



Algoritmos asimétricos

Introducido por Whitfield Diffie y Martin Hellman a mediados de los años 70.

El sistema de cifrado de clave pública usa un par de claves para el envío de mensajes. Las dos claves pertenecen a la misma persona a la que se ha enviado el mensaje. Una clave es *pública* y se puede entregar a cualquier persona. La otra clave es *privada* y el propietario debe guardarla para que nadie tenga acceso a ella. El remitente usa la clave pública del destinatario para cifrar el mensaje, y una vez cifrado, sólo la clave privada del destinatario podrá descifrar este mensaje.



Algoritmos asimétricos - Diffie-Hellman

Este algoritmo nos permite compartir un mensaje cifrado entre dos actores que no han tenido contacto previo; por esta razón suele utilizarse para acordar una clave de cifrado a través de un canal inseguro y sin autenticación.

Sean **A** y **B** los interlocutores en cuestión. En primer lugar, se calcula un número primo **p** y un generador **z** de \mathbb{Z}^* , con $2 \leq z \leq p - 2$. Esta información es pública y **p** conocida por ambos. El algoritmo queda como sigue:

1. **A** escoge un número aleatorio **x**, comprendido entre **1** y **p - 2** y envía a **B** el valor

$$i = z^x \pmod{p}$$

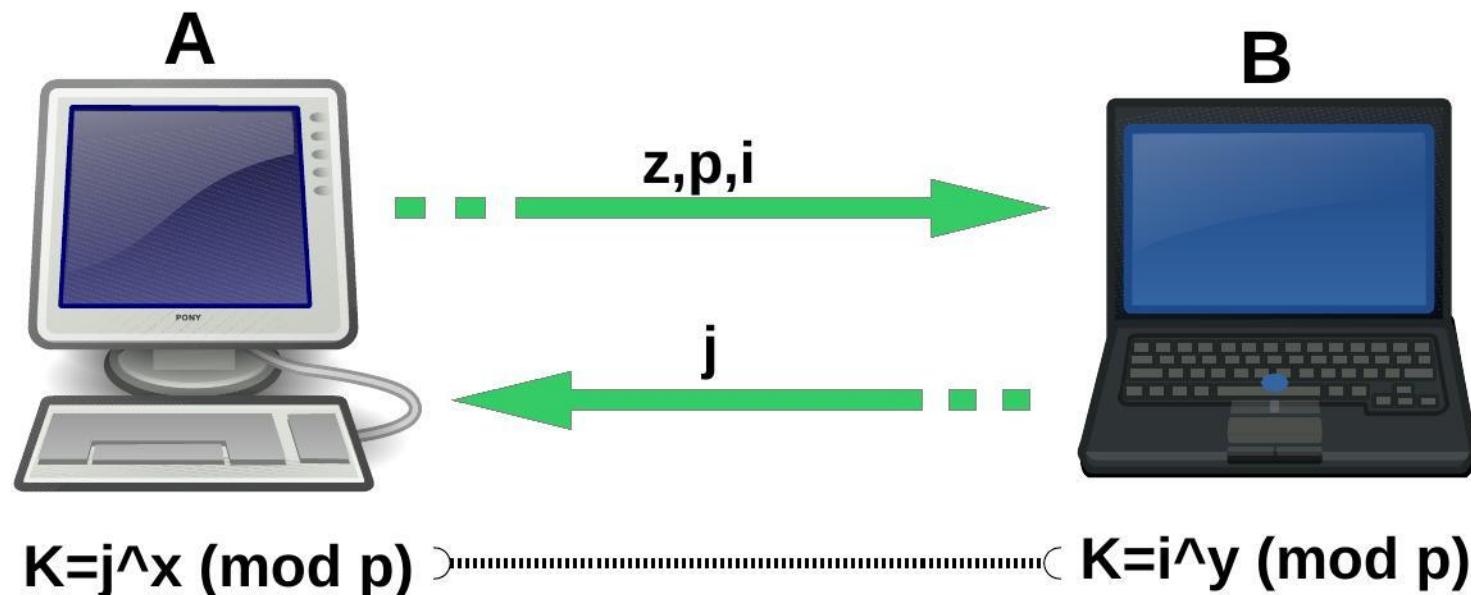
2. **B** escoge un número aleatorio **y**, análogamente al paso anterior, y envía a **A** el valor

