EL GAMAL

KeyGen
$x \leftarrow_R \mathbb{Z}_q$
$\alpha \leftarrow_R g^x$

$Enc(m, \alpha)$
$y \leftarrow_R \mathbb{Z}_q$
$\beta \leftarrow g^y$
$\sigma \leftarrow \alpha^y$
$\zeta \leftarrow \sigma \cdot m$
ret $(\beta, \zeta) = \psi$

$Dec(\psi, x)$
$m = \frac{\zeta}{\beta^x}$

Proof that ELG is semantically secure.

We define the DDH advantage of distinguisher D:

$$Adv(D) = \left| Pr\left[x,y \leftarrow_R \mathbb{Z}_q : D(g^x, g^y, g^{xy}) = 1\right] - Pr\left[x,y,z \leftarrow_R \mathbb{Z}_q : D(g^x, g^y, g^z) = 1\right] \right|$$

it must be negligible.

We will prove that with SoG:

g^{xy}

x,y	(m_0, m_1)		(m_0, m_1)
$\frac{1}{2}$	$\frac{1}{2}$	$\frac{1}{2}$	$\frac{1}{2}$

↯ DDH

G0

$x \leftarrow_R \mathbb{Z}_q \quad \alpha = g^x$

$r \leftarrow_R R, \ (m_0, m_1) \leftarrow \mathcal{A}(r, \alpha)$

$b \leftarrow_R \{0,1\}, \ y \leftarrow_R \mathbb{Z}_q, \ \beta \leftarrow g^y, \ \boxed{\sigma = \alpha^y}, \ \zeta = \sigma \cdot m_b$

$\hat{b} \leftarrow \mathcal{A}(r, \alpha, \beta, \zeta)$

Let define S_0 to be an event that $b = \hat{b}$ in G0, then adversary advantage is $Adv(\mathcal{A}) = \left| Pr[S_0] - \frac{1}{2} \right|$

G1

— || — $\boxed{z \leftarrow_R \mathbb{Z}_q, \sigma \leftarrow g^z}$ — || —

Let define S_1 be an event that $b = \hat{b}$ in G1:

Claim 1. $Pr[S_1] = \frac{1}{2}$ because b, r, α, β are mutually independent and $\zeta = \sigma \cdot m_b$ is uniform distribution ~~over~~ on G

Claim 2. $|\Pr[S_0] - P[S_1]| \leq \varepsilon_{DDH}$

We observe that in G0 the triple $(\alpha, \beta, \sigma) = (g^x, g^y, g^{xy})$ while in the ~~a~~ G1 the triple $(\alpha, \beta, \sigma) = (g^x, g^y, g^z)$

Algorithm D ~~efficiently~~ effectively distinguish G0 and G1 with $|\Pr[S_0] - \Pr[S_1]| \leq \varepsilon_{DDH}$ - what was our claim.

Combining C1 and C2 we have

$$\left|\Pr[S_0] - \tfrac{1}{2}\right| \leq \varepsilon_{DDH}$$

So EG is semantically secure