UNIVERSIDAD PONTIFICIA ICAI ICADE COMILLAS MADRID

Seguridad Informática

Capítulo 05: Criptografía asimétrica

Titulación: Ingeniero en Informática.
Curso 5º - Cuatrimestral (2007-2008)

Javier Jarauta Sánchez
Rafael Palacios Hielscher
José María Sierra

Tema 11: Criptografía

- Introducción y conceptos básicos
- Historia de la criptografía asimétrica
- Criptografía de clave pública (asimétrica)
- Algoritmos asimétricos: Diffie-Hellman, RSA
- Aplicaciones: SSL, Firma electrónica

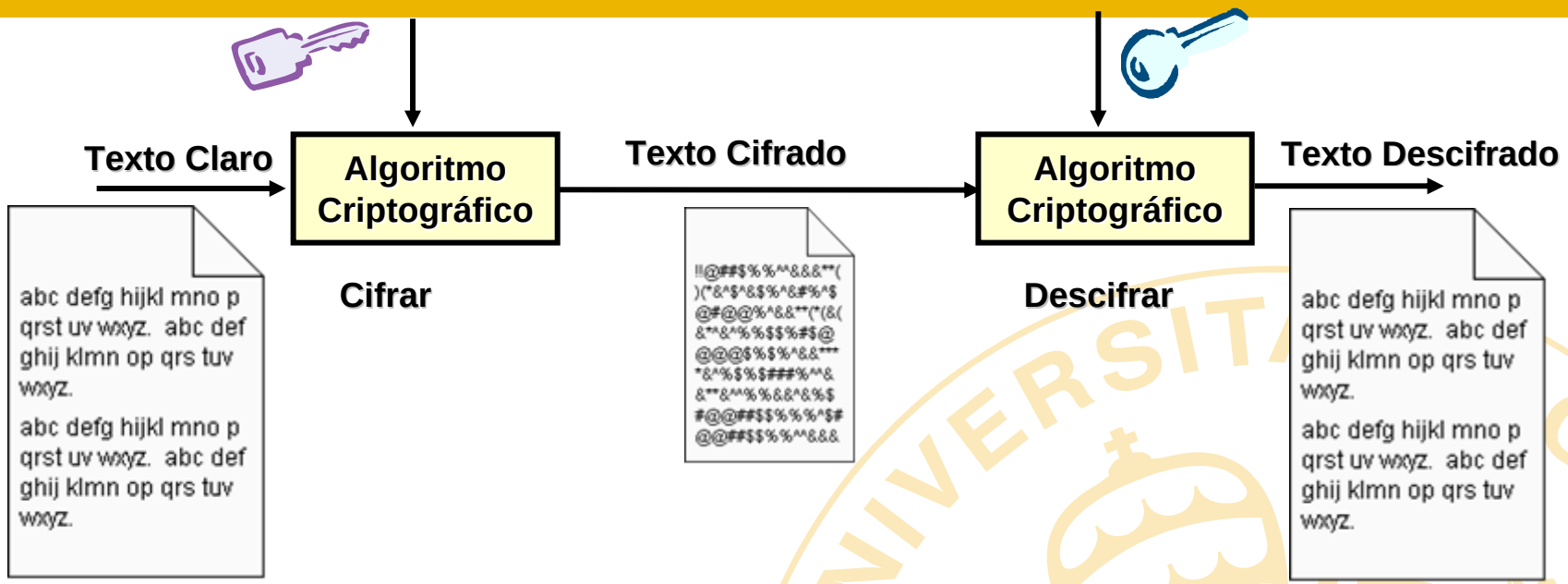
Historia de la criptografía

- Data Encryption Standard (DES)
  - 1975. IBM Lucifer para NIST
- Diffie-Hellman (DH)
  - 1976. New Directions in Cryptography
- Rivest-Shamir-Addleman (RSA)
  - 1977. Válido para firma y cifrado
- Digital Signature Algorithm (DSA)
  - 1991. Desarrollado por NSA para NIST

Tipos de algoritmos criptográficos

- Asimétricos. Clave Pública
  - Utiliza dos claves diferentes, una para cifrar y otra para descifrar
  - Ambas están relacionadas, y de una no puede deducirse la otra
  - Una se mantiene en secreto y la otra se publica
  - Se utilizan para cifrado, autenticación y negociación automática de claves

