Fundamentos de criptografía

Garantía y Seguridad de la Información

Transacciones electrónicas seguras

Transacciones electrónicas seguras

- Un usuario A quiere hacer una transacción con un banco, B
  - B debe poder autenticar a A
  - A debe tener un certificado de B que le asegure que no va a negar la transacción realizada.
- Posteriormente, esa transacción podrá ser usada como contravalor para una compra con un vendedor V, como veremos.

Protocolo de Chaum

- Un comprador, A, quiere interactuar con B, el banco, para pedirle
- *disponer de una cierta cantidad de dinero* que quiere *utilizar para poder pagar alguna compra*.

Protocolo de Chaum

- La notación que usaremos, asociada a un usuario U, será:
  - Id_U: Identidad usuario.
  - $E_U(m)$: Proceso de cifrar/descifrar un mensaje m, con la clave pública de U
  - $D_U(c)$: Proceso de descifrar/cifrar un criptograma c, con la clave privada de U

Resumen de las transacciones

A		B
$\rightarrow$	$Id_A, E_B(D_A(m)), doc_{AB}$	$\rightarrow$
$\leftarrow$	$E_A(D_B(m)), E_A(D_B(doc_{BA}))$	$\leftarrow$

A		V
$\rightarrow$	$Id_A, D_B(m), D_B(doc_{BA})$	$\rightarrow$

B		V
$\leftarrow$	$D_V(D_B(m)), D_V(D_B(doc_{BA}))$	$\leftarrow$
$\rightarrow$	$D_B(doc_{BV})$	$\rightarrow$

Protocolo con el banco

- $A \to B$
- El usuario A genera, al azar, un número m grande
- Firma el número con su clave privada, calculando $D_A(m)$
- Crea un documento personalizado, doc_{AB}, en el que dice al banco que quiere disponer de x€.
- Usa la clave pública de B y le envía:

$$(Id_A, E_B\big(D_A(m)\big), doc_{AB})$$

$(Id_A,\ E_B(D_A(m)),\ doc_{AB})$

- $B \rightarrow A$
- El banco identifica A y lee doc_{AB}
- Recupera el número m
- Firma el número m, $D_B(m)$
- Descuenta x€ de la cuenta de A
- Firma un documento doc_{BA} con la información $(m, x€\ )$, $D_B(doc_{BA)})$
- Envía a A estas dos firmas, cifradas con la clave pública de A

$$(E_A(D_B(m)), E_A(D_B(doc_{BA})))$$

$(E_A(D_B(m)),\ E_A(D_B(doc_{BA})))$

- Al usuario A le interesa tener $D_B(doc_{BA})$, y no solo doc_{BA}
  - para poder demostrar ante terceros que el banco le ha descontado x€ de su cuenta y que estos corresponden a su número m

- Cuando A va a comprar al vendedor V, se siguen los pasos:

Protocolo con vendedor (I)

- $A \rightarrow V$
- El comprador A envía a V $(Id_A, D_B(m), D_B(doc_{BA}))$
- El vendedor
  - autentica los mensajes firmados por B
  - conoce la identidad del comprador A
  - que dispone de un valor de x€
  - El comprador A podría enviar esto cifrado con E_V y firmado con D_A

$$D_A(E_V(D_B(m)))$$

$$D_A(E_V(D_B(doc_{BA})))$$

Protocolo con vendedor (II)

- $V \rightarrow B$
- El vendedor V envía al banco: $D_V(D_B(m))$
- El banco comprueba que el mensaje m es correcto
  - correspondiente a un número firmado previamente por el propio banco
- Deposita en la cuenta de V los x€
- Escribe en una lista de números caducados el número m
  - para evitar que le vuelva a ser presentado otra vez.

Protocolo con vendedor (III)

- $B \rightarrow V$
- El banco envía firmado un doc_{BV} de la transacción hecha al vendedor V, $D_B(doc_{BV})$

- V ya puede dar la mercancía a A, junto con un documento firmado, $D_V(doc_{VA})$, de haber cobrado del banco.

Resumen de las transacciones

A		B
$\rightarrow$	$Id_A, E_B(D_A(m)), doc_{AB}$	$\rightarrow$
$\leftarrow$	$E_A(D_B(m)), E_A(D_B(doc_{BA}))$	$\leftarrow$

A		V
$\rightarrow$	$Id_A, D_B(m), D_B(doc_{BA})$	$\rightarrow$

B		V
$\leftarrow$	$D_V(D_B(m)), D_V(D_B(doc_{BA}))$	$\leftarrow$
$\rightarrow$	$D_B(doc_{BV})$	$\rightarrow$

Protocolo de Chaum

- En el protocolo hay *autenticidad* pero no *privacidad*.
  - El banco sabe (por el número m del billete) que A ha comprado a V
  - Puede seguir el rastro de las operaciones comerciales de A.
- Variante del protocolo
  - Uso de firmas digitales ciegas

Firma digital ciega

Firma digital ciega

- Garantiza la integridad, confidencialidad y autenticidad de los datos.
- Garantiza el anonimato del emisor, frente al receptor.
  - consiste en hacer firmar al banco un documento que contiene el número escondido.