$$j = z^y \pmod{p}$$



Algoritmos asimétricos - Diffie-Hellman

3. B recoge i y calcula $K = i^y \pmod{p} = (z^x \pmod{p})^y \pmod{p}$.
4. A recoge j y calcula $K = j^x \pmod{p} = (z^y \pmod{p})^x \pmod{p}$.
5. Conclusión $K = z^{xy} \pmod{p}$





Algoritmos asimétricos - Diffie-Hellman

p=31
z=12

j = 10

y = 26
 $j = 12^{26} \pmod{31} = 10$

x = 6
 $i = 12^6 \pmod{31} = 2$

i = 2

Clave = $i^y \pmod{31} = 2^{26} \pmod{31} = 2$

Clave = $j^x \pmod{31} = 10^6 \pmod{31} = 2$



Algoritmos asimétricos – Diffie-Hellman – Multiples actores

Las partes (Alicia, Brenda y Carlos) disponen de los valores compartidos para los parámetros de algoritmo **p** y **g**. Cada actor definirá su valor privado al que llamaremos con el nombre **a,b,c** respectivamente.

- 1) Alicia calcula $g^a \text{ mod } p$ y lo envía a Brenda.
- 2) Brenda calcula $(g^a)^b \text{ mod } p = g^{ab} \text{ mod } p$ y lo envía a Carlos.
- 3) Carlos calcula $(g^{ab})^c \text{ mod } p = g^{abc} \text{ mod } p$ y la usa como su clave secreta.
- 4) Brenda calcula $g^b \text{ mod } p$ y lo envía a Carlos.
- 5) Carlos calcula $(g^b)^c \text{ mod } p = g^{bc} \text{ mod } p$ y lo envía a Alicia.
- 6) Alicia calcula $(g^{bc})^a \text{ mod } p = g^{bca} \text{ mod } p = g^{abc} \text{ mod } p$ y lo usa como su clave secreta.
- 7) Carlos calcula $g^c \text{ mod } p$ y lo envía a Alicia.
- 8) Alicia calcula $(g^c)^a \text{ mod } p = g^{ca} \text{ mod } p$ y lo envía a Brenda.
- 9) Brenda calcula $(g^{ca})^b \text{ mod } p = g^{cab} \text{ mod } p = g^{abc} \text{ mod } p$ y lo usa como su clave secreta.



Algoritmos asimétricos

Ejemplos

- Diffie-Hellman
- RSA
- ElGamal
- DSA
- ECC, Criptografía de curva elíptica (ECDH, ECDSA...)



Algoritmos asimétricos - Cifrado

Ventajas

- No requiere confidencialidad en la distribución de clave
- La misma clave puede ser utilizada por múltiples actores en la comunicación
- Permite autenticar mensajes

Desventajas

- Velocidad de cifrado/descifrado
- Longitud de mensaje limitado
- Tamaño del mensaje cifrado es mayor
- Se requieren claves de gran extensión



