CatioCrypto 2025: Curvas Elípticas

26-27 Septiembre 2025

Autor Emanuel Nicolás Herrador
Speaker Armando Faz Hernandez

1 Introducción

1.1 Criptografía simétrica

Clave compartida k entre A y B para intercambiar cifrados. El tercero no puede leerlos sin saber k. El estándar para este tipo de cifrado es el AES (cifrado por bloques). Hay 3 variantes según tamaño de llave (128, 192, 256) y también según el modo que se usa.

Nota. Algoritmos como DES o RC4 usados antes, ya son vulnerables y se conoce cómo romperlos.

Los modos, por ejemplo, son CBC (encadenado por bloques), CTR (counter mode), GCM (Galois counter mode). Este último se usa para cifrado autenticado.

1.2 Función de resumen

Mapean cadenas de bits de tamaño arbitrario en cadeas de tamaño fijo, i.e., $h : \{0,1\}^* \to \{0,1\}^n$. Esta es conocida como función de resumen o hash.

Definición 1.1 (Funciones hash criptográficas)**.** Dada una función hash h, esta es criptográfica si los siguientes problemas son "difíciles":

- **1era Preimagen**: Dado un resumen r, encontrar mensaje M tal que $r = h(M)$
- **2da Preimagen**: Dado un mensaje M_1, encontrar un mensaje diferente M_2 tal que $h(M_1) = h(M_2)$
- **Resistencia a colisón**: Encontrar dos mensajes diferentes M_1, M_2 tal que $h(M_1) = h(M_2)$

Nota. El conjunto de estándares usado es SHA (Secure Hash Algorithm). Dependiendo el tipo de salida son SHA-0, SHA-1, SHA-2 o SHA-3.

También existen funciones con salida extendible (resúmenes de tamaño arbitrario, i.e., vos elegís el tamaño que querés que tenga), las cuales son SHAKE128 y SHAKE256. Notar que no son funciones de resumen.

1.3 Criptografía de llave pública

Se basa en funciones que son fáciles de calcular pero difíciles de invertir. Algunos ejemplos son RSA, Diffie-Hellman los cuales se basan en factorización de primos y logaritmo discreto respectivamente.

1.4 Teoría de grupos

Definición 1.2 (Grupo)**.** Dado un conjunto no vacío G y operación binaria $*$, $(G, *)$ es un grupo si cumple:

- **Cerrado**: $\forall a, b \in G,\ a * b \in G$
- **Asociativo**: $\forall a, b, c \in G,\ (a * b) * c = a * (b * c)$
- **Identidad**: $\exists e \in G : \forall a \in G,\ e * a = a$ (con e identidad)
- **Inversos**: $\forall a \in G, \exists b \in G : a * b = e$

El grupo es conmutativo si $\forall a, b \in G,\ a * b = b * a$.

Definición 1.3 (Subgrupo)**.** Dado un grupo $(G, *)$, si $H \subseteq G$ y $(H, *)$ es un grupo, entonces es un subgrupo.

Los términos exponenciación de grupo y multiplicación escalar son usados indistintamente. Sin embargo, si el grupo es conmutativo se acostumbra a usar la notación aditiva $(+)$.

Definición 1.4 (Grupo cíclico)**.** Un grupo es cíclico si puede ser generado por un elemento del grupo. Denotamos por $\langle g \rangle$ al grupo generado por $g \in G$:

$$\langle g \rangle = \{g^k : k \in \mathbb{Z}\}$$

Nota. Si se habla del orden de G, es el número de elementos de G. Si se habla del orden de g, este es el número de elementos de $\langle g \rangle$

1.4.1 Logaritmo discreto

Definición 1.5 (Logaritmo discreto)**.** Dado G grupo cíclico generado por g, sabemos que $\forall h \in G, \exists k \in \mathbb{Z} : h = g^k$. El logaritmo discreto de h con respecto a g es la operación que dados g, h obtiene $k = \log_g(h) \in \mathbb{Z}$.

Nota. Puesto que g genera $n = |\langle g \rangle|$ elementos, entonces $k \in \{0, \ldots, n-1\}$.

DLP (problema del logaritmo discreto) Dados $g, h \in G : h = g^k$, encontrar el k.

Si este problema es difícil, entonces nos puede servir para la criptografía de llave pública. Algunos algoritmos para resolverlo son:

- Paso de bebé, paso de gigante
- Cálculo del índice
- Algoritmo de Pohlig-Hellman
- Algoritmo Rho de Pollard
- Algoritmo de Shor

2 Curvas Elípticas

Definición 2.1 (Curva Ellíptica - Forma general)**.** Una curva elíptica está definida sobre un cuerpo k por la ecuación

$$E/k : \ y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$$

donde $a_i \in k$ con $i = 1, 2, 3, 4, 6$ y tal que su discriminante cumple $\Delta \neq 0$.

Nota. Notar que cada punto tiene a lo sumo dos valores en el eje vertical.

Existen modelos que representan algunas curvas elípticas:

- *Weierstrass* (Modelo más general): $y^2 = x^3 + ax + b$
- *Montgomery* (Curvas con punto de orden 2): $y^2 = x^3 + ax^2 + bx$
- *Twisted Edwards* (Punto de orden 4): $ax^2 + y^2 = 1 + dx^2y^2$
- *Twisted Hessian*, *intersecciones de Jacobi*, *Kummer*, etc.

