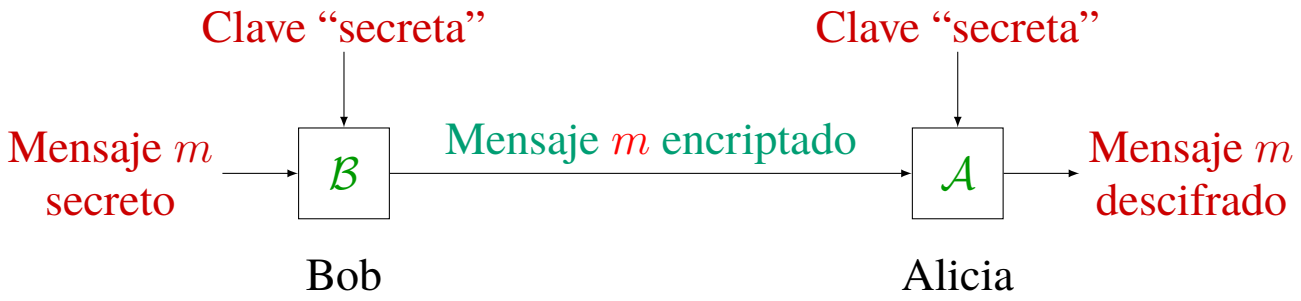
Criptografía RSA

Computación Cuántica: Algorítmica y Software

Joaquín Keller

2026 UCV

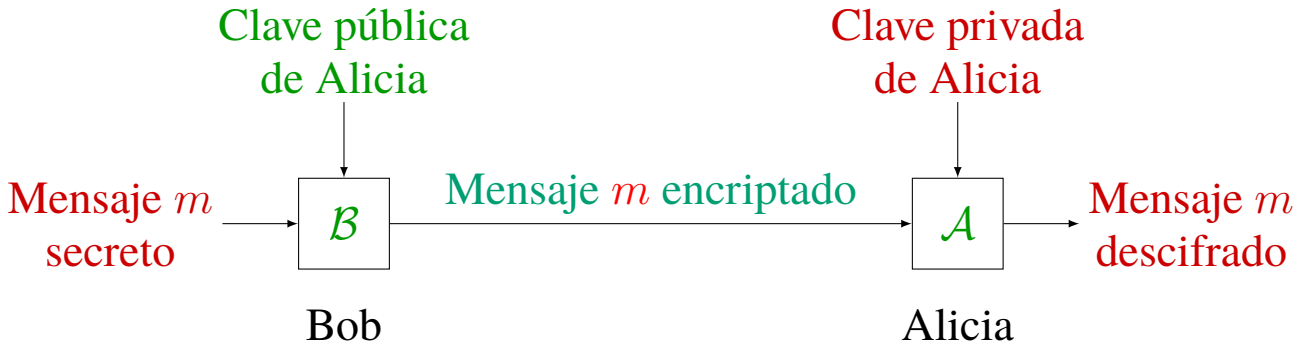
Criptografía de clave secreta o simétrica



Problema: Cómo hacen Bob y Alicia para comunicarse la clave secreta ya que no tienen (todavía) un canal de comunicación secreto

Distribución cuántica de claves (QKD): generación de claves secretas

Criptografía de clave publica



Uso: autenticación, transmisión/generación de claves simétricas

RSA, curvas elípticas (el algoritmo de Shor rompe esos dos métodos)

Autenticación con criptografía de clave pública

Problema: Bob quiere asegurarse que está comunicando con Alicia

1. Bob recupera la clave pública de Alicia en un lugar de confianza
2. Bob le manda un mensaje m encriptado a Alicia
3. Bob y Alicia calculan $h = hash(m)$
4. Alicia le transmite h a Bob por un canal público
5. Bob verifica que h es correcto

$hash(m)$ es fácil de calcular — $hash^{-1}(h)$ es "imposible" de calcular
$hash(m) = hash(m') \implies m = m'$ (casi siempre)

