¿Por qué funciona?

$$T = n_A R = k Q_A = S \Rightarrow \begin{matrix} x_T = x_S \\ y_T = y_S \end{matrix} \text{ (multp)} \Rightarrow \begin{matrix} x_T^{-1} c_1 = x_T^{-1} x_S m_1 = m_1 \\ y_T^{-1} c_2 = y_T^{-1} y_S m_2 = m_2 \end{matrix}$$

---

(2) ¿Factor de expansión de ElGamal?

ElGamal común: M corresponde con punto en $E(\mathbb{F}_p)$. Pero como $\#E(\mathbb{F}_p) \approx p$ se puede pensar como un entero en $\{0, 1, 2, \dots, p-1\}$.

Y el texto cifrado es un par de puntos $E(\mathbb{F}_p)$, o sea de longitud $\approx 4p$.

ElGamal Menezes-Vanstone es 2-1.

---

Un poco de background sobre anillos y anillo de polinomios

$\mathbb{F}$ un cuerpo.

$\mathbb{F}[x] = \{ a_0 + a_1 x + \dots + a_n x^n : n \geq 0, a_i \in \mathbb{F} \}$

Hechos:
- Dado $a, b \in \mathbb{F}[x]$, $\exists\, k, r \in \mathbb{F}[x]$ t.q. $a = bk + r$ con $r = 0$ o $gr(r) < gr(b)$.
- También xmcd: dado $a, b$, $\exists\, u, v$ $au + bv = mcd(a, b)$.

~~Sea $\mathbb{F}$~~

$m \in \mathbb{F}[x]$ ;

$a \equiv b \pmod{m}$ si $\exists\, k \in \mathbb{F}[x]$ t.q

$a = b + km$.

Entonces se puede definir $\left(\mathbb{F}[x]/(m)\right)$ como $\left(\mathbb{Z}/n\mathbb{Z}\right)$.

Prop: $\mathbb{F}$ cuerpo $m \in \mathbb{F}[x]$ Cada clase en $\bar{a} \in \mathbb{F}[x]/(m)$

tiene una rep. única verificando

$gr(r) < gr(m)$ $\quad a \equiv r \pmod{m}$.

Ej $R = \mathbb{F}[x]/(x^2+1)$

Cada elemento de R tiene una representante de la forma

$\overline{\alpha + \beta x}$ con $\alpha, \beta \in \mathbb{F}$.

Sumar:

$$\overline{\alpha_1 + \beta_1 x} + \overline{\alpha_2 + \beta_2 x} = \overline{(\alpha_1 + \alpha_2) + (\beta_1 + \beta_2)x}$$

Multiplicar: ley distributiva + el hecho que $x^2 = -1$.

$m \in \mathbb{F}_p[x]$ de grado $d$.

**Hechos:** • $\mathbb{F}_p[x]/(m)$ tiene $p^d$ elementos.

$\bar{a} \in \mathbb{F}_p[x]/(m) \iff \bar{a} = a_0 + a_1 x + \cdots + a_{d-1} x^{d-1}$
$a_i \in \mathbb{F}_p$.

• $\mathbb{F}$ ~~cuerpo finito~~ un cuerpo $a, m \in \mathbb{F}[x]$ con $m \neq 0$. Entonces $\bar{a}$ tiene inverso si y solo si

$$\text{mcd}(a, m) = 1.$$

**Coro:** $\mathbb{F}$, $m \in \mathbb{F}[x]$ irreducible
$\Rightarrow \mathbb{F}[x]/(m)$ un cuerpo.

**Ej:** $x^2+1 = (x-i)(x+i)$ irreducible en $\mathbb{R}[x]$

$\Rightarrow \mathbb{R}[x]/(x^2+1)$ un cuerpo. ¡De hecho el cuerpo $\mathbb{C}$!

**Coro:** $\mathbb{F}_p[x]/(m)$ un cuerpo con $p^d$ elementos
$\uparrow \text{gr}(m) = d$

**Thm** $\mathbb{F}_p$ cuerpo finito.

(a) $\forall d \geq 1$ $\exists$ un polinomio irreducible de grado $d$.

(b) $\forall d \geq 1$ $\exists$ un cuerpo con $p^d$ elementos

(c) Si $\mathbb{F}$ y $\mathbb{F}'$ finitos con $\#\mathbb{F} = \#\mathbb{F}'$, son isomorfos.

(d) $\mathbb{F}$ con $q = p^d$ elementos Entonces $\mathbb{F}^\times$ tiene una raíz primitiva.