

Key Generation	
Select p, q	p and q both prime
Calculate $n = p \times q$	
Calculate $\phi(n) = (p - 1)(q - 1)$	
Select integer e	$\text{gcd}(\phi(n), e) = 1; 1 < e < \phi(n)$
Calculate d	$d = e^{-1} \text{ mod } \phi(n)$
Public key	$KU = \{e, n\}$
Private key	$KR = \{d, n\}$

Encryption	
Plaintext:	$M < n$
Ciphertext:	$C = M^e \text{ (mod } n)$

Decryption	
Ciphertext:	C
Plaintext:	$M = C^d \text{ (mod } n)$

Figure 3.8 The RSA Algorithm