RSA public-key cryptosystem

1. Select at random two large prime numbers p, q.
2. $n = p * q$.
3. Select a small odd integer e which is relatively prime to $(p-1)*(q-1)$.
4. Compute d as the multiplicative inverse of e, modulo $(p-1)*(q-1)$, i.e., $e*d = 1 \ \underline{\text{mod}} [(p-1)*(q-1)]$.
5. publish $P = (e, n)$ as RSA public key.
6. keep $S = (d, n)$ as RSA secret key.

- Fermat's Theorem

If P is prime and Z_p^* represents the numbers in $Z_p = \{0, 1, \cdots, p-1\}$ which are relatively prime to P, then

$$a^{P-1} \equiv 1 \pmod{P}$$

for all $a \in Z_p^*$.

- Chinese Remainder Theorem

If $n_1, n_2, \cdots, n_k$ are pairwise relatively prime and $n = n_1 \times n_2 \times \cdots \times n_k$, then for all integers x and a,

$$X \equiv a \pmod{n_i},\ i = 1, 2, \cdots, k$$

if and only if

$$X \equiv a \pmod{n}.$$