4.3.4.3 RSA Algorithm with Data (Message = 2)

Q: ① $p = 5$ $q = 11$

② $N = p \times q = 5 \times 11 = 55$

③ $\text{phi}(N) = (p-1)(q-1) = 4 \times 10 = 40$

④ $e = 23$ 与 p 和 Q 互质

⑤ private key d

$e \times d \bmod N = 1$

$23 \times d \bmod 55 = 1$

$d = 7$

⑥ publishes public key (N, e) (55, 23)

⑦ receive encrypts message

$C = M^e \bmod N$

$= 2^{23} \bmod 55$

$= 8$

⑧ decrypts

$M = C^d \bmod N = 8^7 \bmod 55 = 2$

p：大质数 1

q：大质数 2

N：模数

$\phi(N)$：减一模数

e：公钥

d：私钥

(N,e)：模数，公钥

M：消息

C：加密消息