Seguridad y Protección de Sistemas Informáticos

Fco. Javier Lobillo Borrero

Departamento de Álgebra, Universidad de Granada

Curso 2017/2018

Índice

1 Técnicas criptográficas de clave secreta

1 Técnicas criptográficas de clave pública

3 Protocolos criptográficos

4 Certificación digital

5 Marcas de agua

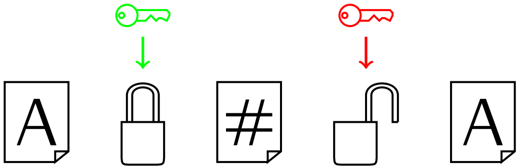
6 Seguridad en redes y comunicaciones

7 Identidad digital e identificación biométrica

8 Comercio electrónico

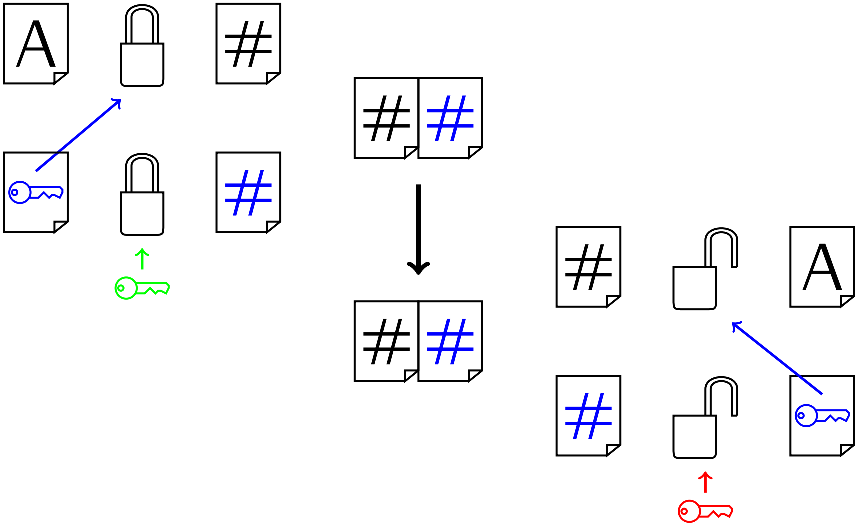
Criptosistemas asimétricos

Distinta clave cifra (pública) y descifra (privada).



1. Ventaja conceptual para Asimétricos: identificación e intercambio de claves.
2. Ventaja en coste para Simétricos: tamaño de las claves y velocidad.

Solución al coste: Criptosistemas híbridos



Análisis conceptual

Criptosistemas simétricos

- Canal seguro entre dos usuarios.
- Cada pareja de usuarios debe acordar una clave común.
- Permiten garantizar confidencialidad e integridad.

Criptosistemas asimétricos

- Cada usuario tiene una pareja de claves $(k, K) \in \mathcal{K}$, manteniendo K en privado y publicando k.
- Sus usos principales son distribución de claves, autenticidad y no repudio.

Construcción formal

- El espacio de claves es $\mathcal{K} = \mathcal{K}_p \times \mathcal{K}_s$.
- Existe una familia de aplicaciones $e_k : \mathcal{P} \to \mathcal{C}$, con $k \in \mathcal{K}_p$, para las que existe un algoritmo eficiente que las calcula pero es computacionalmente imposible calcular preimágenes.
- Estas funciones se llaman *funciones unidireccionales* o *one-way functions*.
- Para cada $k \in \mathcal{K}_p$ existe un $K \in \mathcal{K}_s$, que debe mantenerse en secreto, y una aplicación eficientemente computable $d_K : \mathcal{C} \to \mathcal{P}$, tal que $d_K(e_k(m)) = m$. K se llama *información trampa*.
- Las funciones unidireccionales con información trampa se llaman *funciones trampa* o *trapdoor function*.