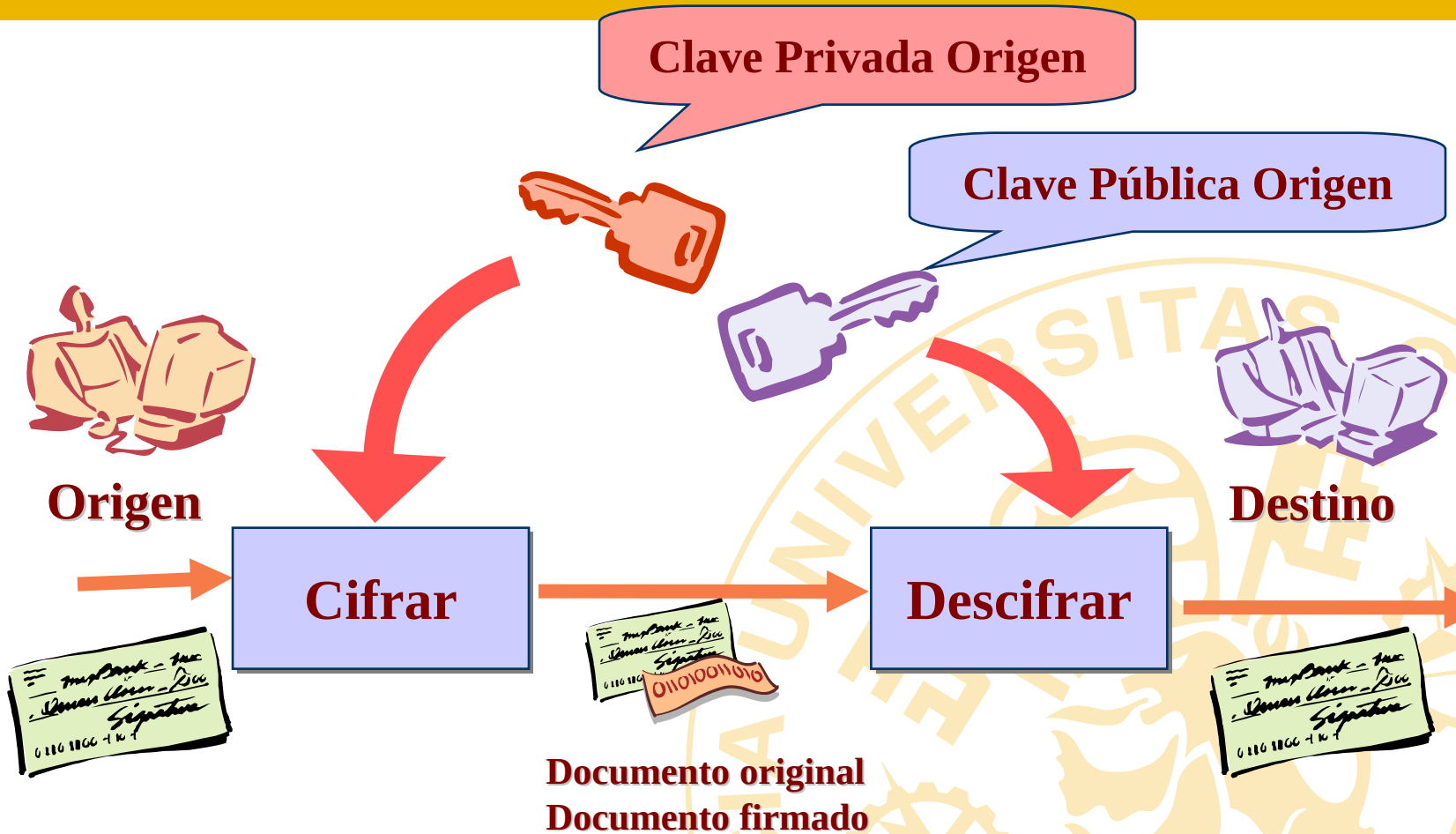
Algoritmos Asimétricos o de Clave Pública



