מבוא להצפנה: תרגיל מס' 7.

1. אליס ובוב משתמשים בפרוטוקול של חתימה שלא ניתן להכחישה של שאום (כפי שהוא מתואר במצגת). אליס בוחר מספר ראשוני 433 ויוצר $g=5$ של $\mathbb{Z}_{433}^*$. המפתח הסודי שלה הוא $x=111$.

   a. אליס משתמשת בפרוטוקול כדי לחתום על ההודעה $m=314$. תארו את תהליך החתימה ובדיקת החתימה כשבוב בוחר במספרים האקראיים $a=419, b=79$ ואליס בוחרת במספרים האקראיים $q=187$.

   b. הראו איך אליס תוכיח לבוב כי 234 אינה חתמיה תקנית של ההודעה 314. השתמשו $k=10$, כשבוב משתמש במספרים $s=3$, $b=295$ ואליס ב- $r=232$. אליס משתמשת בפונקצית הגיבוב $h(r,i)=5^{ri} \bmod 433$.

2. יהיו p ראשוני גדול, α יוצר של $\mathbf{Z}_p^*$, ו- $\beta=\alpha^a$. המספרים p,α,β ציבוריים. פגי רוצה להוכיח לויקטור כי היא יודעת את a **בלי לגלות אותו**. הם משתמשים בפרוטוקול הבא:

   - פגי בוחרת במספר אקראי $r \bmod p-1$.
   - פגי מחשבת את $h_1=\alpha^r \bmod p$ ו- $h_2=\alpha^{a-r} \bmod p$ ושולחת את h_1,h_2 לויקטור
   - ויקטור מבקש את $r_1=r$ או את $r_2=a-r$ מפגי.
   - ויקטור בודק כי $h_1h_2=\beta \bmod p$ וכי $h_i=\alpha^{r_i} \bmod p$.

   א. נניח כי פגי אינה יודעת את a . הסבירו למה לפעמים היא לא תוכל לשכנע את ויקטור. עבור כל סיבוב, מה היא ההסתברות שהיא לא תוכל לשכנע את ויקטור?

   ב. הסבירו למה ויקטור אינו יכול לקבל שום מידע על a . הראו כי ניתן לכתוב סימולציה של התהליך כך שצד שלישי לא יוכל לראות את ההבדל בינה לבין תהליך אמיתי.

3. תהי העקומה האליפטית $E: y^2=x^3+2x+3 \bmod 19$. הערה: הסבירו את כל החישובים שאתם עושים. אפשר להקל על החישובים אם אתם משתמשים במה שלמדתם בפרקים אחרים.) שימו לב כי אפשר לחשב nP בעזרת אלגוריתם "double and add" שהוא הגרסה האדיטיבית של "square and multiply".

   a. מצאו את כל הנקודות של $E(\mathbb{Z}_{19})$.

   b. הוכיחו כי $(1,5)$ יוצרת את החבורה $\left(E(\mathbb{Z}_{19}),+\right)$ (על תשכחו את הנקודה באינסוף כשאתם סופרים את מספר הנקודות).

בהצלחה!