Capítulo 20
Introducción a la Cifra con Curvas Elípticas

Seguridad Informática y Criptografía

v 4.1

Material Docente de
Libre Distribución

Ultima actualización del archivo: 01/03/06
Este archivo tiene: 30 diapositivas

Dr. Josep María Miret Biosca
Universidad de Lleida

Nota de agradecimiento del editor

- Este tema ha sido entregado para su inclusión en el libro electrónico por parte de mi colega y amigo Josep María Miret Biosca, Dr. en Matemáticas y experto en curvas elípticas e hiperelípticas. Josep es profesor de la Universidad de Lleida, en Catalunya, España.

http://www.matematica.udl.es/cas/professor.html?id=23

- Si bien la cifra con curvas elípticas está experimentando últimamente un gran desarrollo, recuerde que lo que aquí se muestra es tan sólo una breve introducción al tema, con ciertas modificaciones con respecto a la documentación de la versión 4.0 del libro.
- Si está interesado en esta línea de investigación, podrá encontrar mucha información en Internet en estos enlaces en español e inglés.

http://www.google.es/search?hl=es&q=criptografia+curvas+el%C3%ADpticas&meta=

http://www.google.es/search?hl=es&q=elliptic+curve+cryptography&meta=

Introducción

- **Criptosistemas de clave compartida**: *Inconvenientes*
  - Distribución de claves
  - Cada usuario tiene que gestionar una gran cantidad de claves
  - Imposibilidad de firmar mensajes

- **Criptosistemas de clave pública**
  - Diffie-Hellman en 1976 proponen un intercambio seguro de claves
  - El receptor hace pública la *clave pública* para que un usuario pueda enviarle mensajes cifrados, pero guarda en secreto *la clave privada* para descifrar
  - La seguridad de un tal criptosistema reside en problemas matemáticos subyacentes computacionalmente difíciles, como
    - *El problema de la factorización*
    - *El problema del logaritmo discreto*
  - **Criptosistemas basados en curvas elípticas**
    - Disminución del tamaño de las claves, garantizando misma seguridad

Curvas elípticas

Una curva elíptica E sobre un cuerpo $\mathbb{K}$ viene definida por una *ecuación de Weierstrass*:

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6, \quad a_i \in \mathbb{K}$$

con la condición que el discriminante sea no nulo, para que no tenga puntos singulares

- Si la característica de $\mathbb{K}$ es distinta de 2 y de 3, esta ecuación se puede expresar como

  $$y^2 = x^3 + ax + b, \quad a, b \in \mathbb{K}$$

  con discriminante $\Delta = -16(4a^3 + 27b^2) \neq 0$, denominada *ecuación reducida de Weierstrass*

- Si la característica de $\mathbb{K}$ es 2, usando también transformaciones lineales de las variables, se obtiene una de las siguientes expresiones:

  $$\begin{array}{lll} y^2 + ay = x^3 + bx + c, & a, b, c \in \mathbb{K}, & \text{con } \Delta = a^4 \neq 0 \\ y^2 + xy = x^3 + ax + b, & a, b \in \mathbb{K}, & \text{con } \Delta = b \neq 0 \end{array}$$

Conjunto de puntos en una curva elíptica

Si E es una curva elíptica E sobre $\mathbb{K}$, denotaremos por $E(\mathbb{K})$ el conjunto de puntos de $\mathbb{K}^2$ que satisfacen la ecuación de la curva junto con el punto del infinito $\mathcal{O}$, es decir,

$$E(\mathbb{K}) = \{(x, y) \in \mathbb{K}^2 \mid y^2 = x^3 + ax + b\} \cup \{\mathcal{O}\}$$

- Si $\mathbb{K} = \mathbb{R}$, la gráfica de una curva elíptica puede ser:

