سوال ۱)

$$k_{pr} = 1 \;\Rightarrow\; k_{pub} = \alpha^1 \; mod\, p = \alpha$$

$$k_{pr} = p - 1 \;\Rightarrow\; k_{pub} = \alpha^{p-1} \; mod\, p = 1$$

بنابراین کلیدهای $p-1$ و 1 ، یک کلید ضعیف به حساب می‌آیند و در صورتی که مورد استفاده قرار بگیرند؛ مهاجم به راحتی می‌تواند مقدار کلید خصوصی را بدست آورد.

سوال ۲)

منظور از primitive root یا مولد یک عدد p عددی مانند α است به‌طوری که باقی‌مانده همه‌ی توان‌های α به پیمانه‌ی p همه‌ی اعداد 1 تا $p-1$ را شامل گردد.

- با توجه به این‌که اعداد داده شده به فرم p^k و $2p^k$ هستند، که p یک عدد اول فرد و $k \geq 1$ است؛ بنابراین همه‌ی آن‌ها دارای مولد می‌باشند.
- عنصر $\alpha \in Z_n^*$ یک مولد گروه Z_n^* است، اگر و تنها اگر $\alpha^{\Phi(n)/p} \neq 1 \; mod\; n$ که مقدار p یک عامل اول $\Phi(n)$ می‌باشد.

۲.۱

اگر مقدار $\alpha = 2$ در نظر بگیریم، باید نشان دهیم که α یک مولد است، بنابراین داریم:

$$if\; \alpha = 2 \;, n = 11 \quad \Rightarrow \quad \Phi(11) = 10 = 2 \times 5 \quad \Rightarrow \quad p = 2,5$$

$$p = 2 \quad \Rightarrow \quad \alpha^{\Phi(n)/p} = 2^{10/2} \; mod\; 11 = 10 \neq 1 \, mod\; 11$$

$$p = 5 \quad \Rightarrow \quad \alpha^{\Phi(n)/p} = 2^{10/5} \; mod\; 11 = 4 \; \neq 1 \, mod\; 11$$

بنابراین $\alpha = 2$ یک مولد گروه Z_{11}^* است.

۲.۲

$$if\; \alpha = 2 \;, n = 11^2 \quad \Rightarrow \quad \Phi(11^2) = 110 = 2 \times 5 \times 11 \quad \Rightarrow \quad p = 2,5,11$$

$$p = 2 \quad \Rightarrow \quad \alpha^{\Phi(n)/p} = 2^{110/2} \; mod\; 11^2 = 120 \; \neq 1 \, mod\; 11^2$$

$$p = 5 \quad \Rightarrow \quad \alpha^{\Phi(n)/p} = 2^{110/5} \; mod\; 11^2 = 81 \; \neq 1 \, mod\; 11^2$$

$$p = 11 \quad \Rightarrow \quad \alpha^{\Phi(n)/p} = 2^{110/11} \; mod\; 11^2 = 56 \; \neq 1 \, mod\; 11^2$$

بنابراین $\alpha = 2$ یک مولد گروه $Z_{11^2}^*$ است.

۲.۳

$$if\ \alpha = 2\ , n = 2 \cdot 11^2 \quad \Rightarrow \quad \Phi(2 \cdot 11^2) = 110 = 2 \times 5 \times 11 \quad \Rightarrow \quad p = 2,5,11$$

$$p = 2 \quad \Rightarrow \quad \alpha^{\Phi(n)/p} = 2^{110/2}\ mod\ 2 \cdot 11^2 = 120\ \neq 1\ mod\ 2 \cdot 11^2$$

$$p = 5 \quad \Rightarrow \quad \alpha^{\Phi(n)/p} = 2^{110/5}\ mod\ 2 \cdot 11^2 = 202\ \neq 1\ mod\ 2 \cdot 11^2$$

$$p = 11 \quad \Rightarrow \quad \alpha^{\Phi(n)/p} = 2^{110/11}\ mod\ 2 \cdot 11^2 = 56\ \neq 1\ mod\ 2 \cdot 11^2$$

بنابراین $\alpha = 2$ یک مولد گروه $Z^*_{2 \cdot 11^2}$ است.

۲.۴

$$if\ \alpha = 2\ , n = 11^{100} \quad \Rightarrow \quad \Phi(11^{100}) = 2 \times 5 \times 11^{99} \quad \Rightarrow \quad p = 2,5,11$$

$$p = 2 \quad \Rightarrow \quad \alpha^{\Phi(n)/p} = 2^{\Phi(n)/2}\ mod\ 11^{100} \neq 1\ mod\ 11^{100}$$

$$p = 5 \quad \Rightarrow \quad \alpha^{\Phi(n)/p} = 2^{\Phi(n)/5}\ mod\ 11^{100} \neq 1\ mod\ 11^{100}$$

$$p = 11 \quad \Rightarrow \quad \alpha^{\Phi(n)/p} = 2^{\Phi(n)/11}\ mod\ 11^{100} \neq 1\ mod\ 11^{100}$$

بنابراین $\alpha = 2$ یک مولد گروه $Z^*_{11^{100}}$ است.