Índice

1 Técnicas criptográficas de clave pública

- RSA
- DH y ElGamal
- Criptosistemas basados en curvas elípticas

One-way function: Potencias, raíces y logaritmos

Sean $n, a, e \in \mathbb{Z}$ positivos con $n \neq 0, 1$. Calcular a^e mód n es computacionalmente rápido mediante los cuadrados iterados, es decir, si $e = e_t e_{t-1} \dots e_1 e_0)_2$,

$$a^e = ((\cdots((a^{e_t})^2 a^{e_{t-1}})^2 a^{e_{t-2}} \cdots)^2 a^{e_1})^2 a^{e_0},$$

luego tenemos que hacer $2\log_2 e + 1$ multiplicaciones para calcular potencias.

Sin embargo, dados $n, a, e \in \mathbb{Z}$, no hay en general un buen algoritmo para calcular $\sqrt[e]{a}$ mód n o $(\log_a e)$ mód n. Sí podemos calcular una raíz e–ésima de a si conocemos $\varphi(n)$, donde φ es la función indicatriz de Euler, y e es primo relativo con $\varphi(n)$. Concretamente, sea $d \in \mathbb{Z}$ tal que $ed \equiv 1$ mód $\varphi(n)$. El Teorema de Euler establece que $a^{\varphi(n)} \equiv 1$ mód n, de donde deducimos que $(a^d)^e = a^{ed} \equiv a$ mód n. Por tanto

$$a^d = \sqrt[e]{a} \text{ mód } n.$$

Descripción de RSA

El algoritmo de cifrado asimétrico RSA, acrónimo de Rivest, Shamir y Adleman, fue publicado en 1978. Se basa en la rapidez del cálculo de potencias y la lentitud del cálculo de raíces a no ser que conozcamos la función φ.

- Elegimos dos primos p, q suficientemente grandes. Calculamos $n = pq$.
- Calculamos $\varphi(n) = (p-1)(q-1)$.
- Elegimos $3 \leq e \leq \varphi(n)$ tal que $(e, \varphi(n)) = 1$.
- Calculamos $d = e^{-1} \pmod{\varphi(n)}$.
- La clave pública es el par (n, e).
- Mantenemos en privado p, q, d.
- La función de cifrado es
$$\mathrm{RSA}_{n,e}(m) = m^e \pmod{n}.$$
- La función de descifrado es
$$\mathrm{RSA}_{n,e}^{-1}(c) = \mathrm{RSA}_{n,d}(c) = c^d \pmod{n}.$$

Acelerando el cifrado y el descifrado

Cifrado

El método de cuadrados iterados es especialmente rápido si en la representación binaria del exponente hay muchos ceros. Una forma de lograr esto es elegir como e un primo de dichas características como $e = 3, 17, 2^{16} + 1$.

Descifrado

El Teorema Chino del Resto establece un isomorfismo

$$\begin{aligned} \phi : \mathbb{Z}_n &\to \mathbb{Z}_p \times \mathbb{Z}_q \\ x \bmod n &\mapsto (x \bmod p, x \bmod q). \end{aligned}$$

Usando este isomorfismo,

$$c^d \bmod n = \phi^{-1}(c^{d \bmod p-1} \bmod p, c^{d \bmod q-1} \bmod q),$$

lo que reduce el tamaño de los números a emplear.

Seguridad de RSA

- Se cree que invertir la función $\mathrm{RSA}_{(n,e)}$ es un problema intratable.
- Conocer p, q nos lleva a conocer $\varphi(n) = (p-1)(q-1)$ y por tanto a calcular fácilmente d, por lo que en este caso sí podemos invertir $\mathrm{RSA}_{(n,e)}$.
- Conocer $\varphi(n)$ nos permite, obviamente, calcular d. En este caso

$$p + q = n - \varphi(n) + 1 \qquad p - q = \sqrt{(p+q)^2 - 4n}.$$

  Por lo tanto es computacionalmente equivalente conocer p, q y conocer $\varphi(n)$.
- Existen algoritmos polinomiales que factorizan n a partir de n, e, d. De nuevo conocer d se convierte en computacionalmente equivalente a factorizar $n = pq$.
- Hay situaciones en las que la estructura de p y q facilita encontrarlos a partir de n. Estas situaciones se evitan usando los llamados *primos fuertes*. Un número primo p es fuerte si
  - $p - 1$ tiene un factor primo grande, llamado r,
  - $p + 1$ tiene un factor primo grande,
  - $r - 1$ tiene un factor primo grande.

