7.2.2 RSA Example

Q: $p = 11$ $q = 3$

we choose the smallest e, d

$M = 8$

C ?

M ?

S ?

M ?

Solution ① $n = p \times q = 11 \times 3 = 33$

$\phi(n) = (p-1) \times (q-1) = 10 \times 2 = 20$

② public key

Factors

10 : 2, 5

2 : 2

Prime: $1 < e < \phi(n)$

2	3	5	7	11	13	17	19
X	✓	X	✓	✓	✓	✓	✓

we choose $e = 3$

③ private key d

$$d = \frac{k\phi(n)+1}{e}$$

$$d = \frac{20k+1}{3}$$

$k = 1$, $d = \frac{21}{3} = 7$

④ public key $(n, e) = (33, 3)$

private key $(n, d) = (33, 7)$

⑤ Message $M = 8$

Encryption $C = M^e \bmod n$

$= 8^3 \bmod 33$

$= 17$

Decryption $M = C^d \bmod n$

$= 17^7 \bmod 33$

$= 8$

Signature Generation

$S = M^d \bmod n$

$= 8^7 \bmod 33$

$= 2$

Validation

$M = S^e \bmod n$

$= 2^3 \bmod 33$

$= 8$