פרופ' בני פנקס

מבוא לקריפטוגרפיה 89-656-01

מועד א'

סמסטר ב' תשע"א

הנחיות:

1. בטופס הבחינה שני דפים מלבד דף זה. ודאו כי כולם נמצאים בידכם.
2. בבחינה 4 שאלות.
3. הבחינה עם חומר פתוח.
4. משך הבחינה שתי שעות וחצי.
5. הנכם רשאים להסתמך על סעיפים קודמים, גם אם לא השבתם עליהם.
6. **נמקו את כל תשובותיכם, פרט לפתרונות סעיפי שאלה 1. פתרון לשאלות 2-4 ללא הוכחה לא יתקבל.**

בהצלחה!

1. ענו על **כל** הסעיפים הבאים שלכולם משקל שווה. אין צורך לנמק את התשובות לשאלה זו.

   א. (8%) אליס ובוב מבצעים הסכמה על מפתח בשיטת Diffie-Hellman בחבורה Z^*_{53}, עם היוצר $g=3$ (החישוב מתבצע בחבורה Z^*_{53} עצמה ולא בתת חבורה שלה). אליס שולחת לבוב את המספר 52 (כלומר $g^a=52$), ובוב מחזיר את המספר $g^b=27$. מהו המפתח עליו הסכימו אליס ובוב?

   ב. (8%) הוצע לממש הצפנת בלוק סימטרית של הודעות באורך 128 ביטים, על ידי מפתח אשר מתאר פרמוטציה אשר תופעל על סדר הביטים בהודעה. (כלומר, המפתח יהיה טבלה K בת 128 כניסות בה כל כניסה מכילה ערך בין 0 ל-127, וכל ערך מופיע רק פעם אחת. ההצפנה מעתיקה את ביט j של הקלט לביט K[j] של ההודעה המוצפנת.) הסבירו מדוע הצפנה זו אינה בטוחה.

   ג. (8%) נגדיר מעל $\mathbf{Z_{13}}$ מערכת שיתוף סוד 2-מתוך-3 (2-out-of-3 secret sharing) לפי השיטה של שמיר. לשלושה משתתפים ישנן הזהויות 1,2, ו-3. החלק (share) של שחקן 1 הוא 12. החלק של שחקן 2 הוא 1. החלק של שחקן 3 הוא 3. חשבו מהו הסוד המוגדר על ידי חלקים אלו (אין צורך לפרט את דרך החישוב).

2. (פונקציות חד-כיווניות) פונקציה F היא חד-כיוונית אם ההסתברות בה היריב יכול לענות על השאלה הבאה היא זניחה: אנו בוחרים x אקראי, מחשבים את $z=F(x)$, ומוסרים את z ליריב. (היריב יכול לחשב את F כרצונו.) על היריב למצוא ערך y שיקיים $F(y)=z$.
   בהינתן פונקציה חד-כיוונית $g:\{0,1\}^n \to \{0,1\}^n$ ניבנה פונקציה חד-כיוונית f המקבלת קלט באורך 2n ומחשבת פלט באורך 2n: $f(x_1 \mid x_2) = 0^n \mid g(x_1)$. (הסימן | מסמן שרשור. אורכם של x_1 ו-x_2 הוא n.)

   א. (10%) הראו כי אם g היא חד-כיוונית, אזי כך גם f. כלומר, הראו שאם ישנו אלגוריתם השובר את חד-הכיווניות של f, אזי ניתן לבנות אלגוריתם השובר את חד-הכיווניות של g. (כלומר, אלגוריתם העונה לשאלה שהוצגה ליריב בהגדרה למעלה.)

   ב. (8%) הראו כי הפונקציה $f(f(x))$ אינה חד-כיוונית (וזאת למרות שהפונקציה f היא חד-כיוונית).

   ג. (8%) עד כה השאלה עסקה ב-f שנבנתה בצורה מיוחדת, ועבורה ראינו ש-$f(f(\cdot))$ אינה חד-כיוונית. נבדוק כעת פונקציה f אחרת: בהינתן f שהיא <u>פרמוטציה</u> חד-כיוונית, הוכיחו כי הפרמוטציה $f(f(x))$ הינה תמיד חד-כיוונית. (כלומר, הראו שאם ישנו אלגוריתם השובר את חד-הכיווניות של $f(f())$, אזי ניתן לבנות אלגוריתם השובר את חד-הכיווניות של $f()$.)

3. יהיו p ו q -ראשוניים אי-זוגיים כך ש- $p=2q+1$.

א. (8%) יהי a איבר ב- Z_p^* כך שמתקיים $a\neq 1$ וגם $a\neq p-1$. הוכיחו כי אם a איננו יוצר של Z_p^* אזי a– הוא יוצר של Z_p^*.

ב. (4%) הראו אלגוריתם דטרמיניסטי יעיל למציאת יוצר של Z_p^*.

ג.(8%) כעת נסמן על ידי p ו- q *שני מספרים* ראשוניים גדולים שונים זה מזה ונגדיר $N=pq$. נסמן $\lambda(N) = (p-1)\cdot(q-1) / \gcd(p-1,q-1)$. הוכיחו כי לכל איבר a ב- Z_N^* מתקיים $a^{\lambda(N)} = 1 \bmod N$.

ד. (5%) הוכיחו כי Z_N^* אינה חבורה ציקלית (כלומר, אין לה יוצר).

4. זוג פונקציות $F0,F1:D\rightarrow R$ יקראו *"חסרות מפגש"* אם קשה למצוא זוג $x,y\in D$ המקיים $F0(x)=F1(y)$.

a. (12%) יהי p ראשוני, g יוצר של Z_p^*, ויהי k איבר אקראי ב- Z_p^*. נניח כי בעיית הלוג הדיסקרטי היא קשה. הוכיחו כי זוג הפונקציות הבאות הן חסרות מפגש: $F0(x)=g^x \bmod p$, $F1(x)=k\cdot g^x \bmod p$. (ניקוד מלא יינתן להוכחה בעזרת רדוקציה.)

b. (13%) יהיו p,q ראשוניים לא ידועים, $n=pq$, ויהיו r איבר אקראי ב-Z_n^* ו- e איבר אקראי זר ל-$\varphi(n)$ (כל הערכים הללו, פרט ל-p ול-q, ידועים לכולם). נניח כי בעיית ה-RSA קשה בחבורה Z_n^*. הוכיחו כי זוג הפונקציות הבאות הן חסרות מפגש: $G0(m)=m^e \bmod n$, $G1(m)=r\cdot m^e \bmod n$. (ניקוד מלא יינתן להוכחה בעזרת רדוקציה.)