

## תרגיל בית 7 במבנים אלגבריים 89-214 סמסטר א' תשע"ח

**הוראות** בהגשת הפתרון יש לרשום בכל דף שם מלא, מספר ת"ז ומספר קבוצת תרגול.

**שאלה 1.** בדקו האם  $a$  הוא עד לראשוניות של  $N$ , לפי אלגוריתם מילר-רבין. הציגו את החישוב לכל  $a$ , גם אם אתם כבר יודעים שהמספר אינו ראשוני. **הציגו כל שלב בחישוב באמצעות חזקה מודולרית!**  
רשמו בכל סעיף האם  $N$  אכן ראשוני.

1.  $N = 233$ . בדקו עבור  $a = 10, a = 53, a = 191$ .

2.  $N = 437$ . בדקו עבור  $a = 101, a = 102, a = 103$ .

**שאלה 2.** אליס ובוב רוצים לתאם ביניהם מפתח סודי בפרוטוקול דיפי-הלמן, בחבורה  $U_{37}$ ,  $g = 17$ . לאליס ידוע המספר  $a = 8$ , לבוב ידוע המספר  $b = 10$ . כתבו מה המפתח אותו הם מקבלים. מצאו את המפתח גם עבור אליס וגם עבור בוב. **הציגו כל שלב בחישוב באמצעות חזקה מודולרית!**

### שאלות רשות

השאלות לא נבדקות, ולא יינתן עליהן ציון.

**שאלה 3.** חשבו האם ניתן לממש את אלגוריתם  $RSA$  באמצעות חבורה לא אבלית (כמו  $S_n$ , למשל)? מה משתבש?

**שאלה 4.** הראו שכאשר  $n = pq$  והראשוניים  $p, q$  "קרובים יחסית", אפשר לתקוף די בקלות את  $RSA$ .

שימו לב שמתקיים:  $n = \left(\frac{p+q}{2}\right)^2 - \left(\frac{p-q}{2}\right)^2$ , ואז  $\frac{p+q}{2}$  יחסית קרוב למספר  $\sqrt{n}$ . סמנו:  $t = \frac{p+q}{2}, s = \frac{p-q}{2}$  והסבירו למה במצב כזה יחסית קל למצוא את  $t, s$  (ובאמצעותם את  $p, q$ ) בהינתן  $n$ .  
הדגימו זאת על  $n = 23360947609$ .