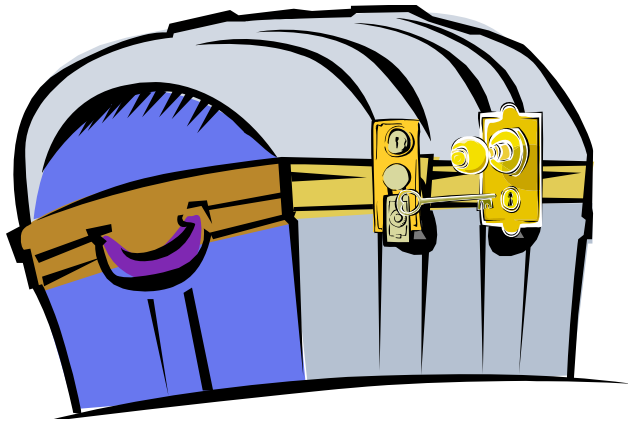
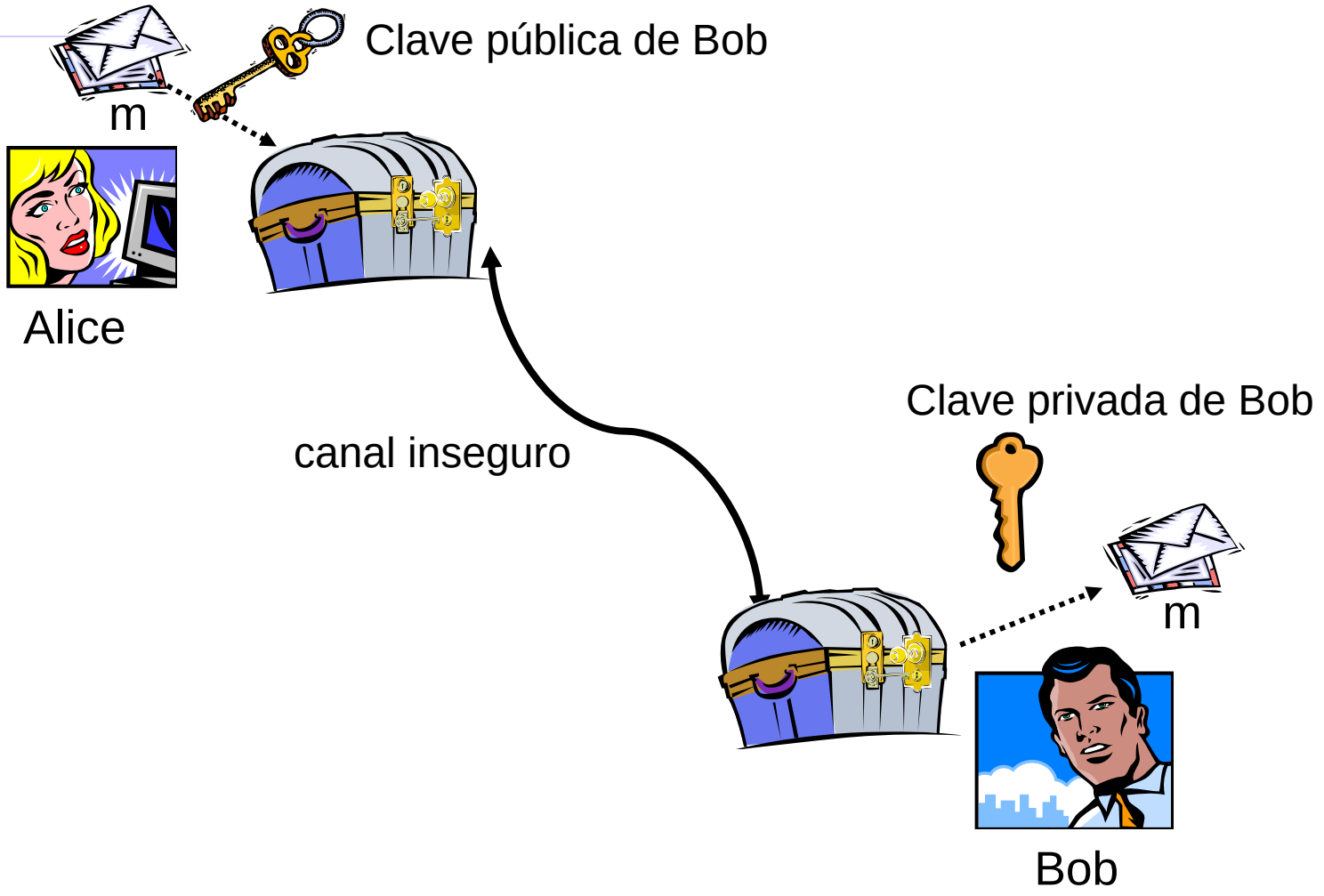
RSA como cifrador: clave pública

- Los sistemas de clave pública usan un tipo especial de cofre con dos cerraduras
  - Con una llave (pública) cerramos el cofre
  - Con la otra (privada) abrimos el cofre



Clave privada ≠ Clave pública

RSA como cifrador: clave pública



RSA como cifrador

- Propuesto en 1978 por Rivest, Shamir y Adelman
- No aceptado como estándar NIST (y sólo de firma) hasta 2000
- Su seguridad se basa en la dificultad de factorizar números grandes

RSA como cifrador

Generación de claves:

- Elegir dos números primos p y q (de aproximadamente el mismo número de bits y de al menos 1024 bits cada uno)
- Elegir aleatoriamente e que cumpla mcd(e, (p-1)(q-1)) = 1
- Calcular d tal que $ed \equiv 1 \pmod{(p-1)(q-1)}$
- n=pq
- Clave pública n,e
- Clave privada d

OJO: mantened p y q secretos

MUY INTERESANTE: $(m^e)^d \equiv m \pmod{n}$ para cualquier m

RSA como cifrador

¿Por qué ...