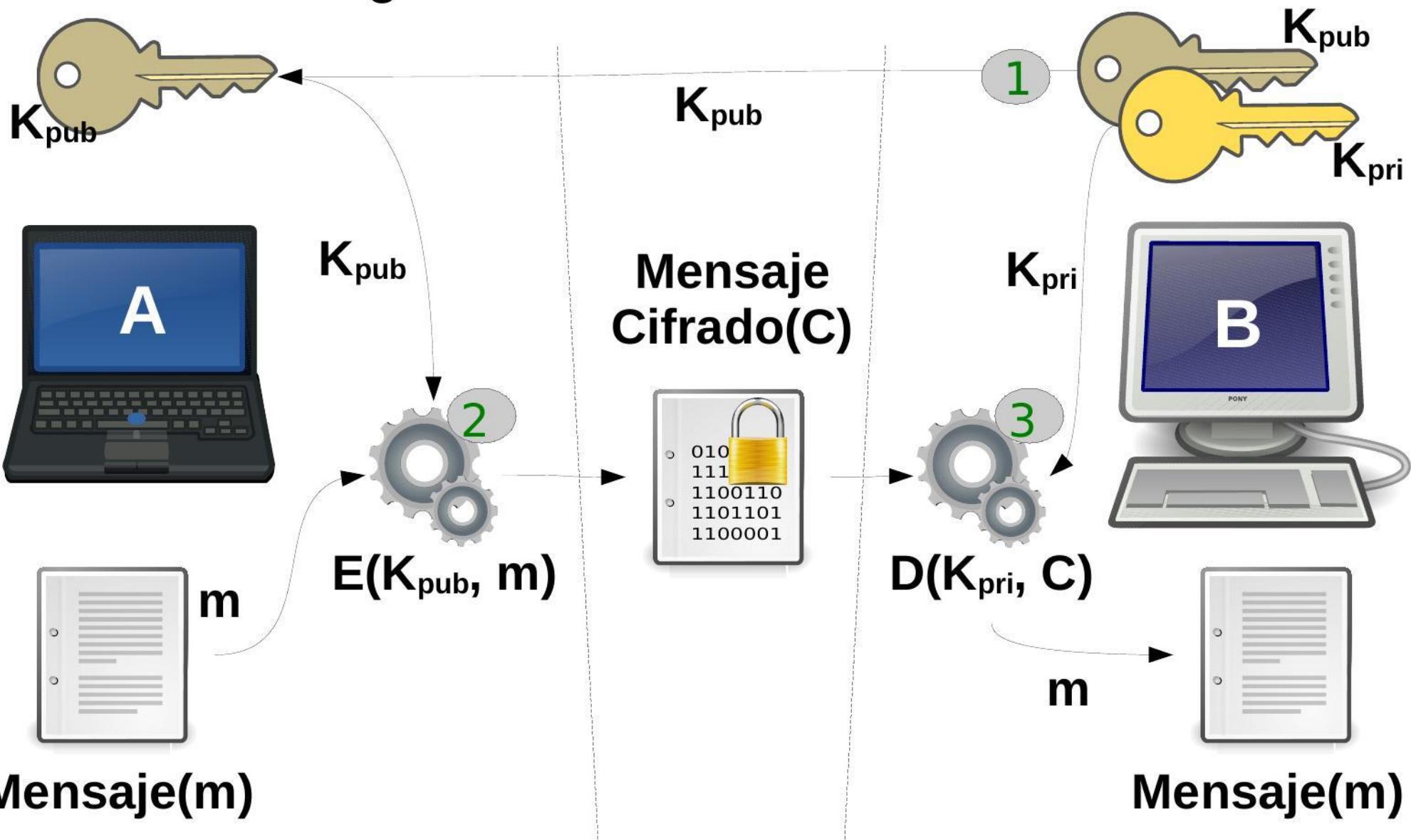
Algoritmos asimétricos - Cifrado

Este tipo de algoritmos suelen disponer de las siguientes operaciones:

1. Generación de claves
2. Cifrado
3. Descifrado
4. Firma
5. Verificación de firma



Algoritmos asimétricos - Cifrado





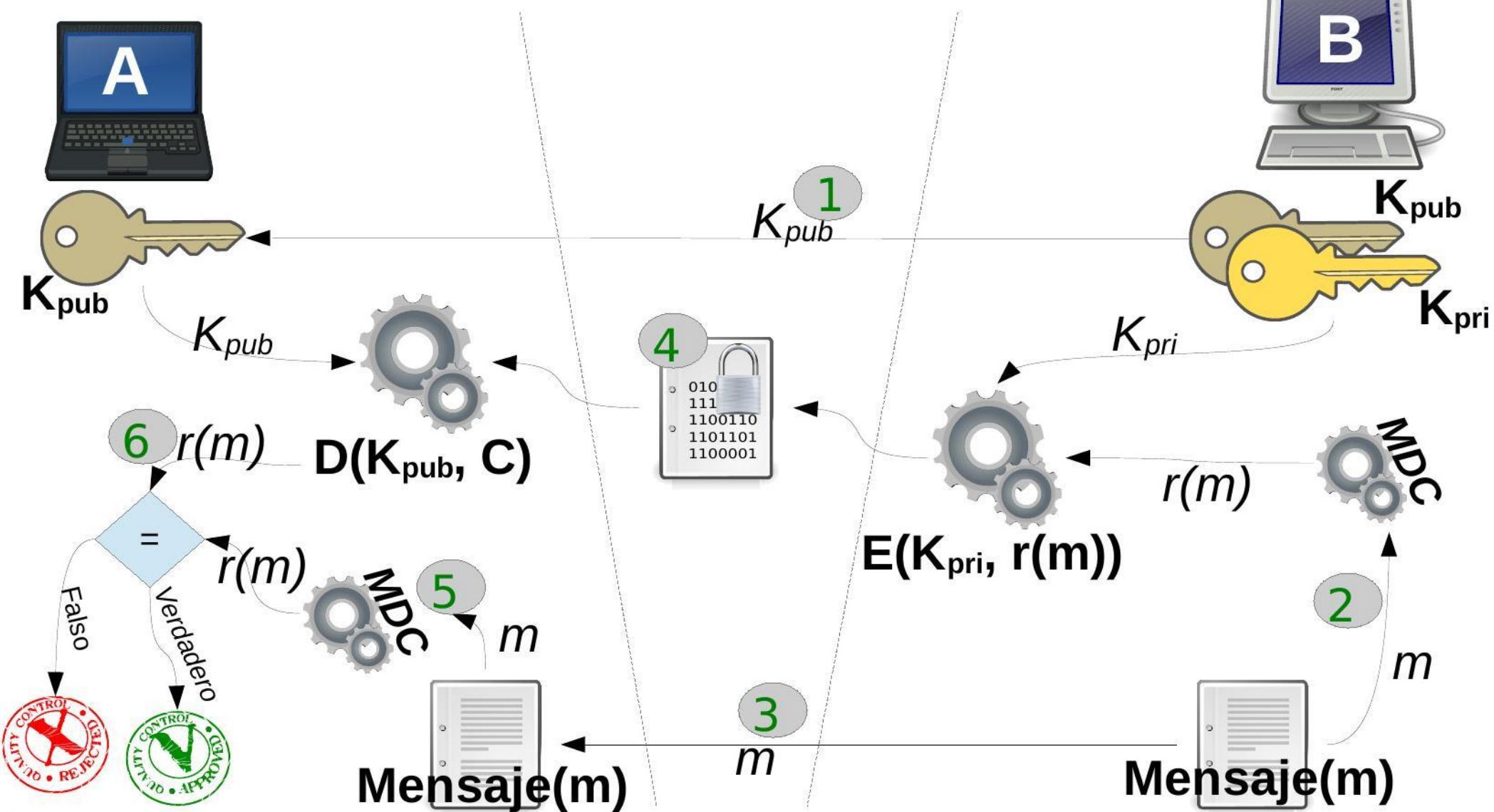
Algoritmos asimétricos - Autentificación

Autentificación de mensaje (Firma)

Algunos algoritmos asimétricos permiten que se pueda autenticar un mensaje para garantizar su integridad. en este caso la clave que se emplea para cifrar es la clave privada, justo al revés que para la simple codificación de mensajes.



Algoritmos asimétricos - Autentificación





Algoritmos asimétricos - RSA

- Su nombre deriva de Ronald Rivest, Adi Shamir y Leonard Adleman
- Fue publicado en 1977
- Estuvo bajo patente de los Laboratorios RSA hasta el 20 de septiembre de 2000
- Se basa en la dificultad para factorizar grandes números



Algoritmos asimétricos - RSA

Se eligen aleatoriamente dos números primos grandes, p y q . Después se calcula el producto $n = pq$. Escogeremos ahora un número e primo relativo con $(p - 1)(q - 1)$. (e, n) sera la clave publica. Nótese que e debe tener **inversa modulo $(p - 1)(q - 1)$** , por lo que existirá un número d tal que

$$\begin{aligned}de &\equiv 1 \pmod{(p - 1)(q - 1)} \\de &\equiv 1 \pmod{\text{lcm}(p - 1, q - 1)}\end{aligned}$$

es decir, que d es la inversa de e modulo $(p-1)(q -1)$. (d, n) sera la clave privada. Esta inversa puede calcularse fácilmente empleando el Algoritmo Extendido de Euclides.

