سوال ۱)

۱. $k_{pr} = 123,\ i = 320,\ x = 71,\ p = 751,\ \alpha = 3$

ابتدا کلید عمومی را محاسبه می‌کنیم: $(k_{pr} = d)$

$$k_{pub} = \beta = \alpha^d \ mod\ p \quad \Rightarrow \quad k_{pub} = \beta = 3^{123} \ mod\ 751 = 743$$

انجام عملیات Encryption توسط Alice:

$$\text{Ephemeral Key: } k_E = \alpha^i \ mod\ p \quad \Rightarrow \quad k_E = 3^{320} \ mod\ 751 = 378$$

$$\text{Masking Key: } k_M = \beta^i \ mod\ p \quad \Rightarrow \quad k_E = 743^{320} \ mod\ 751 = 499$$

$$\text{Encryption: } y = x \cdot k_M \ mod\ p \quad \Rightarrow \quad y = 71 \cdot 499 \ mod\ 751 = 132$$

بنابراین داریم: $\text{Ciphertext: } (k_E, y) = (378, 132)$

انجام عملیات Decryption توسط Bob:

$$\text{Masking Key: } k_M = k_E^d \ mod\ p \quad \Rightarrow \quad k_M = 378^{123} \ mod\ 751 = 499$$

$$\text{Decryption: } x = y \cdot k_M^{-1} \ mod\ p \quad \Rightarrow \quad x = 132 \cdot 499^{-1} \ mod\ 751$$

$$\Rightarrow \quad 499^{-1} \ mod\ 751 = 450 \quad \Rightarrow \quad x = 132 \cdot 450 \ mod\ 751 = 71$$

۲. $k_{pr} = 123,\ i = 210,\ x = 45,\ p = 751,\ \alpha = 3$

ابتدا کلید عمومی را محاسبه می‌کنیم: $(k_{pr} = d)$

$$k_{pub} = \beta = \alpha^d \ mod\ p \quad \Rightarrow \quad k_{pub} = \beta = 3^{123} \ mod\ 751 = 743$$

انجام عملیات Encryption توسط Alice:

$$\text{Ephemeral Key: } k_E = \alpha^i \ mod\ p \quad \Rightarrow \quad k_E = 3^{210} \ mod\ 751 = 485$$

$$\text{Masking Key: } k_M = \beta^i \ mod\ p \quad \Rightarrow \quad k_E = 743^{210} \ mod\ 751 = 51$$

$$\text{Encryption: } y = x \cdot k_M \ mod\ p \quad \Rightarrow \quad y = 45 \cdot 51 \ mod\ 751 = 42$$

بنابراین داریم: $\text{Ciphertext: } (k_E, y) = (485, 42)$

انجام عملیات Decryption توسط Bob:

$$\text{Masking Key: } k_M = k_E^d \ mod\ p \quad \Rightarrow \quad k_M = 485^{123} \ mod\ 751 = 51$$

$$\text{Decryption: } x = y \cdot k_M^{-1} \ mod\ p \quad \Rightarrow \quad x = 42 \cdot 51^{-1} \ mod\ 751$$

$$\Rightarrow \quad 51^{-1}\ mod\ 751 = 162 \quad \Rightarrow \quad x = 42 \cdot 162\ mod\ 751 = 45$$

۳. $k_{pr} = 500,\ i = 120,\ x = 500,\ p = 751,\ \alpha = 3$

ابتدا کلید عمومی را محاسبه می‌کنیم: $(k_{pr} = d)$

$$k_{pub} = \beta = \alpha^d\ mod\ p \quad \Rightarrow \quad k_{pub} = \beta = 3^{500}\ mod\ 751 = 72$$

انجام عملیات Encryption توسط Alice:

$$\text{Ephemeral Key: } k_E = \alpha^i\ mod\ p \quad \Rightarrow \quad k_E = 3^{120}\ mod\ 751 = 556$$

$$\text{Masking Key: } k_M = \beta^i\ mod\ p \quad \Rightarrow \quad k_E = 72^{120}\ mod\ 751 = 1$$

$$\text{Encryption: } y = x \cdot k_M\ mod\ p \quad \Rightarrow \quad y = 500 \cdot 1\ mod\ 751 = 500$$

بنابراین داریم: $\text{Ciphertext: } (k_E, y) = (556, 500)$

انجام عملیات Decryption توسط Bob:

$$\text{Masking Key: } k_M = k_E^d\ mod\ p \quad \Rightarrow \quad k_M = 556^{500}\ mod\ 751 = 1$$

$$\text{Decryption: } x = y \cdot k_M^{-1}\ mod\ p \quad \Rightarrow \quad x = 132 \cdot 1^{-1}\ mod\ 751 = 500$$

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.

.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

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

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

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

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

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

.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.

