سوال ۱)

۱.۱

$gcd(26,7) = 1$ ← معکوس ضربی وجود دارد.

$r_0 = 26 , r_1 = 7$ (26,7)

$26 = 3\times7+5$ (7,5) $5 = 26 - 3\times7 = r_0 - 3r_1$

$7 = 1\times5+2$ (5,2) $2 = 7 - 1\times5 = r_1 - 1(r_0 - 3r_1) = 4r_1 - r_0$

$5 = 2\times2+1$ (2,1) $1 = 5 - 2\times2 = (r_0 - 3r_1) - 2(4r_1 - r_0) = - 11r1 + 3r0$

$\rightarrow 1 = -11\times7 + 3\times26$

$\rightarrow 7^{-1} \equiv -11 \bmod 26 = \mathbf{15}$

i	**q_{i-1}**	**r_i**	**s_i**	**t_i**
2	3	5	1	-3
3	1	2	-1	4
4	2	1	3	**-11**

۱.۲

$gcd(999,19) = 1$ ← معکوس ضربی وجود دارد.

$r_0 = 999 , r_1 = 19$ (999,19)

$999 = 52\times19+11$ (19,11) $11 = 999 - 52\times19 = r_0 - 52r_1$

$19 = 1\times11+8$ (11,8) $8 = 19 - 1\times11 = r_1 - (r_0 - 52r_1) = 53r_1 - r_0$

$11 = 1\times8+3$ (8,3) $3 = 11 - 1\times8 = (r_0 - 52r_1) - (53r_1 - r_0) = 2r_0 - 105r_1$

$8 = 2\times3+2$ (3,2) $2 = 8 - 2\times3 = (53r_1 - r_0) - 2(2r_0 - 105r_1) = 263r_1 - 5r_0$

$3 = 1\times2+1$ (2,1) $1 = 3 - 1\times2 = (2r_0 - 105r_1) - (263r_1 -5r_0) = -368r_1 + 7r_0$

$\rightarrow 1 = -368\times19 + 7\times999$

$\rightarrow 19^{-1} \equiv -368 \bmod 999 = \mathbf{631}$

i	q_{i-1}	r_i	s_i	t_i
2	52	11	1	-52
3	1	8	-1	53
4	1	3	2	-105
5	2	2	-5	263
6	1	1	7	**-368**

سوال ۲)

$m = 6 = 2\times 3 \;\rightarrow\; \varphi(6) = (3-1) \times (2-1) = 2$

قضیه اویلر:

$a^2 \equiv 1 \bmod 6$, if $\gcd(a,6) = 1$

$\gcd(0,6) \neq 1 \quad 0^2 \equiv 0 \bmod 6$

$\gcd(1,6)=1 \quad 1^2 \equiv 1 \bmod 6$

$\gcd(2,6)\neq 1 \quad 2^2 \equiv 4 \bmod 6$

$\gcd(3,6) \neq 1 \quad 3^2 \equiv 9 \equiv 3 \bmod 6$

$\gcd(4,6) \neq 1 \quad 4^2 \equiv 16 \equiv 4 \bmod 6$

$\gcd(5,6)=1 \quad 5^2 \equiv 25 \equiv 1 \bmod 6$

$m = 9 \;\rightarrow\; \varphi(9) = 3^2 - 3^1 = 9-3 = 6$

قضیه اویلر:

$a^6 \equiv 1 \bmod 9$, if $\gcd(a,9) = 1$

$\gcd(0,9) \neq 1 \quad 0^6 \equiv 0 \bmod 9$

$\gcd(1,9) = 1 \quad 1^6 \equiv 1 \bmod 9$

$\gcd(2,9) = 1 \quad 2^6 \equiv 64 \equiv 1 \bmod 9$

$\gcd(3,9) \neq 1 \quad 3^6 \equiv (3^3)^2 \equiv 0^2 \equiv 0 \bmod 9$

$\gcd(4,9) = 1 \quad 4^6 \equiv (2^6)^2 \equiv 1^2 \equiv 1 \bmod 9$

$\gcd(5,9) = 1 \quad 5^6 \equiv 1 \bmod 9$

$\gcd(6,9) \neq 1 \quad 6^6 \equiv 2^6 \times 3^6 \equiv 1 \times 0 \equiv 0 \bmod 9$

$\gcd(7,9) = 1$ $\qquad$ $7^6 \equiv 1 \bmod 9$

$\gcd(8,9) = 1$ $\qquad$ $8^6 \equiv 1 \bmod 9$

سوال ۳)

۳.۱

$r_0 = 7469$, $r_1 = 2464$

7469 = 3 × 2464 + 77	gcd(7469, 2464) = gcd(2464, 77)
2464 = 32 × 77 + 0	gcd(2464, 77) = gcd(77, 0) = 77