Nótese que si desconocemos los factores de n , este cálculo resulta prácticamente imposible.



Algoritmos asimétricos – RSA

Elección de números primos

p=3

q=11

n=3 * 11 = 33

phi(n) = (3-1)*(11-1) = 2*10 = 20

Elección del componente publico

e = 7 (Primo relativo entre 1 y phi(n))

Buscar de 1 a phi(n) el componente privado, para el valor 3 el calculo es:

e * d=1 mod(phi(n))

7 * d = 1 mod (20)

7 * 3 = 1 mod (20)

21 mod 20 = 1

d = 3

**Clave Pública: (e, n) o (7, 33)
Clave Privada: (d, n) o (3, 33)**



Algoritmos asimétricos - RSA

La operación de cifrado se lleva a cabo según la expresión:

$$c = m^e \pmod{n}$$

mientras que el descifrado se hará de la siguiente forma:

$$m = c^d \pmod{n}$$



Algoritmos asimétricos - RSA

Ejemplos de operación sobre el mensaje con valor **2**

$$\begin{aligned}c &= m^e \pmod{n} \\c &= 2^7 \pmod{33} \\c &= 128 \pmod{33} = 29\end{aligned}$$

Descifrado para el valor **29**

$$\begin{aligned}m &= c^d \pmod{n} \\m &= 29^3 \pmod{33} \\m &= 24389 \pmod{33} = 2\end{aligned}$$



Algoritmos asimétricos - RSA

Firmas Digitales de RSA

Para firmar un mensaje h con la clave privada se procede de la siguiente manera:

$$s = h^d \pmod{n}$$

La firma generada se verifica obteniendo el valor de origen con la clave pública mediante el siguiente método:

$$h = s^e \pmod{n}$$



Algoritmos asimétricos - ElGamal

Se basa en el problema de los logaritmos discretos

Se conoce como logaritmo discreto de x en base a módulo n a resolver la ecuación $x=a^y \text{ mod } n$ donde x, n y a son constantes e y es la incógnita. A partir de ahora notamos esta situación como:

$$y = \log_{\text{disc}_a}(x)$$

El hecho de aplicar aritmética modular hace el problema de hallar y irresoluble en un tiempo razonable



Algoritmos asimétricos - ElGamal

Para generar un par de claves, se escoge un número primo **n** y dos números aleatorios **p** y **x** menores que **n**. Se calcula entonces

$$y = p^x \pmod{n}$$

La clave pública es **(p, y, n)**, mientras que la clave privada es **x**.



Algoritmos asimétricos - ElGamal

Número primo seleccionado al azar

n = 17

Números complementarios menores que n, elegidos al azar

p=3

x=6

Calculo del valor para el componente público

$$y=p^x \bmod(n)$$

$$y=3^6 \bmod(17)$$

$$\mathbf{y=15}$$

**Clave Pública: (p, y, n) o (3, 15, 17)
Clave Privada: (p, x, n) o (3, 6, 17)**



Algoritmos asimétricos - ElGamal

Cifrado de ElGamal

Para cifrar el mensaje **m** se escoge primero un número aleatorio **k** primo relativo con **(n – 1)**, que también será mantenido en secreto. Calculamos entonces las siguientes expresiones

$$\begin{aligned} a &= p^k \pmod{n} \\ b &= y^k m \pmod{n} \end{aligned}$$

El par **(a, b)** es el texto cifrado, de doble longitud que el texto original. Para decodificar se calcula

$$m = b \cdot a^{-x} \pmod{n}$$



Algoritmos asimétricos - ElGamal

Ejemplo de cifrado de ElGamal

Para cifrar el mensaje **m** con el valor **9** y un **k** aleatorio con valor **5** se procede de la siguiente manera:

$$\begin{aligned} a &= p^k \bmod(n) \\ a &= 3^5 \bmod(17) = 5 \\ b &= y^k m \bmod(n) \\ b &= 15^5 * 9 \bmod(17) = 1 \end{aligned}$$

