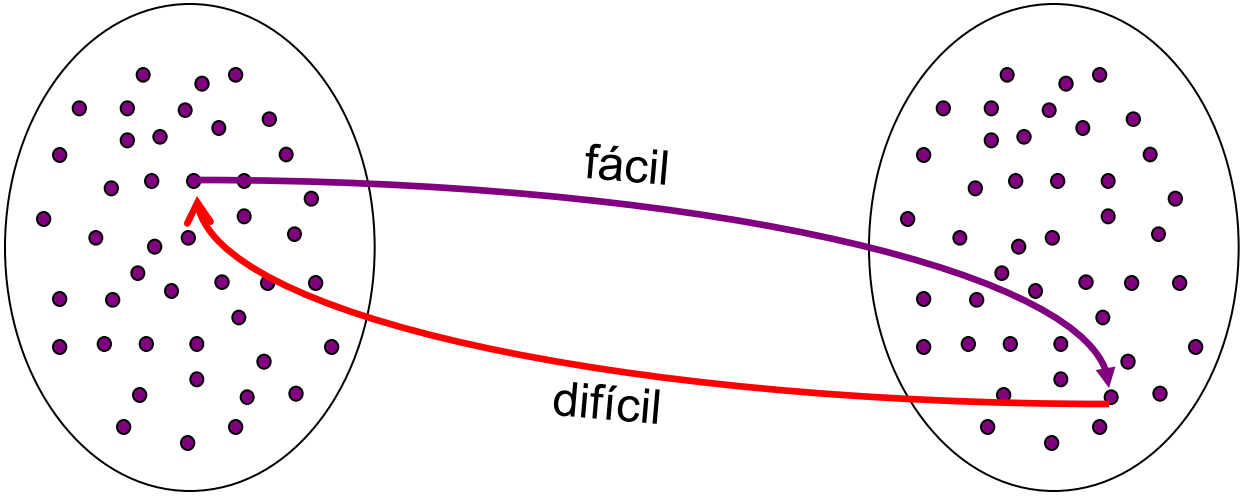
Lección 14: Funciones unidireccionales y hash

intypedia

INFORMATION SECURITY ENCYCLOPEDIA

Dr. Hugo Krawczyk
IBM, Estados Unidos

Funciones de una dirección. Concepto



Funciones de una dirección. RSA-640

p=163473364580925384844313388386509085984178367003309231218111085238933310010450815121211816751157 9

x

q=190087128166482211312685157393541397547189678996851549366663853908802710380210449895719126146557 1

fácil ↓ ↑ difícil

p·q=3107418240490043721350750035888567930037346022842727545720161948823206440518081504556346829671723286782437916272838033415471073108501919548529007337724822783525742386454014691736602477652346609

Source: http://mathworld.wolfram.com/news/2005-11-08/rsa-640/

Funciones de una dirección: hash

Son primitivas criptográficas que reducen una información de cualquier tamaño a un valor o número único que tiene un tamaño fijo, por lo general de centenas de bits.

Esta compresión sirve para:

- Validad la integridad de un archivo o documento
- Adecuar un documento para el proceso de firma digital

Propiedades de las funciones hash I

1. Unidireccionalidad:

   Conocido un resumen h(M), debe ser computacionalmente imposible encontrar M a partir de dicho resumen.

2. Compresión:

   A partir de un mensaje de cualquier longitud, el resumen h(M) debe tener una longitud fija.

3. Facilidad de cálculo:

   Debe ser fácil calcular h(M) a partir de un mensaje M.

Propiedades de las funciones hash II

4. Difusión:

   El resumen h(M) debe ser una función compleja de todos los bits del mensaje M: si se modifica un solo bit del mensaje M, h(M) debería cambiar aproximadamente la mitad de sus bits.

