ב		4ג	

ת.ז.: _____ מס' מחברת: _____

שאלה 1 (סה"כ 20 נק')

לאחר שהתפעל מהרצאתו של צביקה, החליט בני לנסות ולממש בעצמו הצפנה הומומורפית בעזרת קריפטוגרפיה משנות השבעים, מערכת RSA. מאחר והמערכת כבר הומומורפית לכפל מודולו N, כל שנותר לבני לעשות הוא לממש אלגוריתם יעיל לחיבור הומומורפי. האלגוריתם $ADD(N, e, M_1^e, M_2^e)$, מקבל כקלט מפתח פומבי $N = pq$, $e \in \mathbb{Z}^*_{\phi(N)}$ ושתי הודעות מוצפנות $M_1^e, M_2^e \mod N$ ופולט $(M_1 + M_2)^e \mod N$. בני הציע לניר למשכן את דירתו ולהשקיע בחברת הזנק שתפתח את הרעיון. לאחר בדיקת נאותות ממושכת, ניר סרב להשקיע, וטען כי החברה מועדת לכשלון.

הראו כי עבור $e = 3$ ו-$N = pq$ כך ש-$3 \in \mathbb{Z}^*_{\phi(N)}$ ו-p, q ראשוניים גדולים (למשל $2^{100} < p, q$), אם קיים אלגוריתם ADD יעיל כנ"ל , ניתן להשתמש בו על-מנת לפתור ביעילות את בעיית RSA. ספציפית, בהנתן $M^3 \mod N$ עבור $M \in \mathbb{Z}^*_N$ כלשהי, ניתן למצוא ביעילות את M.

תשובה:
בהנתן M^3 נחשב

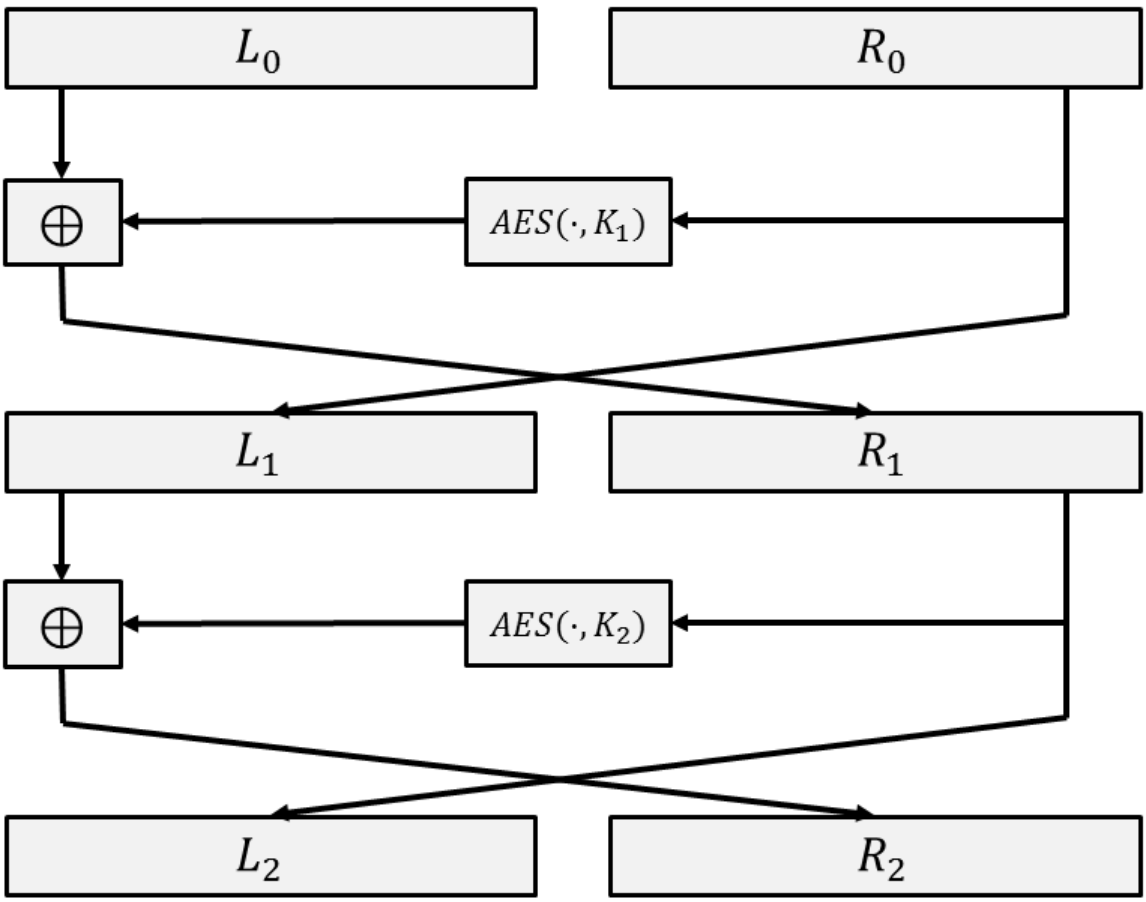
$$\begin{aligned} ADD_{N,3}(M^3, 1^3) &= (M+1)^3 = M^3 + 3M^2 + 3M + 1 \mod N \\ ADD_{N,3}(M^3, (-1)^3) &= (M-1)^3 = M^3 - 3M^2 + 3M - 1 \mod N \end{aligned}$$