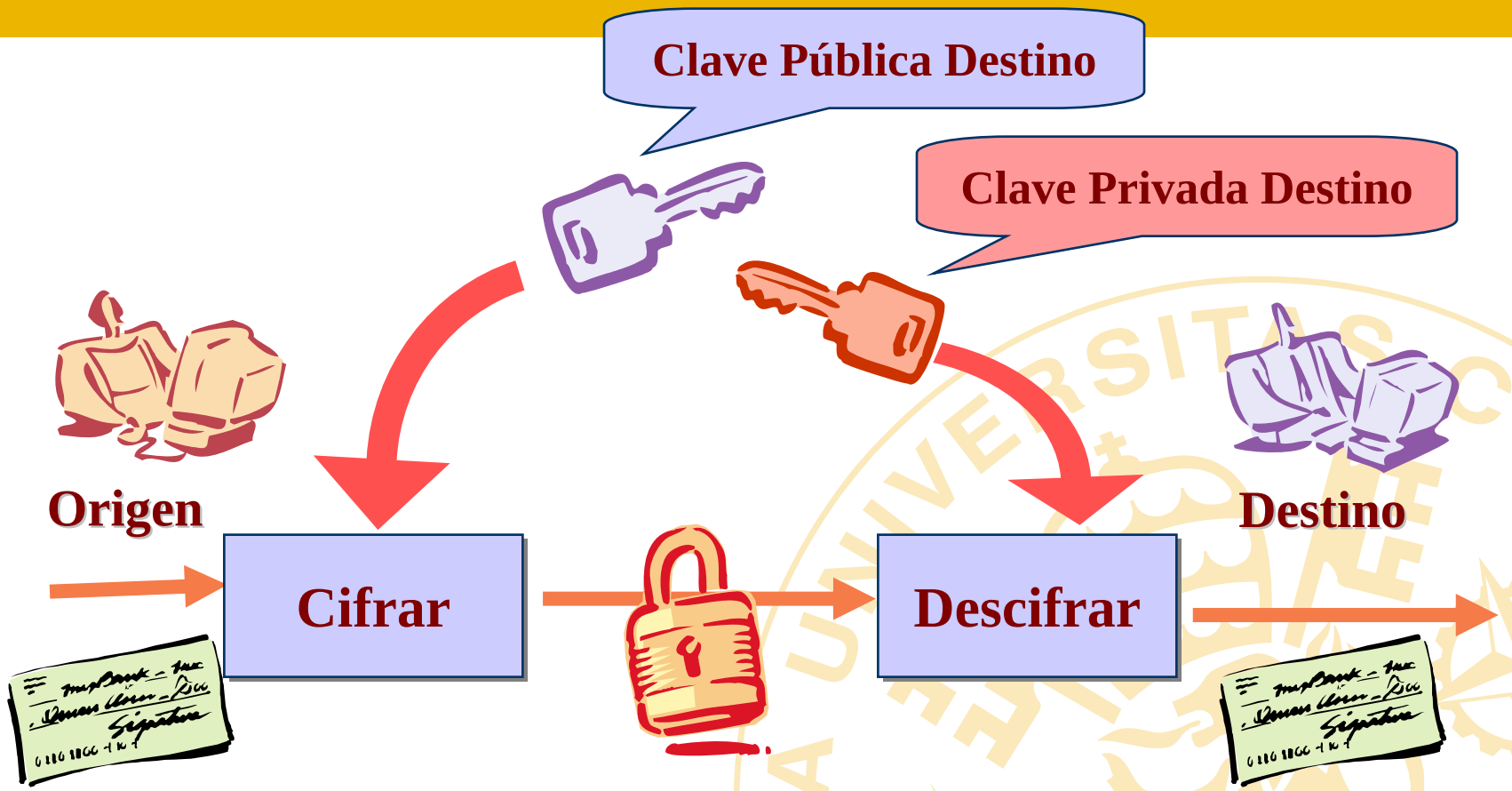
- Utiliza dos claves diferentes matemáticamente relacionadas.
- Lo que una cifra la otra lo descifra, y viceversa.
- Conociendo una, no puede deducirse la otra
- Una de las claves se hace pública y la otra se mantiene privada.
- Fortaleza: Facilita la gestión de claves, permite firma electónica
- Debilidades: Muy lento, ineficiente para grandes cantidades de datos
- Ejemplos: DH, RSA, PGP