۳.۲

$r_0 = 4001$, $r_1 = 2689$

4001 = 1 × 2689 + 1312	gcd(4001, 2689) = gcd(2689, 1312)
2689 = 2 × 1312 + 65	gcd(2689, 1312) = gcd(1312, 65)
1312 = 20 × 65 + 12	gcd(1312, 65) = gcd(65, 12)
65 = 5 × 12 + 5	gcd(65, 12) = gcd(12, 5)
12 = 2 × 5 + 2	gcd(12, 5) = gcd(5, 2)
5 = 2 × 2 + 1	gcd(5, 2) = gcd(2, 1)
2 = 2 × 1 + 0	gcd(2, 1) = gcd(1, 0) = 1

سوال ۴)

$$n = 31 \cdot 37 = 1147$$

$$\Phi(n) = (p-1)(q-1) = 30 \cdot 36 = 1080$$

$$\Rightarrow\ d = e^{-1}\ mod\ \Phi(n) = 17^{-1}\ \ mod\ 1080\ = 953$$

$$y_p = y\ \ mod\ p = 2\ \ mod\ 31 = 2$$

$$y_q = y\ \ mod\ q = 2\ \ mod\ 37 = 2$$

$$d_p = d\ \ mod\ (p-1) = 953\ \ mod\ 30 = 23$$

$$d_q = d\ \ mod\ (q-1) = 953\ \ mod\ 36 = 17$$

$$x_p = y_p^{d_p}\ \ mod\ p = 2^{23}\ \ mod\ 31 = 8$$

$$x_q = y_q^{d_q}\ \ mod\ q = 2^{17}\ \ mod\ 37 = 18$$

$$c_p = q^{-1}\ mod\ p = 37^{-1}\ mod\ 31 = 26$$

$$c_q = p^{-1}\ mod\ q = 31^{-1}\ mod\ 37 = 6$$

بنابراین مقدار متن اصلی (Plain text) برابر است با:

$$x = (q \cdot c_p \cdot x_p) + (p \cdot c_q \cdot x_q)\ mod\ n$$

$$\Rightarrow\ x = (37 \cdot 26 \cdot 8) + (31 \cdot 6 \cdot 18)\ \ mod\ 1147$$

$$= 8440\ \ mod\ 1147 = 721$$

سوال ۵)

۵.۱

در این حالت انجام حمله brute-force به راحتی امکان پذیر بوده و می‌توان به کلید مورد نظر رسید.

۵.۲

حداقل طول ۱۲۸ بیت برای جلوگیری از انجام حمله brute-force بر روی کلید خصوصی مورد نیاز است. ولی به دلیل وجود حمله‌های تحلیلی (Analytical Attacks) قدرتمند، باید طول کلید را بزرگتر هم انتخاب کنیم. توصیه می‌شود که طول کلید خصوصی حداقل برابر با $d = 0.3 \cdot n$ انتخاب شود؛ حتی بهتر است که $d = 0.5 \cdot n$ باشد.

سوال ۶)

هدف ما محاسبه تعداد اعداد صحیح نا منفی کوچک‌تر از $n = p^a$ است که نسبت به n اول هستند؛ بنابراین ابتدا تعداد اعدادی که نسبت به n اول نیستند را محاسبه کرده و از مقدار کل کم می‌کنیم.

اعداد صحیح نا منفی کوچک‌تر از p^a عبارت‌اند از $0,1,2, \dots , p^a - 1$ ؛ که تعداد آنها برابر با p^a است.

اعدادی که یک عامل مشترک با p^a دارند، مضارب p هستند که تعداد آن‌ها برابر است با : ${p^a}/{p} = p^{a-1}$

بنابراین داریم:

$$\Phi(p^a) = p^a - p^{a-1}$$

راه دیگر:

$$\Phi(p^a) = p^a \cdot \left(1 - \frac{1}{p}\right) = p^a \cdot \frac{p-1}{p} = p^{a-1} \cdot (p-1) = p^a - p^{a-1}$$

سوال ۷)

۷.۱

$$\Phi(n) = (p-1)(q-1) = 40 \cdot 16 = 640$$

مقدار e باید به گونه‌ای انتخاب شود که $gcd\big(e, \Phi(n)\big) = 1$ باشد:

$$e_1 = 32 \;\Rightarrow\; gcd(32, 640) = 32 \quad \times$$

$$e_2 = 49 \;\Rightarrow\; gcd(49, 640) = 1$$

۷.۲

$$640 = 13 \cdot 49 + 3$$

$$49 = 16 \cdot 3 + 1$$

$$\Rightarrow 1 = 49 - 16 \cdot 3 = 49 - 16(640 - 13 \cdot 49) = 209 \cdot 49 - 16 \cdot 640$$

$$\Rightarrow\; 49^{-1} \; mod\; 640 = 209$$

$$\Rightarrow\; k_{pr} = (p, q, d) = (41, 17, 209)$$