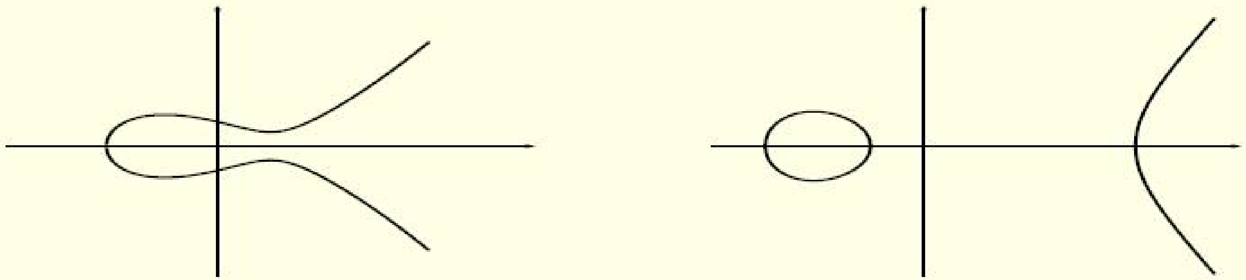

Figura 1: Curvas $y^2 = x^3 - 3x + 3$ e $y^2 = x^3 - 13x - 12$ sobre $\mathbb{R}$

- Si $\mathbb{K}$ es un cuerpo finito, obviamente $E(\mathbb{K})$ tiene un número finito de puntos. Por ejemplo, el conjunto de puntos de la curva $E:\ y^2 = x^3 + x + 1$ sobre $\mathbb{F}_7$ es

$$E(\mathbb{F}_7) = \{(0, 1), (0, 6), (2, 2), (2, 5), \mathcal{O}\}$$

Suma de puntos en una curva elíptica

En $E(\mathbb{K})$ se puede definir una operación $+$ mediante el método de la cuerda y la tangente:

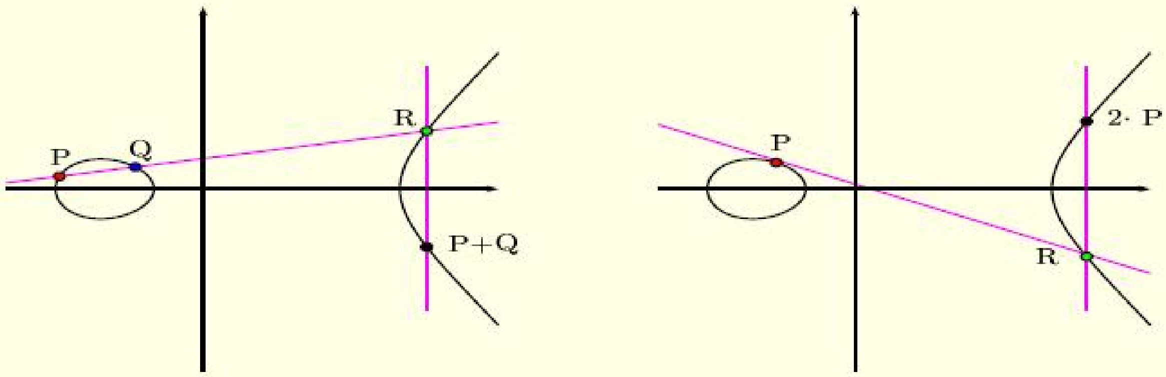

Figura 2: Suma y doblado de puntos en una curva elíptica

- $(E(\mathbb{K}), +)$ es un grupo abeliano con neutro el punto $\mathcal{O}$
  - El opuesto o simétrico de un punto $P = (x, y)$ de $E(\mathbb{K})$ es el punto $-P = (x, -y)$

Expresiones analíticas del punto suma

Sea E una curva elíptica de ecuación $y^2 = x^3 + ax + b$ sobre $\mathbb{K}$

Sean $P = (x_1, y_1)$ y $Q = (x_2, y_2)$ dos puntos de $E(\mathbb{K})$

Entonces las coordenadas del punto $P + Q = (x_3, y_3)$ son

$$P + Q = (\lambda^2 - x_1 - x_2,\ (x_1 - x_3)\lambda - y_1)$$

donde

$$\lambda = \begin{cases} (y_1 - y_2)/(x_1 - x_2), & \text{si } x_1 \neq x_2 \\ (3x_1^2 + a)/2y_1, & \text{si } x_1 = x_2 \text{ e } y_1 \neq -y_2 \end{cases}$$