Criptografía de Clave Pública (Asimétrica)

Autenticación con claves públicas



Confidencialidad con claves publicas



Algoritmos asimétricos

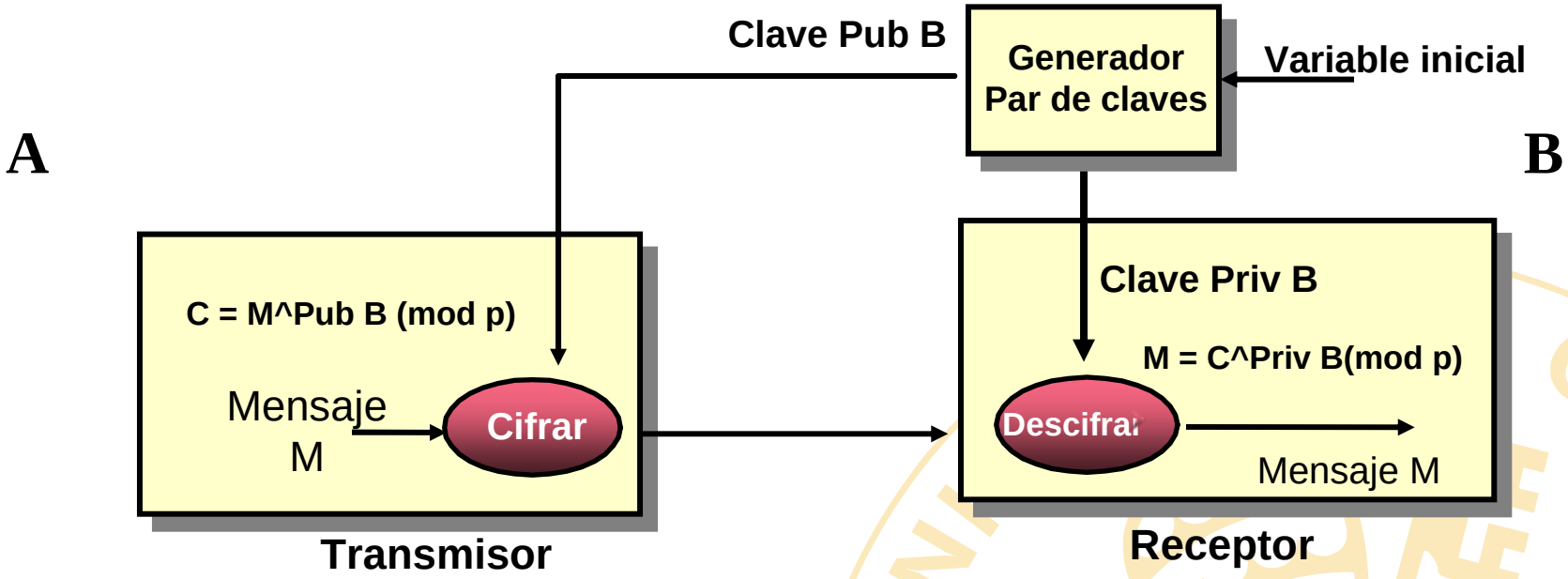
- **RSA**:
  - Diseñado en 1977 por Rivest, Shamir y Adleman
  - Utiliza claves de 512, 768, 1024 o 2048 (típico 1024)
  - Basado en la complejidad de factorizar enteros muy grandes
  - Utilizado mayoritariamente para firmar
- **DH**:
  - Diseñado en 1977 por Diffie y Hellman.
  - Claves de 512, 1024
  - Basado en las propiedades de los logaritmos discretos
  - Utilizado mayoritariamente para negociar claves
  - Necesita autenticación adicional (man-in-the-middle)

Algoritmos Asimétricos

- **El Gammal**:
  - Diseñado en 1984 por Taher ElGamal
  - Puede realizar cifrado y firma
  - Basado en la dificultad de calcular logaritmos discretos

