

Criptografía y Blockchain

Módulo 2

Criptografía asimétrica

Criptografía asimétrica

- Los algoritmos de cifrado asimétricos usan dos claves, una clave pública y la otra privada. La clave privada se usa para cifrar, y la pública para descifrar.
- Son necesarias cuando es difícil o imposible enviar una clave simétrica a través de un canal inseguro.
- Es muy lenta comparado al cifrado simétrico, y sus claves son más grandes. El mensaje cifrado es mayor al texto plano.
- Mientras que las claves simétricas no tienen estructura, son flujos de bytes aleatorios, **las claves asimétricas tienen estructura, poseen varios componentes que deben cumplir ciertos requisitos.**
- Se usa para cifrado/descifrado, para generar claves y para firmar.

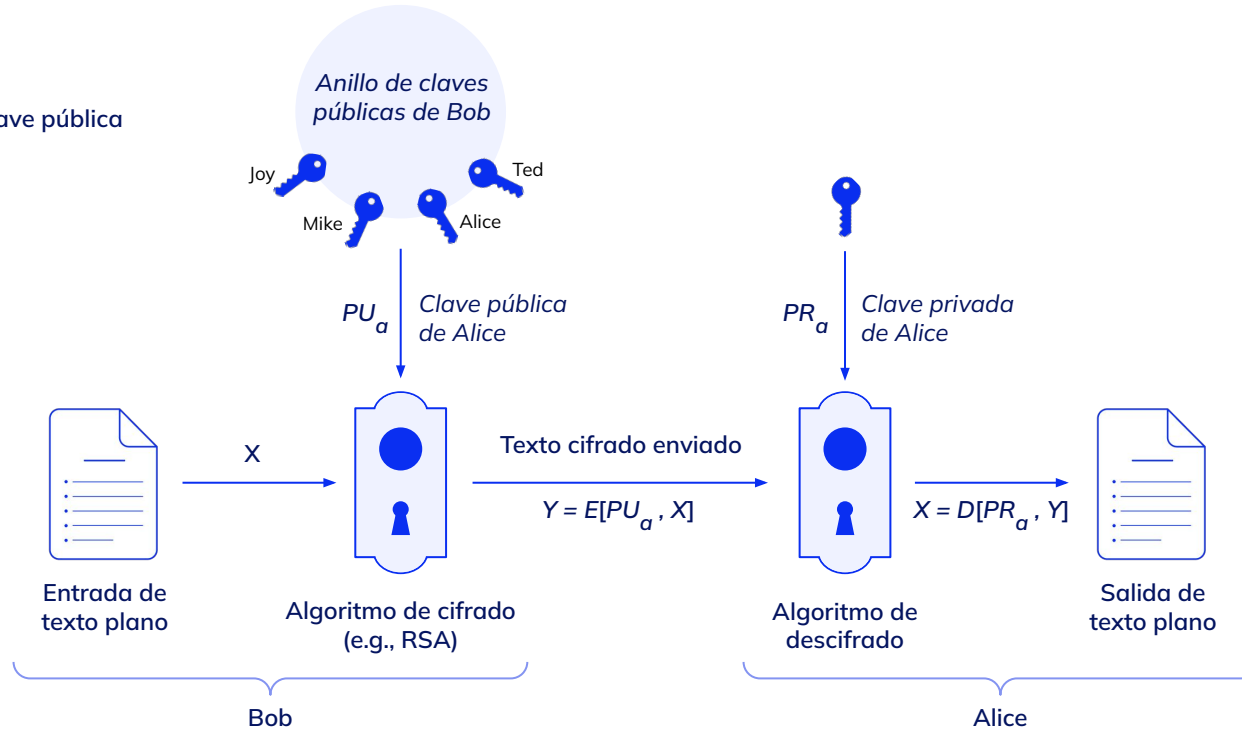
Esquema HPKE

Los cifrados asimétricos son mucho más lentos. Por eso, en una conexión remota, se suelen usar para cifrar claves asimétricas y poder enviar dichas claves al receptor y luego usar esta clave simétrica para cifrar la comunicación. Este esquema de cifrado se conoce como **esquema híbrido de clave pública (HPKE)**.