- Por ejemplo, dados la curva $E:\ y^2 = x^3 + x + 1$ sobre $\mathbb{F}_{13}$ y los puntos $P = (0, 1)$ y $Q = (1, 4)$ de $E(\mathbb{F}_{13})$ se tiene:

$$\begin{array}{ll} P + Q = (8, 1) & 2 \cdot P = P + P = (10, 7) \\ 2 \cdot P + Q = (5, 12) & 2 \cdot Q = Q + Q = (8, 12) \\ P + 2 \cdot Q = (1, 9) & P - Q = P + (-Q) = (11, 2) \end{array}$$

Múltiplos de un punto de una curva

Sea E una curva elíptica sobre $\mathbb{K}$

Si P es un punto de $E(\mathbb{K})$ y k un entero, entonces se puede definir el punto $k \cdot P$ de la siguiente forma:

$$k \cdot P = \begin{cases} P + \overset{k}{\cdots} + P, & \text{si } k > 0 \\ \mathcal{O}, & \text{si } k = 0 \\ (-P) + \overset{k}{\cdots} + (-P), & \text{si } k < 0 \end{cases}$$

- El cálculo de $k \cdot P$, usando el método binario, se reduce a doblar y sumar puntos un número $\log_2(k)$ de veces
- Por ejemplo, dados la curva $E : y^2 = x^3 + x + 1$ sobre $\mathbb{F}_{101}$ y el punto $P = (0, 1)$ de $E(\mathbb{F}_{79})$, el punto $21 \cdot P$ se puede calcular como sigue:

$$21 \cdot P = 2 \cdot (2 \cdot (2 \cdot (2 \cdot P) + P)) + P = (23, 74)$$

Curvas elípticas sobre cuerpos finitos

Las curvas elípticas que interesan en criptografía son las definidas sobre cuerpos finitos, más concretamente, cuerpos finitos $\mathbb{F}_q$ con $q = p$, p primo, o $q = 2^m$

Si E es una curva elíptica sobre un cuerpo finito $\mathbb{F}_q$, se conocen resultados acerca del cardinal y la estructura de su grupo de puntos

Teorema de Hasse El cardinal $m = \#E(\mathbb{F}_q)$ satisface

$$q + 1 - 2\sqrt{q} \leq m \leq q + 1 + 2\sqrt{q}$$

Si escribimos $\#E(\mathbb{F}_q) = q + 1 - t$, donde t es la traza del endomorfismo de Frobenius de E, entonces $|t| \leq 2\sqrt{q}$

Teorema de Waterhouse Sobre un cuerpo finito primo $\mathbb{F}_p$ existen curvas elípticas con cardinal cada uno de los posibles enteros del intervalo $[p + 1 - 2\sqrt{p},\ p + 1 + 2\sqrt{p}]$, denominado intervalo de Hasse

Teorema de Cassels El grupo $E(\mathbb{F}_q)$ está generado por uno o dos puntos, es decir, $E(\mathbb{F}_q)$ es isomorfo al grupo $\mathbb{Z}_m$ o bien al grupo $\mathbb{Z}_{m_1} \times \mathbb{Z}_{m_2}$, con $m_1 \cdot m_2 = m = \#E(\mathbb{F}_q)$, $m_2 | m_1$ y $m_2 | (q - 1)$

