ת.ז: _____ מספר מחברת: _____

# מבחן בקורס "מבוא לקריפטוגרפיה מודרנית"

## פתרון

סמסטר א' תשע"ז, מועד א'

**תאריך:** 30.1.2017

**מרצה:** פרופ' בני שור

**מתרגלת:** אורית מוסקוביץ'

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 חמש שאלות פתוחות ולחלקן 2 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, בתרגול 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.
- רמזים הניתנים בשאלות הינם בגדר המלצה, ואין חובה להשתמש בהם.
- המבחן מנוסח בלשון נקבה מטעמי נוחות בלבד, אך מיועד לנשים וגברים כאחד.

## בהצלחה!

| שאלה 1 | שאלה 2 | שאלה 3 | שאלה 4 | שאלה 5 | ציון בחינה |
|---|---|---|---|---|---|
| | | | | | |
| | | | | | |

## **שאלה 1 (סה"כ 15 נק')**

תהי $F:\{0,1\}^n \times \{0,1\}^n \to \{0,1\}^n$ פונקציה פסאודו-אקראית (Pseudorandom function, PRF).

לכל מפתח $k \in \{0,1\}^n$, $F_k$ היא פונקציה מ-$\{0,1\}^n$ ל-$\{0,1\}^n$.

נגדיר את הפונקציה הבאה $F':\{0,1\}^n \times \{0,1\}^n \to \{0,1\}^{2n}$ על ידי

$$F'_k(x) = F_k(x)||F_k\big(rev(x)\big)$$

כאשר עבור $x = x_1x_2 \dots x_n$, מתקיים $rev(x) = x_n \dots x_2x_1$

הוכיחו\הפריכו: $F'$ הינה פונקציה פסאודו-אקראית.

<u>פתרון:</u>

נראה כי $F'$ אינה פונקציה פסאודו-אקראית.

נראה אלגוריתם $A$ המקבל גישת אורקל לפונקציה אקראית $f$ או לפונקציה מהמשפחה $F'$.

נסמן את האורקל ב-$g$.

1. $A$ יבחר $x \in \{0,1\}^n$ המקיים $x = rev(x)$ ויבקש את $g(x)$
2. אם $g(x)$ הינו מהצורה $yy$ כאשר $y \in \{0,1\}^n$, $A$ יחזיר 1 (פונקציה מהמשפחה $F'$)
3. אחרת, יחזיר 0 (פונקציה אקראית $f$)

$$\Pr[A^{F'}\ returns\ 1] = 1$$

$$\Pr\big[A^{f}\ returns\ 1\big] = \frac{1}{2^n}$$

לכן מתקיים:

$$\left|\Pr\big[A^{F'}\ returns\ 1\big] - \Pr\big[A^{f}\ returns\ 1\big]\right| = 1 - \frac{1}{2^n}$$

# שאלה 2 (סה"כ 25 נק')

**סעיף א' (15 נק')**

ביבי ונוני הם ביישנים קיצוניים. שניהם רוצים לבדוק בזהירות האם הצד השני מעוניין לקיים פגישה, להפגש אם שניהם מעוניינים בכך, ובכל מקרה לשמור על פרטיותם.

נסמן ב-$a$ את הביט המציין האם ביבי מעוניין שהם יפגשו, ונסמן ב-$b$ את הביט המציין האם נוני מעוניין שהם יפגשו.

השניים מעוניינים להריץ פרוטוקול המשתמש ב-1 out of 2 oblivious transfer כקופסא שחורה שבסופו הם ידעו את $a \wedge b$ (אחד מהשניים יגלה את התוצאה, ויפרסם אותה).

שימי לב: אין להשתמש במימוש ספציפי עבור OT וכן לא במעגל המקושקש של YAO.

דרישת הפרטיות: אם צד אחד מעוניין להיפגש, והצד השני לא מעוניין - נדרוש שהצד הלא מעוניין לא ידע אם הצד השני היה מעוניין או לא.

אנו מניחים (כמובן) כי שניהם ישרים ועוקבים אחר הפרוטוקול.

תארי פרוטוקול מתאים.

