**שאלה 1:**

תחילה נראה האם איירון צריך לקבל עודף, פעולה זו היא 1,000,000%5279, במידה ולא אז יש עסקה.

אחרת, ניקח את השארית מהפעולה הנ"ל(סה"כ העודף שאיירון צריך לקבל מלוקי) ונבצע שוב מודולו במטבעות, סה"כ נקבל חישוב : %797(1,000,000%5279).

במידה והשארית היא 0 אז ישנה עסקה, אחרת אין.

**תשובה סופית : אין עסקה בין לוקי לאיירון.**

**שאלה 2:**

על מנת לחשב את ספרת המאות של  **,** נחשב את שארית החלוקה ב-1000 של המספר.

כלומר את **,** לכך נעזרנו בפונקציה modular\_exponent, ובייצוג בינארי.

נשים לב כי 673 1000 , והייצוג הבינארי של החזקה הוא :1101000110011111011110.

נחשב את התוצאה ע"י השיטה שהוצגה במסמך התרגיל :.

(ביצענו מודולו לאחר כל פעולה של כפל.)

לתוצאה הסופית המתקבלת (בבסיס 1000) , לקחנו את ספרת המאות וזו התשובה הסופית.

**תשובה סופית: ספרת המאות היא 3.**

**שאלה 4:**

ההודעה שבחרנו להצפין היא ״elon״, יחד עם המפתח הציבורי (e,N) = (30934349 , 54173879) ולאחר תהליך ההצפנה קיבלנו ״yjin״ כצופן של ההודעה.

תהליך ההצפנה שלנו נעשה בצורה הבאה:

* כל תו בהודעה הומר לערך ה-ascii שלו
* כל ערך ascii שכזה הועלה בחזקת e מודלו N
* על התוצאה הופעל מודולו 32 פלוס 101 ע״מ לחזור לטווח האותיות בטבלת ascii