Firma digital ciega

- El banco firma un documento que contiene el número escondido.
- El usuario A sacará a la luz el número y lo hará servir junto con el documento firmado por el banco, cuando le convenga.
- El banco no sabe a quién corresponden los números que se utilizan.

Firma digital ciega

- Protocolo entre un usuario V y un firmante U
  - U firma digitalmente una serie de datos enviados por V sin conocer el contenido de los mismos.
- El propósito es obtener una serie de datos firmados, m, cuyo contenido solo es conocido por el usuario

Firma digital ciega

- Se requiere
  - El firmante tiene firma digital.
    - $S(m)$ es la firma digital del mensaje m
  - Hay funciones conocidas por V, de cegado/ocultación, f, y de descegado/recuperación, g
    - $g(S(f(m)) = S(m)$

Firma digital ciega

- V quiere que U firme.
  - V crea un hash de su mensaje, $h(m)$
  - V ciega dicho hash (usando la **función de cegado**) y se lo envía a U, $f(h(m))$
  - U realiza la firma (usando protocolo de **firma digital**) y la envía a V, $S(f(h(m)))$
  - V desciega la firma (usando la **función de descegado**), $g(S(f(h(m)))) = S(h(m))$

Firma digital ciega de Chaum

- Tenemos p y q, dos primos muy grandes y $n = p \cdot q$
- El protocolo de firma digital de U es RSA con clave pública (n, e) y clave privada d
- V quiere que U firme m, sin conocerlo

Firma digital ciega de Chaum

- Fase de inicialización
  - Sea $0 \leq m \leq n-1$ el mensaje de V a firmar por U
  - Sea k, elegido por V, $0 \leq k \leq n-1$ y $mcd(n,k) = 1$
  - V calcula $k^{-1} \ (mod\ n)$

Firma digital ciega de Chaum

- Fase de ocultación
  - V calcula $E_U(D_V(m \cdot E_U(k)))$
  - Se lo envía a U
- Fase de firma
  - U obtiene $m \cdot E_U(k)(mod\ n)$
  - Lo firma
    - U calcula $D_U\big(m \cdot E_U(k)\big) = k \cdot D_U(m)\ mod\ n$
  - Se lo envía a V

Firma digital ciega de Chaum

- Fase de recuperación
  - V calula

$$k \cdot D_U(m) \cdot k^{-1} \ (mod\ n) = \ D_U(m)$$

  - que es la firma digital del mensaje m por U

Firma ciega de Chaum. Ejemplo

- *A* desea que el Banco, *B*, le firme el mensaje *m* = 65.
- Las claves pública y privada de *B* son: $\boldsymbol{n_B = 851,\ e_B = 13,\ d_B = 61}$.
  - Los parámetros de *B* son: $p_B = 23$, $q_B = 37$, $\varphi(n_B) = 792$
- A escoge $k = 51$, y calcula $51^{-1}(mod\ 851) = 267$.
- **A->B. El usuario *A* calcula:**
- $M = m \cdot k^{e_B}(mod\ nB) = 65 \cdot 51^{13}\ (mod\ 851) = 65 \cdot 458(mod\ 851) = 836$ y envía M al Banco.
- **B->A. El Banco hace:**
- firma este mensaje recibido, M, con su clave privada:
- $M^{d_B}(mod\ n_B) = 836^{61}\ (mod\ 851) = 220$, y lo envía a A.
- **El usuario *A***, conoce $k^{-1}(mod\ n_B) = 267$,
- puede calcular: $267 \cdot 220\ (mod\ 851) = 21$, que es la firma del banco de *m*, sin que el banco conozca *m*.

Firma ciega de Chaum. Ejemplo

- Con esta operación, el banco ha firmado el mensaje original *m* = 65, sin conocer su valor.
  - 21 es el mismo valor que obtendría el banco si hubiera firmado con su clave privada el mensaje *m* = 65
    - 65^{61} (mod 851) = 21.

Identificación de conocimiento nulo

Prueba de conocimiento nulo

- El candidato, A, debe convencer al verificador que posee un secreto
- El verificador, B, no puede extraer ninguna información sobre el candidato y su secreto, pero garantiza la veracidad de la posesión
  - Si *A* no posee el secreto, la probabilidad de que engañe a *B* puede hacerse tan pequeña como se quiera, repitiendo el procedimiento el suficiente número de veces.