Esquema de cifrado asimétrico

(a): Cifrado con clave pública



Algoritmo RSA

Debe su nombre a sus tres inventores: **Ronald Rivest, Adi Shamir y Leonard Adleman**, y estuvo bajo patente del MIT hasta el 20 de septiembre de 2000, por lo que su uso comercial estuvo restringido hasta esa fecha.

Clifford Cocks, un matemático británico de la agencia de inteligencia británica GCHQ, había descrito un sistema equivalente en un documento interno en 1973. Su descubrimiento, sin embargo, no fue revelado hasta 1997 ya que era confidencial, por lo que Rivest, Shamir y Adleman desarrollaron RSA de forma independiente.

La seguridad de RSA descansa en la dificultad **en factorizar enteros grandes como el producto de dos números primos**. Ambas claves contienen un módulo, un exponente, y opcionalmente primos y coeficientes. Los números enteros usados tienen cientos o miles de dígitos. El tamaño de la clave RSA es el tamaño de módulo.

RSA tiene un rendimiento pobre, que cae muy rápidamente. Cuando doblamos el tamaño de la clave en el rango 1024-4096 el cifrado/firmado es 7 veces más lento y el descifrado/verificado es 3 veces más lento.


Los bloques de datos cifrados tienen el mismo tamaño que la clave. Considerando que se usa usualmente para cifrar claves simétricas y IV, el texto cifrado suele ser de mayor tamaño al texto plano.

Por ejemplo


Una clave simétrica de 256 bits y un IV de 128 bits se suele cifrar con una clave de 2048 bits.

El tamaño de la firma RSA es el estándar PKCS#1 que tiene el mismo tamaño de la clave RSA. Firmas más largas son problemáticas.

Es importante remarcar que el nivel de seguridad es mucho menor al tamaño de la clave. La siguiente es una lista estimada por NIST.



RSA key size in bits	Security level in bits
1,024	80
2,048	112
3,072	128
4,096	152
7,680	192
8,192	200
15,360	256

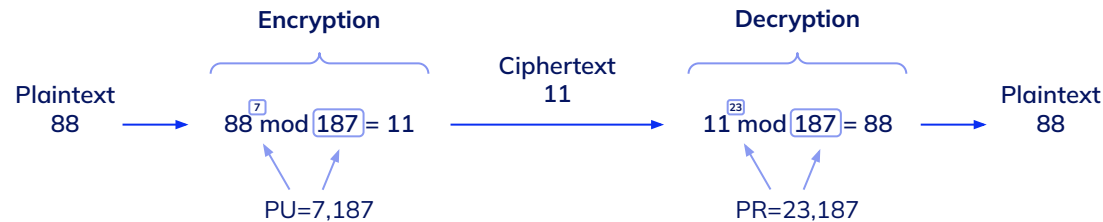


¿Qué tamaño elegir? NIST recomienda:

- Al menos 2048 bits hasta 2030.
- Al menos 3072 bits después de 2030.

Cuando lleguen las computadoras cuánticas, el cifrado asimétrico estará completamente roto. Se cree que no sucederá antes del 2030.

Ejemplo de implementación



Curvas elípticas

La **criptografía de curva elíptica** es una de las disciplinas con mayor importancia en el campo de los cifrados asimétricos. Constituyen un formalismo matemático conocido y estudiado desde hace más de 150 años.

Presentan una serie de propiedades que da lugar a **problemas difíciles de resolver análogos a los de la aritmética modular**, lo cual permite adaptar a ellas algunos de los algoritmos asimétricos más conocidos.



Las primeras propuestas de uso de las curvas elípticas fueron hechas por Neal Koblitz y Victor Miller en 1985.

Si bien su estructura algebraica es algo compleja, su implementación suele resultar tanto o más eficiente que la de la aritmética modular, con la ventaja adicional de que se pueden alcanzar niveles de seguridad análogos con claves mucho más cortas.

Los algoritmos criptográficos se desarrollan en base al problema de los logaritmos discretos en las curvas elípticas.

Existen diversas recomendaciones de curvas elípticas concretas, con aplicaciones en Criptografía. Cada una de ellas consta de una **curva específica**, con sus correspondientes parámetros, más un punto base p , que genera el conjunto que se usa en los cálculos.

En algunos casos, las curvas propuestas presentan propiedades que las hacen más eficientes, o más resistentes a algunos tipos de ataques.

Secp256k1 es una curva propuesta originalmente por Certicom Research, esta curva es la que se emplea en la red Bitcoin.