RSA generar las claves

1. Alicia genera p y q primos
   para generar un número primero: generar números al azar...
   ...hasta dar con uno primo (test de primalidad)
2. Calcular $n = pq$ (conseguir p y q a partir de n es 'imposible')
3. Calcular $\varphi(n) = (p-1)(q-1)$
4. Escoger un e tal que $mcd(e, \varphi(n)) = 1$
   empezar con $e = 3$ calcular el mcd, si no es ok, ensayar $e = 5$, etc...
5. Calcular d el inverso de e módulo $\varphi(n)$: $ed \equiv 1 \pmod{\varphi(n)}$

La clave pública es n, e la clave privada es d

RSA-2048: n y d tienen 2048 bits $2^{2048} \simeq 10^{617}$

RSA encriptar/descifrar un mensaje

La clave pública está compuesta del modulus n y del exponente e

Un mensaje es un entero positivo $m < n$

El mensaje encriptado es $x \equiv m^e \pmod{n}$

La clave privada es d

Para descifra el mensaje $m \equiv x^d \pmod{n}$

Demostración de RSA (1)

Teorema de Euler: $\boxed{mcd(a,n) = 1 \implies a^{\varphi(n)} \equiv 1 \pmod{n}}$

Lo que queremos demostrar es:

Si $\boxed{x \equiv m^e \pmod{n}}$ entonces $m \equiv x^d \pmod{n}$

Por definición de d: $ed \equiv 1 \pmod{\varphi(n)} \Leftrightarrow \exists k \in \mathbb{Z}$ $\boxed{ed = 1 + k\varphi(n)}$

Supongamos que $mcd(m,n) = 1$ (las alternativas son $p|m$ o $q|m$)

Por el teorema de Euler: $\boxed{m^{\varphi(n)} \equiv 1 \pmod{n}}$

Demostración de RSA (2)

$x \equiv m^e \pmod{n}$ $\quad ed = 1 + k\varphi(n)$ $\quad m^{\varphi(n)} \equiv 1 \pmod{n}$

$$x^d \equiv (m^e)^d \equiv m^{ed} \equiv m^{1+k\varphi(n)} \equiv m\,(m^{\varphi(n)})^k \equiv m\,(1)^k \equiv m \pmod{n}$$

Si $mcd(m,n) \neq 1$ entonces $p|m$ o $q|m$ pero no las dos cosas
Supongamos $p|m$ entonces $mcd(m,q) = 1$
por Euler $m^{\varphi(q)} \equiv 1 \pmod{q}$

$$m^{ed} \equiv m^{1+k\varphi(n)} \equiv m^{1+k\varphi(p)\varphi(q)} \equiv m\,(m^{\varphi(q)})^{k\varphi(p)} \equiv m\,(1)^{k\varphi(p)} \equiv m \pmod{q}$$

$m \equiv 0 \pmod{p}$ y $m^{ed} \equiv 0 \pmod{p}$ es decir que $m^{ed} \equiv m \pmod{p}$

Demostración de RSA (3)

$m^{ed} \equiv m \pmod{p}$ y $m^{ed} \equiv m \pmod{q}$ entonces $m^{ed} \equiv m \pmod{n}$

$a \equiv b \pmod{p} \wedge a \equiv b \pmod{q} \implies a \equiv b \pmod{pq}$

$a - b = kp \wedge q|(a - b) \Rightarrow q|kp \Rightarrow q|k \Rightarrow k = k'q$

$a - b = k'qp \implies a \equiv b \pmod{pq}$

$m^{ed} \equiv m \pmod{n} \wedge x^d \equiv m^{ed} \pmod{n}$ es decir $x^d \equiv m \pmod{n}$

Ejemplo RSA

Alicia (generación de claves):

$p = 5$ $q = 11$ $n = pq = 55$ $\varphi(n) = (p-1)(q-1) = 40$

$e = 3$ $mcd(\varphi(n), e) = 1$ $\varphi(n)$ y e son coprimos

$d = 27$ d es inverso módulo $\varphi(n)$ de e $27 \times 3 \equiv 81 \equiv 1 \pmod{40}$

Clave pública: $(n, e) = (55, 3)$ clave privada: $d = 27$

Bob: mensaje $m = 41$ $x \equiv m^e \equiv 41^3 \equiv 68921 \equiv 6 \pmod{55}$

Bob: manda el mensaje encriptado $x = 6$ a Alicia

Alicia: recibe x $m \equiv x^d \equiv 6^{27} \equiv 6^{1+2+8+16} \equiv 41 \pmod{55}$