MA-53G Intr. a la Criptografía **Semestre Otoño, 1998**

2^{da} Cátedra de Sistemas de firmas Digitales

Transcriptor: Miguel Barrera M.

1 Sistema de firmas digitales

Veremos un sistema de firmas digitales basado en el criptosistema de El Gamal, en el cual la firma digital se puede expresar como

- $\mathcal{K} = \{(p,g,a,\beta) \mid p$ primo, g generador de $\mathcal{Z}_p^*$ y $\beta \equiv_p g^a\}$

En la definición anterior, las claves públicas son g,b y p y la clave secreta es a.

Uso del sistema de firmas de El Gamal

En el sistema de firmas basado en El Gamal, en el proceso de firmar un documento se tiene que:

$\forall\ \mathcal{K} = (p,g,a,b)$

si se desea firmar $x \in \mathcal{Z}_p^*$ se elige $j \in \mathcal{Z}_{p-1}$ al azar y se genera (γ,δ) donde

$\gamma = g^j \bmod p$

$\delta = (x - a\gamma)\ j^{-1} \bmod (p\text{-}1)$

para verificar que (γ,δ) es firma de x se chequea lo siguiente:

$\beta^\gamma\ \gamma^\delta \equiv_p g^x$

Observación

para toda firma válida se cumple que

$\beta^\gamma\ \gamma^\delta \equiv g^{a\gamma+j\delta} \equiv_p g^{a\gamma+x-a\gamma} \equiv_p g^x$

Cabe decir que no se conocen formas computacionalmente eficientes de falsificar una firma de El Gamal para un mensaje conocido dado pero se puede generar x y (γ,δ) firma válida para x, i.e.:

$\gamma = g^i\ b^i \bmod p$

$\delta = -\gamma\ j^{-1} \bmod (p\text{-}1)$

$x = -\gamma\ i\ j^{-1} \bmod (p\text{-}1)$

donde $i \in \mathcal{Z}_p$ y $j \in \mathcal{Z}_{p-1}^*$

luego se tiene que

$\beta^\gamma \gamma^\delta \equiv_p g^{a\gamma} g^{(i+aj)\delta} \equiv_p g^{a\gamma+i\delta+aj\delta} \equiv_p g^{a\gamma-\gamma ij^{-1}-a\gamma} \equiv_p g^x$

Este proceso genera una firma válida de algun texto pero ya que no se puede elegir este sino sólo los numeros que dan origen a una firma válida, el mensaje correspondiente a esta firma es inteligible.

Una de desventajas que tiene este método de firmas digitales basado en el criptosistema de El Gamal es que la firma de un mensaje cualquiera queda del doble del tamaño de los primos elegidos, asi por ejemplo si los primos son de 512 bits (que es lo estándar por seguridad) entoces la firma queda de 1024 bits, lo cual se aleja mucho de ser óptimo, debido a que involucra enviar un texto de tamaño considerable a través de la red, para cada mensaje; lo cual es engorroso para el firmante y para el destinatario.

Veremos a continuación el sistema de firmas DSS (estábasado en El Gamal) utiliza firma mas pequeñas, que las del método anterior.

2 DSS (digital signature standard)

Es una variacion de sistema de firmas digitales normal basado en El Gamal. Este nuevo sistema utiliza primos de 512 bits (al igual que el anterior) sin embargo genera firmas de 320 bits.

Esta mejora se consigue considerando que ahora γ ya no esta en $\mathcal{Z}_p$ si no en un subgrupo ciclico suficientemente grande de este. Se ha especulado que quebrar este sistema de firmas es un problema de similar dificultad que resolver el problema del logaritmo discreto.

3 Otros sistemas de firmas

Ahora enunciaremos brevemente otros sistemas de firmas

- Firmas no repudiables

  Estas firmas poseen la característica de que no pueden ser verificadas sin la colaboración del firmante. Esto sirve mucho para evitar chantajes, al no dejar que terceros verifiquen firmas hechas sin el consentimiento del firmante.

- Firmas fail-stop

  Mecanismo de firmas digitales que ademas de una firma cuenta con un algoritmo de demostración de firmas falsas. Para este sistema se pueden hacer firmas que pasen el test de verificación pero el sistema de demostración de firmas falsa que posee permite saber que para determinada firma generada por un adversario el autor original de la firma la detecte como falsa.

- Firmas de grupo

  Sistema de firmas que hacen que un grupo posea una sola firma. Esta firma se puede generar en un porceso que involucra a n personas que forman parte del grupo, y para firmar se necesita la colaboración de estas n personas también.

- Firmas umbral

  Es un sistema de firmas de grupo en que se requiere de la participacion de un umbral de t personas de un total de n para poder efectuar una firma.

4 Seguridad de un sistemas de firmas digital

Una definición que se presta mejor para estudiar la seguridad de un sistema de firmas digitales es la siguiente Un sistema de firmas digitales es una tripleta (G, σ, D) tal que

- El algoritmo de generación (G)

  Es un algoritmo probabilista a tiempo polinomial que en la entrada 1^k produce una clave pública de firmas denotada P y una clave privada denotada S

- El algoritmo de firma (σ)

  Es también un algoritmo probabilista a tiempo polinomial que en la entrada 1^k y un mensaje $m \in \{0,1\}^k$ y la clave secreta S, entrega s la firma de m.

- El algoritmo de verificación (V)

  Es un algoritmo probabilista a tiempo polinomial que en la entrada P (clave pública), un mensaje m y una suspuesta firma s, produce un 1 o 0 dependiendo si la firma es válida o no, o lo que es igual si $s \in \sigma\ (1^k,n,S)$ el algoritmo genera un 1.

5 Tipos de ataque para sistemas de firmas

Existen varios posibles tipos de ataques

- Ataque de clave pública

  El adversario sólo conoce la clave pública de la persona a plagiar. La clave pública es el mínimo de informacion que tiene que obtener el adversario para efectuar un ataque, cuando no es posible obtener más puede ser debido a que el firmante original, encripta los mensajes después de haberlos firmado.

- Ataque de firma conocida

  El adversario posee n pares de mensajes con sus respectivas firmas pero no son mensajes de su elección. Esto ocurre cuando el adversario se ha dedicado a coleccionar pares de mesajes-firmas del firmante original, interceptándolos en la red o mediante algún otro medio.

- Ataque de mensaje elegido

  El adversario puede elegir los mensajes que el desee (en forma adaptativa) y puede obtener las firmas para ese mensaje del firmante real. Este es el caso, por ejemplo, de pedirle al firmante que firme un texto que el adversario desee, lo cual ocurre cuando el firmante es notario o algo similar.

6 Definición de falsificación

Hasta ahora no hemos definido que concepto se engloba en el término falsificación

Para esto vamos a dar a conocer primero todos los tipos de de falsificación existentes.

- Falsificación existencial,

  Un adversario produce una firma válida a un mensaje que no es de su elección

- Falsificación selectiva

  El adversario produce una firma a un mensaje que es de su elección.

- Falsificación universal

  El adversario puede producir una firma válida de cualquier mensaje. (No necesariamente descubre la clave secreta del firmante original)

7 Concepto de seguridad de un sistema de firmas digitales

Para definir seguridad de un sistema de firmas digitales, primero veamos lo que es un algoritmo de falsificación.

Un algoritmo de falsificación F probabilístico, que usa al firmante real como "oráculo" (el adversario puede obtener pares mensaje-firma, de cualquier mensaje elegido) es tal que puede en tiempo polinomial al tamaño de la clave pública generar una firma de cualquier mensaje cuya firma no haya sido obtenida del firmante real. Denotemos como B al oráculo entonces el algoritmo que usa este oráculo será F^B.

Este algoritmo tiene como entrada una clave publica de firmas P y produce un mensaje m y su supuesta firma s.

Decimos que (G, σ, D) es un sistema de firmas digitales seguro si

$\forall$ F (algoritmo de falsificación) $\exists$ ν_F función despreciable, tal que $\forall$ k suficientemente grande:

$\Pr[V(P, m, s) = 1 | (P, \delta) \leftarrow G(1^k), (n, \delta) \leftarrow F^B(P)] \leq \nu_F(k)$

8 Análisis de los algoritmos vistos

Según nuestras nuevas definiciones veamos que tan seguros son los sistemas de firmas digitales vistos hasta ahora.

- El Gamal

  Este sistema no es seguro deacuerdo a las definiciones anteriores pues es existencialmente falsificable.

- RSA

  Las firmas por RSA tampoco son seguras debido a que son universalmente fasificable porque $\sigma(n1) \cdot \sigma(n2) \equiv_n \sigma(n1 \cdot n2)$

- Sistema de Diffie-hellman

  El trabajo fundacional de Diffie-Hellman en el cual se necesita poseer una colección de funciones de puerta secreta $F = \{f_i\}_{i \in I}$ para firmar un texto, i.e.:

  - genera $i \in I \cap \{0,1\}^k$ y f_i la puerta secreta
  - eligen $n \in \mathrm{REC}(f_i)$ y obtiene $s = f_i^{-1}(n)$ para firmar
  - y para verificar (m, s) chequear que $f_i(s) = n$

  Es existencialmente falsificable dperoque dado $s \in \mathrm{DOM}(f_i)$ y calculando m=$f_i(s)$ generan un par de (m, s) mensaje-firma válido