Protocolo básico

- $A \rightarrow B$.
  - El usuario *A* quiere probar algo al verificador *B* y le envía algún elemento para su identificación.
- $B \rightarrow A$.
  - El verificador *B* presenta un desafío a *A*.
- $A \rightarrow B$.
  - El usuario *A* tiene que efectuar unos cálculos privadamente y enviar al verificador *B* una respuesta al desafío planteado.

Ejemplo: Conocimiento de una clave privada

- A debe probar ante B que conoce la clave privada, Pr , asociada a una clave pública conocida Pu. (*Yo soy A*)
  1. B selecciona un mensaje aleatorio m, calcula $c = e_{Pu}(m)$ y envía c a A.
  2. A calcula $m' = d_{Pr}(c)$ y lo envía a B.
  3. B acepta si y sólo si $m = m'$.

Prueba de conocimiento nulo. Protocolo de Fiat-Shamir

- $A \rightarrow B$
  - A genera al azar un valor $r \in \mathbb{Z}_n^*$
  - calcula $y_1 = r^2 (mod\ n)$
  - lo envía a B, junto con un mensaje diciendo que quiere probar su identidad.
- $B \rightarrow A$
  - envía a A un bit, al azar: $y_2 \in \{0,1\}$

Protocolo de Fiat-Shamir

- $A \rightarrow B$
  - A calcula y_3
    - si $y_2 = 0,\ y_3 = r\ (mod\ n)$
    - si $y_2 = 1,\ y_3 = r \cdot x_A\ (mod\ n)$
  - envía a B el valor y_3

Protocolo de Fiat-Shamir

- B verifica
  - si $y_2 = 0$, $y_3^2 = r^2 (mod\ n) = y_1$
  - si $y_2 = 1$, $y_3^2 = r^2 \cdot y_A (mod\ n) = y_1 \cdot y_A (mod\ n)$
- Si no se cumple la verificación, B rechaza la identidad de A

Protocolo de Fiat-Shamir. Ejemplo

- Supongamos
  - $n = p_1 \cdot p_2 = 5 \cdot 11 = 55$
  - la clave secreta de *A*, $x_A = 13$
  - la clave pública de *A*, $y_A = x_A^2 \pmod{n} = 13^2 \pmod{55} = 4$
- A->B.
  - *A* toma $r = 30$ y calcula $y_1 = r^2 \pmod{n} = 30^2 \pmod{55} = 20$
  - lo envía a *B*, junto con un mensaje diciendo que quiere probar su identidad.
- *B*->*A*.
  - *B* envía a *A* un bit al azar entre 0 y 1. Supongamos $y_2 = 1$.
- *A*->*B*.
  - A calcula y_3. Como $y_2 = 1$, $y_3 = r \cdot x_A \pmod{n} = 30 \cdot 13 \pmod{55} = 5$
  - lo envía a *B*.
- B verifica
  - Como $y_2 = 1$, $y_3^2 = y_1 \cdot y_A \pmod{n} = 20 \cdot 4 \pmod{55} = 25$.
  - Por lo tanto, $y_3 = 5$ y acepta la identidad de A

Protocolos de reparto de secretos

Protocolo básico

- Un dato secreto se trocea en n piezas de manera segura y se reparte entre el mismo número de usuarios.
- Una coalición de algunos de los usuarios debe ser capaz de recuperar el dato secreto.

- Sistema de compartición de secretos de Shamir

Votaciones electrónicas

Garantías

- Democracia: Solo las personas registradas en el censo pueden emitir su voto y solamente pueden hacerlo una vez.
- Transparencia: Ningún voto puede ser eliminado ni alterado.
- Privacidad: No se puede establecer ninguna relación entre un voto y un votante.
- No coercibilidad: Para evitar coacciones el votante no puede demostrar cuál ha sido el sentido de su voto.
- Verificabilidad: Cada votante, y eventualmente un auditor, puede comprobar que el voto ha sido correctamente contabilizado.

Objetivos

- Garantizar la privacidad de los votantes y la corrección de los resultados:
  - asegurando que todos los votos que se han utilizado para obtener los resultados pertenecen a votantes válidos
    - por ejemplo, forman parte de la lista del censo y no han sido suplantados
  - verificando que un votante no emita más de un voto
  - haciendo que no pueda correlacionar en ningún momento la papeleta del voto y la identidad del votante.

Objetivos

- Facilitar la auditoría de la elección
  - permitiendo tanto a votantes como a observadores verificar que los votos emitidos contienen la opción del voto original seleccionado por el votante
  - el resultado refleja totalmente la intención de voto de los votantes.

Bibliografía

- Llorenç Huguet Rotger, Josep Rifà Coma, Juan Gabriel Tena Ayuso. “Protocolos criptográficos”. *FUOC. Fundació per a la Universitat Oberta de Catalunya*