Una curva sobre un cuerpo finito F_p

- Cuerpo: $\mathbb{F}_p$ con $p = 314159265359$
- Curva:
$$E : y^2 = x^3 + 102x + 2005$$
- Cardinal:
$$\#E(\mathbb{F}_p) = 314159228780 = 2^2 \cdot 5 \cdot 15707961439$$
- Para encontrar un punto sobre la curva se escoge una x aleatoria y se comprueba si $x^3 + ax + b$ es un cuadrado en $\mathbb{F}_p$. De esta forma se ha obtenido el punto
$$P = (217516809030, 126715600995)$$
- El orden de un punto Q de $E(\mathbb{F}_p)$ es el mínimo natural $k > 0$ tal que $k \cdot Q = \mathcal{O}$. El orden de cualquier punto de la curva es un divisor del cardinal de la misma. Así,
  - El punto $P = (217516809030, 126715600995)$ tiene orden 314159228780 y, por tanto, es un generador del grupo $E(\mathbb{F}_p)$
  - El punto $20 \cdot P = (228726321069, 127116812494)$ tiene orden 15707961439

Criptosistemas con curvas elípticas

ElGamal propone en 1985 un criptosistema basado en problema del logaritmo dicreto: en su artículo usa el grupo multiplicativo de un cuerpo finito $\mathbb{F}_p$

Koblitz y Miller proponen en 1987 el uso en criptografía de las curvas elípticas sobre cuerpos finitos

Criptosistemas tipo ElGamal

- Basados en la intratabilidad del *problema del logaritmo discreto*:

  PLD: Dado un grupo finito cíclico G, un generador g de G y un elemento x de G, encontrar el entero n tal que

  $$x = g^n$$

- Versión elíptica del problema del logaritmo dicreto:

  PLDE: Dada una curva elíptica E sobre $\mathbb{F}_p$, un generador P de un subgrupo cíclico G de puntos de $E(\mathbb{F}_p)$ y un punto Q de G, encontrar el entero n tal que

  $$Q = n \cdot P$$

Criptosistema ElGamal elíptico

Tiene rango normativo, es decir, forma parte de los estándares criptográficos, como el NIST: *National Institute of Standards and Technology*

- **Configuración del criptosistema**
  - Generar un primo p para definir el cuerpo $\mathbb{F}_p$
  - Escoger los parámetros a y b de la curva E sobre $\mathbb{F}_p$
  - Escoger un punto P de la curva cuyo orden sea un entero n que tenga un factor primo del tamaño de p
- **Clave privada** Un entero d en el intervalo $[1, n-1]$
- **Clave pública** El punto $Q = d \cdot P$ de la curva
- **Mensaje**

  El mensaje que se quiere cifrar se supone que se ha convertido en un número natural m, $0 < m < p$.

Cifrado ElGamal elíptico

Algoritmo (Cifrado criptosistema ElGamal elíptico)

INPUT: Los parámetros (p, a, b, P, n), la clave pública Q y el mensaje en claro m
OUTPUT: El mensaje cifrado $(\alpha_1, \alpha_2, \gamma)$

- Escoger un entero aleatorio r en $[1, n-1]$
- Calcular los puntos $r \cdot P = (\alpha_1, \alpha_2)$ y $r \cdot Q = (\beta_1, \beta_2)$ en $E_{a,b}(\mathbb{F}_p)$
- Calcular $\gamma = m \cdot \beta_1$ en $\mathbb{F}_p$
- Devolver $(\alpha_1, \alpha_2, \gamma)$

Descifrado ElGamal elíptico

Algoritmo (Descifrado criptosistema ElGamal elíptico)

INPUT: Los parámetros (p, a, b, P, n), la clave privada d y el mensaje cifrado $(\alpha_1, \alpha_2, \gamma)$

OUTPUT: El mensaje en claro m

- Calcular el punto $d \cdot (\alpha_1, \alpha_2) = d \cdot r \cdot P = r \cdot Q = (\beta_1, \beta_2)$ en $E_{a,b}(\mathbb{F}_p)$
- Obtener el mensaje en claro $m = \gamma \cdot \beta^{-1}$ en $\mathbb{F}_p$
- Devolver m

