RSA金鑰

- Bob取相異質數 p、q (保密)，計算**RSA模數(RSA Modulus)** $n = pq$ 將其公開，
- 取 e 為加密鑰將其公開，其中 e 必須與 $\phi(n)$ 互質，在此情況
  $\phi(n) = (p-1)(q-1)$(保密)，
  Bob之公開鑰**(Public Key)**為 (n, e)；
- Bob計算 d 為解密鑰(保密)，(n, d) 為Bob之私鑰**(Private Key)**，其中

$$ed \equiv 1 \pmod{\phi(n)}。$$