بنابراین $\alpha = 2$ یک مولد برای اعداد 11 ، 11^2 ، $2 \cdot 11^2$ و 11^{100} است.

سوال ۳)

ابتدا کلید عمومی باب را محاسبه می‌کنیم:

$$\beta = \alpha^d\ \ mod\ p = 7^{22105}\ \ mod\ 44927 = 40909$$

$$\Rightarrow \quad k_{pub} = (p, \alpha, \beta) = (44927, 7, 40909)$$

برای رمز کردن متن، یک i تصادفی در محدوده $2 \leq i \leq p - 2$ انتخاب می‌کنیم، سپس داریم:

$$i = 67 \quad \Rightarrow \quad k_E = \alpha^i\ \ mod\ p = 7^{67}\ \ mod\ 44927 = 38737$$

$$\Rightarrow \quad k_M = \beta^i\ \ mod\ p = 40909^{67}\ \ mod\ 44927 = 25566$$

$$\Rightarrow \quad y = m \cdot k_M\ \ mod\ p = 10101 \cdot 25566\ \ mod\ 44927 = 1770$$

بنابراین آلیس متن رمز شده $(k_E, y) = (38737, 1770)$ را برای باب می‌فرستد.

باب برای رمزگشایی متن رمزشده عملیات زیر را انجام می‌دهد:

$$k_M = k_E^d \ mod\ p = 38737^{22105} \ mod\ 44927 = 25566$$
$$\Rightarrow \quad m = y \cdot k_M^{-1} \ mod\ p = 1770 \cdot 25566^{-1} \ mod\ 44927 = 10101$$

سوال ۴)

۴.۱

$$y^2 = x^3 + 2x + 2 \quad mod\ 17 \quad \Rightarrow \quad a = 2\,, \ \ b = 2\,, \ \ p = 17$$
$$4a^3 + 27b^2 = 4 \times 2^3 + 27 \times 2^2 = 140 \ \ mod\ 17 = 4 \neq 0 \quad mod\ 17$$

۴.۲

$$(2,7) + (5,2) \ \ \Rightarrow \ \ x_1 = 2\,, \ \ x_2 = 5\,, \ \ y_1 = 7\,, \ \ y_2 = 2$$
$$s = (y_2 - y_1)(x_2 - x_1)^{-1} \ mod\ 17$$
$$\Rightarrow \ s = (2-7)(5-2)^{-1} \ mod\ 17 = (-5)(3)^{-1} \ mod\ 17$$
$$\Rightarrow \ s = (-5)(6) = -30 = 4 \ \ mod\ 17$$
$$\Rightarrow \ \ x_3 = s^2 - x_1 - x_2 \ \ mod\ 17 = 4^2 - 2 - 5 \ \ \ mod\ 17 \ = 9$$
$$\Rightarrow \ \ y_3 = s(x_1 - x_3) - y_1 \ mod\ 17 = 4(2-9) - 7 \ \ mod\ 17 = 16$$
$$\Rightarrow \quad (x_3, y_3) = (2,7) + (5,2) = (9,16)$$

۴.۳

$$Hesse's\ Theorem: \quad p + 1 - 2\sqrt{p} \leq \#E \leq p + 1 + 2\sqrt{p}$$
$$\#E = 19, \ \ p = 17 \quad \Rightarrow \quad 17 + 1 - 2\sqrt{17} \leq 19 \leq 17 + 1 + 2\sqrt{17}$$
$$\Rightarrow \quad 9.75 \leq 19 \leq 26.24$$

۴.۴

طبق قضیه ۸.۲.۴ کتاب درسی، با توجه به این‌که تعداد نقاط بر روی این خم که تشکیل یک گروه دوری محدود می‌دهند، عددی اول است، بنابراین تمامی عناصر این گروه primitive elements می‌باشند.

