Example: A Simple RSA Demonstration

(Toy model — not secure, but perfect for learning!)

Goal

Encrypt and decrypt the message $M = 7$ using a tiny RSA setup.

Step 1. Choose primes

Let $p = 5$ and $q = 11$.

Then

$$n = p \times q = 5 \times 11 = 55, \quad \phi(n) = (p-1)(q-1) = 4 \times 10 = 40.$$

Step 2. Choose public key exponent e

We need e such that $1 < e < 40$ and $\gcd(e, 40) = 1$.
Let's choose $e = 3$, since $\gcd(3, 40) = 1$.

Step 3. Compute private key exponent d

We need d such that

$$e \times d \equiv 1 \pmod{40}.$$

Try small values:

$$3 \times 27 = 81 \equiv 1 \pmod{40}.$$

So $d = 27$.

Public key: $(n, e) = (55, 3)$ **Private key:** $(n, d) = (55, 27)$

Step 4. Encrypt a message

Let our message be $M = 7$. Compute ciphertext:

$$C \equiv M^e \pmod{n} = 7^3 \bmod 55 = 343 \bmod 55 = 13.$$

$$\boxed{C = 13}$$

Step 5. Decrypt the ciphertext

Now compute:

$$M \equiv C^d \pmod{n} = 13^{27} \bmod 55.$$

We can reduce step-by-step (or use a calculator):

$$13^2 \equiv 4, \quad 13^4 \equiv 16, \quad 13^8 \equiv 36, \quad 13^{16} \equiv 31,$$

and after combining exponents properly,

$$13^{27} \bmod 55 = 7.$$

$$\boxed{M = 7 \text{ (original message recovered!)}}$$

Summary

- $p = 5, q = 11 \Rightarrow n = 55, \phi = 40$
- $e = 3, d = 27$
- Encrypt $M = 7 \Rightarrow C = 13$
- Decrypt $C = 13 \Rightarrow M = 7$

Even though our numbers are tiny, this is exactly the same math that powers real RSA with 2048-bit primes.