

אורג המספרים (89-256)

4 היג'יג

1. אמתו גאלקוריקס מן השיזור בני למצטו זיג (x,y) של מספרים שלמים כך $e -$

$$19x + 25600y = 1$$

2. לחשב $25^{1541} \pmod{4187}$. לטו להפתח בשום מכשיר מעבר למחשבון.

3. Alice מקימה מערכת הלפנה RSA. המפתח הציבורי שלה הינו $(n, e) = (25957, 19)$. המצטאו אג המפתח הפרטי ל

4. Bob שולח ל-Alice אג ההוצרה המולפנה $E(m) = 8236$. מה היגה ההוצרה המקורי מ? (Bob משמש במפתח הציבורי מן השאלה הקודמת.)

5. בהוצרה שלו, Bob מספר ל-Alice מה הוא קנה בוק. אם הוא חוקם טקסט למספר כמו ששינו בשיזור ($a=1, b=2$, וכו'), מה הוא קנה?

6. Alice הקימה מערכת הלפנה RSA בה המפתח הציבורי הינו מכפלה של מספרים ראשוניים בעלי כשס מאוג ספרוג. Bob שולח לה הוצרה, אך הוא שולח גם אוג בפרוג. האם זה באות? מתחוק.