Ejemplo de cifrado con ElGamal elíptico

Adela enviará a Benito el mensaje $m = 1234567890$ cifrando con el esquema ElGamal elíptico de parámetros:

$$p = 314159265359,\ a = 102,\ b = 2005,$$
$$P = (228726321069, 127116812494),\ n = 15707961439$$

- Benito ha elegido su clave privada $d = 2718281828$ y ha hecho pública su clave $Q = d \cdot P = (218896057517, 64059238278)$.
- Adela escoge el entero $r = 2351458452$ en $[1, 15707961438]$
- Adela calcula los puntos $(\alpha_1, \alpha_2) = r \cdot P = (179839104564, 285023636671)$ y $(\beta_1, \beta_2) = r \cdot Q = (299109926557, 21259762324)$ en $E_{a,b}(\mathbb{F}_p)$
- Adela calcula $\gamma = m \cdot 299109926557 = 24770511096$ en $\mathbb{F}_p$
- Adela envía a Benito el mensaje $(\alpha_1, \alpha_2, \gamma)$, es decir,

$$(179839104564, 285023636671, 24770511096)$$

Ejemplo de descifrado con ElGamal elíptico

Benito descifra el mensaje

$$(\alpha_1, \alpha_2, \gamma) = (179839104564, 285023636671, 24770511096)$$

enviado por Adela cifrado con el esquema ElGamal elíptico de parámetros:

$$p = 314159265359,\ a = 102,\ b = 2005,$$
$$P = (228726321069, 127116812494),\ n = 15707961439$$

- Benito con su clave privada $d = 2718281828$ calcula en $E_{a,b}(\mathbb{F}_p)$ el punto $d\cdot(\alpha_1, \alpha_2) = (299109926557, 212597623624)$, que coincide con $r \cdot Q = (\beta_1, \beta_2)$
- Benito obtiene a partir de la abscisa β_1 el mensaje

$$m = \gamma \cdot \beta_1^{-1} = 1234567890$$

ElGamal elíptico vs ElGamal multiplicativo

- **Algoritmos generales para resolver el PLD**
  - Pasos de niño - pasos de gigante, ρ de Pollard,...
    tienen coste exponencial
  - Método de Pohlig-Hellman:
    para evitar este ataque es necesario que $n = \#(G)$ tenga un factor primo grande
- **Algoritmo específico para resolver el PLD sobre el grupo $\mathbb{F}_p^*$**
  - El ataque del *Index-Calculus* tiene coste subexponencial
- *Ventajas* **ElGamal elíptico**
  - Disminución del tamaño de las claves, garantizando misma seguridad
  - Amplio abanico de grupos sobre el mismo cuerpo base
- **Problemas por resolver...**
  - Encontrar curvas criptográficamente útiles

Tamaños de clave

Equivalencias: tamaños claves para obtener misma seguridad

PLD y RSA (bits)	PLDE (bits)	Ratio tamaño claves	AES (bits)
1024	163	1:6	
3072	256	1:12	128
7680	384	1:20	192
15360	512	1:30	256

Cuadro 1: NIST guidelines for public key sizes for AES

Dificultad del PLDE

Tiempo aproximado para resolver el PLD/PLDE con una máquina de capacidad computacional $450 \cdot 10^6$ operaciones básicas por segundo

- Aplicando Index-Calculus sobre $\mathbb{F}_p^*$, p de 160 bits, de coste $\mathrm{O}(e^{\sqrt{\log p \log \log p}})$

$$\text{coste} = 8{,}4 \cdot 10^9 \text{ operaciones básicas}$$
$$\text{tiempo} = \frac{\text{coste}}{450 \cdot 10^6} \approx 18 \text{ segundos}$$

- Aplicando ρ de Pollard sobre $E(\mathbb{F}_p)$, p de 160 bits, de coste $\mathrm{O}(\sqrt{n})$, $n = \#E(\mathbb{F}_p)$

$$\text{coste} = 1{,}2 \cdot 10^{24} \text{ operaciones básicas}$$
$$\text{tiempo} = \frac{\text{coste}}{450 \cdot 10^6 \cdot 60 \cdot 60 \cdot 24 \cdot 365} \approx 8{,}5 \cdot 10^7 \text{ años}$$

