P_{245}.

7. 解：取 $\alpha=2$ 是模 $p=5$ 的本原元，理由如下：

~~$\because \alpha^1=2, \alpha^2=4, \alpha^3=3, \alpha^4=$~~

$\alpha^1=2, \alpha^2=4, \alpha^3=3, \alpha^4=1$.

随机选 $d=2$，则 $y=\alpha^d \bmod p = 2^2 \bmod 5 = 4$.

随机选 $k=2$，则

$u = y^k \bmod p = 4^2 \bmod 5 = 1$.

$C_1 = \alpha^k \bmod p = 2^2 \bmod 5 = 4$.

$C_2 = u\,m \bmod p = 3\times 1 \bmod 5 = 3$

$\therefore$ 密文为 $(4, 3)$

解密如下：

$m = C_2 \times (C_1{}^d)^{-1} \bmod p$

$= 3\times(4^2)^{-1} \bmod 5$

$= 3\times 1 \bmod 5$

$= 3$.

---

12. 椭圆曲线 $y^2 = x^3+4x+20$ 的解点.

x	$x^3+4x+20 \bmod 29$.	是模11平方剩余吗？	y.
0	20	Yes	7 22
1	25	Yes	5 24
2.	7.	Yes.	~~12, 17.~~ 6 · 13.

选 P 为 $(0, 7)$ Q 为 $(1, 5)$.

$P(0,7)+Q(1,5) = R(x_3, y_3)$.

$$\begin{cases} \lambda = 5-7/1-0 = -2. \\ x_3 = \cancel{(-2)^2}\ \lambda^2 - x_2 - x_1 = (-2)^2 - 0 - 1 = 3. \\ y_3 = \lambda(x_1 - x_3) - y_1 = -2\times(0-1) - 7 = -5. \end{cases}$$

$\therefore$ Q 为 $(3, -5)$