  Se conjetura que son infinitos y fáciles de construir.

Índice

1. Técnicas criptográficas de clave pública
   - RSA
   - DH y ElGamal
   - Criptosistemas basados en curvas elípticas

Logaritmo discreto, conjetura de Diffie y Hellman

- La potencia es una one way function en relación con el logaritmo, es decir, calcular $g^a \bmod n$ es computacionalmente rápido, pero calcular $\log_g b \bmod n$ no lo es en general.
- Si los factores primos de n son pequeños, sí podemos calcular el logaritmo rápido usando el Teorema Chino del Resto. Para su uso en criptografía lo más útil es utilizar $n = p$ un número primo grande.
- Si g tiene pocas potencias distintas, también es rápido calcular logaritmos, por lo que es conveniente que g sea un generador de $\mathbb{Z}_p^*$, es decir, que todo elemento de $\mathbb{Z}_p$ distinto de 0 sea potencia de g.

Conjetura de Diffie y Hellman

Calcular $g^{ab} \bmod p$ a partir de $g^a \bmod p$ y $g^b \bmod p$ es computacionalmente equivalente a calcular $a = \log_g g^a \bmod p$ o $b = \log_g g^b \bmod p$.

ElGamal: generación de claves

- Seleccionamos aleatoriamente un número primo $p = 2rq + 1$ donde q es también primo grande y r tiene factores pequeños.
- Seleccionamos aleatoriamente g generador de $\mathbb{Z}_p^*$. Para que este proceso sea eficiente necesitamos que r tenga factores pequeños.
- Elegimos aleatoriamente $2 \leq x \leq p - 2$ y calculamos $y = g^x \mod p$.
- La clave privada es (p, g, x), y la clave pública (p, g, y).

ElGamal: cifrado y descifrado

Cifrado

- El mensaje es un elemento $m \in \mathbb{Z}_p$.
- Aleatoriamente seleccionamos $2 \leq k \leq p-2$.
- El criptograma es
$$(c_1, c_2) = (g^k \bmod p, y^k m \bmod p).$$

Descifrado

Observemos que

$$c_1^{p-1-x} c_2 \equiv (g^k)^{p-1-x} y^k m \equiv (g^k)^{p-1-x} (g^x)^k m \equiv (g^{p-1})^k g^{-kx+xk} m \equiv m \pmod p,$$

luego el descifrado es $c_1^{p-1-x} c_2 \bmod p$.

Seguridad de ElGamal

- El algoritmo de cifrado no es determinista. El criptograma depende de m, la clave pública (p, g, y) y de k, que es aleatorio para cada cifrado. Cifrar el mismo mensaje con la misma clave proporcionará dos criptogramas distintos.
- El atacante conoce $y = g^x$ y $c_1 = g^k$ para tratar de encontrar $y^k = g^{xk}$ con el que calcular $m = g^{-xk} c_2$.
- Si la conjetura de Diffie y Hellman es cierta, el atacante debe calcular $x = \log_g y \text{ mód } p$ o $k = \log_g c_1 \text{ mód } p$, computacionalmente difícil.

Índice

1. Técnicas criptográficas de clave pública
   - RSA
   - DH y ElGamal
   - Criptosistemas basados en curvas elípticas

Conjetura de Diffie y Hellman en grupos

En realidad, para diseñar un sistema basado en la conjetura de Diffie y Hellman sólo hace falta una estructura multiplicativa y un elemento de orden finito, es decir, un grupo G y un elemento $g \in G$ tal que $g^n = 1$ para cierto n suficientemente grande.

Conjetura de Diffie y Hellman en grupos

Sea $g \in G$ un elemento de orden finito. Calcular g^{ab} a partir de g^a y g^b es computacionalmente equivalente a calcular $a = \log_g g^a$ o $b = \log_g g^b$.