- **DSA - Digital Standard Algorithm**:
  - Diseñado por el NIST (National Institute of Standards and Techonology)
  - Inicialmente se utilizaban claves de 512 y posteriormente se incrementó a 1024 para mayor seguridad
  - Es una variante de Schnorr y ElGamal

Algoritmos de exponenciación



Los algoritmos criptográficos exponenciales cifran y descifran según la siguiente formula:

$$C = M^{P_{ubE}} \bmod p$$

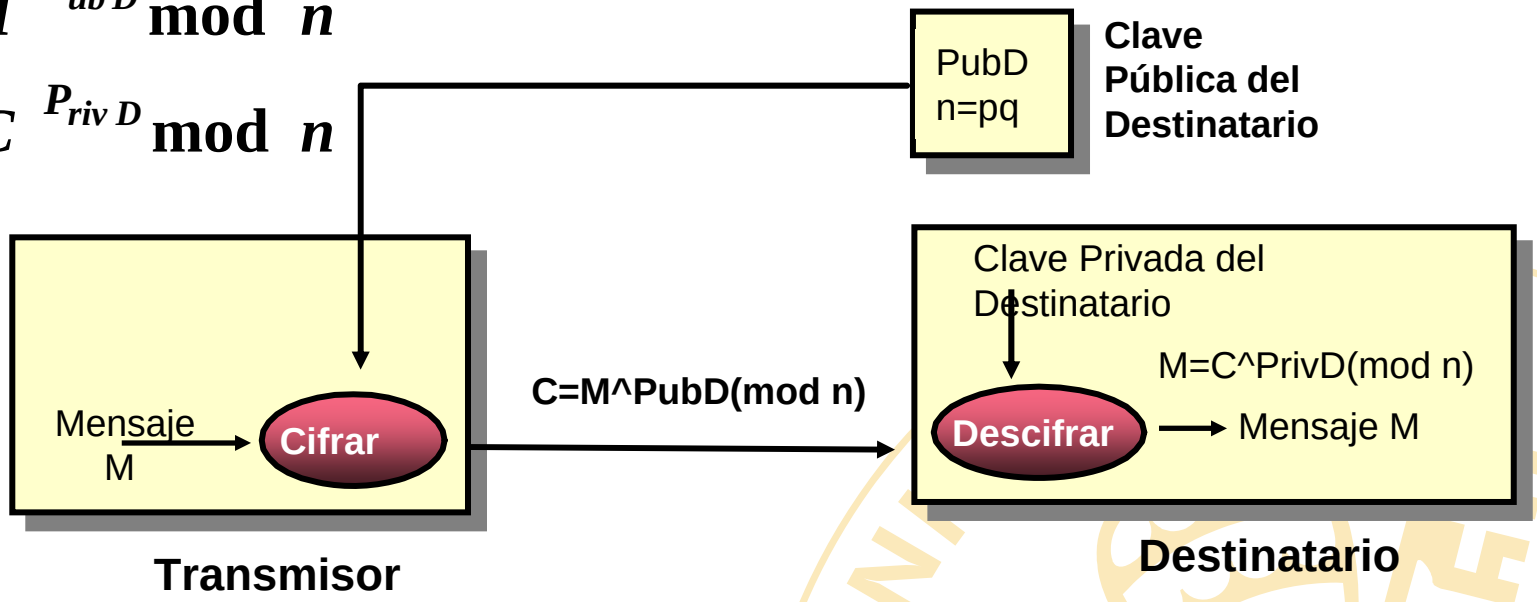
$$M = C^{P_{rivD}} \bmod p$$

***M* es el texto claro y *C* el texto cifrado**

Algoritmo RSA

$$C = M^{P_{ub\,D}} \bmod n$$

$$M = C^{P_{riv\,D}} \bmod n$$



- **Inventado en 1977 por Ronald Rivest, Adi Shamir, y Leonard Adleman.**
- **Sistema de clave pública utilizado para cifrar y autenticar.**
- **Modulo *n* está basado en dos números largos, *p* y *q*.**

