FIRMA DIGITAL

LA FIRMA DIGITAL TIENE PROPIEDADES PARECIDAS A LA FIRMA MANUSCRITA Y SE USA PARA FIRMAR DOCUMENTOS ELECTRÓNICOS

SI ALICE FIRMA DE FORMA MANUSCRITA UN DOCUMENTO, TODO EL MUNDO QUE VEA ESE DOCUMENTO Y CONOZCA LA FIRMA DE ALICE SABE QUE ALICE LO HA FIRMADO Y PUEDE USARSE COMO PRUEBA DE QUE ALICE TIENE CONOCIMIENTO DE ESE DOCUMENTO Y ESTÁ DE ACUERDO CON SU CONTENIDO.

DE LA MISMA FORMA QUE LOS DOCUMENTOS MANUSCRITOS, LOS DOCUMENTOS DIGITALES TAMBIÉN DEBEN SER FIRMADOS. POR EJEMPLO, CONTRATOS, TRANSACCIONES FINANCIERAS, ...

¿COMO FUNCIONA?

SI ALICE QUIERE FIRMAR EL DOCUMENTO M, ALICE USA UNA CLAVE SECRETA d Y CALCULA LA FIRMA S.

BOB, USANDO LA CLAVE PÚBLICA e ASOCIADA A LA CLAVE SECRETA d, PUEDE VERIFICAR QUE s ES LA FIRMA DE M.

SEGURIDAD

- SEGURIDAD CLAVE

SE REQUIERE QUE EL PROBLEMA DE CONSTRUIR LA CLAVE SECRETA DE FIRMA A PARTIR DE LA INFORMACIÓN QUE ES PÚBLICA, SEA NO TRATABLE (COMPUTACIONALMENTE IMPOSIBLE).

COMO EN COS CRIPTOSISTEMAS DE CLAVE PÚBLICA, SE USAN PROBLEMAS DE TEORIA DE NÚMEROS.

- ATAQUES SIN MENSAJE (FALSIFICACIÓN EXISTENCIAL)

EVE PUEDE TAMBIÉN INTENTAR GENERAR NUEVAS FIRMAS VÁLIDAS SIN EL CONOCIMIENTO DE LA CLAVE

DE FIRMA SECRETA. ESTO SE LLAMA FALSIFICACIÓN DE LA FIRMA DIGITAL (FALSIFICACIÓN EXISTENCIAL)

1) EVE OBTIENE LA CLAVE PÚBLICA DE VERIFICACIÓN

2) EVE CALCULA UN MENSAJE M Y CALCULA UNA FIRMA s PARA M QUE SE PUEDE VERIFICAR DE FORMA POSITIVA CON LA CLAVE DE VERIFICACIÓN DE ALICE

INCLUSO, EVE PUEDE CALCULAR EL DOCUMENTO M EN FUNCIÓN DE LA CLAVE PÚBLICA DE VERIFICACIÓN.

- ATAQUES CON MENSAJE

MISMA SITUACIÓN QUE EN EL CASO ANTERIOR, PERO ADEMÁS EVE USA INFORMACIÓN DE FIRMAS VÁLIDAS DE OTROS DOCUMENTOS

- ATAQUES CON MENSAJE ELEGIDO

EVE CONOCE ALGUNAS FIRMAS VÁLIDAS Y LAS USA PARA CONSTRUIR NUEVAS FIRMAS PARA UN MENSAJE QUE EVE ESCOGE

↳ESTO ES EL PEOR ESCENARIO POSIBLE

FIRMA DIGITAL CON RSA

1) ALICE FIRMA EL DOCUMENTO M CALCULANDO LA FIRMA

↳ $0 \leq M < n$

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

d ES LA CLAVE PRIVADA DE RSA DE ALICE Y n ES DE SU CLAVE PÚBLICA.

2) BOB VERIFICA LA FIRMA CALCULANDO

$$S^e \bmod n \equiv M^{de} \bmod n \equiv M \bmod n$$

ES UN PROCESO ANÁLOGO A CIFRAR Y DESCIFRAR CON RSA, PERO CAMBIANDO EL ORDEN.

¿POR QUÉ ES UNA FIRMA?

ELEVANDO S A LA e (S^e) BOB PUEDE RECUPERAR EL MENSAJE M.

ENTONCES $S = \sqrt[e]{M} \mod n$

¿COMO CALCULA S?

$\sqrt[e]{M} \mod n = M^d \mod n$

↳ SÓLO LO PUEDES HACER SI CONOCES d

ALICE ES LA ÚNICA PERSONA QUE CONOCE d => EL DOCUMENTO DEBE HABER SIDO FIRMADO POR ALICE, PORQUE:

SABEMOS, DE RSA, QUE NO SE PUEDE OBTENER d A PARTIR DE e

GENERACIÓN CLAVES

- EXACTAMENTE IGUAL QUE PARA RSA

EJ: $p=11$, $q=23$, $e=3$

$n = pq = 253$ $\quad d = 147$

MENSAJE ALICE 111 (QUIERE SACAR 111 € DE UN CAJERO)

$S = 111^{147} \bmod 253 = 89$ FIRMA DE ALICE

CAJERO CALCULA: $S^3 \bmod 253 = 111$

CAJERO SABE QUE ALICE HA PEDIDO 111 EUROS. Y LO PUEDE PROBAR EN UN FUTURO SI HAY UNA RECLAMACIÓN

ATAQUES

- PARA VERIFICAR LA FIRMA DE ALICE, BOB USA LA CLAVE PÚBLICA DE ALICE.

