Breaking El-Gamal Encryptions

September 5, 2013

David Leonard

DrkSephy1025@gmail.com

$$(\mathbb{Z}_{p-1}) = \mathbb{Z}_q X \mathbb{Z}_2$$

$$((r_0, r_1), (m_0), (m_1) + a(r_0, r_1)) = (g^r, (g^a)^r m)$$
$$\uparrow \mathbb{Z}_q \text{ X } \mathbb{Z}_2 \qquad\qquad \uparrow (\mathbb{Z}_p)^*$$

$$M \in m_0, m_1$$
$$\uparrow (\mathbb{Z}_p)^* \uparrow (\text{mod } q, \text{mod } 2)$$

$$q(m_0, m_1) = ((\underline{qm_0}, qm_1)$$

$$1 \longrightarrow 0 \longrightarrow (0, 0)$$

$$(\mathbb{Z}_p)^* \longrightarrow (\mathbb{Z}_{p-1}) \longrightarrow \mathbb{Z}_q X \mathbb{Z}_2$$

In $\mathbb{Z}_{\shortparallel} X \mathbb{Z}_2$, we isolate m_1:

$$q(m_0, m_1) = (0, m_1)$$

We know that the equivalent form of the above expression in the multiplicative group, $(\mathbb{Z}_p)^*$ is exponentiation.

$$\therefore M^q | \mathbb{Z}_q X \mathbb{Z}_2$$

We now see that $m_1 = 1 \Leftrightarrow m^q \text{ mod } p \neq 1$

$$((r_0, r_1), (m_0, m_1) + a(r_0, r_1)) = (g_r, (g^a)^r m)$$

Using the above information, we arrive at the following set of linear equations of M:

$$(r_1, m_1 + ar_1)$$

$$y = x + ar_1 \longrightarrow M = (M_0, M_1)$$
$$y - ar_1 = x \longrightarrow M' = (M_{0'}, M_{1'}$$

We know how to compute r_1 and a from:

$$g^a = a = (a_0, a_1)$$

The adversary A can now efficiently compute M!