מבחן ביסודות הקריפטוגרפיה: מועד ב' 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 סכמת התחייבות על ביט (bit-commitment).

   נתונה פרמוטציה חד כוונית. נסתכל בהצעה הבאה לפרוטוקול לסכמת התחייבות על ביט: כאשר ה-sender רוצה "לשים ביט a בקופסא", הוא יבחר באקראי $x \in_R \{0,1\}^n$ תחת האילוץ שהביט הראשון ב-x הוא a. ה-sender יישלח ל-receiver את f(x) בתור "קופסא סגורה". מאוחר יותר כאשר ה- sender רוצה "לפתוח את הקופסא", הוא יישלח את x בתור מפתח (וה- receiver יכול לחשב בעצמו את a).

   ב. (10 נקודות) תאר את הפרוטוקול המוצע בצורה פורמלית (בהתייחס להגדרה שנתת בסעיף א).
   ג. (10 נקודות) האם הפרוטוקול הוא binding?
   ד. (20 נקודות) האם הפרוטוקול הוא hiding?

2. ענה על הסעיפים הבאים:

   א. (10 נקודות) הגדר מהו גנרטור פסאודו אקראי (pseudorandom generator).
   ב. (20 נקודות) יהיה G גנרטור פסאודו אקראי עם פונקצית מתיחה 2n. נסתכל בפונקציה $H(x_1,x_2)=G(x_1) \circ G(x_2)$ (כאשר הסימן "$\circ$" מציין שרשור). הוכח כי H היא pseudorandom generator. (יש להוכיח באופן ישיר מההגדרה ואין להשתמש בתכונות אחרות שנלמדו בכיתה). מהי פונקצית המתיחה של H?
   ג. (20 נקודות) הפעם נסתכל בבנייה אחרת מ-G של הסעיף הקודם. נסמן ב-$G_1(x)$ את n הביטים הראשונים בפלט של G(x), וב-$G_2(x)$ את n הביטים האחרונים. נסתכל בפונקציה $F(x)=G(G_1(x)) \circ G(G_2(x))$. הוכח כי F היא pseudorandom generator. (הדרכה: כדאי להשתמש בסעיף ב). מהי פונקצית המתיחה של F?

3. ענה על הסעיפים הבאים:

   א. (10 נקודות) הגדר מהי OWP ומהו ביט קשה.

   תהי f(x) פונקציה שהיא OWP, ויהי b(x) ביט קשה עבור f. נסתכל בשפה:
   $L=\{ (f(x),b(x)) : x \in \sum^* \}$.

   ב. (10 נקודות) הוכח כי L ב-NP.
   ג. (10 נקודות) הוכח כי L איננה ב-P.
   ד. (20 נקודות) הוכח כי השפה המשלימה ל-L ב-NP.

בהצלחה.