⑥ El Gamal Cryptosystem.

Let $p = 11$ & $d = 3$

$e_1 = 2$ which is primitive root in Z_{11}^*

$e_2 = e_1^d = 2^3 = 8$

Public key => $(2, 8, 11)$

Private key => 3

Plaintext = 7, $r = 4$

$C_1 = e_1^r \bmod p$

$= 2^4 \bmod 11$

$C_1 = 5$

$C_2 = (P \times e_2^r) \bmod 11$

$= (7 \times 8^4) \bmod 11$

$= 28672 \bmod 11$

$C_2 = 6$

=> **Cipher text => (5, 6)**

$$P = \left[C_2 \times (C_1^q)^{-1}\right] \bmod 11$$

$$= \left(6 \times (5^3)^{-1}\right) \bmod 11$$

$$= \left(6 \times 125^{-1}\right) \bmod 11$$

q	r_1	r_2	r	t_1	t_2
11	125	11	4	0	1
2	11	4	3	1	-11
1	4	3	1	-11	23
3	3	1	0	23	-34

$$P = 6 \times 3 \bmod 11$$

$$= 18 \bmod 11$$

$$\boxed{P = 7}$$

---

⑦ Elliptical curve :

Given $P(3,10)$ $Q(9,7)$ for $E_{23}(1,1)$

Find $P+Q$.

Let $R = P + Q$

$$\lambda = \frac{x_q - x_p}{y_q - y_p} \quad \frac{y_q - y_p}{x_q - x_p}$$

$$= \frac{-3}{6}$$

$$= -2^{-1} \bmod 23$$

q	r_1	r_2	r	t_1	t_2
11	23	2	1	0	1
2	2	1	0	1	-11

$$= (-1)(-11) \bmod 23$$

$$\boxed{\lambda = 11}$$

$$x_r = \lambda^2 - x_p - x_q$$

$$= 121 - 3 - 9$$

$$= 109 \bmod 23$$

$$x_r = 17$$

$$y_r = \lambda(x_p - x_r) - y_p$$

$$= 11(3 - 17) - 10$$

$$= -164 \bmod 23$$

$$= -3 \bmod 23$$

$$y_r = 20$$

$$\Rightarrow \boxed{R(17, 20)}$$

(8) $P(3,10)$ $Q(9,7)$ $E_{23}(1,1)$

Find $2P$

$$\lambda = \frac{3x_p^2 + a}{2y_p}$$

$$= \frac{3 \times 9 + 1}{2 \times 10}$$

$$= \frac{28}{20} = \frac{14}{10} = \frac{7}{5}$$

$$= 7 \times 5^{-1} \bmod 23$$

q	r_1	r_2	r	t_1	t_2
4	23	5	3	0	1
1	5	3	2	1	-4
1	3	2	1	-4	5
2	2	1	0	5	-9

$$= 7 \times 14 \bmod 23$$

$$\boxed{\lambda = 6}$$

$x_r = \lambda^2 - x_p - x_q$

$= 6^2 - 3 - 3$

$= 36 - 3 - 3$

$= 30 \bmod 23$

$\boxed{x_r = 7}$

$y_r = \lambda(x_p - x_r) - y_p$

$= 6(3-7) - 10$

$= -34 \bmod 23$

$\boxed{y_r = 12}$

$\boxed{R \Rightarrow 2P \Rightarrow (7, 12)}$

(9) Find 2Q.

$$\lambda = \frac{3x_q^2 + a}{2y_q}$$

$$= \frac{3 \times 9^2 + 1}{2 \times 7}$$

$$= \frac{244}{14} = 122 \times 7^{-1} \bmod 23$$

q	r_1	r_2	r	t_1	t_2
3	23	7	2	0	1
3	7	2	1	1	-3
2	2	1	0	-3	10

$$\lambda = 11 \times 10 \bmod 23$$

$$= 1220 \bmod 23$$

$$\boxed{\lambda = 1}$$

$$x_r = \lambda^2 - x_p - x_q \qquad y_r = \lambda(x_q - x_r) - y_q$$

$$= 1^2 - 9 - 9 \qquad = 1(9-6) - 7$$

$$= -17 \bmod 23 \qquad = 3 - 7$$

$$x_r = 6 \qquad = -4 \bmod 23$$

$$= 19$$

$$\boxed{R \Rightarrow 2Q \Rightarrow (6, 19)}$$

---

(10) Diffie - Hellman key exchange.

$$g = 7, \quad p = 23$$

$$R_1 = g^x \bmod p \qquad R_2 = g^y \bmod p$$

Let $x = 3$ Let $y = 6$

$$= 7^3 \bmod 23 \qquad = 7^6 \bmod 23$$

$$R_1 = 21 \qquad R_2 = 4$$

3728961

$K = (R_2)^x \bmod p$

$= 4^3 \bmod p$

$= 18$

$K = (R_1)^y \bmod p$

$= 21^6 \bmod 23$

$= 18$

$\Rightarrow$ Key has been secretly exchanged.