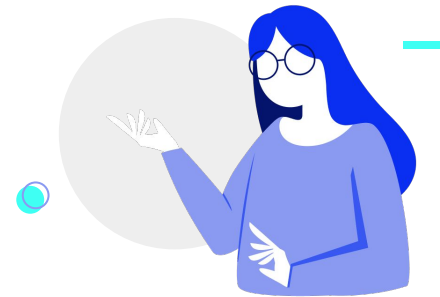
Curve25519 fue propuesta por Daniel J. Bernstein en 2006, esta curva es en la actualidad una de las que da lugar a implementaciones más eficientes en términos computacionales. Presenta mayor resistencia a los ataques basados en tiempo de computación y de consumo energético.

Existen versiones de curva elíptica de alguno de los algoritmos asimétricos más populares, como los algoritmos de ElGamal y Diffie-Hellman.



Otros algoritmos

- **RSA:** es el algoritmo más importante. Es el único que permite cifrar datos directamente.
- **DSA** (*Digital Signature Algorithm*) y **ECDSA** (*Elliptic Curve Digital Signature Algorithm*): pueden utilizarse para firmas digitales.
- **DH** (*Diffie-Hellman*) y **ECDH** (*Elliptic Curve Diffie-Hellman*): pueden ser usados para intercambio de claves en el protocolo TLS (*Transport Layer Security*).
- **ElGamal:** utiliza un algoritmo DH con claves DSA o un algoritmo ECDH con claves ECDSA para cifrado asimétrico. Involucra una clave efímera (temporal) DSA/ECDSA adicional para el intercambio de la clave secreta compartida (clave de sesión).



Claves de sesión

Una sesión tiene lugar en una red, y **empieza cuando dos dispositivos se reconocen mutuamente** y abren una conexión virtual.

Termina cuando los dos dispositivos han obtenido la **información que necesitan** el uno del otro y envían los mensajes de cerrar_notificar.

La conexión también puede terminar debido a la inactividad.



Una clave de sesión es cualquier clave criptográfica simétrica utilizada para **encriptar una sola sesión de comunicación**.

Una **clave de sesión es temporal**, y solo se utiliza una vez, durante un tramo de tiempo, para encriptar y descifrar datos enviados entre dos partes.

Las futuras conversaciones entre partes se encriptarían con claves de sesión diferentes.

En protocolos de redes seguros tales como TLS, SSH o IPsec, la sesión de comunicación inicia con el **handshaking**, en el cual se produce una operación de intercambio de claves.

En las versiones antiguas de estos protocolos, se utilizaba el esquema de cifrado híbrido (HPKE).

En las versiones actuales de estos protocolos se utiliza el **intercambio de claves DH o ECDH** donde se deriva la misma clave de sesión para luego cifrar la comunicación.



El **algoritmo ElGamal** utiliza un algoritmo DH con claves DSA, o un algoritmo ECDH con claves ECDSA para cifrado asimétrico.

ElGamal involucra la creación de claves efímeras (temporales) DSA/ECDSA para establecer un secreto compartido del cual se deriva una clave asimétrica para cifrar la comunicación.

Otro esquema similar es el **Esquema de Cifrado Integrado (IES)**, posee dos variantes:

- Esquema de cifrado integrado de logaritmo discreto (DLIES).
- Esquema de cifrado integrado de curva elíptica (ECIES).

Ejemplo de claves de sesión

A continuación, un ejemplo de intercambio de claves **Diffie-Hellman** (DH) o **Diffie-Hellman de curva elíptica** (ECDH):

Alice y Bob se ponen de acuerdo en usar el número primo $q=353$ y una raíz $a=3$.

Alice elige su clave privada $X_a=97$ y Bob la suya, $X_b=233$.

Cada uno calcula su clave pública:

- $Y_a = 3^{97} \bmod 353 = 40$
- $Y_b = 3^{233} \bmod 353 = 248$

Alice y Bob intercambian sus claves públicas y calculan la clave privada común:

- Alice calcula

$$K = (Y_b)^{X_a} \bmod 353 = 248^{97} \bmod 353 = 160.$$

- Bob calcula

$$K = (Y_a)^{X_b} \bmod 353 = 40^{233} \bmod 353 = 160.$$

**¡Sigamos
trabajando!**

