1) נרצה בעזרת למצוא x,y כך שמתקיים:

$$911\cdot x - 7879\cdot y = 1{,}000{,}000.$$

נשתמש בפונקציה extended_gcd שכתבנו, עם הערכים 911 ו- 7879-. ינקבל כי הם זרים. לכן מתקיים: $1=911\cdot x-7879\cdot y$

לכן נוכל לחפש x,y כך ש- $1=911\cdot x-7879\cdot y$

ואז להכפיל את שניהם ב- 1,000,000.

נשתמש בפונקציה extended_gcd עם אותם ערכים ונקבל

כי $x=-2733$, $y=316$, לכן לאחר ההכפלה

$1{,}000{,}000\cdot x=-2733\cdot 10^6$ $\qquad$ $1{,}000{,}000\cdot y=316\cdot 10^6$

$\Leftarrow$ לוקי ישלם עם $316\cdot 10^6$ שקלים של 7879 דולר

סנ"אדמן יחזיר לו $2733\cdot 10^6$ שקלים של 911 דולר.

שאלה 2:

נתון: $a = 456457$

$\Rightarrow a \pmod{1000} = 57$

$(a, 1000) = 1$

$\Rightarrow a^{\varphi(1000)} = 1$

התבלבלו את ספרת האחדות ל-7 בהוראת עדי

נפרק את $7896543^{74365753}$ באופן הבא:

$$7896543^{74365753} = q \cdot \varphi(100) + r$$

$$\Rightarrow \quad 57^{q \cdot \varphi(1000) + r} = 57^{q \cdot \varphi(1000)} \cdot 57^{r}$$

לפי משפט אוילר:

$$57^{q \cdot \varphi(1000)} = 1$$

$$\Rightarrow 57^{\left(7896543^{74365753}\right)} = (57)^{\left(\underbrace{7896543}_{a}{}^{\overset{\downarrow}{74365753}}\right) \pmod{\underbrace{\varphi(100)}_{n}}}$$

$$1000 = 5^3 \cdot 2^3 = \varphi(5^3) \cdot \varphi(2^3)$$

$$125\left(1 - \frac{1}{5}\right) \cdot 8\left(1 - \frac{1}{2}\right) =$$

$$= 100 \cdot 4 = 400$$

נקרא לפונקציה modular_exponent

כאשר: $a=7896543$, $d=74365753$, $n=400$

נקבל: 143

כעת נחשב את $457 \pmod{1000}$

נקרא שוב לפונקציה modular_exponent

כאשר: $a=457$, $d=143$, $n=1000$

נקבל:

$$\Longrightarrow \text{סה"כ}: 993 = 456457^{\left(7896543^{74365753}\right)} \pmod{100}$$

לכן, ספרת המאות היא 9.

<u>שאלה 4:</u>

$$E(x) = x^e (modN) \quad N = 991, e = 11$$

$$\phi(N) = \phi(991) = 984$$

$\gcd(984,11) = 1$ ולכן $11 \in U_{\phi(N)=984}$, כאשר בשוויון האחרון השתמשנו בפונקציית העזר שכתבנו בפייתון.

נסתכל על $D(y) = y^d (modN)$ עבור $d = e^{-1}(mod(\phi(N)))$.

ונמצא את d:

$$ed = 1(mod(\phi(N))) \quad \Leftrightarrow \quad d = modularInverse(e, \phi(N))$$

ובעזרת פונקציית העזר שכתבנו בפייתון: $d = 179$.

אכן E הפיכה, מפני שמתקיים:

$$\forall x \in U_N: \ D(E(x)) = D(x^e) = (x^e)^d = x^{ed} = x^{ed-1}x =_{euler} 1 \cdot x = x \ (mod(N))$$

עם הפונקציה ההופכית: $D(y) = y^{179}(modN)$

שאלה 3:

נשתמש בכללי הבדלה ונפרק את n לראשוניים:

לפי כללי הבדלה $n = 3491 \cdot 3499$

נתון: $e = 3499$

$\varphi(n) = \varphi(12215009) = 12208020$

נשתמש בפונקציה modular_inverse

כאשר $a = e,\ n = \varphi(n)$

נקבל: $d = 5425399$

נחשב את הבעלות של 42 מן המידע שמצאנו לפי הפונקציה decrypt(42)

באמצעות RSA הנתון נקבל: 3023178.

שאלה 5:

נתונים הראשוניים $p = 6841$, $q = 7919$. נבין את הודעה מן הנתונים

הציבורי $e = 4091$, $N = 5417387$. נחזור לבין את ההודעה 25, על

ידי encrypt(25) בעזרה נקבל את ההודעה המוצפנת 816397.