۱.

$$c_1 = m^{e_A} \mod N \quad , \quad c_2 = m^{e_B} \mod N$$

با توجه به این‌که $\gcd(e_A, e_B) = \gcd(3,5) = 1$ است، بنابراین داریم:

$$\exists\, a, b \in Z_n \ : \ a \cdot e_A + b \cdot e_B = 1$$

$$\Rightarrow \ c_1^a \cdot c_2^b = (m^{e_A})^a \cdot (m^{e_B})^b = m^{e_A \cdot a} \cdot m^{e_B \cdot b} = m^{e_A \cdot a + e_B \cdot b} = m^1 = m \mod N$$

۲.۱ برای مقادیر e_A و e_B که $\gcd(e_A, e_B) = 1$ باشد، می‌توان از این حمله استفاده کرد.

۲.

۱.۲. سوال ۱.۷ :

۱.۱.۷.

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

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

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

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

۲.۱.۷.

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

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

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

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

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

۲.۲. سوال ۵.۷ :

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

۲.۵.۷. 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.

۳.

$$\gcd(999,19) = 1$$
$$999 = 52 \cdot 19 + 11$$
$$19 = 1 \cdot 11 + 8$$
$$11 = 1 \cdot 8 + 3$$
$$8 = 2 \cdot 3 + 2$$
$$3 = 1 \cdot 2 + 1$$
$$\Rightarrow 1 = 3 - 1 \cdot 2 = 3 - 1(8 - 2 \cdot 3) = 3(11 - 1 \cdot 8) - 1 \cdot 8$$
$$= 3 \cdot 11 - 4 \cdot 8 = 3 \cdot 11 - 4(19 - 1 \cdot 11) = 7 \cdot 11 - 4 \cdot 19$$
$$= 7(999 - 52 \cdot 19) - 4 \cdot 19 = 7 \cdot 999 - 368 \cdot 19$$
$$\Rightarrow\ 19^{-1}\ mod\ 999 = 368$$

۴.

۱.۴.

$$n = 2623 = 43 \cdot 61 \quad \Rightarrow p = 43 \quad , \quad q = 61$$
$$\Rightarrow \quad d = e^{-1}\ mod\ \Phi(n)$$
$$\Phi(n) = (p-1)(q-1) = 42 \cdot 60 = 2520$$
$$\Rightarrow \quad d = 2111^{-1}\ mod\ 2520\ = 191$$

خیر. به طور کلی برای مقادیر بزرگ n ، تجزیه‌کردن آن بسیار سخت و غیرممکن است و نمی‌توان مقدار $\Phi(n)$ و کلید خصوصی را محاسبه کرد (در اینجا به دلیل کوچک بودن مقدار n ، تجزیه آن امکان‌پذیر بود).

۲.۴.

$$m = c^d \quad mod\ 2623 = 1141^{191} \quad mod\ 2623 = 1088$$

۵.

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:

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

۶.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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