1. **Cryptography intro.** We focus on how to encode a single integer message m with $0 \leq m < N$.
   e is the encoding key, and d is the decoding key.

2. In *public-key* cryptography, I give you (e, N) so you can send me a message, but I keep d private.

3. **RSA:** Choose two large primes p and q, and let N = pq.

4. Choose any number e that is relatively prime to N' = (p-1)(q-1). Then
   a. the mapping $x \rightarrow x^e \bmod N$ is a bijection on {0, 1, …, N-1}, and
   b. If d is the inverse of e mod N', then for all x in {0, 1, …, N-1}, $(x^e)^d \equiv x \pmod N$.

5. Example: p=63, q=53 (so N=3233):

6. **Property that is the basis of RSA:** If N=pq for 2 primes p and q, and if e is any number that is relatively prime to N' = (p-1)(q-1), then
    a. the mapping x→xe mod N is a bijection on {0, 1, …, N-1}
    b. If d is the inverse of e mod (p-1)(q-1), then for all x in {0, 1, …, N-1}, (xe)d ≡ x (mod N)