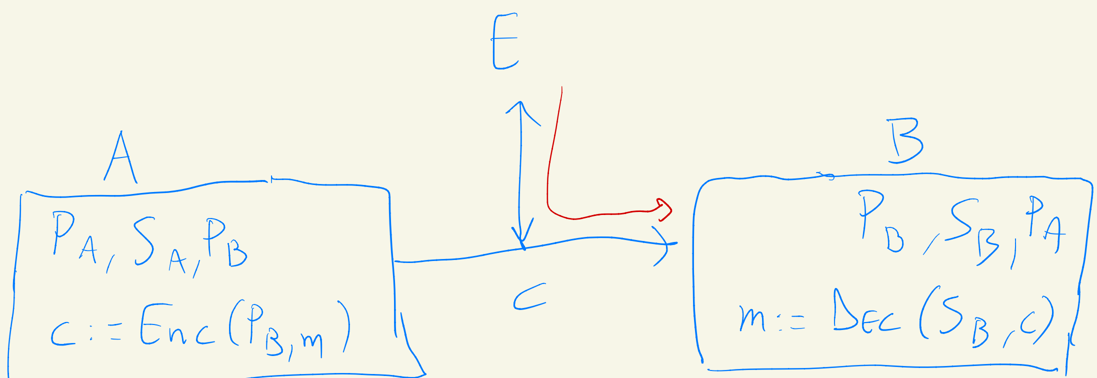
Firmas digitales



$P_A = (e, N)$ $\quad S_A = (d, N)$

$$E(m) = m^e \bmod N$$

$$D(m) = m^d \bmod N$$

$$D(E(m)) = (m^e \bmod N)^d \bmod N$$
$$= m^{e \cdot d} \bmod N = m$$

$$\boxed{E(D(m))} = (m^d \bmod N)^e \bmod N$$
$$= m^{e \cdot d} \bmod N = m$$

A B

$c := Enc(P_B, m)$

$\boxed{f := Dec(S_A, m)}$ $\xrightarrow{c,\, f}$ $m_1 := Dec(S_B, c)$

$m_2 := Enc(P_A, f)$

$¿\, m_1 = m_2 ?$

$m = Enc(P_A, f)$

$c := Enc(P_B, m)$

$\boxed{f := Dec(S_A, h(m))}$ $\longrightarrow$

$m_1 := Dec(S_B, c)$

$m_2 := Enc(P_A, f)$

$¿\, h(m_1) = m_2 ?$

$\downarrow f$

$h(m) = x$

$c := Enc(P_B, m)$

$m = Dec(S_B, c)$

$f := Enc(P_B, Dec(S_A, m))$

$Enc(P_A, Dec(S_B, f)) = m$

Firma digital con El Gamal

A: g, p $\qquad \mathbb{Z}_p^* = (\{1, \dots, p-1\}, \cdot)$

elegí $x \in \{1, \dots, p-1\}$

Clave pública: (g, p, g^x)

B quiere enviar mensaje m a A:

- genera $y \in \{1, \dots, p-1\}$
- $s := (g^x)^y$
- $c_1 := g^y$
- $c_2 := m \cdot s$

$$B \xrightarrow[c_1, c_2]{} A$$

Dec A:

$$c_1^x = (g^y)^x = g^{xy} = s$$

$$c_2 \cdot s^{-1} = m$$

$$\begin{array}{l} \alpha \equiv \beta \mod n \\ \delta \equiv \gamma \mod n \end{array} \Rightarrow \alpha + \delta \equiv \beta + \gamma \mod n$$

$$¿\, \alpha \equiv \beta \mod p \cancel{\Rightarrow a^{\alpha} \equiv a^{\beta}} \mod p\,?$$

$$2 \equiv 9 \mod 7$$

$$2^2 \mod 7 = 4$$

$$2^9 \mod 7 = (2^3)(2^3)(2^3) \mod 7 = 1$$

$$\begin{array}{l} \alpha \equiv \beta \mod p-1 \\ p \text{ es primo} \end{array} \Rightarrow a^{\alpha} \equiv a^{\beta} \mod p$$

Dem: $\alpha \equiv \beta \mod p-1$

$$(p-1) \mid (\alpha - \beta)$$

$$\Rightarrow c \cdot (p-1) = \alpha - \beta$$

$$\Rightarrow \boxed{\alpha = \beta + c \cdot (p-1)}$$

$$\Rightarrow a^{\alpha} \equiv a^{\beta + c \cdot (p-1)} \mod p$$

$$a^{\alpha} \equiv a^{\beta + c(p-1)} \bmod p$$

$$\Rightarrow \quad a^{\alpha} \equiv a^{\beta} \cdot a^{c(p-1)} \bmod p$$

$$\left(\underbrace{a^{p-1} \bmod p}_{\hookrightarrow 1}\right)^{c} \bmod p$$

Clave pública de A: (g, p, g^{x})

firmar m:

- genera $r \in \{1, \dots, p-1\}$
- $\boxed{s := (m - x \cdot r) \bmod p-1}$

$f := (r, s)$

$$\Rightarrow \quad s = (m - x \cdot r) + \alpha(p-1)$$

$$g^{s + x \cdot r} \equiv g^{m + \alpha(p-1)} \bmod p$$

$$g^{s} \cdot (g^{x})^{r} \equiv g^{m} \bmod p$$

$$g^s (g^x)^r \equiv g^m$$

$r = 1$

$(1, s)$

$$g^s \cdot g^x = g^m$$

$$g^s = g^m \cdot (g^x)^{-1}$$

$$g^s = v$$

$$s \equiv m - x r \mod p-1$$

$$x \cdot r \equiv m - s \mod p-1$$

$$x \equiv (m-s) r^{-1} \mod p-1$$

$$\boxed{x = \underbrace{(m-s) r^{-1}}_{v} + \alpha(p-1)}$$

$$(g^y)^x = (g^y)^{(m-s) \cdot r^{-1} + \alpha(p-1)}$$

$$\boxed{(g^y)^x \equiv (g^y)^v \mod p}$$

X

$A: (g, p, g^x)$

$y \in \{1, \dots, p-1\}$

$z \cdot c_1^x \equiv 1 \mod p$

$S = (g^x)^y$

$c_1 = g^y$

$c_2 = m \cdot S$

A

$\Rightarrow c_1^x = g^{xy} = S$

$m \cdot c_1^x \cdot z \equiv m$

E

$c_1^v \equiv c_1^x \mod p$

$z' \cdot c_1^v \equiv 1 \mod p$

$$m \equiv \underbrace{m \cdot c_1^x \cdot z} \equiv \underbrace{m \cdot c_1^v \cdot z'} \mod p$$

A va a firmar m: (g, p, g^x)

- genera $k \in \{1, \dots, p-2\}$ tal que $\operatorname{MCD}(k, p-1) = 1$

- $r := g^k \bmod p$

- $s := (m - x \cdot r) \cdot k^{-1} \bmod p-1$

$f := (r, s)$

$h(m)$

$$s \equiv (m - x \cdot r) \cdot k^{-1} \bmod p-1$$

$$\Rightarrow k \cdot s \equiv m - x \cdot r \bmod p-1$$

$$m \equiv x \cdot r + k \cdot s \bmod p-1$$

$$g^m \equiv g^{x \cdot r + k \cdot s + \alpha(p-1)} \bmod p$$

$$g^m \equiv g^{x \cdot r} \cdot g^{k \cdot s} \bmod p$$

$h(m)$

$$g^m \equiv (g^x)^r \cdot (g^k)^s \bmod p$$

$$\boxed{g^m \equiv (g^x)^r \cdot r^s \bmod p}$$