Firma digital con curvas elípticas: ECDSA

El algoritmo DSA (Digital Signature Algorithm) es una variante de la firma ElGamal

El algoritmo ECDSA es el análogo al algoritmo DSA con curvas elípticas

Algoritmo (Generación de firma digital del ECDSA)

INPUT: Los parámetros (p, a, b, P, n), la clave pública Q, la clave privada d y el mensaje en claro m

OUTPUT: El mensaje m con la firma (r, s)

- Calcular el Hash del mensaje: $h = H(m)$
- Escoger un entero aleatorio k en $[1, n-1]$
- Calcular el punto $k \cdot P = (x, y)$ en $E_{a,b}(\mathbb{F}_p)$
- Calcular $r = x \pmod{n}$ (si $r = 0$ ir al inicio)
- Calcular $s = k^{-1}(h + d \cdot r) \pmod{n}$ (si $s = 0$ ir al inicio)
- Devolver m y (r, s)

Verificación de firma con ECDSA

Algoritmo (Verificación de firma digital del ECDSA)

INPUT: Los parámetros (p, a, b, P, n), la clave pública Q, la clave privada d, el mensaje en claro m y la firma (r, s)

OUTPUT: Aceptación o rechazo de la firma

- Comprobar que r y s son enteros del intervalo $[1, n-1]$. En otro caso devolver *rechazar firma*
- Calcular el Hash del mensaje: $h = H(m)$
- Calcular el inverso w de s módulo n
- Calcular el punto $R = (w \cdot h) \cdot P + (w \cdot r) \cdot Q$ en $E_{a,b}(\mathbb{F}_p)$
- Si $R = \mathcal{O}$ devolver *rechazar firma*
- Si la abscisa módulo n del punto R coincide con r, devolver *aceptar firma*, sino devolver *rechazar firma*

Ejemplo generación de firma ElGamal

Benito enviará a Adela un mensaje m, cuyo hash es $h = H(m)$, firmado con el ECDSA usando los parámetros

$$p = 314159265359,\ a = 102,\ b = 2005,$$
$$P = (228726321069, 127116812494),\ n = 15707961439$$

- Benito ha elegido su clave privada $d = 2718281828$
- Benito calcula el hash de su mensaje m: sea pues $h(m) = 79135$
- Benito escoge el entero $r = 1618033988$ en $[1, 15707961438]$
- Benito calcula el punto $k \cdot P = (148171555207, 12849853842)$ en $E_{a,b}(\mathbb{F}_p)$
- Benito calcula $r = x \pmod n$ y obtiene $r = 6799902256$
- Benito calcula $k^{-1} \pmod n$ y obtiene $k^{-1} = 3016422147$
- Benito calcula $s = k^{-1}(h + d \cdot r) \pmod n$ y obtiene $s = 4363974999$
- Benito envía a Adela el mensaje m con la firma $(r, s) = (6799902256, 4363974999)$

Ejemplo verificación de firma ElGamal

Adela verificará que el mensaje recibido m con firma $(r, s) = (6799902256, 4363974999)$, ha sido enviado y firmado por Benito con el ECDSA usando los parámetros

$$p = 314159265359,\ a = 102,\ b = 2005,$$
$$P = (228726321069, 127116812494),\ n = 15707961439$$

- Benito ha hecho pública su clave $Q = d \cdot P = (218896057517, 64059238278)$.
- Adela calcula el hash de m y obtiene $h = H(m) = 79135$
- Adela calcula el inverso w de s módulo n y obtiene $w = 11808724700$
- Adela calcula en $E(\mathbb{F}_p)$ el punto

$$R = (w \cdot h) \cdot P + (w \cdot r) \cdot Q = (148171555207, 12849853842)$$

- Adela comprueba que la abscisa de R módulo n coincide con $r = 6799902256$ y, por tanto, que m que ha sido firmado por Benito