.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 $2 \le i \le p-2$ 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)

.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:

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

.۲

مرتبه گروه برابر است با:

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

.۳

$$0 \cdot \alpha = O \quad , \quad 1 \cdot \alpha = (0,3) \quad , \quad 2 \cdot \alpha = (2,3) \quad , \quad 3 \cdot \alpha = (5,4)$$

$$4\cdot\alpha=(4,6)\quad,\quad 5\cdot\alpha=(4,1)\quad,\quad 6\cdot\alpha=(5,3)\quad,\quad 7\cdot\alpha=(2,4)$$

$$8\cdot\alpha=(0,4)\quad,\quad 9\cdot\alpha=\mathcal{O}=0\cdot\alpha$$

$$\Rightarrow\quad ord(\alpha)=9=\#E\quad\Rightarrow\quad \boldsymbol{\alpha}\ \ is\ primitive\ element$$

سوال ۵)

ابتدا عدد ۱۳ را به صورت باینری نمایش می‌دهیم: $13P=1101_2P=(d_3d_2d_1d_0)_2P$

$d_3=1\ \Rightarrow\ Initial\ Setting\ \Rightarrow\ P=1_2P\ \Rightarrow\ P=(6,3)$

$d_2=1\ \Rightarrow\ Double\ \&\ Add$

$$\Rightarrow Double:\ P+P=2P=10_2P\quad\Rightarrow\quad 2P=(3,1)$$

$$\Rightarrow s=\frac{3x_1^2+a}{2y_1}=\frac{3\cdot 6^2+2}{2\cdot 3}=110\cdot 6^{-1}\ \ mod\ 17=8\cdot 3\ \ mod\ 17=7$$

$$\Rightarrow\ x_3=s^2-x_1-x_2\ \ mod\ p=7^2-6-6\ \ mod\ 17=3$$

$$\Rightarrow\ y_3=s(x_1-x_3)-y_1\ \ mod\ p=7(6-3)-3\ \ mod\ 17=1$$

$$\Rightarrow Add:\ 2P+P=3P=11_2P\quad\Rightarrow\quad 3P=(16,13)$$

$$\Rightarrow s=\frac{y_2-y_1}{x_2-x_1}=\frac{3-1}{6-3}=2\cdot 3^{-1}\ \ mod\ 17=2\cdot 6\ \ mod\ 17=12$$

$$\Rightarrow\ x_3=s^2-x_1-x_2\ \ mod\ p=12^2-3-6\ \ mod\ 17=16$$

$$\Rightarrow\ y_3=s(x_1-x_3)-y_1\ \ mod\ p=12(3-16)-1\ \ mod\ 17=13$$

$d_1=0\ \Rightarrow\ Double$

$$\Rightarrow Double:\ 3P+3P=6P=110_2P\quad\Rightarrow\quad 6P=(0,11)$$

$$\Rightarrow s=\frac{3x_1^2+a}{2y_1}=\frac{3\cdot 16^2+2}{2\cdot 13}=770\cdot 26^{-1}\ \ mod\ 17=5\cdot 2\ \ mod\ 17=10$$

$$\Rightarrow\ x_3=s^2-x_1-x_2\ \ mod\ p=10^2-16-16\ \ mod\ 17=68\ \ mod\ 17=0$$

$$\Rightarrow\ y_3=s(x_1-x_3)-y_1\ \ mod\ p=10(16-0)-13\ \ mod\ 17=11$$

$d_0=1\ \Rightarrow\ Double\ \&\ Add$

$$\Rightarrow Double:\ 6P+6P=12P=1100_2P\quad\Rightarrow\quad 12P=(9,16)$$

$$\Rightarrow s=\frac{3x_1^2+a}{2y_1}=\frac{3\cdot 0^2+2}{2\cdot 11}=2\cdot 22^{-1}\ \ mod\ 17=2\cdot 7\ \ mod\ 17=14$$

$$\Rightarrow\ x_3=s^2-x_1-x_2\ \ mod\ p=14^2-0-0\ \ mod\ 17=9$$

$$\Rightarrow\ y_3 = s(x_1 - x_3) - y_1\ mod\ p = 14(0-9) - 11\ mod\ 17 = 16$$

$$\Rightarrow\ Add:\ 12P + P = 13P = 1101_2P \quad \Rightarrow \quad 13P = (0,6)$$

$$\Rightarrow s = \frac{y_2 - y_1}{x_2 - x_1} = \frac{3-16}{6-9} = (-13)\cdot(-3)^{-1}\ mod\ 17 = 4\cdot 11\ mod\ 17 = 10$$

$$\Rightarrow\ x_3 = s^2 - x_1 - x_2\ mod\ p = 10^2 - 9 - 6\ mod\ 17 = 85\ \ mod\ 17 = 0$$

$$\Rightarrow\ y_3 = s(x_1 - x_3) - y_1\ mod\ p = 10(9-0) - 16\ mod\ 17 = 6$$

بنابراین پاسخ نهایی برابر است با: $13P = (0,6)$

سوال ۶)

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

$$2B = (x_3, y_3):\ \ x_1 = x_2 = 5\,,\ \ y_1 = y_2 = 9$$

$$s = (3x_1^2 + a)\cdot 2{y_1}^{-1}\ \ mod\ 11 =\ (3\cdot 5^2 + 1)(2\cdot 9)^{-1}\ \ mod\ 11 = 3$$

$$x_3 = s^2 - x_1 - x_2\ \ mod\ 11 = 3^2 - 5 - 5\ \ \ mod\ 11\ = 10$$

$$y_3 = s(x_1 - x_3) - y_1\ mod\ 11 = 3(5-10) - 9\ \ mod\ 11 = 9$$

$$\Rightarrow \quad 2B = (x_3, y_3) = (10,9)$$

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

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

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

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

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

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

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

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

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

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

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