Can the reader say what two numbers multiplied together will produce the number 8616460799? I think it unlikely that anyone but myself will ever know.

William Stanley Jevons

In what follows, “number” always means “positive whole number.”

A number is prime if it cannot be written as a product of two smaller numbers. Every number can be decomposed (factored) into a product of primes. For example:

\[ 12345678 = 2 \cdot 3 \cdot 3 \cdot 47 \cdot 14593. \]

There exist efficient ways to check if a given number is prime. However, there are no known methods to quickly factor a given number. It is conjectured that the factoring problem is not in the class \( P \), but also not \( NP \)-complete.

Here is how the public key \((N, e)\) and the private key \(d\) for the RSA are generated:

1. **Step 1.** Alice picks two (large) prime numbers \(p\) and \(q\) and sets

\[ N = p \cdot q. \]

2. **Step 2.** Alice randomly picks a number \(e\).*

3. **Step 3.** Alice finds the number \(d\) such that

\[ e \cdot d = 1 \pmod{(p - 1) \cdot (q - 1)}. \]

**Example:** Take \(p = 1063\) and \(q = 2111\). Then

\[ N = p \cdot q = 1063 \cdot 2111 = 2243993. \]

Suppose we decided to take \(e = 7\). Note that

\[ (p - 1) \cdot (q - 1) = 1062 \cdot 2110 = 2240820. \]

Hence, the private key \(d\) must satisfy

\[ 7 \cdot d = 1 \pmod{2240820}. \]

Alice finds that \(d = 1920703\) works, as

\[ 7 \cdot 1920703 = 13444921 = 6 \cdot 2240820 + 1. \]

Note that if somebody knows \(N\) and \(e\), they cannot simply find \(d\) the same way Alice did, because they don’t know what \(p\) and \(q\) are, so they can’t compute \((p - 1)(q - 1)\). If you come up with a quick way to factor numbers, you will be able to essentially subvert all of the modern electronic commerce and collapse a few governments!

*There some additional requirements this number must satisfy for the rest of the procedure to work, but let’s ignore them. (If you are interested, \(e\) must be coprime to \((p - 1)(q - 1)\), i.e., they must not have any common prime divisors.)