Curvas criptográficamente útiles

En los criptosistemas elípticos y en los esquemas de firma digital tipo ElGamal es necesario generar curvas sobre $\mathbb{F}_p$ cuyo cardinal tenga ciertas buenas condiciones:

- El cardinal del grupo de puntos $E(\mathbb{F}_p)$ sea de la forma $f \cdot q$, con q primo y f un entero *pequeño*
- La curva no debe ser *supersingular* (son las que tienen cardinal $p+1$)
- La curva no debe ser *anómala* (son las que tienen cardinal p)

El cálculo del cardinal de las curvas para comprobar que satisfacen las condiciones requeridas está resuelto teóricamente por el conocido **algoritmo de Schoof**:

- Tiene coste polinómico $O(\log^8 p)$, pero su implementación resulta inviable a efectos prácticos para primos p grandes
- La idea básica reside en calcular la traza t de la curva $E/\mathbb{F}_p$ módulo distintos primos pequeños ℓ convenientemente elegidos de manera que $\prod \ell > 4\sqrt{p}$
- Las ideas aportadas por Atkin y Elkies constituyen el cuerpo del denominado **SEA**

ECC challenges

Retos propuestos por Certicom: sobre el PLDE

Se denotan por ECCp-d, ECC2-d o ECC2k-d

- ECCp-d o ECC2-d: según curva elíptica definida sobre $\mathbb{F}_p$ o sobre $\mathbb{F}_{2^m}$ (con un subgrupo cíclico de orden d bits)
- ECC2k-d: cuando es una curva de Koblitz

Últimos retos resueltos:

- ECCp-97: En 1998 con 740 máquinas y 16000 años MIPS
- ECC2k-108: En 2000 con 9500 máquinas y 400000 años MIPS
- ECCp-109: En 2002 con 10000 máquinas
- ECC2k-109: En 2004, tardaron 17 meses con 2600 ordenadores

http://www.certicom.com/index.php?action=res,ecc_solution

ECC challenges por resolver

ECCp-131

======== ECCp-131 ========

p = 04 8E1D43F2 93469E33 194C4318 6B3ABC0B

seed$E$ = ECF764D6 96E67687 56151758 05744809 00C4742C

r = 01 F6CE5106 86622B77 6D651862 12A8E281

a = 04 1CB121CE 2B31F608 A76FC8F2 3D73CB66

b = 02 F74F717E 8DEC9099 1E5EA9B2 FF03DA58

h = 01

n = 04 8E1D43F2 93469E31 7F7ED728 F6B8E6F1

seed$P$ = 232881DF CF57E4D6 96E67687 5615175D 990B21A7

x = 03 DF84A96B 5688EF57 4FA91A32 E197198A

y = 01 47211619 17A44FB7 B4626F36 F0942E71

seed$Q$ = 2773E8F6 E4AE54D6 96E67687 56151755 2EA42393

x = 03 AA6F004F C62E2DA1 ED0BFB62 C3FFB568

y = 00 9C21C284 BA8A445B B2701BF5 5E3A67ED

- **Otros retos propuestos**: ECCp-163, ECCp-191, ECCp-239, ECC2k-130, ECC2-131, ECC2-163,...

Notaciones usadas en los ECC challenges

- Los valores de los parámetros están dados en base hexadecimal
- seed$E$ es la semilla usada en su algoritmo para generar un parámetro auxiliar r, a partir del cual se determinan los parámetros a y b de la curva E sobre $\mathbb{F}_p$
- seed$P$ y seed$Q$ son las semillas para generar las coordenadas (x, y) de cada uno de los puntos P y Q de $E(\mathbb{F}_p)$
- n es el orden del punto P y $n \cdot h$ el cardinal de $E(\mathbb{F}_p)$

El reto propuesto consiste en encontrar el logaritmo discreto de Q en la base P, es decir, el entero d tal que $Q = d \cdot P$

Software libre para usar curvas elípticas

Algunas librerías criptográficas en C o C++ que tienen un módulo de curvas elípticas:

Crypto++. Librería C++ con gran número de algoritmos criptográficos. Incluye principales primitivas con curvas elípticas. Disponible vía `http://www. cryptopp.com/`.