ע"י חיבור המשוואות וחיסור $2M^3$ נמצא את $6M \mod N$, וכעת על שנותר הוא להכפיל ב-$6^{-1} \mod N$. אפשר להניח כי $\gcd(N, 6) = 1$ משום ש-p, q גדולים.

שאלה 2 (סה"כ 20 נק')

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

- **המפתח** $(K_1, K_2) \in \{0,1\}^{2k}$ **מורכב מזוג מפתחות 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 המפתחות** K_1, K_2**:**
  - **הקלט** M **מחולק לשני חצאים** L_0, R_0.
  - **בסיבוב הראשון** $L_1 = R_0, R_1 = AES(R_0, K_1) \oplus L_0$.
  - **בסיבוב השני** $L_2 = R_1, R_2 = AES(R_1, K_2) \oplus L_1$.
  - **הפלט הנו** L_2, R_2.
- **בהנתן** K_1, K_2 **הפונ'** $MAC(\cdot, K_1, K_2)$ **הנה דטרמיניסטית.**
- **ניתן להניח (אם כי לא חייבים) כי לכל** $M \in \{0,1\}^n$ **קבועה,** $AES(M, K)$ **מתפלג באופן אחיד, עבור** K **אקראי.**



סעיף א' (10 נק')

הראו כי יריב היכול לבקש תגים עבור שתי הודעות M_1, M_2 לבחירתו יכול לייצר תג חוקי על הודעה חדשה $M^* \notin \{M_1, M_2\}$ בהסתברות $1 - O(2^{-n})$, על־פני בחירת המפתחות K_1, K_2 והבחירות האקראיות של היריב (במידה והוא הסתברותי). במידה ואינכם מצליחים, ניתן לבקש תג על הודעה שלישית M_3 (ולמצוא תג על $M^* \notin \{M_1, M_2, M_3\}$) - פתרון שכזה יחויב ב"קנס" של שתי נקודות.

תשובה:
נשים לב כי הפונקציה מוגדרת ע"י:

$$L_2 = AES_{K_1}(R_0) \oplus L_0 \quad R_2 = AES_{K_2}(AES_{K_1}(R_0) \oplus L_0) \oplus R_0$$

נבקש תג על $M, 0^n$**, ונקבל:** $L_2 = AES_{K_1}(0^n) \oplus M \quad R_2 = AES_{K_2}(AES_{K_1}(0^n) \oplus M)$
נבקש תג על $0^n, 1^n$**, ונקבל:** $L_2 = AES_{K_1}(1^n) \quad R_2 = AES_{K_2}(AES_{K_1}(1^n)) \oplus 1^n$
כעת נקבע $M^* = AES_{K_1}(0^n) \oplus AES_{K_1}(1^n), 0^n$**, ונחשב**

$$MAC_K(M^*) \begin{matrix} = \\ = \end{matrix} \begin{matrix} AES_{K_1}(0^n) \oplus AES_{K_1}(0^n) \oplus AES_{K_1}(1^n) \\ AES_{K_2}(L_2) \oplus 0^n \end{matrix} = \begin{matrix} AES_{K_1}(1^n) \\ AES_{K_2}(AES_{K_1}(1^n)) \end{matrix}$$

ואת המידע הזה אנו כבר יודעים מהשאילתא שביצענו. נותר לשים לב כי, בהסתברות $1 - 2^{-n}$**,** $AES_{K_1}(0^n) \oplus AES_{K_1}(1^n) \neq M$ **, כי** M **נבחרה באקראי ולכן** $M^* \notin \{M_1, M_2\}$**.**

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

$$MAC'(M, K_1, K_2, K_3) = MAC(F(M, K_3), K_1, K_2)$$

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 מפתחות K_1, K_2 עבור AES נסמן ב־P את הפרמוטציה המתקבלת ע"י שני סיבובי פייסטל אם AES_{K_1}, AES_{K_2}. המבחין A' יריץ את A אשר יפיק שאילתא M. A' ישאל את האוב על M ובהנתן תשובה Y, יחזיר את התשובה $T = P(Y)$ ל-A. במידה והאוב הנו פונ' פסאודו־אקראית F_K, A בהכרח יפיק הודעה חדשה M^* ביחד עם $P(F_K(M^*))$, אם האוב הנו פונקציה אקראית R, הסיכוי של A לחשב את $P(R(M^*))$ הנו זניח (לכל היותר 2^{-2n}). לכן A' יוכל להבחין ע"י שישאל את האוב על M^* , ובהנתן תשובה Y ישווה את $P(Y)$ לתג T^* ש-A הפיק.

