This is the standard protocol for secure communication using the RSA. Imagine that Bob wants to send a message to Alice. They perform the following steps:

**Step 1.** Alice generates the keys \((N, e)\) and \(d\). (We will talk more about this step later.)

**Step 2.** Alice sends the public key \((N, e)\) to Bob.

**Step 3.** Bob uses the public key \((N, e)\) to encrypt his message \(M\). Denote the result by \(M^*\).

**Step 4.** Bob sends \(M^*\) to Alice.

**Step 5.** Alice uses her private key \(d\) to decrypt \(M^*\) and thus uncover \(M\).

Notice that the private key \(d\), necessary for deciphering messages, is *never sent to anybody*: Alice is the only person in the world who knows it!

The RSA has many applications besides just ciphering. For instance, it is widely used for authentication purposes: when you load a website whose address starts with `https://`, your browser uses the RSA to make sure it is the correct website and not a fake. To see how that works, imagine that, a week later, Bob wants to send another message to Alice, but first he wants to make sure it is really her and not an impostor. Here is what he does:

**Step 1.** Bob picks a random number \(R\) between 0 and \(N - 1\) and encrypts it using Alice’s public key \((N, e)\). Denote the result by \(R^*\).

**Step 2.** Bob sends \(R^*\) to Alice and asks her to decrypt it.

**Step 3.** If Alice succeeds, Bob can be sure it is her, because nobody else knows the private key \(d\).

Further reading:

- N. Stephenson (1999). *Cryptonomicon*. This is a pretty awesome book centered around cryptography!