Algoritmo RSA

$$C = M^{P_{ub}\,D} \bmod n$$

$$M = C^{P_{riv}\,D} \bmod n$$

Donde,

M = Mensaje Claro *C* = Mensaje Cifrado

Pub = Clave Pública (Para Cifrar) *Priv* = Clave Privada (Para Descifrar)

n = p . q *Pub* . *Priv* = *1 mod (p-1) (q-1)*

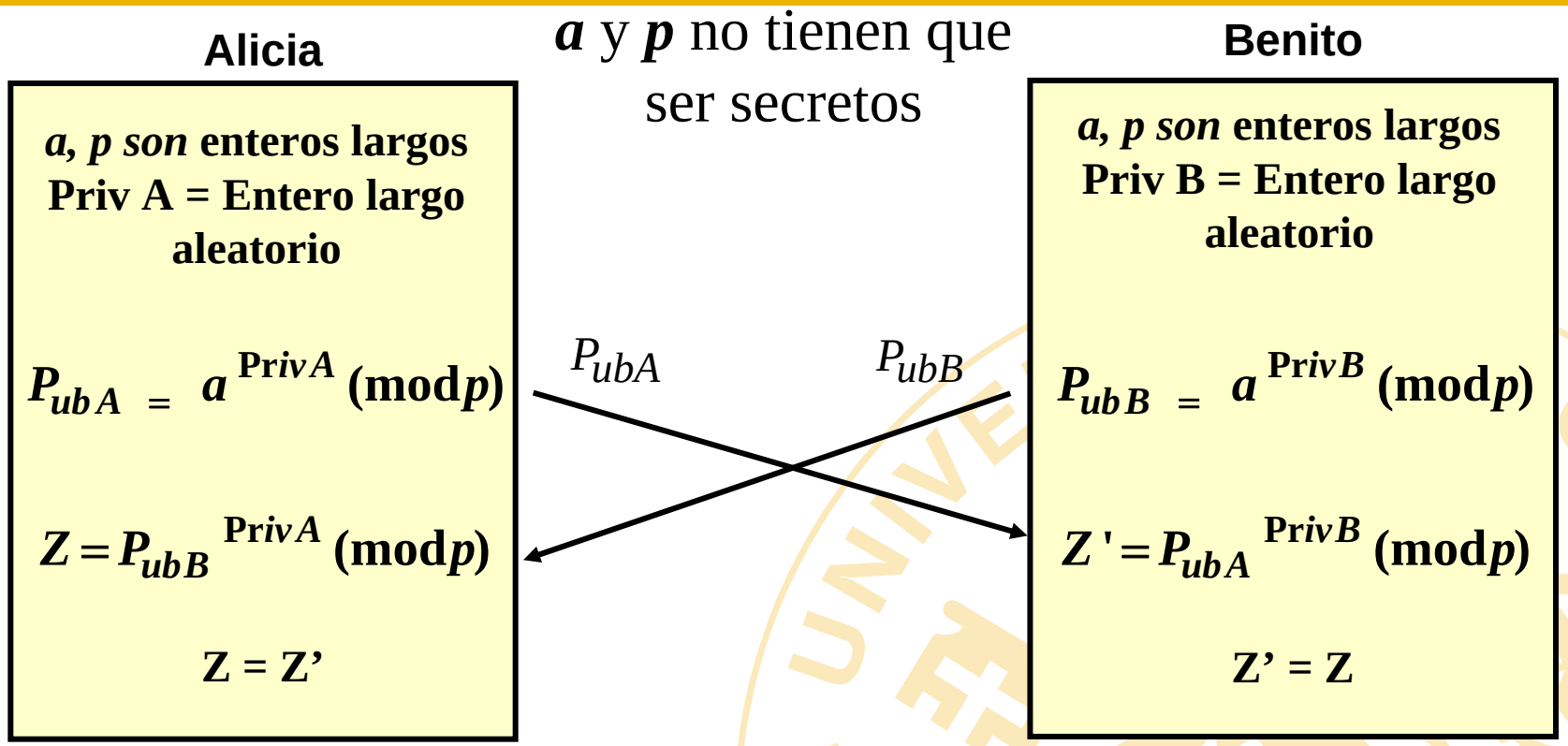
La clave pública, P_{ub} , y el módulo *n* se hacen públicos mientras que la clave privada, P_{riv} , se mantiene en secreto.

