מבוא להצפנה: תרגיל מס' 6.

הקפידו בכל התרגיל על נימוקים והסברים!

1. יהי המספר הראשוני $p=97$.
   a. הוכיחו כי 5 הוא היוצר הקטן ביותר של $\mathbb{Z}_{97}^*$.
   b. כמה יוצרים יש ל- $\mathbb{Z}_{97}^*$ ואיך ניתן למצוא אותם בלי לבחון את כל האיברים של $\mathbb{Z}_{97}^*$?
   c. השתמשו בשיטת אינדקס קלקולוס כדי למצוא את $L_5(31)$ (הלוג בדסקרטי בבסיס 5). הדרכה: תקחו עבור בסיס הראשוניים שלכם את המספרים הראשוניים עד 7 .
   d. השתמשו בשיטת Baby steps-giant steps של Shanks כדי לחשב שוב את $L_5(31)$.

2. נגדיר סכימת חתימה מסוג אל-גמל בצורה הבאה: אליס בוחרת ראשוני גדול p , יוצר α של $\mathbb{Z}_p^*$, ו- $a\in\mathbb{Z}_{p-1}^*$. היא מחשבת את $\beta=\alpha^a$, מפרסמת את (p,α,β), ושומרת את a כמפתח סודי. אליס רוצה לחתום על ההודעה $x\in\mathbb{Z}_p$. היא בוחרת באופן אקראי $k\in\mathbb{Z}_p$ ומחשבת את החתימה $\mathbf{sig}(x)=(\gamma,\delta)$ באופן הבא: $\gamma=\alpha^k$ ו- $\delta=(x-k\gamma)a^{-1}\bmod(p-1)$. (בחתימת אל-גמל הרגילה $\delta=(x-a\gamma)k^{-1}\bmod(p-1)$), היא שולחת לבוב את ההודעה x עם החתימה $\mathbf{sig}(x)$.
   a. תארו איך בוב בודק את החתימה בעזרת המפתח הציבורי של אליס.
   b. הסבירו למה לגרסה הזו של חתימת אל-גמל יש יתרון חישובי על חתימת אל-גמל הרגילה.
   c. הראו כי אם אליס משתמשת באותו k כדי לחתום על שתי הודעות x_1 ו- x_2, אזי ניתן לחשב את a בעזרת $x_1,\mathbf{sig}(x_1)$ ו- $x_2,\mathbf{sig}(x_2)$.
   d. המפתח הציבורי של אליס עבור החתימה המוגדרת בשאלה זו הוא $(97,5,71)$. אליס חותמת על שתי הודעות $\mathbf{sig}(75)=(87,66)$ ו- $\mathbf{sig}(78)=(87,75)$. מצאו את המפתח הסודי של אליס.

3. יהי $n=151\times167=25217$. מצאו את כל השורשים הריבועיים ב- $\mathbb{Z}_{25217}$ (אם יש) של המספרים הבאים: 4681 , 15704 , 15919 (תזכורת: במצגת על מישוש ה-RSA, בשקף 14 יש נוסחאות למשפט השאריות הסיני).

4. בנו שתי דוגמאות נומריות של פרוטוקול הטלת מטבע בו $n=25217$, אחת בה אליס מנצחת ואחת בה בוב מנצח.

בהצלחה!