(5) El Gamal

zyklische Gruppe
Ordnung der Gruppe
Generatorelement

$$Gen(n) = pk = \langle G, q, g, h := g^x \rangle$$

$$sk = \langle G, q, g, x \rangle$$

$$x \leftarrow \mathbb{Z}_q \quad \text{(zufällig ausgewählt)}$$

$\mathbb{Z}_q$: Gruppe der ganzen Zahlen mod q

Nachricht

$$Enc(pk, m) = y \leftarrow \mathbb{Z}_q \quad \text{(zufällig)}$$

verschl. Nachricht $\rightarrow C = \langle c_1, c_2 \rangle$, $h = g^x$

$$= \langle g^y, (h^y) \cdot m \rangle$$

$$Dec(sk, C) = \frac{c_2}{c_1^x}$$

$$\frac{c_2}{c_1^x} = \frac{h^y \cdot m}{(g^y)^x} = \frac{g^{x \cdot y} \cdot m}{g^{y \cdot x}} = m$$