Kid RSA

Public-key generation:

Each user does:
- choose any two integers a and b
- set $M = ab - 1$
- choose two more integers a' and b'
- set $e = a'M + a$, $d = b'M + b$, $n = (ed-1)/M$

The public key is (n, e). The private key is d.

Exercise: Show that n is an integer.

$$ed - 1 = (a'M + a)(b'M + b) - 1 = a'b'M^2 + a'Mb + b'Ma + \underbrace{ab - 1}_{=M} \Rightarrow M \mid ed-1 \Rightarrow n = \frac{ed-1}{M}$$

is an integer.

Encryption and Decryption

To encrypt a plaintext message m, we compute

$$c = e \cdot m \pmod{n}.$$

The ciphertext c can be decrypted by multiplying with $d \pmod{n}$.

Exercise: Show that $dc \equiv m \pmod{n}$