פתרון:

נשתמש ב-1-out-of-2 OT כקופסא שחורה באופן הבא:

נוני יחזיק:

$$s_0 = 0, s_1 = b$$

ביבי יבקש את $s_a$ באמצעות OT.

**נכונות:**

- אם $a = 1$, ביבי יקבל את $b$ ויחשב את $a \wedge b = b$
- אם $a = 0$, ביבי יקבל $0$ ויוציא $0$

**פרטיות:**

- אם נוני לא מעוניין להפגש, תוצאת הפרוטוקול תהיה $0$, ונוני לא ידע מהו הביט של ביבי
- אם ביבי לא מעוניין להפגש, הוא יקבל את $s_0 = 0$ בכל מקרה, ולכן לא ידע מהו הביט של נוני

**סעיף ב' (10 נק')**

נתון הפרוטוקול הבא להוכחת ידע של פענוח ערך מוצפן תחת RSA בין מוכיח (נכלולי) ושמו *בני*, לבין מוודאת (נרגנת וחשדנית) ושמה *אורית*:

<u>קלט משותף:</u> $m = pq$, $e \geq 3$ טבעי זר ל-$(p-1)(q-1)$, וכן $y = x^e \ mod \ pq$, $y \in Z_{pq}^*$

<u>קלט פרטי לבני:</u> $x$

<u>פרוטוקול:</u>

*בני* ← *אורית*: בוחר $r \in Z_{pq}^*$ באקראי, מחשב $t = r^e \ mod \ pq$ ושולח את $t$ לאורית

*אורית* ← *בני*: מטילה מטבע $b$ ושולחת לבני

*בני* ← *אורית*: אם $b = 0$, בני שולח לאורית את $r$

אם $b = 1$, בני שולח לאורית את $z = rx$

*אורית*: אם $b = 0$, מוודאת כי $r^e = t$

אם $b = 1$, מוודאת כי $z^e = ty$

בני ואורית חוזרים על הפרוטוקול 100 פעמים, אם בכל פעם מצליח בני לשכנע את אורית, אורית תשתכנע כי בני אכן יודע $x$ כנ"ל.

אורית מתעצלת להטיל מטבע בכל סיבוב של הפרוטוקול ולכן שולחת באופן קבוע את הביט $b = 1$.

הראי כיצד בני יכול לרמות ולשכנע את אורית כי הוא יודע $x$ כנ"ל, למרות שאין לו מושג מהו $x$.

<u>פתרון:</u>

בני יבחר $a \in Z_{pq}^*$ באקראי, ויחשב $t = a^e y^{-1}$. בהודעה הראשונה בני ישלח את $t$ לאורית.

בהודעה השלישית בני ישלח את $z = a$ לאורית.

אורית תחשב $z^e = a^e$ . כיון ש- $t = a^e y^{-1}$, אז $ty = a^e = z^e$ , ולכן

הבדיקה תצליח, ואורית תשתכנע.

## שאלה 3 (סה"כ 25 נק')

תהיינה $f_0, f_1 : \{0,1\}^n \to \{0,1\}^n$ פונקציות חד חד ערכיות (תמורות). נאמר כי פונקציות אלה הן קשות חיתוך אם קשה (חישובית) למצוא $x, y$ כך ש- $f_0(x) = f_1(y)$.

נגדיר פונקציית ערבול (hash) $h : \{0,1\}^{2n} \to \{0,1\}^n$ באופן הבא: בהנתן $z = b_{2n-1}b_{2n-2} \dots b_n \dots b_1 b_0$

$$h(z) = f_{b_{2n-1}}\left(f_{b_{2n-2}}\left(\dots f_{b_n}\left(\dots f_{b_1}\left(f_{b_0}(0^n)\right)\right)\right)\right)$$

**סעיף א' (15 נק')**

הראי כי הפונקציה $h$ היא עמידה להתנגשויות, כלומר קשה למצוא $s, t \in \{0,1\}^{2n}$ שונים, כך ש-$h(s) = h(t)$.

<u>רמז</u>: הראי כי אם ניתן למצוא $s, t \in \{0,1\}^{2n}$ כך ש-$h(s) = h(t)$ אז ניתן למצוא $x, y$ כך ש-$f_0(x) = f_1(y)$ .

