Public-key generation

Each user does:

- chooses any two integers a and b,
- sets $M = ab - 1$,
- chooses two more integers a' and b',
- sets $e = a'M + a$, $d = b'M + b$, $n = (ed - 1)/M$.

Show that n is an integer.

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

Encryption and Decryption

- To send Alice a plaintext m, one computes

$$c = em \mod n.$$

- Alice deciphers the ciphertext by multiplying c by d modulo n.
- Why does this recover the plaintext? I.e. explain why

$$m = dc \mod n$$

  holds.
- Try to break the scheme!