4.3.4.6 Example 3 RSA

Q $p = 53$ $q = 59$

Solution ① $n = p \cdot q = 3127$

② $\phi(n) = (p-1)(q-1) = 52 \times 58 = 3016$

③ select e as public key

1	2	3	5	7
X	X	✓	✓	✓

$e = 3$

④ calculate d as private key

$e \cdot d \bmod \phi(n) = 1$

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

$$= \frac{3016k + 1}{e}$$

$k=1$, $d = \frac{3017}{3}$ ✗

$k=2$, $d = 2011$ ✓

⑤ Encrypt Message = "HI"

a	b	c	d	e	f	g	h	i
1	2	3	4	5	6	7	8	9

Message $M = 89$

$C = M^e \bmod n$

$= 89^3 \bmod 3127$

$89^3 \div 3127 = 225.4458$

$89^3 - 225 \times 3127 = 1394$

⑥ decryption

$M = C^d \bmod n$

$= 1394^{2011} \bmod 3127$

$- 89$

HI