<u>פתרון:</u>

נניח כי $s_{2n-1}s_{2n-2} \dots s_{i+1} = t_{2n-1}t_{2n-2} \dots t_{i+1}$ ואילו הביט הראשון משמאל עבורו s ו-t שונים הוא הביט ה-$i$, כלומר $s_i \neq t_i$ (שימו לב כי $i$ יכול להיות $2n-1$, וחייב להיות $i$ כזה).

נקבל בפרט כי

$$f_{s_{2n-1}}\left(f_{s_{2n-2}}\left(\dots f_{s_n}\left(\dots f_{s_1}\left(f_{s_0}(0^n)\right)\right)\right)\right) = f_{t_{2n-1}}\left(f_{t_{2n-2}}\left(\dots f_{t_n}\left(\dots f_{t_1}\left(f_{t_0}(0^n)\right)\right)\right)\right)$$

אם הביטים השמאליים ביותר של $s, t$ שוים, אז $f_{s_{2n-1}}$ ו- $f_{t_{2n-1}}$ הן אותה פונקציה. כיון שנתון שפונקציות אלה הן חח"ע, נקבל כי

$$\left(f_{s_{2n-2}}\left(\dots f_{s_n}\left(\dots f_{s_1}\left(f_{s_0}(0^n)\right)\right)\right)\right) = \left(f_{t_{2n-2}}\left(\dots f_{t_n}\left(\dots t_{b_1}\left(f_{t_0}(0^n)\right)\right)\right)\right)$$

נוכל להמשיך כך עד שנגיע לביט הביט הראשון משמאל עבורו $s$ ו-$t$ שונים, דהיינו הביט ה-$i$, כאן נקבל

$$\left(f_{s_i}\left(f_{s_{i-1}}\left(\dots f_{s_1}\left(f_{s_0}(0^n)\right)\right)\right)\right) = \left(f_{t_i}\left(f_{t_{i-1}}\left(\dots t_{b_1}\left(f_{t_0}(0^n)\right)\right)\right)\right)$$

מצאנו לכן שני ערכים $x, y$ כך ש-$f_0(x) = f_1(y)$ . סתירה להיות הפונקציות קשות חיתוך.

**סעיף ב' (10 נק')**

מצאי דוגמא (פשוטה!) של זוג פונקציות $f_0, f_1: \{0,1\}^n \to \{0,1\}^n$ קשות חיתוך שאינן חח״ע, ופונקציית הערבול המושרית על ידן כמו קודם אינה עמידה להתנגשויות

<u>פתרון:</u>

ניקח $f_0(x) = 0^n$ לכל $x$, וכן $f_1(x) = 1^n$ לכל $x$.

ברור כי הן קשות חיתוך ואינן חח"ע.

הפעם, $h$ אינה עמידה להתנגשויות.

בפרט,

$$h(100 \dots 0) = h(111 \dots 1) = 1^n$$

## שאלה 4 (סה"כ 15 נק')

תהי $E_k:\{0,1\}^n \to \{0,1\}^n$ פונקציית הצפנה עם מפתח פרטי $E_k$ היא תמורה).

נתון כי לכל שני מפתחות $k_1, k_2 \in \{0,1\}^n$ קיים מפתח שלישי $k_3 \in \{0,1\}^n$ כך שלכל $m \in \{0,1\}^n$ מתקיים:

$$E_{k_1}\left(E_{k_2}(m)\right) = E_{k_3}(m)$$

הוכיחי כי קיים $k \in \{0,1\}^n$ כך שלכל $m \in \{0,1\}^n$

$$E_k(m) = m$$

<u>רמז:</u> מה יקרה אם נפעיל את $E_k$ על עצמה?

<u>פתרון:</u>

יהי $k \in \{0,1\}^n$ מפתח כלשהו.