SI EVE ES CAPAZ DE REEMPLAZAR LA CLAVE PÚBLICA DE DE ALICE CON LA SUYA PROPIA, SIN QUE BOB SE DE CUENTA, ENTONCES EVE PUEDE FIRMAR EN NOMBRE DE ALICE.

↳ IMPORTANTE: USAR UNA AUTORIDAD CERTIFICACIÓN

- EVE ESCOGE UN ENTERO $s \in \{0, \ldots, n-1\}$.
  - EVE LE DICE A BOB QUE ES UNA FIRMA DE ALICE.
  - BOB COMPRUEBA SI ES CIERTO QUE LO HA FIRMADO ALICE, PARA ELLO CALCULA

$$M = S^e \bmod n$$

Y SE CREE QUE ALICE HA FIRMADO M.

- SI M ES UN MENSAJE CON SENTIDO, ENTONCES EVE HA SIDO CAPAZ DE FALSIFICAR LA FIRMA DE ALICE (ATAQUE SIN MENSAJE)

EJ: EN EL EJEMPLO ANTERIOR

ALICE < CLAVE PUBLICA (n=253, e=3)
ALICE < CLAVE PRIVADA (d=147)

EVE, QUIERE SACAR DINERO DE LA CUENTA DE ALICE
ENVIA S=123 AL CAJERO

EL CAJERO CALCULA $M = 123^3 \bmod 253 = 52$
EL CAJERO CREE QUE ALICE QUIERE SACAR 52 EUROS

- UN PROBLEMA ES QUE RSA ES MULTIPLICATIVO

$M_1, M_2 \in \{0, \dots, n-1\}$

$S_1 = M_1^d \bmod n$ FIRMA DE M_1

$S_2 = M_2^d \bmod n$ FIRMA DE M_2

$\Longrightarrow$

$S = S_1 \cdot S_2 \bmod n \equiv (M_1 M_2)^d \bmod n$ FIRMA DE $M_1 \cdot M_2$

ES DECIR, DE DOS FIRMAS VÁLIDAS PUEDE CALCULARSE UNA TERCERA FIRMA VÁLIDA.

USANDO ESTO, EVE PUEDE FIRMAR UN DOCUMENTO DE SU ELECCIÓN: $M \in \{0, \dots, n-1\}$

- EVE SELECCIONA $M_1 \in \{0, \dots, n-1\}$ TAL QUE

$M_1 \neq M$ Y $\gcd(M_1, n) = 1$

- EVE CALCULA

$$M_2 = M M_1^{-1} \bmod N$$

- SI EVE ES CAPAZ DE OBTENER FIRMAS VÁLIDAS S_1 Y S_2 PARA M_1 Y M_2. ENTONCES CALCULA

$$S = S_1 \cdot S_2 \bmod N$$

QUE ES UNA FIRMA DEL MENSAJE M

¿CÓMO SE PUEDEN EVITAR ESTOS ATAQUES?

FIRMA CON REDUNDANCIA

SI SÓLO USAMOS MENSAJES CIERTOS MENSAJES PODEMOS EVITAR DOS DE LOS ATAQUES ANTERIORES

POR EJEMPLO SI REQUERIMOS QUE $w \in \{0,1,\dots,n-1\}$ TENGA UNA EXPRESIÓN EN BINARIO DE LA FORMA

$w \circ w$ CON $w \in \{0,1\}^*$ CON $0:\{0,1\}^* \longrightarrow \{0,1\}^{2^{2\ell}=e}$

$w \longmapsto w \circ w$ (FUNCIÓN REDUNDANCIA) $= M$

$M = \boxed{w \mid w}$

EL TEXTO QUE REALMENTE SE FIRMA ES w, PERO ES M LO QUE TÉCNICAMENTE SE FIRMA.

CUANDO BOB COMPRUEBA LA FIRMA, CALCULA

- $M \equiv s^e \bmod n$
- COMPRUEBA QUE M SEA DE LA FORMA $w \circ w$

ASÍ EVITAMOS LA FALSIFICACIÓN EXISTENCIAL (FIRMA SIN MENSAJE) PORQUE EVE TENDRÍA QUE INVENTARSE UNA FIRMA FALSA DE FORMA QUE $M \equiv s^e \bmod n$ SEA DE LA FORMA $\omega \circ \omega$ NO SE SABE COMO HACERLO SIN LA CLAVE PRIVADA d.

TAMPOCO LA MULTIPLICABILIDAD DE RSA ES UN PROBLEMA PORQUE ES POCO PROBABLE QUE $M = M_1 M_2$ TENGA UNA EXPRESIÓN DE LA FORMA $\omega \circ \omega$