

מבחן ביסודות הקריפטוגרפיה: מועד א' סמסטר ב' 2012.

מרצה: רונן שאלתיאל.

זמן: 2.5 שעות.

חומר עזר: אין.

הוראות:

ענה על 2 מתוך 3 השאלות הבאות.

יש לכתוב תשובות בהירות ומדויקות. כאשר אתם נדרשים להגדיר מושגים יש לתת הגדרה פורמלית מלאה. אם אינכם יודעים התשובה לאחד הסעיפים, ניתן לענות "לא יודע". תשובה כזו תקבל 20% מהניקוד, ומותר להשתמש בנכונות הסעיף בהמשך השאלה.

1. ענה על הסעיפים הבאים:

א. (10 נקודות) הגדר מהי הוכחה אינטראקטיבית (Interactive proof), ומתי הוכחה כזו היא Zero Knowledge.

יהיו L_1, L_2 שפות ב-NP, ונגדיר את השפה $L = \{x: \exists i \in \{1, 2\}, x \in L_i\}$. ראינו בכיתה שגם ל- L_1 וגם ל- L_2 ישנם פרוטוקולים להוכחה אינטראקטיבית ב-Zero Knowledge. מוצע הפרוטוקול הבא להוכחה אינטראקטיבית עבור L: בהינתן $x \in L$ המוכיח P ימצא i כך ש- $x \in L_i$, ישלח אותו למוודא V ויוכיח ויוכיח למוודא V ש- $x \in L_i$ לפי הפרוטוקול שציינו קודם. הוכח או הפרך את הטענות הבאות לגבי הפרוטוקול המוצע.

ב. (8 נקודות) לפרוטוקול יש completeness.

ג. (8 נקודות) לפרוטוקול יש soundness.

ד. (8 נקודות) הפרוטוקול הוא Zero Knowledge.

ה. (16 נקודות) הצע פרוטוקול אחר שיש לו את כל שלוש התכונות.

2. ענה על הסעיפים הבאים:

א. (10 נקודות) הגדר מהו גנרטור פסאודו אקראי (pseudorandom generator).

ב. (20 נקודות) יהיה G גנרטור פסאודו אקראי עם פונקציית מתיחה n^2 . ותהי H פונקציה שניתנת לחישוב בזמן פולינומי, כך שעל קלט מאורך n, H פולטת פלט מאורך n^2 . הוכח כי הפונקציה: $G'(x_1, x_2) = G(x_1) \text{ xor } H(x_2)$ היא pseudorandom generator. מהי פונקציית המתיחה שלה?

ג. (20 נקודות) נתונות שתי פרמוטציות f_1, f_2 שניתנות לחישוב בזמן פולינומי. ידוע לנו שלפחות אחת מהן היא פרמוטציה חד כוונית אבל איננו בטוחים ששתיהן פרמוטציות חד כווניות. כיצד ניתן לבנות pseudorandom generator בהסתמך אך ורק על שתי הפרמוטציות? (כדאי להשתמש בסעיף ב).

3. ענה על הסעיפים הבאים:

א. (10 נקודות) תהי $f(x)$ פונקציה. הגדר מהו ביט קשה עבור f .

תהי $f(x)$ פונקציה, ונניח שקיים אלגוריתם פולינומי B כך שלכל n גדול מספיק, כאשר בוחרים באקראי מחרוזת x מאורך n ומספר i בין 1 ל- n . מתקיים $\Pr_{x,i}[B(f(x),i)=x_i] \geq 1-1/4n$ (כאשר x_i מסמן את הביט ה- i ב- x). מטרתנו היא להוכיח ש- f אינה חד כוונית. לשאלה שתי גרסאות. גרסה קלה בסעיף ב, וגרסה קשה יותר בסעיף ג. אם אתם יודעים לפתור את ג, אין צורך לפתור את ב.

ב. (20 נקודות) הוכח כי f אינה חד כוונית תחת ההנחה החזקה יותר שהמספר $1-1/4n$ מוחלף ב- 1 כלומר לכל x ו- i מתקיים $B(f(x),i)=x_i$.

ג. (40 נקודות) הוכח כי f אינה חד כוונית תחת ההנחה המקורית. הדרכה: כדאי להסתכל בקבוצה הבאה:

$G = \{x : \Pr_i[B(f(x),i)] \geq 1-1/2n\}$ (שימו לב שההסתברות בהגדרת G הינה על i בלבד) ולנסות להוכיח כי כאשר בוחרים x מאורך n באקראי, $\Pr_x[x \in G] \geq 1/2n$. אם אינך יודע להוכיח זאת מותר להשתמש בנכונות הטענה הנ"ל ועדיין לקבל 30 נקודות.

בהצלחה.