Vamos a trabajar con el modelo de Weierstrass.

Teorema 2.1 (Teorema de Hasse)**.** *La cantidad de puntos N de una curva elíptica E sobre $\mathbb{F}_q$ cumple que* $|N - (q+1)| \leq 2\sqrt{q}$

Nota. Con esto, existen algoritmos para hallar N dados E y $\mathbb{F}_q$, como otros para hallar E dados N y $\mathbb{F}_q$.

2.1 Curvas elípticas como grupo

Definición 2.2 (Grupo de curva elíptica)**.** El conjunto de puntos racionales sobre k de la curva E es denota como $E(k) = \{(x, y) \in E\} \cup \{O\}$ donde O es el punto al infinito. Los puntos de la curva forman un grupo $(E(k), +)$ con O como la identidad del grupo.

A continuación podemos ver diferentes operaciones en este grupo. Se puede hacer algebraicamente pero veamos un par de ejemplos geométricos.

Suma de puntos Consideramos P, Q puntos en la curva. Para calcular $P + Q$, geométricamente hacemos:

1. Trazar la recta que pasa por P y Q
2. Sea R el 3er punto que interseca a la curva, trazamos la recta vertical allí
3. El punto donde se interseca ahora es $P + Q$

Nota. Sale de la idea de que, sean P, Q, R los puntos que una recta interseca a la curva, entonces $P+Q+R = 0$. Luego, $-R = P + Q$ y también se cumple que si $R = (x_R, y_R)$ entonces $-R = (x_R, -y_R)$.

Doblado de puntos Es el caso especial de suma si queremos hacer $P + P = 2P$. Para ello, la recta que usamos es la tangente a la curva que pasa por P y el procedimiento sigue igual que antes.

Multiplicación escalar Dado $P \in E, k \in \mathbb{Z}$, la multiplicación escalar es $kP = \overbrace{P + \cdots + P}^{k \text{ veces}}$. Existen algoritmos lineales en la cantidad de bits que lo calculan como el de *Montgomery* que escanea del más al menos significativo y el de *Joye* que lo hace al revés. (la idea de este último es similar a la de exponenciación binaria).

Logaritmo discreto en curvas elípticas (ECDLP) Dados $P, Q \in E : Q = kP$, queremos encontrar k. El algoritmo de Pollard es el mejor algoritmo conocido para resolver ECDLP cuya complejidad es $O\left(\sqrt{\#E(\mathbb{F}_p)}\right)$ donde $\#E(\mathbb{F}_q) \approx p$ es el número de puntos de la curva.

Nota. Este es un problema fuerte de resolver y es lo que vamos a usar para hacer criptografía. Por ejemplo, si $p \approx 2^{256}$ entonces se requieren de 2^{128} operaciones para resolverlo.

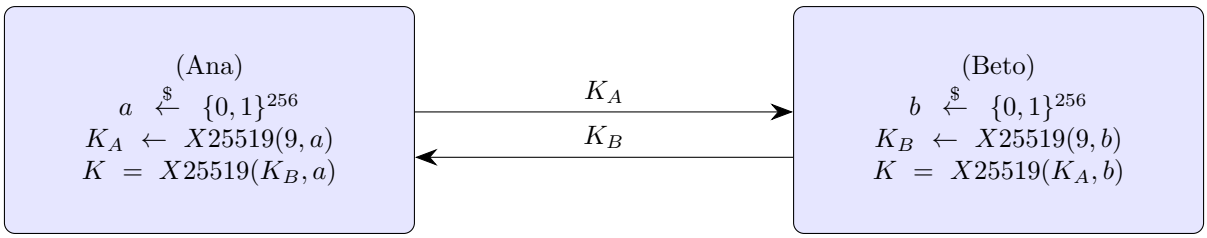
Este problema se resuelve con el *algoritmo cuántico de Shor* (aunque aún no hay computadoras cuánticas relevantes que rompan la criptografía actual).

3 Curvas Elípticas en criptografía

Koblitz y Miller sugirieron ECC para criptografía. Esta brinda un nivel de seguridad equivalente a RSA usando llaves más pequeñas (por ej., para un nivel de seguridad de 128 bits, RSA necesita llaves de 3072 bits mientras que ECC 256 bits). Otro uso fue el de Montgomery, el cual utilizó curvas para criptoanálisis (factorización de enteros).

3.1 Protocolo Diffie-Hellman con Curvas de Montgomery

El $RFC - 7748$ define dos funciones para calcular un secreto compartido: $X25519$ (llaves de 32 bytes) y $X448$ (llaves de 56 bytes). El esquema es el siguiente (donde K es la llave compartida):



Nota. Internamente, X calcula una multiplicación escalar.

TODO: Completar con el uso de curvas en firmas (ECDSA) que mencionó en las filminas.

3.2 Aplicaciones

Algunas aplicaciones de ECC son:

- Protocolos de internet (DNS y DNSSEC, TLS y PKI, SSH, IPSec)
- Cifrado end to end
- Blockchain (Smart contracts, virtual machines, computación verificable)
- Autenticación
- Autorización
- Pruebas de conocimiento

4 Libros recomendados

La lista de libros recomendados es:

- Guide to Elliptic Curve Cryptography
- Handbook of Elliptic and Hyperelliptic Curve Cryptography
- The Arithmetic of Elliptic Curves
- Introduction to Elliptic Curves
- Elliptic Curve Cryptography for Developers