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 $e = a'M + a$, $d = b'M + b$, $m = (ed - 1)/M$

The public key is $(m, e)$. The private key is $d$.

Exercise: Show that $m$ is an integer.

\[
\begin{align*}
ed - 1 &= (a'M + a)(b'M + b) - 1 = a'b'M^2 + a'Mb' \\
&\quad + b'Ma + ab - 1 \Rightarrow M \mid ed - 1 \Rightarrow m = \frac{ed - 1}{M}
\end{align*}
\]

is an integer.

Encryption and Decryption

To encrypt a plaintext message $m$, we compute

\[c = e \cdot m \pmod{m}.
\]

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

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