La conjetura estándar es para $G = \mathbb{Z}_p^*$, con p un primo suficientemente grande.

Curvas elípticas en característica positiva

Característica impar

Una curva elíptica es el conjunto de puntos

$$E(\mathbb{Z}_p) = \left\{(x, y) \in \mathbb{Z}_p \times \mathbb{Z}_p \mid y^2 = x^3 + \alpha x + \beta\right\}$$

donde $4\alpha^3 + 27\beta^2 \neq 0$, junto con un punto $\mathcal{O}$ llamado punto del infinito. Esta es la forma de Weierstrass.

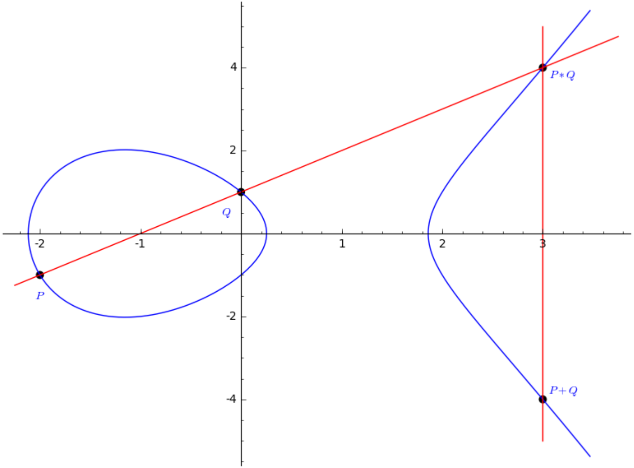
Característica 2

Una curva elíptica es el conjunto de puntos

$$E(\mathbb{F}_{2^l}) = \left\{(x, y) \in \mathbb{F}_{2^l} \times \mathbb{F}_{2^l} \mid y^2 + xy = x^3 + \alpha x^2 + \beta\right\}$$

donde $\beta \neq 0$, junto con un punto $\mathcal{O}$ llamado punto del infinito. Esta es una de las formas de Weierstrass en característica 2.

Aritmética en una curva elíptica I



Aritmética en una curva elíptica II

Aritmética en característica impar

Sean

$$E = \left\{(x, y) \in \mathbb{Z}_p \times \mathbb{Z}_p \mid y^2 = x^3 + \alpha x + \beta\right\},$$

$P = (x_0, y_0)$, $P_1 = (x_1, y_1)$ y $P_2 = (x_2, y_2)$.

- $-P = (x_0, -y_0)$.
- Si $P_2 = -P_1$, $P_1 + P_2 = \mathcal{O}$.
- Si $P_2 \neq -P_1$, $P_1 + P_2 = P_3$, viene dado por

$$P_3 = (x_3, y_3) = (\lambda^2 - x_1 - x_2, \lambda(x_1 - x_3) - y_1),$$

donde $\lambda = \dfrac{y_2 - y_1}{x_2 - x_1}$ si $P_1 \neq P_2$, y $\lambda = \dfrac{3x_1^2 + \alpha}{2y_1}$ si $P_1 = P_2$.

Aritmética en una curva elíptica III

Aritmética en característica 2

Sean

$$E = \left\{(x, y) \in \mathbb{F}_{2^l} \times \mathbb{F}_{2^l} \mid y^2 + xy = x^3 + \alpha x^2 + \beta\right\},$$

$P = (x_0, y_0)$, $P_1 = (x_1, y_1)$ y $P_2 = (x_2, y_2)$.

- $-P = (x_0, x_0 + y_0)$.
- Si $P_2 = -P_1$, $P_1 + P_2 = \mathcal{O}$.
- Si $P_2 \neq -P_1$, $P_1 + P_2 = P_3$, viene dado por

$$P_3 = (x_3, y_3) = (\lambda^2 + \lambda + \alpha + x_1 + x_2, \lambda(x_1 + x_3) + x_3 + y_1),$$

donde $\lambda = \dfrac{y_2 + y_1}{x_2 + x_1}$ si $x_1 \neq x_2$, y $\lambda = x_1 + \dfrac{y_1}{x_1}$ si $x_1 = x_2$.

