חידה 1:

$$1000,000 = 911x - 7879y$$

7879 , 911 הם מספרים ראשוניים. בנוסף $911 \nmid 7879 \Leftarrow (7879,911)=1$

לפי המשפט קיים זוג: $911a - 7879b = 1$

מאלגוריתם אוקלידס:

$7879 = 911\cdot 8 + 591$

$911 = 591 + 320$

$591 = 320 + 271$

$320 = 271 + 49$

$271 = 49\cdot 5 + 26$

$49 = 26 + 23$

$26 = 23 + 3$

$23 = 3\cdot 7 + 2$

$3 = 2 + 1$

$2 = 2\cdot 1 + 0$

$\Downarrow$

$1 = 3 - 2 = 3 - (23 - 3\cdot 7) = 3\cdot 8 - 23$

$1 = -23 + 8(26 - 23) = 8\cdot 26 - 9\cdot 23$

$1 = 8\cdot 26 - 9\cdot(49 - 26) = -9\cdot 49 + 17\cdot 26$

$1 = -9\cdot 49 + 17(271 - 5\cdot 49)$

$1 = -94\cdot 49 + 17\cdot 271$

$1 = 17\cdot 271 - 94(320 - 271) = 111\cdot 271 - 94\cdot 320$

$1 = 111\cdot(591 - 320) - 94\cdot 320 = 111\cdot 591 - 205\cdot 320$

$1 = 111\cdot 591 - 205\cdot(911 - 591) = -205\cdot 911 + 316\cdot 591$

$1 = -205\cdot 911 + 316\cdot(7879 - 8\cdot 911)$

$= -2733\cdot 911 + 316\cdot 7879$

$\Downarrow$

$$1000000 = -2733\cdot 10^6\cdot 911 + 316\cdot 10^6\cdot 7879$$

מילה - במקרה הזה ההפרש הזה באמת 10^6 אבל יוצא שלוקי משלם לספיידרמן ולא להפך.

ניתן לייצר קומבינציות נוספות, לדוגמה $911\cdot 2153040 - 7879\cdot 2490079 = 1$

אבל בכל זוג לינארי, לוקי משלם לספיידרמן ולא להיפך.

$\Leftarrow$ עסקה בכסף שלפי אופטימיות בה לוקי מקבל -1000000

.3

$N = 12215009$

$e = 3499$

$M = 42$

$\varphi(N) = 12208020$

$(3499, 12208020) = 1$

$$\varphi(N) = 12215009 \cdot \frac{3490}{3491} \cdot \frac{3498}{3499} = 12208020$$

נעזר באלגוריתם אוקלידס כדי למצוא את e^{-1} מודולו 12208020

$12208020 = 3499 \cdot 3489 + 9$

$3499 = 9 \cdot 388 + 7$

$9 = 7 \cdot 1 + 2$

$7 = 2 \cdot 3 + 1$

$2 = 1 \cdot 2 \cdot 0$

$1 = 7 - 2 \cdot 3 = 7 - 3(9 - 7) = -3 \cdot 9 + 4 \cdot 7$

$1 = -3 \cdot 9 + 4(3499 - 9 \cdot 388)$

$1 = 4 \cdot 3499 - 1555 \cdot 9$

$1 = 4 \cdot 3499 - 1555(12208020 - 3489 \cdot 3499)$

$1 = -1555 \cdot 12208020 + 5425349 \cdot 3499$

לכן $d = 5425349$

נמצא את הקוד

$42^{5425349} = x \bmod (12215009)$

$x = 3023178$

נפתור את המשוואה באמצעות הקוד שעתיקנו

$\Rightarrow$ modular_exponent

5. נתון $p = 7917$

$q = 6841$

לכן

$$N = 7917 \cdot 6841 = 54173879$$

$$\varphi(N) = 54173879 \cdot 7916 \cdot 6840 = 54167038$$

נשתמש במפתח ציבורי $e = 3$

$$\gcd(54167038, 3) = 1$$

ההודעה שנצפין $M = 40$

$$40^3 = x \pmod{54173879}$$

לפי modular_exponent

$$x = 64000$$

ההודעה המקורית	$M=40$	
המפתח הציבורי	$e=3$	
ההודעה המוצפנת	$x=64000$	