שאלה 3 (סה"כ 30 נק')

בפרוטוקול OR-Oblivious Transfer (OR-OT) למשתתף S שלושה קלטים $m_0, m_1, s \in \{0,1\}$ ולמשתתף R קלט יחיד $r \in \{0,1\}$. 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 משתתפים S, R ישרים אך סקרנים:

1. S דוגם ארבעה מפתחות אקראיים ובלתי תלויים $K_S^0, K_S^1, K_R^0, K_R^1$.
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", R מקבל גם את K_R^r.

סעיף א' (10 נק')

ניר הציע לממש את סכמת ההצפנה על-ידי One-Time Pad מודולו p. כלומר כל מפתח הנו איבר אקראי $K \in \mathbb{Z}_p$, עבור p ראשוני גדול. ההצפנה של ביט $m \in \{0,1\} \subset \mathbb{Z}_p$ מחושבת על-ידי

$$E_K(m) = m + K \mod p.$$

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

תשובה:
R ישתמש במפתחות העומדים לרשותו על-מנת לפתוח כל אחת מההצפנות. בשורה הנכונה המתאימה לפלט m_b הוא יראה $m_b \in \{0,1\}$. נראה כי למעט בהסתברות $O(p^{-1})$ בשורות האחרות המחרוזות אינן בקבוצה $\{0,1\}$. בכל אחת מהשורות האחרות הערך הנו סכום (או הפרש) של מפתחות אקראיים ב"ת ואיבר ב-$\{0,1\}$. סכום מפתחות זה מתפלג יוניפורמית ב-$\mathbb{Z}_p$ ופוגע בקבוצה $\{0,1\}$ בהסתברות לכל היותר $2/p$ וסה"כ ההתסברות לשגיאה באחת משלושת השורות הנה לכל היותר $6/p$.

סעיף ב' (10 נק')

נניח כי S פעל לפי הפרוטוקול, אך שכח לערבב באקראי את ארבעת ההצפנות.

הראו כי כאשר $(s,r)=(0,0)$, R ישר אך סקרן יכול ללמוד לא רק את m_0 אלא גם את m_1.

תשובה:
נתבונן בהצפנות לפני הפרמוטציה האקראית:

$$\begin{array}{ccccc} K_S^0 & + & K_R^0 & + & m_0 \mod p \\ K_S^0 & + & K_R^1 & + & m_1 \mod p \\ K_S^1 & + & K_R^0 & + & m_1 \mod p \\ K_S^1 & + & K_R^1 & + & m_1 \mod p \end{array}$$

נחבר את המשוואה הראשונה לרביעית, נחסר את המשוואות השניה והשלישית ונקבל $m_0 - m_1 \mod p$, בעזרת K_S^0, K_R^0 נלמד מהשורה הראשונה את m_0 וכעת נחלץ את m_1.

סעיף ג' (10 נק')

בני טוען כי גם אם S פעל בדיוק לפי הפרוטוקול, ולא שכח לערבב באקראי את ארבעת ההצפנות, הפרוטוקול עדיין אינו בטוח.

הראו כי כאשר $(s,r)=(0,0)$, R ישר אך סקרן עדיין יכול ללמוד לא רק את m_0 אלא גם את m_1, בהתסתברות $1-O(p^{-1})$, על־פני בחירת המפתחות האקראיים.

תשובה:
ראשית נגלה מהי השורה הראשונה (לפני הערבוב האקראי) בהס' $1-O(p^{-1})$ כמו בסעיף א'. כעת ננסה שלוש אפשרויות שונות עבור השורה הרביעית. עבור על אחד מהאפשרויות נפעל לפי אלגוריתם השחזור שתיארנו בסעיף ב'. עבור האפשרות הנכונה נמצא את m_1. נשים לב שבכל אחת משתי האפשרויות הלא נכונות נקבל אחת מהתוצאות:

$$\begin{array}{l} 2(K_R^0 - K_R^1) + m_0 - m_1 \\ 2(K_S^0 - K_S^1) + m_0 - m_1 \end{array}$$

בכל מקרה התוצאה מתפלגת יוניפורמית ב-$\mathbb{Z}_p$ ולכן תהיה ב־$\{0,1\}$ בהסתברות לכל היותר $O(p^{-1})$. (שימו לב כי 2 הפיך לכפל מודולו p, כי p ראשוני גדול.) בהתאם, נוכל לזהות מתי בחרנו באפשרות הנכונה.

