מבוא להצפנה: תרגיל 4

1. כדי לשלוח הודעה באמצעות RSA, אליס קודם מתרגמת את האותיות למספר בין 01 ל-26 (כך ש-$a=01$ ו- $z=26$. כך $cat=30120$ (לא מתחילים מ- $a=00$ כי אז אם a מופיעה בתחילת ההודעה היא הייתה נעלמת). המפתח הציבורי של בוב הוא $(n,e)=(2237579,17)$.
   a. אליס שולחת חבילה סודית לבוב והיא סיכמה עם בוב שהיא תשלח לו את ההודעה one עם השליח יביא את החבילה במכונית ואת ההודעה two אם הוא יביע אותה במסוק. היא שולחת את ההודעה 1409602. מצאו איך השליח יגיע בלי לפרק את n .
   b. פרקו את n בעזרת האלגוריתם $p-1$ של פולארד. הסבירו בקצרה למה האלגוריתם עבד (עם המספרים האלה, לא באופן כללי).
   c. השתמשו בפירוק שמצאתם כדי לברר שלבים היה לוקח לפרק את n בעזרת אלגוריתם הפירוק של פרמה.
   d. השתמשו באלגוריתם האוקלידי המורחב כדי לחשב את d (המפתח הפרטי של בוב). הראו את כל השלבים של החישובים .
   e. אליס שולחת לבוב גם את השם של השליח. היא שולחת לו $c=1863490$. השתמשו בשיטה של הפענוח המהיר (עם משפט השאריות הסינית). השתמשו בלגוריתם square and multiply להעלה לחזקה. הראו את כל החישובים.

2. יהי $n=38200901201$. בחנו את הראשוניות של n בעזרת האלגוריתם של פרמה והאלגוריתם של מילר רבין עבור כל הבסיסים מ- $a=2$ ל- $a=20$. עבור כל בסיס, ציינו את תוצאות המחבן ובמקרה של מילר רבין מחזיר ש- n פריק, ציינו אם ניתן לפרק את n בעזרת התוצאות של האלגוריתם. מותר להשתמש ב-wolframalpha כדי לעשות את החישובים.

3. המפתח הציבורי של אליס ל-RSA הוא $(11413,17)$ והמפתח הציבורי של בוב הוא $(11413,129)$. המזכירה שולחת לשניהם את קוד מכונת הצילום: היא שולחת לאליס את $c_A=4772$ ולבוב את $c_B=1495$. מצאו את הקוד בלי לפרק את 11413 .

בהצלחה!