Selección de curva y punto base

La curva se selecciona estableciendo los llamados parámetros de dominio:

- El cuerpo finito $\mathbb{F}_q$,
- los parámetros de la curva $\alpha, \beta \in \mathbb{F}_q$,
- un punto base $Q \in E(\mathbb{F}_q)$,
- el orden n de Q, es decir, el número $n > 0$ tal que $nQ = \mathcal{O}$ y $mQ \neq \mathcal{O}$ para cualquier $0 < m < n$,
- el cofactor h tal que $hn = |E(\mathbb{F}_q)|$.

La séxtupla $(\mathbb{F}_q, \alpha, \beta, Q, n, h)$ es pública.

Es recomendable que n sea un primo grande y que h sea pequeño. Hay procedimientos para lograr curvas variadas con todos estos requerimientos.

Conjetura de Diffie y Hellman en curvas elípticas

Dados unos parámetros $(\mathbb{F}_q, \alpha, \beta, Q, n, h)$, calcular $(ab)Q$ a partir de aQ y bQ es computacionalmente equivalente a calcular $a = \log_Q aQ$ o $b = \log_Q bQ$.

ElGamal en curvas elípticas

Generación de claves

- Fijamos unos parámetros $(\mathbb{F}_q, \alpha, \beta, Q, n, h)$.
- Elegimos aleatoriamente $1 \leq x \leq n-1$ y calculamos $P = xQ$.
- La clave privada es $(\mathbb{F}_q, \alpha, \beta, Q, n, h, x)$, y la clave pública $(\mathbb{F}_q, \alpha, \beta, Q, n, h, P)$.

Cifrado

- El mensaje es un elemento $m \in E(\mathbb{F}_q)$. Cómo realizar esta "codificación" no es evidente.
- Aleatoriamente seleccionamos $1 \leq k \leq n-1$.
- El criptograma es $(C_1, C_2) = (kQ, m + kP)$.

Descifrado

El descifrado es $C_2 - xC_1$ ya que

$$C_2 - xC_1 = m + kP - x(kQ) = m + k(xQ) - (xk)Q = m + (kx)Q - (kx)Q = m.$$

Curva P-192

- La curva se define en $\mathbb{F}_p$ donde

$$\begin{aligned} p &= 2^{192} - 2^{64} - 1 \\ &= 6277101735386680763835789423207666416083908700390324961279. \end{aligned}$$

- Tiene por ecuación

$$y^2 = x^3 - 3x + \beta,$$

donde

$$\beta = 0x\ 64210519\ e59c80e7\ 0fa7e9ab\ 72243049\ feb8deec\ c146b9b1.$$

- La curva tiene orden

$$6277101735386680763835789423176059013767194773182842284081.$$

Curva B-163

- La curva se define en $\mathbb{F}_{2^{163}}$ donde

$$\mathbb{F}_{2^{163}} = \mathbb{F}_2[x]_{x^{163}+x^7+x^6+x^3+1}$$

- Tiene por ecuación

$$y^2 + xy = x^3 + x^2 + \beta,$$

donde

$$\beta = 0x\ 00000002\ 0a601907\ b8c953ca\ 1481eb10\ 512f7874\ 4a3205fd.$$

- La curva tiene orden $2r$ donde

$$r = 5846006549323611672814742442876390689256843201587.$$

Resumen de características

Confidencialidad Es el objeto fundamental de los criptosistemas, garantizar confidencialidad, sólo emisor y receptor tienen acceso a la información.

Autenticidad Los cifrados de clave pública no garantizan autenticidad.

Integridad La alteración de la información se detecta.

No repudio Tampoco se garantiza.

Bibliografía I

Hans Delfs and Helmut Knebl.
Introduction to Cryptography. Principles and Applications.
Information Security and Cryptography. Springer, third edition, 2015.

National Institute of Standards and Technology (NIST).
DATA ENCRYPTION STANDARD (DES), October 1999.

National Institute of Standards and Technology (NIST).
ADVANCED ENCRYPTION STANDARD (AES), November 2001.