سوال ۵)

۵.۱

$$x = 0 \quad \Rightarrow \quad y^2 = 0^3 + 3 \cdot 0 + 2 = 2 \quad mod\ 7 \quad \Rightarrow \quad y = 3,4$$

$$x = 1 \quad \Rightarrow \quad y^2 = 1^3 + 3 \cdot 1 + 2 = 6 \quad mod\ 7 \Rightarrow$$ جواب ندارد

$$x = 2 \quad \Rightarrow \quad y^2 = 2^3 + 3 \cdot 2 + 2 = 2 \quad mod\ 7 \quad \Rightarrow \quad y = 3,4$$

$$x = 3 \quad \Rightarrow \quad y^2 = 3^3 + 3 \cdot 3 + 2 = 3 \quad mod\ 7 \Rightarrow$$ جواب ندارد

$$x = 4 \quad \Rightarrow \quad y^2 = 4^3 + 3 \cdot 4 + 2 = 1 \quad mod\ 7 \quad \Rightarrow \quad y = 1,6$$

$$x = 5 \quad \Rightarrow \quad y^2 = 5^3 + 3 \cdot 5 + 2 = 2 \quad mod\ 7 \quad \Rightarrow \quad y = 3,4$$

$$x = 6 \quad \Rightarrow \quad y^2 = 6^3 + 3 \cdot 6 + 2 = 5 \quad mod\ 7 \Rightarrow$$ جواب ندارد

بنابراین نقاط این منحنی برابر است با:

$$\{(0,3)\,,(0,4)\,,(2,3)\,,(2,4)\,,(4,1)\,,(4,6)\,,(5,3)\,,(5,4)\}$$

۵.۲

مرتبه گروه برابر است با:

$$\#E = \#\{O\,,(0,3)\,,(0,4)\,,(2,3)\,,(2,4)\,,(4,1)\,,(4,6)\,,(5,3)\,,(5,4)\} = 9$$

۵.۳

$$0 \cdot \alpha = O \quad , \quad 1 \cdot \alpha = (0,3) \quad , \quad 2 \cdot \alpha = (2,3) \quad , \quad 3 \cdot \alpha = (5,4)$$
$$4 \cdot \alpha = (4,6) \quad , \quad 5 \cdot \alpha = (4,1) \quad , \quad 6 \cdot \alpha = (5,3) \quad , \quad 7 \cdot \alpha = (2,4)$$
$$8 \cdot \alpha = (0,4) \quad , \quad 9 \cdot \alpha = O = 0 \cdot \alpha$$
$$\Rightarrow \quad ord(\alpha) = 9 = \#E \quad \Rightarrow \quad \boldsymbol{\alpha}\ is\ primitive\ element$$

سوال ۶)

$$k_{pr} = a = 6\,,\ \ k_{pub} = B = (5,9) \quad \Rightarrow \quad K = aB = 6 \cdot B = 2(2B + B)$$

$$2B = (x_3, y_3):\ \ x_1 = x_2 = 5\,,\ \ y_1 = y_2 = 9$$
$$s = (3x_1^2 + a) \cdot 2y_1{}^{-1} \ \ mod\ 11 = \ (3 \cdot 5^2 + 1)(2 \cdot 9)^{-1} \ \ mod\ 11 = 3$$
$$x_3 = s^2 - x_1 - x_2 \ \ mod\ 11 = 3^2 - 5 - 5 \ \ mod\ 11 \ = 10$$
$$y_3 = s(x_1 - x_3) - y_1 \ \ mod\ 11 = 3(5 - 10) - 9 \ \ mod\ 11 = 9$$
$$\Rightarrow \quad 2B = (x_3, y_3) = (10,9)$$

$$3B = 2B + B = (x_3', y_3') : \quad x_1 = 10\,, x_2 = 5\,, \quad y_1 = y_2 = 9$$

$$s = (y_1 - y_2)(x_2 - x_1)^{-1} \quad mod\ 11 = \ (9-9)(5-10)^{-1} \quad mod\ 11 = 0$$

$$x_3' = s^2 - x_1 - x_2 \quad mod\ 11 = 0^2 - 10 - 5 \quad mod\ 11 \ = 7$$

$$y_3' = s(x_1 - x_3') - y_1 \ \ mod\ 11 = 0(5-7) - 9 \quad mod\ 11 = 2$$

$$\Rightarrow \quad 3B = (x_3', y_3') = (7{,}2)$$

$$6B = 2 \cdot 3B = (x_3'', y_3'') : \quad x_1 = x_2 = 7\,, \quad y_1 = y_2 = 2$$

$$s = (3x_1^2 + a) \cdot 2{y_1}^{-1} \quad mod\ 11 = \ (3 \cdot 7^2 + 1)(2 \cdot 2)^{-1} \quad mod\ 11 = 4$$

$$x_3'' = s^2 - x_1 - x_2 \quad mod\ 11 = 4^2 - 7 - 7 \quad mod\ 11 \ = 2$$

$$y_3'' = s(x_1 - x_3'') - y_1 \ \ mod\ 11 = 4(7-2) - 2 \quad mod\ 11 = 7$$

$$\Rightarrow \quad 6B = (x_3'', y_3'') = (2{,}7)$$

$$\Rightarrow \quad K_{AB} = x_3'' = 2$$