ת.ז.: _____ מס' מחברת: _____

מבחן בקורס "מבוא לקריפטוגרפיה מודרנית"

סמסטר א' התשע"ד מבחן חלקי לדוג'

תאריך: 12.1.2014

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.

בהצלחה!

1	
2	
3	

שאלה 1

בני וניר חולקים מפתח $K \in \{0,1\}^k$ לפונקציית אותנטיקציה $MAC : \{0,1\}^n \times \{0,1\}^k \to \{0,1\}^n$ המתייגת הודעות באורך n ע"י מחרוזות באורך n.

בני מעוניינת לשלוח לניר הודעות מתוייגות באורך $3n$, לשם כך ניר הציע לו לבנות פונ' חדשה $MAC' : \{0,1\}^{3n} \times \{0,1\}^k \to \{0,1\}^n$ המוגדרת ע"י $MAC'(M,K) = MAC(H(M),K)$, כאשר $H : \{0,1\}^{3n} \to \{0,1\}^n$. שפ וניר לא מצליחים להסכים כיצד יש לממש את H.

סעיף א'

ניר מציע לממש את H באופן הבא: בהנתן קלט $M \in \{0,1\}^{3n}$, נפרשו כייצוג בינארי של מספר $0 \leq m < 2^{3n}$ נחשב $m' = m \mod 2^n$ ונחזיר את הייצוג הבינארי $M' \in \{0,1\}^n$ של m'.

הראו כי בהנתן הודעה שרירותית $M \in \{0,1\}^{3n}$ ותג $T = MAC'(M,K)$, ניתן לזייף תג חוקי T^* על הודעה חדשה $M \neq M^*$. (הניחו כי, בהנתן K, $MAC(\cdot,K)$ דטרמיניסטית.)

תשובה:

סעיף ב'

איזו תכונה ניתן לדרוש מ־H על־מנת לשמור על הבטיחות של המערכת כנגד יריבים חסומים חישובית (בהנחה כי הפונ' MAC בטוחה נגד יריבים חסומים). כלומר יריב חסום היכול לבקש תגים על הודעות $\{M_i\}$ לבחירתו, אינו יכול לזייף תג חוקי עבור הודעה $M^* \notin \{M_i\}$. נמקו תשובתכם בקצרה.

תשובה:

שאלה 2

נציע פרוטוקול (S,R) ל-Oblivious Transfer נגד יריבים ישרים אך סקרנים:

קלט של R: ביט b.
קלט של S: שני ביטים $m_0, m_1 \in \{0,1\}$
$R \to S$: **בוחר** $N = pq : p,q = 3 \mod 4$, $r_0, r_1 \leftarrow Z_N^*$, **ושולח את N ואת** $\begin{matrix} c_0 = (-1)^{1-b} r_0^2 \mod N \\ c_1 = (-1)^b r_1^2 \mod N \end{matrix}$.
$S \leftarrow R$: **שולח את** $a = c_0^{m_0} \cdot c_1^{m_1} \mod p$.
S: **אם a הנו שארית ריבועית קובע $m_b = 0$ אחרת קובע $m_b = 1$.**

סעיף א'

נסמן ב-QR_p,QR_q, QR_N את חבורות השאריות הריבועיות ב-Z_p^*,Z_q^* וב-Z_N^* בהתאמה. הראו כי $-1 \notin QR_p \cup QR_q$. הסבירו מדוע מכך נובע כי $-1 \notin QR_N$.

תשובה:

סעיף ב'

הראו כי בפרוטוקול הנ"ל R אכן יכול לבדוק ביעילות, בהנתן p, q, האם $a \in QR_N$ וכי הוא אכן לומד בסוף את הערך הנכון m_b.

תשובה:

סעיף ג'

הראו כי בפרוטוקול הנ"ל R סקרן יכול גם ללמוד את m_{1-b}. הציעו תיקון לפרוטוקול שימנע זאת (אין צורך בהוכחה).

תשובה:

שאלה 3

בהנתן גרף $G = ([n], M)$ עם קודקודים $[n] = \{1, 2, \ldots, n\}$ ומטריצת שכנויות $M \in \{0,1\}^{n \times n}$ (כלומר, יש קשת (i,j) אמ"מ $M[i,j] = 1$), נאמר כי בגרף **מעגל המילטוני** אם קיים מעגל המורכב מקשתות העובר דרך כל הקודקודים. כלומר, קיימת פרמוטציה של הקודקודים $c : [n] \to [n]$ כך ש-לכל $i \in [n]$, $M[c(i), c(i+1 \mod n)] = 1$.

נציע פרוטוקול אינטרקטיבי (P, V) להוכחה כי בגרף נתון קיים מעגל המילטוני.

<u>קלט משותף</u>: $G = ([n], M)$ גרף עם מעגל המילטוני.
<u>קלט סודי של המוכיח P</u>: מעגל המילטוני $c : [n[\to [n]$

$P \to V$: P שולח n^2 התחייבויות, אחת לכל אחד מערכי מטריצת השכנויות $M[i,j]$.

$P \leftarrow V$: V שולח ביט אקראי b.

$P \to V$: P אם $b = 0$ פותח את כל ההתחייבויות. אם $b = 1$, שולח את c ופותח רק את ההתחייבויות של קשתות המעגל $M[c(i), c(i+1 \mod n)]$.

V: אם $b = 0$, מקבל רק אם ההתחייבויות אכן למטריצה הנכונה M. אם $b = 1$, מקבל רק אם c אכן מתאר מעגל. כלומר, c פרמוטציה ולכל $i \in [n]$, $M[c(i), c(i+1 \mod n)] = 1$.

סעיף א'

הראו כי אם $G = ([n], M)$ **אינו** מכיל מעגל המילטוני, V מקבל בהס' לכל היותר $1/2$. כלומר לפרוטוקול נאותות $1/2$.

תשובה:

סעיף ב'

האם הפרוטוקול הנו פרוטוקול אפס־ידע נגד V^* רשע? נמקו תשובתכם. (הניחו כי לא ניתן לחשב ביעילות מעגל המילטוני.)

תשובה:

סעיף ג'

הציעו כיצד להפוך את הפרוטוקול לפרוטוקול אפס־ידע נגד V ישר אך סקרן (ומבלי לפגוע בנאותות או שלמות). נמקו תשובתכם (אין צורך בהוכחה פורמלית). רמז: עבור פרמוטציה שרירותית $c : [n] \to [n]$ ופרמוטציה אקראית $\sigma : [n] \to [n]$, ההרכבה $\sigma \circ c$ מתפלגת כפרמוטציה אקראית.

תשובה: