Criptografía de clave pública

Características de la Criptografía de clave pública
Complejidad computacional
Servicios de seguridad

eman ta zabal zazu
Universidad del País Vasco
Euskal Herriko Unibertsitatea
KISA

Criptografía de clave pública

Características

- Cifrado en bloque. Tamaño de bloques de al menos 1024 bits.
- Se construye sobre funciones unidireccionales ("one-way"), basadas en problemas matemáticos de difícil solución.
- Cada usuario posee dos claves: una *clave pública* y una *clave privada*.
- Las claves son de mayor tamaño que en el cifrado simétrico.
- La tasa de cifrado es sensiblemente inferior a la del cifrado simétrico.
- Aparece en 1976: Intercambio de claves de Diffie-Hellman.
- Algunos criptosistemas de clave pública: RSA, ElGamal, ECC, criptosistema de Rabin.

- Se utilizan diferentes algoritmos para cifrar y descifrar.
- Dos claves:
  - Clave de cifrado K_{E} (pública).
  - Clave de descifrado K_{D} (privada).
- K_{D} no puede deducirse de K_{E} (bajo el mismo coste computacional).
- Es más eficiente para distribuir claves que el cifrado simétrico.
- Es fácil efectuar ataques de texto en claro elegido:

$$C = \mathrm{E}(M, K_{\mathrm{E}}).$$

Fundamentos

$\mathcal{M}$ conjunto de mensajes en claro, $\mathcal{C}$ conjunto de mensajes cifrados,

$$\begin{array}{ccc} \mathcal{M} & \xrightarrow{\mathrm{E}} & \mathcal{C} \\ M & \mapsto & C \end{array}$$

E función de cifrado, biyectiva, E^{-1} función de descifrado.

Características de E:

- $C = \mathrm{E}(M, K_{\mathrm{E}})$ fácil de calcular conociendo K_{E}.
- $M = \mathrm{E}^{-1}(C, K_{\mathrm{D}})$ cálculo imposible sin K_{D} (*"trapdoor"*).

Una función con estas propiedades se denomina función "*one-way*".

Orden de una función

Definición

Sean $f, g : \mathbb{R} \longrightarrow \mathbb{R}$, g *función positiva.*
Se dice que $f = \mathcal{O}(g)$ *si existen* $C > 0$ *y* $x_0 \in \mathbb{R}$, *tales que*

$$|f(x)| \leq C \cdot g(x), \quad \forall\, x \geq x_0.$$

Ejemplos:

$$x = \mathcal{O}(x), \quad x = \mathcal{O}(x^2), \quad \log x = \mathcal{O}(x), \quad x^r = \mathcal{O}(e^x), \ r \in \mathbb{N}$$

Nota: Si f y g son evaluadas sobre los enteros positivos, la definición anterior sigue siendo válida.

Representación de un entero decimal en base 2

Dado n entero positivo, existe k entero tal que

$$2^{k-1} \leq n < 2^k,$$

entonces,

$$(k-1)\log 2 \leq \log n < k \log 2,$$

$$(k-1) \leq \frac{\log n}{\log 2} \longrightarrow k = \mathcal{O}(\log n).$$

Nota: Observemos que k es el número de bits necesarios para representar n $(k = [\log_2 n] + 1)$.

Complejidad computacional

Definición

Sea n el mayor entero positivo que interviene en un algoritmo. Se dice que el algoritmo tiene

- *coste computacional polinomial si existe $r \in \mathbb{N}$ tal que el número de operaciones necesarias para su ejecución es $\mathcal{O}(\log^r n)$.*
- *coste computacional exponencial si el número de operaciones necesarias para su ejecución no es polinomial.*

Funciones "one-way"

Una función $\mathrm{E} : \mathcal{M} \longrightarrow \mathcal{C}$ biyectiva es "one-way" si

- la función de cifrado E presenta complejidad polinomial (computacionalmente factible (conocida K_{E})).
- la función de descifrado E^{-1} complejidad exponencial (coste computacional prohibitivo (desconocida K_{D})).

Nota:

- Una función es "one-way" computacionalmente (podría cambiar en el futuro: paralelismo, nuevos algoritmos, ...).
- No se ha demostrado que ninguna función sea "one-way".

Algunos costes computacionales

a, b, x, n enteros de a lo sumo k-bits,

Multiplicación ab:	$\mathcal{O}(k^2)$
Convertir entero de k-bits bin a dec:	$\mathcal{O}(k^2)$
Hallar $\mathrm{mcd}(a, b)$, (alg. Euclides):	$\mathcal{O}(k^3)$
Calcular potencias a^x mód n:	$\mathcal{O}(k^3)$
Factorial $n!$:	no algoritmo polinomial

Coste computacional de la multiplicación

Sean m, n enteros de k, ℓ bits respectivamente, $k \geq \ell$

Ejemplo:

				1	1	0	0	1	k bits (entero mayor)
					1	1	0	1	ℓ bits
				1	1	0	0	1	entero n
		1	1	0	0	1	0		desplazamiento a izda
	1	1	0	0	1				$\leq \ell$ filas de $\leq k + \ell$ bits
1	0	1	0	0	0	1	0	1	$\ell - 1$ sumas de enteros de $\leq k + \ell$ bits

Nota:

- Suma de dos enteros de k bits $\rightarrow$ entero de a lo sumo $k + 1$ bits.
- Cada suma produce un entero de a lo sumo $(k + \ell)$ bits (la última a lo sumo $\leq k + \ell + 1$).
- Cada suma: $k + \ell$ operaciones de bit.
- Coste total $\leq \ell(k + \ell) \sim O(k^2)$.

Coste computacional del cifrado-descifrado afín

Ejemplo

Sea $k = [\log_2 M] + 1$ *la longitud en bits de un mensaje* M

Para cifrar:	$C = (aM + b) \mod n$
Clave de cifrado:	$K_{\mathrm{E}} = (a, b)$
Coste computacional:	$\mathcal{O}(k^2)$

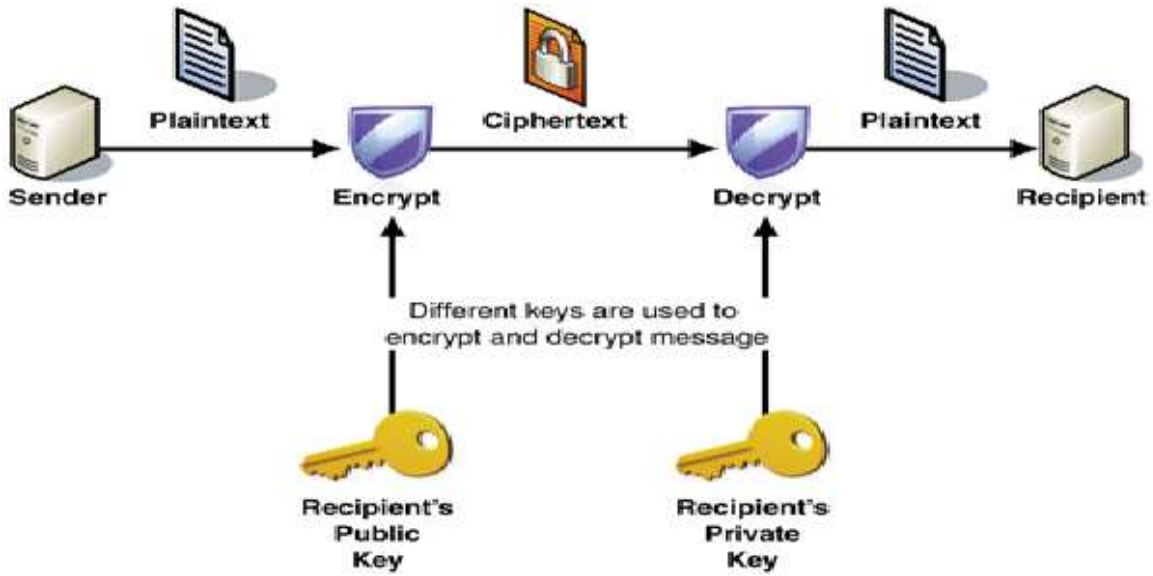
Para descifrar:	$M = (a^{-1}C - a^{-1}b) \mod n$
Clave de descifrado:	$K_{\mathrm{D}} = (a^{-1}, -a^{-1}b)$
Coste computacional:	$\mathcal{O}(k^3)$ *(inversos)*

Servicios Criptográficos

Los servicios criptográficos que ofrece la Criptografía de clave pública son:

- Confidencialidad (cifrado).
- Intercambio de claves.
- Establecimiento de comunicación.
- Autenticación de origen (se requiere Firma Digital).
- Integridad (se requiere MAC o Funciones Hash).

Esquema de cifrado de clave pública



Fuente: Internet, "draw+of+public+key+cryptography"

Cifrado

Usuarios: A y B. $\mathrm{E}_A, \mathrm{E}_B$ funciones de cifrado de A y B.

Objetivo: A pretende enviar a B un mensaje cifrado M.

Protocolo:

A envía: $\mathrm{E}_B(M)$

Observaciones:

- Se necesita autenticación de la clave pública de B
  (se requiere una Infraestructura de Clave Pública (PKI) que la certifique).
- Confidencialidad (sólo B puede leer M).
- No se garantiza autenticidad de origen (se requiere firma digital).
- No se garantiza integridad (se requiere MAC o funciones hash).

Intercambio de claves

Usuarios: A y B. E_A, E_B funciones de cifrado de A y B.

Objetivo: A, B pretenden intercambiar una clave secreta.

Protocolo:

A envía:	$\mathrm{E}_B\,\mathrm{E}_A^{-1}(K)$
B calcula:	$\mathrm{E}_B^{-1}\,\mathrm{E}_B\,\mathrm{E}_A^{-1}(K)$
B envía:	$\mathrm{E}_A\,\mathrm{E}_B^{-1}\,\mathrm{E}_A^{-1}(K)$
A calcula:	$\mathrm{E}_A^{-1}\,\mathrm{E}_A\,\mathrm{E}_B^{-1}\,\mathrm{E}_A^{-1}(K)$

Observaciones:

- $\mathrm{E}_B^{-1}\,\mathrm{E}_A^{-1}(K)$ es la clave compartida.
- Disponible para iniciar un criptosistema simétrico.
- Se necesita autenticación de $\mathrm{E}_A, \mathrm{E}_B$ (requiere una PKI).

Establecimiento de comunicación

Usuarios: A y B. $\mathrm{E}_A, \mathrm{E}_B$ funciones de cifrado de A y B.

Objetivo: A, B pretenden establecer comunicación (demostrar a la otra parte quienes son).

Protocolo:

A elige:	un número aleatorio n y envía $\mathrm{E}_B(n)$
B elige:	un número aleatorio m y envía $\mathrm{E}_A(m)$
A descifra:	$\mathrm{E}_A^{-1}\,\mathrm{E}_A(m)$ y envía $\mathrm{E}_B(m)$
B descifra:	$\mathrm{E}_B^{-1}\,\mathrm{E}_B(n)$ y envía $\mathrm{E}_A(n)$
A descifra:	$\mathrm{E}_A^{-1}\,\mathrm{E}_A(n)$
B descifra:	$\mathrm{E}_B^{-1}\,\mathrm{E}_B(m)$

Nota: Se necesita autenticación de $\mathrm{E}_A, \mathrm{E}_B$ (requiere una PKI).

Autenticidad de origen: Firma Digital

Usuarios: A y B. $\mathrm{E}_A, \mathrm{E}_B$ funciones de cifrado de A y B.

Objetivo: A pretende enviar a B un mensaje firmado M.
Sea S la firma.

Protocolo:

A envía:	$M \;\; \mathrm{y} \;\; \mathrm{E}_A^{-1}(S)$
B recibe:	$M \;\; \mathrm{y} \;\; \mathrm{E}_A^{-1}(S)$
B descifra y verifica:	$\mathrm{E}_A\,\mathrm{E}_A^{-1}(S)$

Observaciones:

- Garantiza a B que el mensaje viene de A.
- No garantiza autenticidad de contenido de M.
- No garantiza confidencialidad.
- La firma S puede ser el propio mensaje M. Conviene que S incluya datos de identificación personal de A, datos temporales, u otros.
- Si M grande, firma de un resumen de M.

Integridad

Usuarios: A y B. $\mathrm{E}_A, \mathrm{E}_B$ funciones de cifrado de A y B.

Objetivo: A pretende enviar a B un mensaje M con autenticación de contenido. A y B acuerdan utilizar una función hash $H(.)$.

Protocolo:

A envía:	$M \ \mathrm{y} \ H(M)$
B recibe:	$M \ \mathrm{y} \ H(M)$
B calcula y verifica:	$H(M)$

Problemas matemáticos en los que se basa

- Cálculo del logaritmo discreto en cuerpos finitos:
  - Intercambio de claves de Diffie-Hellman.
  - Cifrado de Massey-Omura.
  - Criptosistema de ElGamal.
- El problema de la factorización de enteros:
  - Algoritmo RSA (Rivest, Shamir, Adleman).
- Cálculo de raíces cuadradas modulares:
  - Criptosistema de Rabin.
- Cálculo del logaritmo elíptico en cuerpos finitos:
  - Intercambio de claves (análogo de Diffie-Hellman).
  - Cifrado análogo al de Massey-Omura.
  - Cifrado análogo al de ElGamal.

Fin de la sección