Theorem 141. Let $N = pq$ and d, e be as in RSA. Then, for any m, $m \equiv m^{de} \pmod{N}$.

Comment. Using Euler's theorem, this follows immediately for residues m which are invertible modulo N. However, it then becomes tricky to argue what happens if m is a multiple of p or q.

Proof. By the Chinese remainder theorem, we have $m \equiv m^{de} \pmod{N}$ if and only if $m \equiv m^{de} \pmod{p}$ and $m \equiv m^{de} \pmod{q}$.

Since $de \equiv 1 \pmod{(p-1)(q-1)}$, we also have $de \equiv 1 \pmod{p-1}$. By little Fermat, it follows that $m^{de} \equiv m \pmod{p}$ for all m that are invertible modulo p. On the other hand, if m is not invertible modulo p, then this is obviously true (because both sides are congruent to 0). Thus, $m \equiv m^{de} \pmod{p}$ for all m.

Likewise, modulo q. □

Theorem 142. Determining the secret private key d in RSA is as difficult as factoring N.

Proof. Let us show how to factor $N = pq$ if we know e and d.

- First, let t be as large as possible such that 2^t divides $ed - 1$. (Note that $t \geqslant 2$. Why?!)
  Write $m = (ed - 1)/2^t$.
- Pick a random invertible residue a. Observe that $a^{ed-1} \equiv 1 \pmod{N}$. In particular, $(a^m)^{2^t} \equiv 1$.
  Hence, the multiplicative order of a^m must divide 2^t.
- Suppose that a^m has different order modulo p than modulo q. (Both orders must divide 2^t.)
  [This works for at least half of the (invertible) residues a. If we are unlucky, we just select another a.]
- Suppose a^m has order 2^s modulo p, and larger order modulo q.
  Then, $a^{2^s m} \equiv 1 \pmod{p}$ but $a^{2^s m} \not\equiv 1 \pmod{q}$. Consequently, $\gcd(a^{2^s m} - 1, N) = p$.
- Of course, we don't know s (because we don't know p and q), but we can just go through all $s = 1$, $2, \ldots, t-1$. One of these has to reveal the factor p. □

However. It is not known whether knowing d is actually necessary for Eve to decrypt a given ciphertext c. This remains an important open problem.

Example 143. (homework) Bob's public RSA key is $N = 323$, $e = 101$. Knowing $d = 77$, factor N using the approach of the previous theorem.

Solution. Here, $de - 1 = 7776$, which is divisible by 2^5. Hence, $t = 5$ and $m = 243$.

- Let's pick $a = 2$. $a^m = 2^{243} \equiv 246 \pmod{323}$ must have order dividing 2^5.
  $\gcd(246^2 - 1, 323) = 19$ (so we don't even need to check $\gcd(246^{2^s} - 1, 323)$ for $s = 2, 3, 4$)
  Hence, we have factored $N = 17 \cdot 19$.

Comment. Among the $\phi(323) = 16 \cdot 18 = 288$ invertible residues a, only 36 would not lead to a factorization. The remaining 252 residues all reveal the factor 19.

Another project idea. Run some numerical experiments to get a feeling for the number of residues that result in a factorization.

Armin Straub
straub@southalabama.edu

The ElGamal public key cryptosystem and discrete logarithms

- Proposed by Taher ElGamal in 1985

  The original paper is actually very readable: https://dx.doi.org/10.1109/TIT.1985.1057074

- Whereas the security of RSA relies on the difficulty of factoring, the security of ElGamal relies on the difficulty of computing discrete logarithms.

- Suppose $b = a^x \pmod{N}$. Finding x is called the **discrete logarithm problem** mod N. If N is a large prime p, then this problem is believed to be difficult.

  Note. If $b = a^x$, then $x = \log_a(b)$. Here, we are doing the same thing, but modulo N. That's why the problem is called the discrete logarithm problem.

(ElGamal encryption)

- Bob chooses a prime p and a primitive root $g \pmod{p}$.
  Bob also randomly selects a secret integer x and computes $h = g^x \pmod{p}$.

- Bob makes (p, g, h) public. His (secret) private key is x.

- To encrypt, Alice first randomly selects an integer y.
  Then, $c = (c_1, c_2)$ with $c_1 = g^y \pmod{p}$ and $c_2 = h^y m \pmod{p}$.

- How does Bob decrypt?

We'll see next time!