Ejemplo: p = 11, q = 31, n = 11 * 31 = 341
Pub = 53, *Priv* = 17 and M=2.

$C = 2^{53} \pmod{341} = 8$ $M = 8^{17} \pmod{341} = 2$

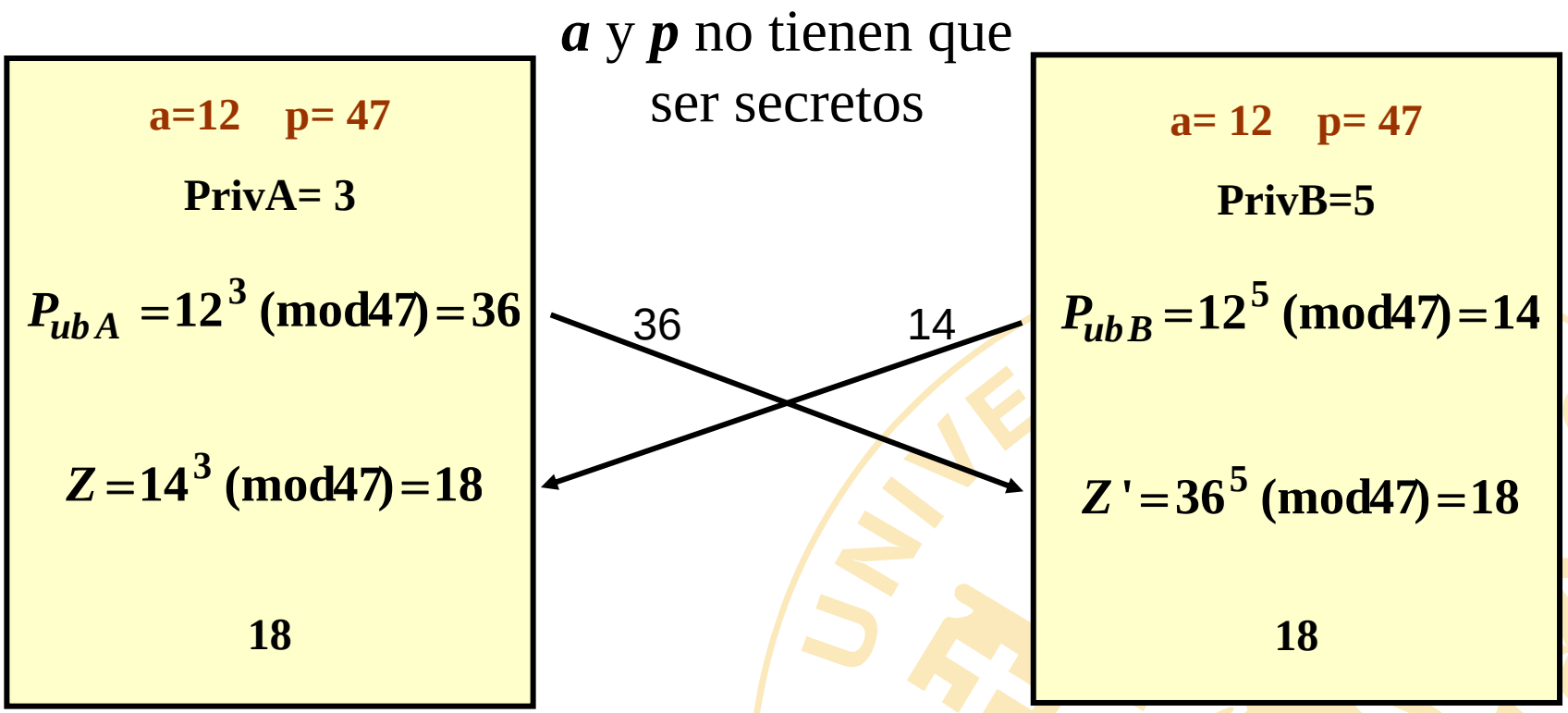
El cifrado con RSA es muy lento.