LibTomCrypt. Es una librería criptográfica desarrollada por Tom St Denis que tiene el algoritmo ECDSA de firma digital con curvas elípticas.

LiDIA. Es una librería de teoría de números computacional desarrollada por el grupo LiDIA de la Universidad Técnica de Darmstadt. Disponible vía `ftp.informatik.tu-darmstadt.de/pub/TI/systems/LiDIA`.

MIRACL. Es una *Multiprecision Integer and Rational Arithmetic C/C++ Library* que contiene algoritmos de clave compartida y clave pública.

NTL. Es una librería para hacer Teoría de Números que tiene un módulo criptográfico con curvas elípticas. Disponible vía `http://shoup.net/ntl/`.

OpenSSL. Librería criptográfica que tiene incorporado el ECDSA con curvas que siguen los estándares del NIST y ANSI. Disponible vía `http://www.opensource.org`.

Fin del capítulo

Cuestiones y ejercicios (1 de 2)

1. Consideremos la curva elíptica E sobre $\mathbb{F}_{11}$ de ecuación $y^2 = x^3 + x + 1$.
   - i) Encontrar todos puntos de la curva E (14 en total contando el punto del infinito) y comprobar que el punto $P = (3, 3)$ tiene orden 7.
   - ii) Si queremos cifrar y descifrar mensajes con el esquema ElGamal elíptico con parámetros $(p, a, b, P, n) = (11, 1, 1, 3, 3, 7)$ y hemos elegido como clave privada $d = 4$, ¿cuál es nuestra clave pública?
   - iii) Cifrar el mensaje $m = 9$ con la clave pública del apartado anterior.

2. Consideremos la curva elíptica $y^2 = x^3 + 333x + 2$ sobre el cuerpo $\mathbb{F}_{347}$ y el punto $P = (110, 136)$ de la curva.
   - i) Sabiendo que el orden de la curva es 358, ¿podemos decir que la curva es criptográficamente buena? ¿Cuál es el orden del punto? ¿Entre qué posibles valores se puede escoger la clave secreta?
   - ii) Si habéis escogido vuestra clave secreta y vuestra clave pública, ¿es posible que os llegue el mensaje cifrado $(\alpha_1, \alpha_2, \gamma) = (1, 9, 312)$? Si un amigo os quiere enviar el mensaje $m = 73$, dar dos posibles mensajes cifrados con vuestra clave pública que os podría enviar.
   - iii) Hacer los cálculos correspondientes para descifrar uno de los mensajes que os ha enviado vuestro amigo.

Cuestiones y ejercicios (2 de 2)

1. Queremos enviar un mensaje cifrado a Adela cifrando con el esquema ElGamal elíptico de parámetros

$$p = 314159, \quad a = 217, \quad b = 2006$$
$$P = (123456, 43989), \quad n = 314423$$

El mensaje que le queremos enviar está formado por las dos primeras inciales de nuestro nombre. Para ello, miramos en la tabla de 128 carácteres del código ASCII las codificaciones correspondientes a dichas letras.

i) Determinar el entero m que se obtiene al considerar la representación decimal de las dos primeras iniciales del nombre en base 128.

ii) Cifrar el mensaje m con la clave pública $Q = (198903, 289358)$ de Adela.

iii) Supongamos que Adela tiene que firmar el mensaje $m = 6000$ (cantidad de euros que quiere retirar de su cuenta mediante transferencia). Generar, sin usar ninguna función hash, la firma digital de m.

iv) ¿Qué cómputos hará el banco para verificar la firma de Adela?