- $(m^e)^d \equiv m \pmod{n}$ para cualquier m
  - Teoría de números ...

- hay que mantener p y q secretos?
  - Porque si no se podría encontrar d a partir de e
  - Por eso mismo si se factoriza n=pq se rompe RSA

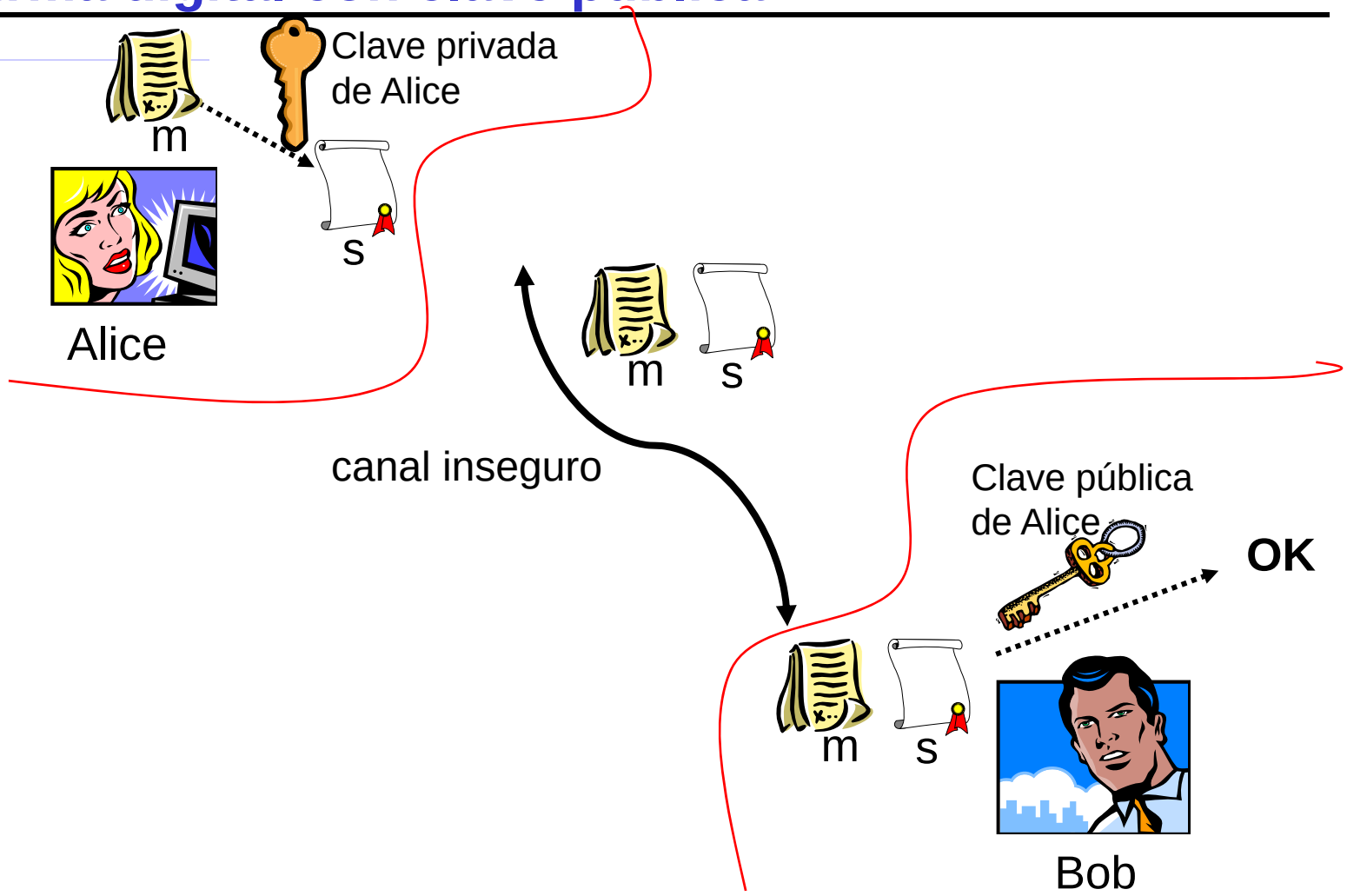
RSA como cifrador

- Clave pública n,e
- Clave privada d
- Cumplen que $(m^e)^d \equiv m \pmod n$

- Para cifrar un número m menor que n:
  - Cifrado: $c = m^e \bmod n$
  - Descifrado: $m = c^d \bmod n$

- Los números más grandes se parten en bloques menores que n

Firma digital con clave pública



Firma digital: Protocolo de firma con clave pública

Alice tiene su clave privada $A_{privada}$ y todos tienen la clave pública de Alice, $A_{pública}$

1. Alice firma su mensaje m usando su clave privada: $s=sig(m, A_{privada})$
2. Alice manda [m,s] a Bob
3. Bob recibe [m,s].
4. Bob verifica s usando la clave pública de Alice: $ver(m,s,A_{pública})$

RSA como firma digital

- Clave pública n,e
- Clave privada d
- Cumplen que $(m^e)^d \equiv m \pmod n$

- Para firmar un número m menor que n:
  - Firma: $s = m^d \bmod n$
  - Verificación: comprobar que $m = s^e \bmod n$

- Estándar NIST desde 2000

Para usar RSA

- Muy importante: no usar la misma clave para firma y para cifrado
- Un grupo de usuarios no debe usar un n común