RSA公鑰密碼系統(RSA public key cryptosystem):

系統是1976年由MIT的研究員Ron Rivest, Adi Shamir及Len Adleman所提出的。在一個密碼系統中,一般分成加密(encryption)及解密(decryption)二個基本的動作。

在RSA加密系統中,一個欲傳送的訊息首先轉換成整數區塊(由ASCII對照表轉換成整數),假設這個整數為M,然後取兩個夠大的相異質數p和q,使得到加密鑰(encryption key)為n和e,

其中 $n=pq$,e與 $\phi(n)=n\left(1-\frac{1}{p}\right)\left(1-\frac{1}{q}\right)=(p-1)(q-1)$ 互質。

最後將M轉換成C傳送出去。

公式:

$$C=M^e \bmod n$$

因為 $\gcd(e, \phi(n)) = 1$，所以 e 的乘法反元素存在，

取解密金鑰 (decryption key) d，其中 d 為

$$d \equiv e^{-1} \pmod{\phi(n)}$$

$$\Rightarrow de \equiv 1 \pmod{(p-1)(q-1)}$$

$$\Rightarrow \exists k \in \mathbb{Z}, \text{使得 } de = 1 + k[(p-1)(q-1)]$$

解密

$$\Rightarrow C \equiv M^e \pmod{n}$$

$$\Rightarrow \underbrace{C \cdot C \cdots C}_{d \text{ 個}} \equiv \underbrace{(M^e)(M^e)\cdots(M^e)}_{d \text{ 個}} \pmod{n}$$

$$\Rightarrow C^d \equiv (M^e)^d \pmod{n}$$

$$\Rightarrow C^d \equiv M^{de} \pmod{n}$$

$$\Rightarrow M^{de} = M^{1+k[(p-1)(q-1)]}, \exists k \in \mathbb{Z}$$

根據 Fermat's little theorem

$$M^{p-1} \equiv 1 \pmod{p} \quad 且 \quad M^{q-1} \equiv 1 \pmod{q}$$

$$\Rightarrow M^{de} = M^{1+k[(p-1)(q-1)]} = M \cdot M^{k(p-1)(q-1)}$$

$$\Rightarrow M \cdot \left(M^{(p-1)}\right)^{k(q-1)} \equiv M \cdot 1 \pmod{p}$$

且

$$M \cdot \left(M^{(q-1)}\right)^{k(p-1)} \equiv M \cdot 1 \pmod{q}$$

因為 $\gcd(p, q) = 1$ 且 $pq = n$，

根據 chinese remainder theorem，得

$$C^d \equiv M \pmod{pq}$$

$$\Rightarrow C^d \equiv M \pmod{n}$$