4.3.4.7 Example 4 RSA

Q: $p = 43$ $q = 59$

Solution ① $n = p \cdot q = 43 \times 59 = 2537$

② $\phi(n) = (p-1)(q-1) = 42 \times 58 = 2436$

③ select e as public key

1	2	3	5	7	11	13
×	×	×	✓	×	✓	✓

$e = 13$

④ calculate d

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

$$d = \frac{k\phi(n)+1}{13}$$

$$= \frac{2436k+1}{13}$$

$k = 1$, $d = \frac{2437}{13}$ ×

$k=2,\ d=\frac{4873}{13}$ ✗

$k=3,\ d=\frac{7309}{13}$ ✗

$k=4,\ d=\frac{9745}{13}$ ✗

$k=5,\ d=937$ ✓

⑤ Encrypt $M = STOP$

a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t
1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20
0	1	2												14	15			18	19

18 19 | 14 15

1 group 1 group

$M_1 = 1819$

$M_2 = 1415$

$C_1 = M_1^{e} \bmod n$

$= 1819^{13} \bmod 2537$

$= 2081$

$$C_2 = M_2^{e} \bmod n$$

$$= 1415^{13} \bmod 2537$$

$$= 2182$$

$$C = 2081\,2182$$