Negociación de claves mediante Diffie-Hellman



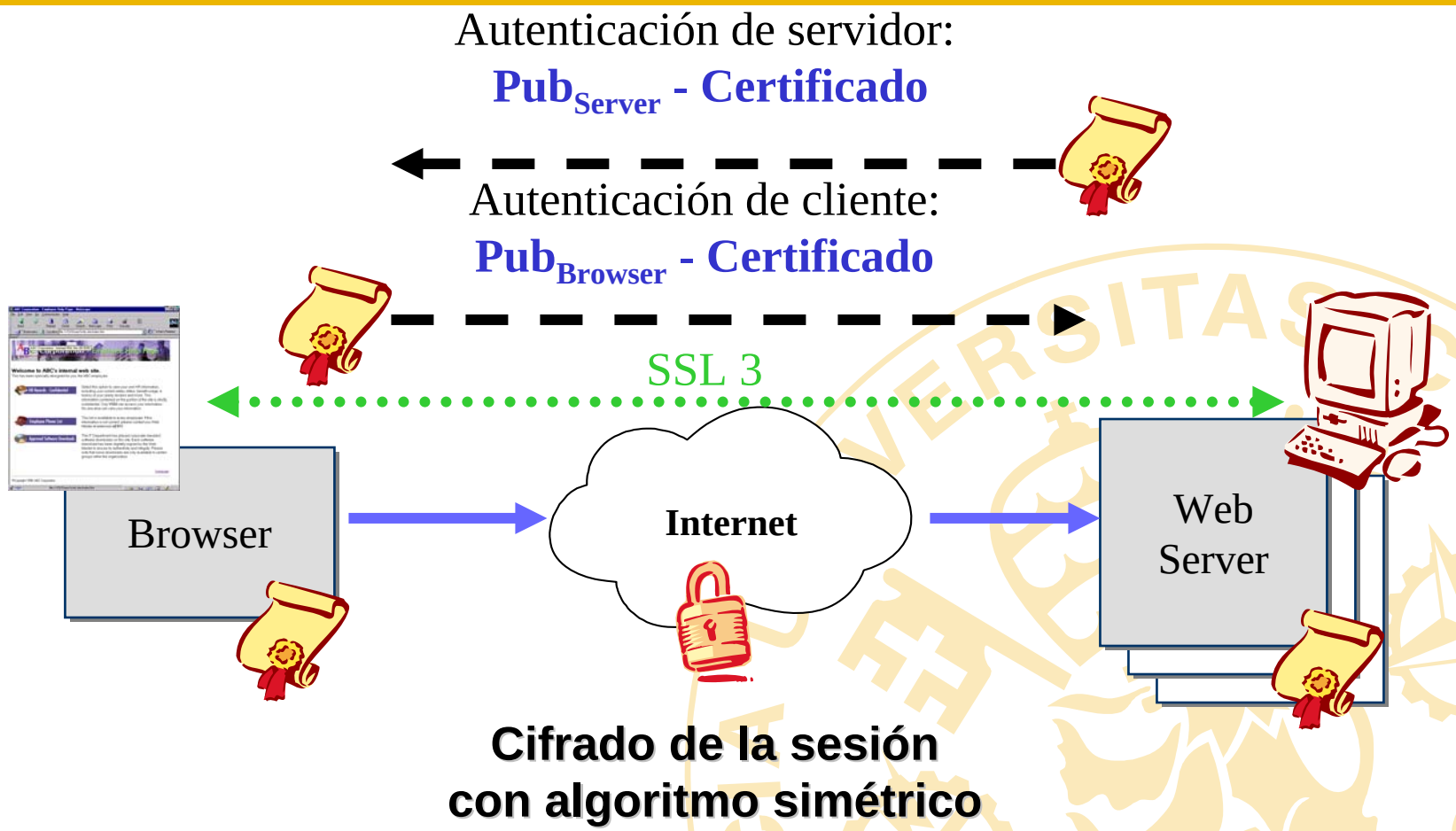
El transmisor Alicia y el receptor Benito utilizan *Z* como la clave de sesión para cifrar el mensaje.

Ejemplo de intercambio de clave mediante Diffie-Hellman



Ambas partes utilizarán 18 como Clave de Sesión para cifrar el mensaje.

SSL - Secure Sockets Layer



Aplicación: Firma electrónica