[a4paper,11pt,openany]book knowledge
:
2022 .
document

:

tabular——c—c—c—— p g k

, $g \in Z_p^*$ – Z_p.
$p = 23$ – , $\phi(p) = p - 1 = 22$. : $\phi(p) = 2 \cdot 11$. 2 :

$$g^{\phi(p)2} = (-8)^{11} = 15 \cdot 15^{10} = 15 \cdot 18^5 = 17 \cdot 2^2 = 22 \not\equiv 1 \pmod{p},$$

$$g^{\phi(p)11} = (-8)^2 = 18 \not\equiv 1 \pmod{p},$$

:

$$g^{\phi(p)} = (-8)^{22} = 18^{11} = 18 \cdot 2^5 = 18 \cdot 9 \equiv 1 \pmod{p}.$$

, g Z_p.
h $Z_{p^2}^*$
$Z_{p^n}^*, n \geq 2$:

$$h = g + t_0 p,\ t_0 \not\equiv g\nu \pmod{p};\ \nu = (g^{p-12} + 1p))(\cdot (-2))($$

,

$$\nu = ((-8)^{23-12} + 123)3) \cdot (-223)) = (1 \cdot (-2)23)) = 21$$

$$t_0 \not\equiv (-8) \cdot 21 \pmod{23} = 16 \pmod{23}$$

$$t_1 = 1 \Rightarrow h = (-8) + 1 * 23 = 15$$

, $h = 15$ – $Z_{23^2}^*$
$Z_{p^3}^*$
a $Z_{p^2}^*$ k
. , ... , . ( ). . . . . , ... , , . , , ... - . - . . . . $f(x) = xp^n x$ . . . , (). . . . . , , ... () . . , . . . (. 13.4). . . . . (. 13.5). . . . .