RSA Encryption

1. The receiver chooses two distinct large primes $p$ and $q$. The receiver also finds $k$ such that $1 < k < \varphi(pq)$ and $\gcd(k, \varphi(pq)) = 1$, and finds a $d$ such that $kd \equiv 1 \pmod{\varphi(pq)}$.

2. The receiver keeps $d$ private and makes $k$ and $n = pq$ public.

3. The sender, intending to send message $m$ where $m < n$, computes

$$r \equiv m^k \pmod{n}, \quad r < n$$

and sends $r$ to the receiver.

4. The receiver decodes $x \equiv r^d \pmod{n}, \quad x < n$.

Claim: $x = m$. (Proven.)