שאלה 4 (סה"כ 30 נק')

בני וניר מחזיקים בקלט משותף N. בני טוען כי בידו p, q כך ש-$N = pq$. ניר חושד כי N הנו מהצורה pqr. על-מנת להפיג את חשדו של ניר, הם מריצים את פרוטוקול ההוכחה הבא.

1. ניר דוגם $x \in \mathbb{Z}_N^*$ באקראי ושולח לבני את $y = x^2 \mod N$.
2. בני מוצא את כל השורשים $X = \{ x_i \in \mathbb{Z}_N^* : y = x_i^2 \mod N\}$ ושולח את הרשימה X לניר.
3. ניר מקבל אמ"מ $|X| = 4$ וכן $x \in X$. (כלומר בני שולח רשימה בת ארבעה איברים ו-x הנו אחד מהם.)

סעיף א' (10 נק')

יהי $N = pqr$ עבור p, q, r ראשוניים שונים. יהי $y = x^2 \in \mathbb{Z}_N^*$, הראו כי ל-$y$ שמונה שורשים ריבועיים שונים, כלומר $X = \{x_1, \ldots, x_8\}$ כך שלכל i מתקיים $y = x_i^2 \mod N$.

תשובה:
ל-y יש שני שורשים $(x_p, -x_p), (x_q, -x_q), (x_r, -x_r)$ מודולו כל אחד מהראשוניים p, q, r. לפי משפט השאריות הסיני קבוצת השורשים מודולו N נתונה בדיוק ע"י בחירת אחת משמונה קומבינציות

$$x_{b_p b_q b_r} = \begin{cases} (-1)^{b_p} x_p & \mod p \\ (-1)^{b_q} x_q & \mod q \\ (-1)^{b_r} x_r & \mod r \end{cases}$$

עבור $b_p b_q b_r \in \{0,1\}^3$.

סעיף ב' (10 נק')

הראו כי בפרוטוקול הנ"ל, אם N הנו מהצורה pq, בני משכנע את ניר בהסתברות 1 (שלמות). הראו כי אם N הנו מהצורה pqr, ניר מקבל בהסתברות שאינה עולה על $1/2$ (נאותות). ניתן להשתמש בסעיף א' גם אם לא פתרתם אותו.

תשובה:
אם אכן $N = pq$ קיימים ל-y בדיוק ארבעה שורשים והשורש x אשר ניר בחר הנו אחד מהם. בני, היודע את p, q יחשב נכונה שורשים אלו וישלח רשימה בגודל המתאים המכילה את x. אם $N = pqr$ ל-y שמונה שורשים שונים $x_1 \dots x_8$. ההודעה $y = x^2$ הנשלחת ע"י ניר אינה תלויה בבחירה של איזה מבין השורשים נשלח (כלומר בעבור איזה i מתקיים $x = x_i$), בפרט הקבוצה X שבני שולח חזרה אינה תלויה ב-i. מאחר וניר בוחר את x באקראי, לכל x_i יש סיכוי שווה של $1/8$ להבחר, ולכן אם $|X| = 4$, ההסתברות כי $x \in X$ הנה לכל היותר $1/2$ כנדרש.

סעיף ג' (10 נק')

כאשר בני הגון ואכן $N = pq$, הפרוטוקול הנ"ל מאפשר לניר ללמוד את כל ארבעת השורשים של ריבוע s אקראי (בפרט הפרוטוקול אינו "אפס־ידע" בהנחה שקשה לחשב שורשים ב-$\mathbb{Z}_N^*$). הציעו פרוטוקול בן ארבע הודעות, המשתמש בסכמת התחייבות, ובו ניר לא לומד אף שורש שאינו יכול ללמוד בעצמו ביעילות. על הפרוטוקול לשמור על תכונות השלמות והנאותות. אין צורך בהוכחה. (אנו מזכירים כי התחייבות להודעה מסתירה בפני יריב מוגבל חישובית את תוכן ההודעה עד לפתיחת ההתחייבות, וכי לא ניתן לפתוח את ההתחייבות אלא באופן יחיד. הניחו כי התחייבות דורשת הודעה אחת, ופתיחת ההתחייבות דורש הודעה אחת.)

תשובה:
במקום לשלוח את הקבוצה X בהודעה השני, בני שולח ארבע התחייבויות, אחת לכל שורש $x_i \in X$. כעת בהודעה השלישית ניר חושף את x אשר בחר. לבסוף, בהודעה הרביעית, בני פותח את ההתחייבות אך ורק לשורש x.

מסגרת "חירום" לשאלה מספר _____, סעיף _____:

מסגרת "חירום" לשאלה מספר _____, סעיף _____: