FIRMA CON FUNCIONES HASH

UNA FUNCIÓN HASH O RESUMEN ES UNA FUNCIÓN QUE PARA MENSAJE M DE LONGITUD ARBITRARIA PRODUCE UN NUEVO MENSAJE M DE LONGITUD ℓ, NORMALMENTE PEQUEÑA.

$$h : \mathcal{M} \longrightarrow A^{\ell} \left(= \{0,1\}^{\ell} \right)$$

QUE VERIFICA QUE ES

- DE UNA VÍA: CONOCIDO $h(M)$ ES COMPUTACIONALMENTE IMPOSIBLE RECUPERAR M' CON $h(M') = h(M)$
- COMPRESORA: ℓ DEBE SER PEQUEÑO
- FÁCIL DE CALCULAR
- DIFUSORA: PEQUEÑOS CAMBIOS DE M PRO-

VOCAN GRANDES CAMBIOS EN $h(M)$

- RESISTENTE A COLISIONES: ES COMPUTACIONALMENTE DIFÍCIL ENCONTRAR M Y M' TALES QUE ($M \neq M'$)

$$h(M) = h(M')$$

EJ:

MD5	$\ell = 128$	
SHA-1	$\ell = 126$	← STANDARD FIRMA DIGITAL
SHA-256	$\ell = 256$	

SI ALICE QUIERE FIRMAR EL DOCUMENTO M (DE LONGITUD ARBITRARIA) ENTONCES USA UNA FUNCIÓN HASH

$$h: \mathcal{M} \longrightarrow \{0, \ldots, n-1\}$$

COMO h ES RESISTENTE A COLISIONES, ES UNA FUNCIÓN DE UNA VÍA.

LA FIRMA DE UN MENSAJE M ES

$$S = h(M)^d \text{ MOD } n.$$

DE ESTA FORMA, ÚNICAMENTE EL VALOR $h(M)$ PUEDE SER RECONSTRUIDO, NO SE PUEDE RECONSTRUIR M.

PROCEDIMIENTO

ALICE FIRMA UN MENSAJE M DIRIGIDO A BOB

- ALICE CALCULA $h(M)$
- ALICE CALCULA LA FIRMA DE $h(M)$

$$S = h(M)^d \bmod n$$

- ALICE ENVIA EL PAR (M, S)

SI BOB RECIBE (M, S) Y QUIERE COMPROBAR LA FIRMA DEL MENSAJE

- GENERA $h(M)$ (h ES PÚBLICA)
- CALCULA $S^e \bmod n$
- COMPRUEBA QUE $h(M) = S^e \bmod (n)$

SI SON IGUALES, ACEPTA LA FIRMA. Y SI NO, LA RECHAZA

LA FIRMA ANTERIOR YA NO ESTA EXPUESTA A FALSIFICACIÓN EXISTENCIAL.

- SUPONGAMOS QUE EVE ESCOGE UNA FIRMA S
- COMO EVE DEBE ENVIAR EL MENSAJE M JUNTO CON LA FIRMA S A BOB, DEBE ENCONTRAR UN MENSAJE M TAL QUE

$$h(M) = S^e \bmod n$$

$$\Rightarrow M \in h^{-1}(M = S^e \bmod n)$$

PERO COMO h ES DE UNA VÍA ES IMPOSIBLE

- LA MULTIPLICATIVIDAD TAMPOCO ES UN PROBLEMA PORQUE ES IMPOSIBLE ENCONTRAR x TAL QUE

$$h(x) = M = M_1 M_2 \mod n$$

- EVE TAMPOCO PUEDE REEMPLAZAR UN DOCUMENTO M FIRMADO POR ALICE POR OTRO DOCUMENTO M' PORQUE ENTONCES ENTONCES M Y M' SERÍAN UNA COLISIÓN DE h.

FIRMA DIGITAL A PARTIR DE UN CRIPTOSISTEMA DE CLAVE PÚBLICA ARBITRARIO.

CLAVE PÚBLICA: e

CLAVE PRIVADA: d

FUNCIÓN CIFRADO MENSAJE M: $E(M,e)$

FUNCIÓN DESCIFRADO MENSAJE C: $D(C,d)$

$$M = D(E(M,e),d) \quad \forall M$$

SI ADEMÁS

$$M = E(D(M,d),e) \quad \forall M$$

← POR EJEMPLO RSA

PODEMOS CONSTRUIR UN SISTEMA DE FIRMA DIGITAL:

LA FIRMA DE M ES

$$S = D(h(M), d)$$

QUE SE COMPRUEBA CALCULANDO

$$h(M) = E(S, e)$$

SI ADEMÁS QUEREMOS QUE EL MENSAJE SEA CONFIDENCIAL, M SERÁ CIFRADO USANDO LA CLAVE PÚBLICA DE BOB Y SERÁ ENVIADO POR ALICE A BOB JUNTO CON S.

PROCEDIMIENTO CON CONFIDENCIALIDAD MENSAJE

CLAVES ALICE : e_a PÚBLICA d_a PRIVADA

CLAVES BOB : e_b PÚBLICA d_b PRIVADA

ALICE FIRMA UN MENSAJE M DIRIGIDO A BOB

- ALICE CALCULA $h(M)$
- ALICE CALCULA LA FIRMA DE $h(M)$ USANDO SU CLAVE PRIVADA

$$S = h(M)^{d_a} \bmod n$$

- ALICE CIFRA M USANDO LA CLAVE PÚBLICA DE BOB

$$C = M^{e_b} \bmod n$$

- ALICE ENVIA EL PAR (C, S)

SI BOB RECIBE (C, S) Y QUIERE RECUPERAR EL MENSAJE CIFRADO Y COMPROBAR LA FIRMA DEL MENSAJE:

- BOB DESCIFRA C USANDO SU CLAVE PRIVADA

$$M = C^{d_b} \bmod n = M^{d_b e_b} \bmod n$$

- CALCULA $h(M)$ (h ES PÚBLICA)
- BOB CALCULA, USANDO LA CLAVE PÚBLICA DE ALICE: $S^{e_a} \bmod n$
- COMPRUEBA QUE $h(M) = S^{e_a} \bmod n$

FIRMA DIGITAL CON ELGAMAL

- SE GENERAN CLAVES COMO EN EL CRIPTOSISTEMA DE CLAVE PÚBLICA DE EL GAMAL

$$\begin{cases} a \in \{2, \ldots, p-2\} & \text{PRIVADA} \\ (p, g, A = g^a \bmod p) & \text{PUBLICA} \end{cases}$$

- SE USA UNA FUNCIÓN HASH

$$h : \{0,1\}^t \to \{1, 2, \ldots, p-2\}$$

SE TRUNCA SI NECESARIO

- GENERACIÓN DE LA FIRMA
  - ALICE ESCOGE AL AZAR $k \in \{1, \ldots, p-2\}$ TAL QUE $\mathrm{mcd}(k, p-1) = 1$ ⊛
  - ALICE CALCULA PARA UN MENSAJE M

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

$$s = \underset{\text{OK POR ⊛}}{k^{-1}}(h(M) - ar) \bmod (p-1)$$

$\mathbb{Z}_p$

$a^x = a^{x+\lambda(p-1)}$

OJO EXPONENTE

- LA FIRMA DE M ES (r, s)
- ADEMÁS M NO PUEDE OBTENERSE DE (r, s). ALICE LO TIENE QUE ENVIAR, CIFRADO O SIN CIFRAR, SEGÚN LA NECESIDAD DEL CANAL O CONFIDENCIALIDAD NECESARIA.

- VERIFICACIÓN DE LA FIRMA
  - BOB PRIMERO COMPRUEBA QUE

$$1 \leq r \leq p-1$$

SI NO ES CIERTO, RECHAZA LA FIRMA

• BOB COMPRUEBA QUE

$$\boxed{A^r r^s \equiv g^{h(M)} \bmod p}$$

LA ACEPTA SI ES CIERTO Y LA RECHAZA EN CASO CONTRARIO

¿POR QUÉ FUNCIONA?

$(a^b)^c = a^{b \cdot c}$ $\quad a^b \cdot a^c = a^{b+c}$

$$A^r r^s \equiv (g^a)^r \left(g^{\cancel{k}}\right)^{\cancel{k^{-1}}(h(M)-ar)} \equiv g^{ar}\, g^{h(M)-ar} \equiv$$

$$\equiv g^{\cancel{ar}+h(M)\cancel{-ar}} \equiv g^{h(M)} \bmod p$$

RECIPROCAMENTE, SI SE VERIFICA QUE $A^r r^s \equiv g^{h(M)} \bmod p$

PARA UN PAR (r,s) Y $k = \log_g r \bmod p$

$\Downarrow$

$$\boxed{r = g^k \bmod p}$$

$$\Rightarrow (g^a)^r (g^k)^s \equiv g^{h(M)}$$

$$g^{ar+ks} \equiv g^{h(M)} \bmod p$$

OJO: MUNDO EXPONENTES $g^{p-1} \equiv 1$

$$\Rightarrow ar + ks \equiv h(M) \bmod p-1$$

$$\Rightarrow ks \equiv h(M) - ar \bmod p-1$$

$$\Rightarrow \boxed{s \equiv k^{-1}(h(M) - ar) \bmod p-1}$$

$\operatorname{mcd}(k, p-1) = 1 \Rightarrow \exists\, k^{-1}$

SEGURIDAD

PARA FALSIFICAR LA FIRMA ES NECESARIO CALCULAR r Y s DE MANERA QUE

$$g^{h(M)} = A^{r} r^{s}$$

NO ESTÁ DEMOSTRADO QUE SEA TOTALMENTE EQUIVALENTE AL PROBLEMA DEL LOGARITMO DISCRETO. PERO EN CUALQUIER CASO, SE CONSIDERA UN PROBLEMA COMPUTACIONALMENTE IMPOSIBLE.

EN CUALQUIER CASO SI SE ROMPE EL PROBLEMA DE LOGARITMO DISCRETO, SE ROMPE ESTA FIRMA DIGITAL PORQUE CON a SE PUEDE FIRMAR CUALQUIER COSA

EJ: COMO EN EL EJEMPLO DE EL GAMAL QUE VIMOS EL MARTES ALICE ESCOGE

$p=23$, $g=7$, $a=6$ Y CALCULA $A=g^a \bmod p$
$=7^6 \bmod p = 4$

CLAVE PÚBLICA: $(p=23, g=7, A=20)$

CLAVE PRIVADA: $a=13$

ALICE QUIERE FIRMAR M, CON $h(M)=7$.

ALICE ESCOGE $k=14$ Y OBTIENE

$$r = g^k \bmod p = 2$$

$$\underline{k^{-1}} \bmod p-1 = 5$$

POR TANTO

$$s = k^{-1}(\underline{h(x)} - \underline{a \cdot r}) \bmod p-1 =$$

$$=$$

LA FIRMA ES (,)

- SI BOB QUIERE COMPROBAR LA FIRMA.

CALCULA

$$A^r r^s \bmod p =$$

$$g^{h(M)} \bmod p =$$

$\Big\}$ $\underline{OK}$