RSA Public-Key Cipher:

- Plaintext Space $M = \{0, 1\}^*$.
- Ciphertext Space $C = \{0, 1\}^*$.
- Let $N = pq$.
- Choose e relatively prime to $(p-1)(q-1)$.
- Find d such that $ed = 1 \pmod{(p-1)(q-1)}$.
- Public key is (N, e).
- Private key is d.

Encryption:
$C = M^e \mod N$

Decryption:
$M = C^d \mod N$

Proof of correctness:

- Chinese Remainder Theorem
    - Let p and q be two co-prime integers. If $x = a \pmod{p}$ and $x = a \pmod{q}$, then $x = a \pmod{pq}$.
- Fermat's Little Theorem
    - If p is a prime number and a is not divisible by p, then $a^{p-1} = 1 \pmod{p}$.
- Proof
    - It suffices to prove that $M = C^d \pmod{p}$ and $M = C^d \pmod{q}$, because they lead to $M = C^d \pmod{N}$ by Chinese Remainder Theorem.
    - First we prove $M = C^d \pmod{p}$.
      From $C = M^e \pmod{N}$, we know $C = M^e \pmod{p}$ and hence $C^d = M^{ed} \pmod{p}$.
    - $ed = 1 \pmod{(p-1)(q-1)}$,
      so $ed = k(p-1)(q-1) + 1$ for some integer k.
    - $M^{ed} = M * M^{k(p-1)(q-1)} \pmod{p}$
      $M^{ed} = M * (M^{(p-1)})^{k(q-1)} \pmod{p}$
    - According to Fermat's Little Theorem:
      $M^{ed} = M * (1)^{k(q-1)} \pmod{p}$
      $M^{ed} = M \pmod{p}$
    - By symmetry, we also have $M^{ed} = M \pmod{q}$. Thus $M = C^d \mod N$.