El par **(5, 1)** es el texto cifrado, que podrá descifrarse de la siguiente forma

$$\begin{aligned} m &= b \cdot a^{-x} \bmod(n) \\ m &= 1 * 5^{-6} \bmod(17) = 9 \end{aligned}$$



Algoritmos asimétricos - ElGamal

Firmas de ElGamal

Para firmar un mensaje **m** basta con escoger un número **k** aleatorio, que sea primo relativo con **n - 1**, y calcular

$$\begin{aligned} a &= p^k \pmod{n} \\ b &= (m - xa)k^{-1} \pmod{(n - 1)} \end{aligned}$$

La firma la constituye el par **(a, b)**. En cuanto al valor **k**, debe mantenerse en secreto y ser diferente cada vez. La firma se verifica comprobando que

$$y^a a^b = p^m \pmod{n}$$



Algoritmos asimétricos - DSA

El algoritmo DSA (Digital Signature Algorithm) es una parte del estándar de firma digital DSS (Digital Signature Standard), definido en el FIPS-186. Este algoritmo, propuesto por el NIST, data de 1991, es una variante del método asimétrico de ElGamal.



Algoritmos asimétricos - DSA

Creación del par clave pública-clave privada

1. Seleccionar un número primo q tal que $2^{159} < q < 2^{160}$.
2. Escoger t tal que $0 \leq t \leq 8$, y seleccionar un número primo p tal que $2^{511+64t} < p < 2^{512+64t}$, y que ademas q sea divisor de $(p - 1)$.
3. Seleccionar un elemento $g \in \mathbb{Z}_p^*$ y calcular $\alpha = g^{(p-1)/q} \bmod p$.
4. Si $\alpha = 1$ volver al paso 3.
5. Seleccionar un número entero aleatorio a , tal que $1 \leq a \leq q - 1$
6. Calcular $y = \alpha^a \bmod p$.
7. La clave pública es (p, q, α, y) . La clave privada es a .



Algoritmos asimétricos - DSA

Generación de la firma

Siendo h la salida de una función MDC sobre el mensaje m , la generación de una firma se hace mediante el siguiente algoritmo:

1. Seleccionar un número aleatorio k tal que $0 < k < q$.
2. Calcular $r = (\alpha^k \bmod p) \bmod q$.
3. Calcular $k^{-1} \bmod q$.
4. Calculate $s = k^{-1} (h + ar) \bmod q$.
5. La firma del mensaje m es el par (r, s) .



Algoritmos asimétricos - DSA

Verificación de la firma

El destinatario efectuar las siguientes operaciones, suponiendo que conoce la clave pública (p , q , α , y), para verificar la autenticidad de la firma:

1. Verificar que $0 < r < q$ y $0 < s < q$. En caso contrario, rechazar la firma.
2. Calcular el valor de h a partir de m .
3. Calcular $\omega = s^{-1} \bmod q$.
4. Calcular $u_1 = \omega \cdot h \bmod q$ y $u_2 = \omega \cdot r \bmod q$.
5. Calcular $v = (\alpha^{u_1} y^{u_2} \bmod p) \bmod q$.
6. Aceptar la firma si y solo si $v = r$.



Algoritmos públicos y privados

Los algoritmos públicos son aquellos cuya definición y funcionamiento se ponen a disposición pública, permitiendo que cualquier persona o entidad acceda al mismo para su evaluación o investigación.

En contraparte los privados son aquellos cuyo funcionamiento interno es desconocido; en el ámbito de la criptografía estos últimos son considerados menos confiables.

Nota: Las patentes pueden condicionar el uso de ambos tipos de algoritmos