The RSA Public Key Cryptosystem

Say that Bob wants to send a message to Alice.

Step 1: Key Creation (Alice)

Alice chooses two secret primes p and q. She then chooses any integer e satisfying

$$\gcd(e, (p-1)(q-1)) = 1.$$

Alice publishes $N = pq$ and e. (Note: e is often called the *encryption exponent*).

Step 2: Convert Message using Encoding Scheme (Bob).

Bob uses the agreed upon encoding scheme to write his message as a number m.

We will convert our messages to base 10 using the scheme

$$\text{space} = 0,\ a = 1,\ b = 2,\ \ldots,\ z = 26.$$

Note that Bob's message must be small enough so that $2 \leq m \leq N - 1$.

Step 3: Encrypt Message (Bob)

Bob uses the public key (N, e) that Alice published in Step 1 to compute

$$c \equiv m^e (\text{mod}\, N).$$

Bob then sends c to Alice.

Step 5: Decrypt Message (Alice)

Alice computes the inverse of e modulo $(p-1)(q-1)$, say $d \equiv e^{-1} (\text{mod}\, (p-1)(q-1))$. Alice then uses this to compute $c^d (\text{mod}\, N)$. Observe that this quantity is equal to m.

Step 6: Convert Message to Base 27 (Alice)

Alice takes the value m and converts it back to base 27 using the agreed upon encoding scheme to reveal the secret message.

Example 1. Show how Bob could send the secret message "hi" to Alice using RSA.