מהנתון, קיים $k_2 \in \{0,1\}^n$ כך שלכל $m \in \{0,1\}^n$ מתקיים:

$$E_k\left(E_k(m)\right) = E_{k_2}(m)$$

באופן דומה, קיים $k_3 \in \{0,1\}^n$ כך שלכל $m \in \{0,1\}^n$ מתקיים:

$$E_k\left(E_k\left(E_k(m)\right)\right) = E_{k_3}(m)$$

נמשיך עם התהליך $2^n + 1$ פעמים:

$$E_k\left(E_k\left(E_k\left(E_k(m)\right)\right)\right) = E_{k_4}(m)$$

...

$$E_k\left(E_k\left(E_k\left(\dots E_k(m)\right)\right)\right) = E_{k_{2^n+1}}(m)$$

מרחב המפתחות הוא סופי, לכן קיימים אינדקסים $j > i$ עבורם המפתחות $k_i = k_j$. אז מתקיים לכל $m$:

$$E_{k_j}(m) = E_k\left(E_k\left(\dots E_k\left(E_k\left(\dots E_k(m)\right)\right)\right)\right) = E_k\left(E_k\left(\dots E_k(m)\right)\right) = E_{k_i}(m)$$

$E_k$ היא תמורה, לכן מתקיים כי:

$$E_k\left(\dots E_k(m)\right) = m$$

מהנתון, קיים מפתח $k^*$ המקיים:

$$E_k\left(\dots E_k(m)\right) = E_{k^*}(m) = m$$

## שאלה 5 (סה"כ 20 נק')

בשאלה זו נעסוק בחבורה הכפלית $Z_{pq}^*$, ונניח כי $p > q$ ראשוניים גדולים ואינם ידועים (אך $pq$ כן).

כזכור, בחבורה זו אין יוצר כפלי.

בנוסף, נניח כי $g$ יוצר כפלי של $\mathbb{Z}_p^*$ וכי כי $h$ יוצר כפלי של $\mathbb{Z}_q^*$ ($g, h$ ידועים ופומביים).

**סעיף א' (10 נק')**

הראי כי לכל $a \in Z_{pq}^*$ קיימים $0 \leq i \leq p-2$, $0 \leq j \leq q-2$ יחידים כך ש:

$$a = g^i \bmod p$$

$$a = h^j \bmod q$$

פתרון:

ממשפט השאריות הסיני ידוע כי $Z_{pq}^* \sim Z_p^* \times Z_q^*$, לכן, לכל $a \in Z_{pq}^*$ קיימים $r, s$ יחידים כך ש:

$$a = r \bmod p$$

$$a = s \bmod q$$

כיוון ו-$g, h$ הינם יוצרים כפליים ב-$Z_p^*, Z_q^*$ בהתאמה, נקבל כי קיימים $0 \leq i \leq p-2$, $0 \leq j \leq q-2$ יחידים כך ש:

$$a = g^i \bmod p$$

$$a = h^j \bmod q$$

**סעיף ב' (10 נק')**

נניח כי קיים אלגוריתם יעיל $A$ אשר בהנתן $a, g, h \in Z_{pq}^*$, מחזיר את ה-$i, j$ שהוגדרו בסעיף ב':

$$a = g^i \bmod p$$

$$a = h^j \bmod q$$

הראי כיצד להיעזר ב-$A$ על מנת לפרק ביעילות את $pq$.

<u>פתרון:</u>

נריץ את אלגוריתם $A$ על הקלט $g^{pq}$, ונקבל $0 \le i \le p-2$, $0 \le j \le q-2$ יחידים כך ש:

$$g^{pq} = g^i \bmod p$$

$$g^{pq} = h^j \bmod q$$

נרצה לבחון מיהו $i$.

$$g^{pq} \bmod p = g^{pq \bmod p-1} = g^{pq-q(p-1)} = g^{pq-(pq+q)} = g^q$$

לכן, נקבל כי $i = q$ ומכאן קל לגלות את $p$.

<u>פתרון אלטרנטיבי:</u>

נריץ את אלגוריתם $A$ על הקלט $g^{-1}$, ונקבל $0 \le i \le p-2$, $0 \le j \le q-2$ יחידים כך ש:

$$g^{-1} = g^i \bmod p$$

$$g^{-1} = h^j \bmod q$$

נרצה לבחון מיהו $i$.

$$g^{-1} \bmod p = g^{-1 \bmod p-1} = g^{p-2}$$

לכן, נקבל כי $i = p-2$ ומכאן קל לגלות את $p, q$.