LAB 5

Kid Krypto

Kid Krypto is a *public key* cryptosystem. If Nick would like to receive secret messages, he first chooses any four positive integers that only he will know: a, b, c, and d. Then he computes:

$$\begin{aligned} M &= ab - 1, \\ e &= cM + a, \\ f &= dM + b, \\ n &= \frac{ef - 1}{M}. \end{aligned}$$

Nick tells everyone who wants to send him a message the numbers e and n, these numbers form Nick's *public key*. However, Nick keeps his *private key*, the number f, completely secret. (Nick can securely delete the other numbers used to generate the keys.)

To send Nick a message x, encoded as an integer in the range $0 \leq x \leq n - 1$, the sender computes

$$y = \text{REM}\ (ex, n)$$

and sends y. To decipher the message y, Nick computes

$$\text{REM}\ (fy, n)$$

to recover x.

EXPERIMENT 5.1. Suppose Nick chooses $a = 47$, $b = 22$, $c = 11$, and $d = 5$.

(a) What numbers M, e, f, and n would Nick calculate?

(b) Write a Mathematica function called `Encrypt` to encode message for the public key pair e, n you just computed. Use your function to encode the message $x = 2020$.

(c) Write a Mathematica function called `Decrypt` that decodes a message y using the private key f. Use your function to decode the encrypted message $y = 43155$.

PROBLEM 5.2. On a different day, Nick announces a new public key:

$$n = 17\,239\,722\,505 \quad e = 25\,540\,219.$$

Nora sends him an encrypted message that you intercept: $y = 7\,218\,695\,996$. Crack the encryption to read Nora's message. What does it say?

PROBLEM 5.3. You intercept another message from Nora to Nick: $y = 8\,617\,388\,745$. What does it say? (Hint: try the command `IntegerDigits[263,26]` and improvise based on that.)

PROBLEM 5.4. Explain why Kid Krypto works. In other words, how do you know that $x = \text{REM}\ (fy, n)$?

PROBLEM 5.5. Is Kid Krypto secure? How would you write a Mathematica program to break Kid Krypto?