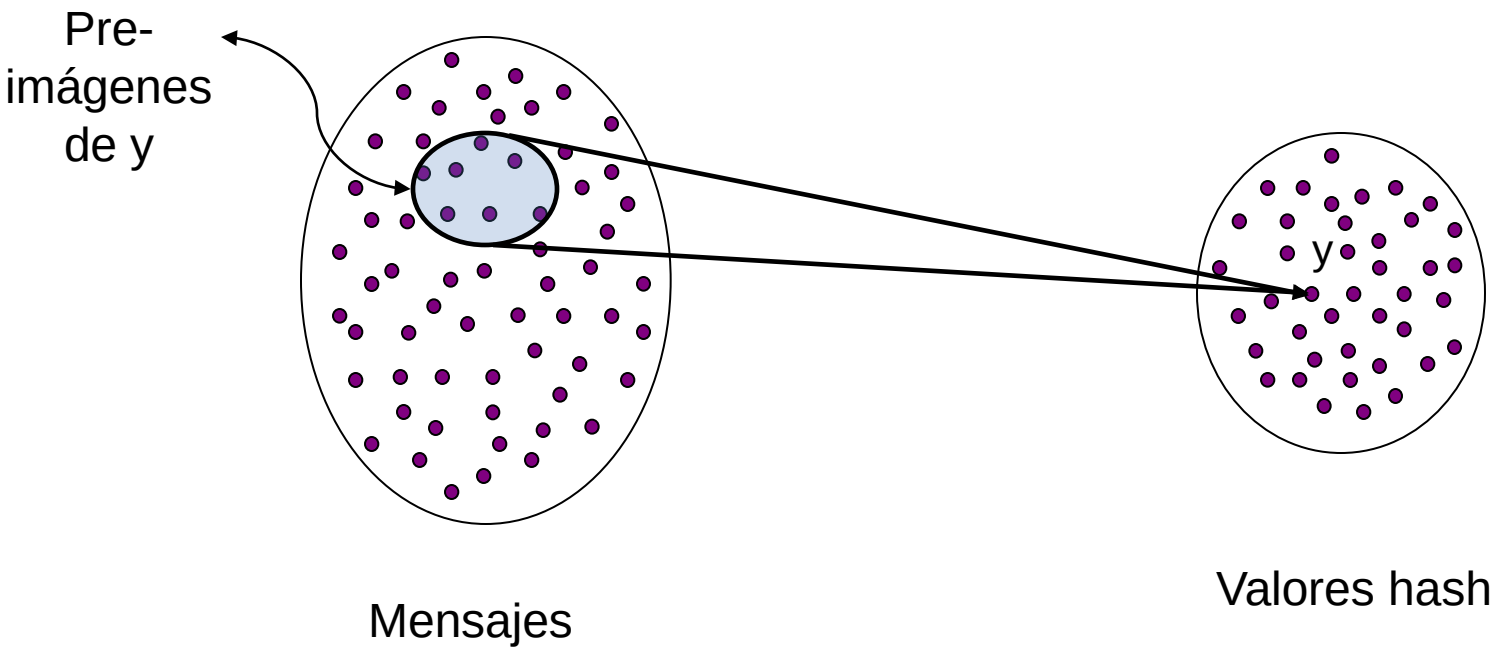
5. Colisión simple:

   Será computacionalmente imposible conocido M, encontrar otro M' tal que h(M) = h(M'). Esto se conoce como *resistencia débil a las colisiones*, primera pre-imagen.

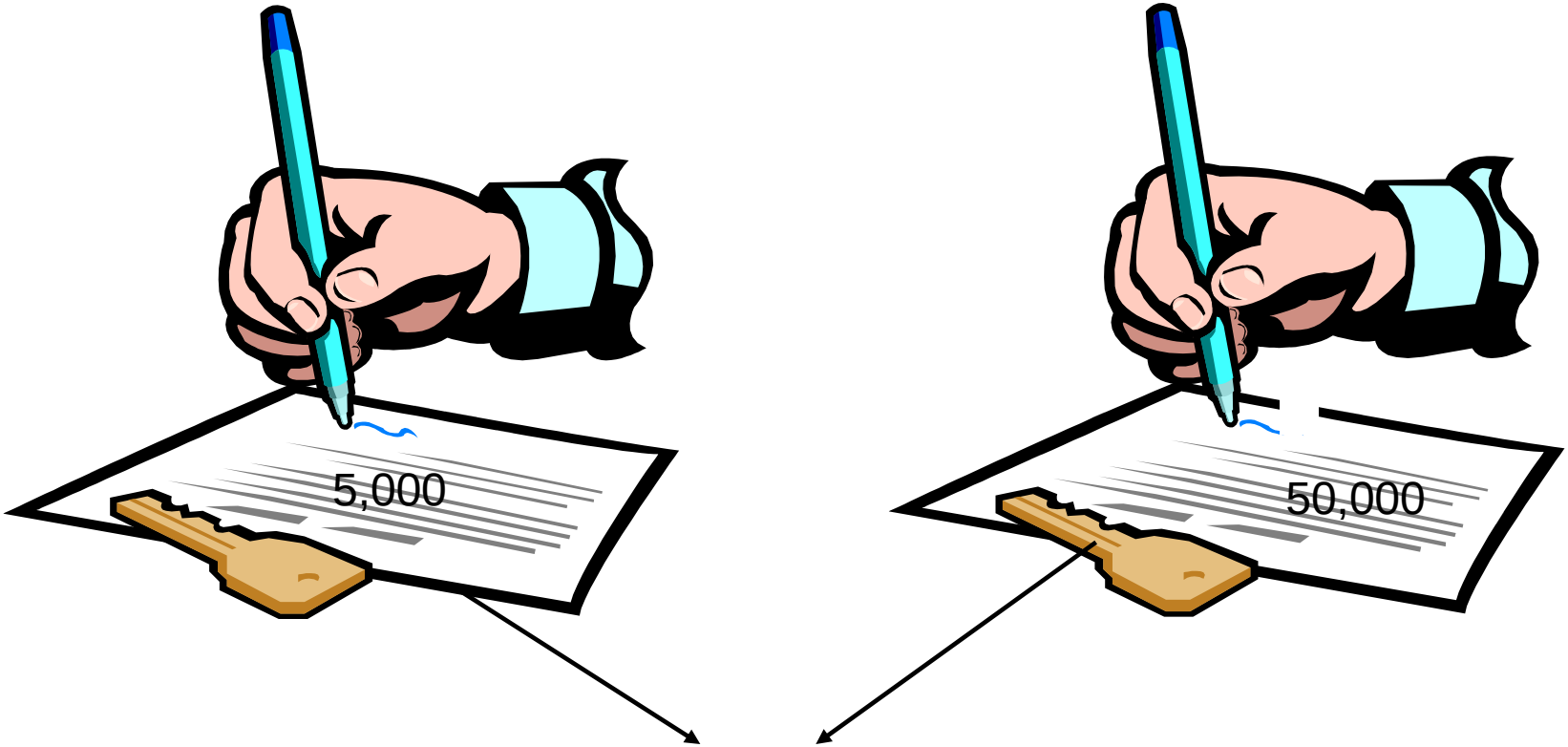
6. Colisión fuerte:

   Será computacionalmente difícil encontrar un par (M, M') de forma que h(M) = h(M'). Esto se conoce como *resistencia fuerte a las colisiones*, segunda pre-imagen.

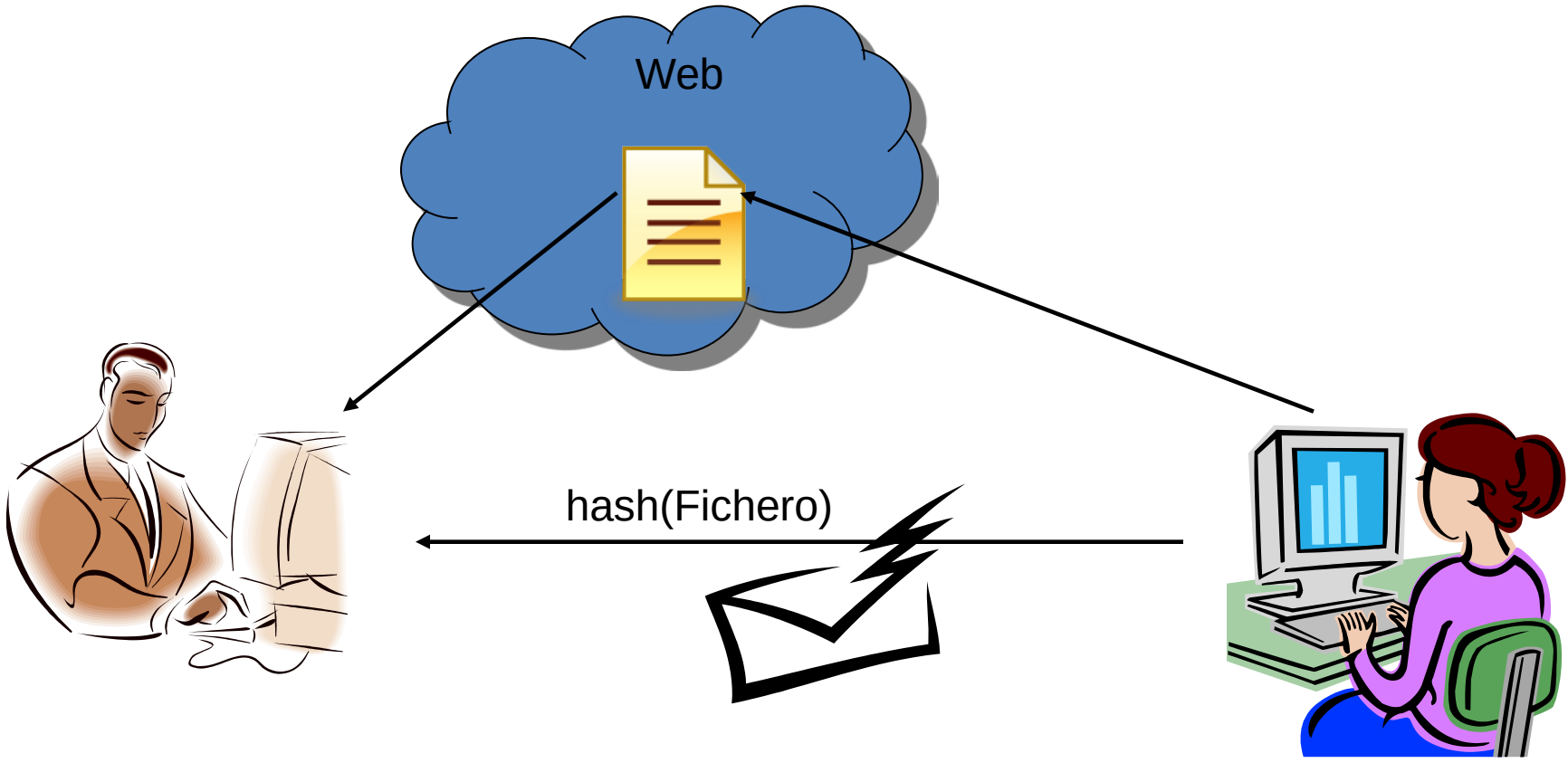
Primera pre-imagen



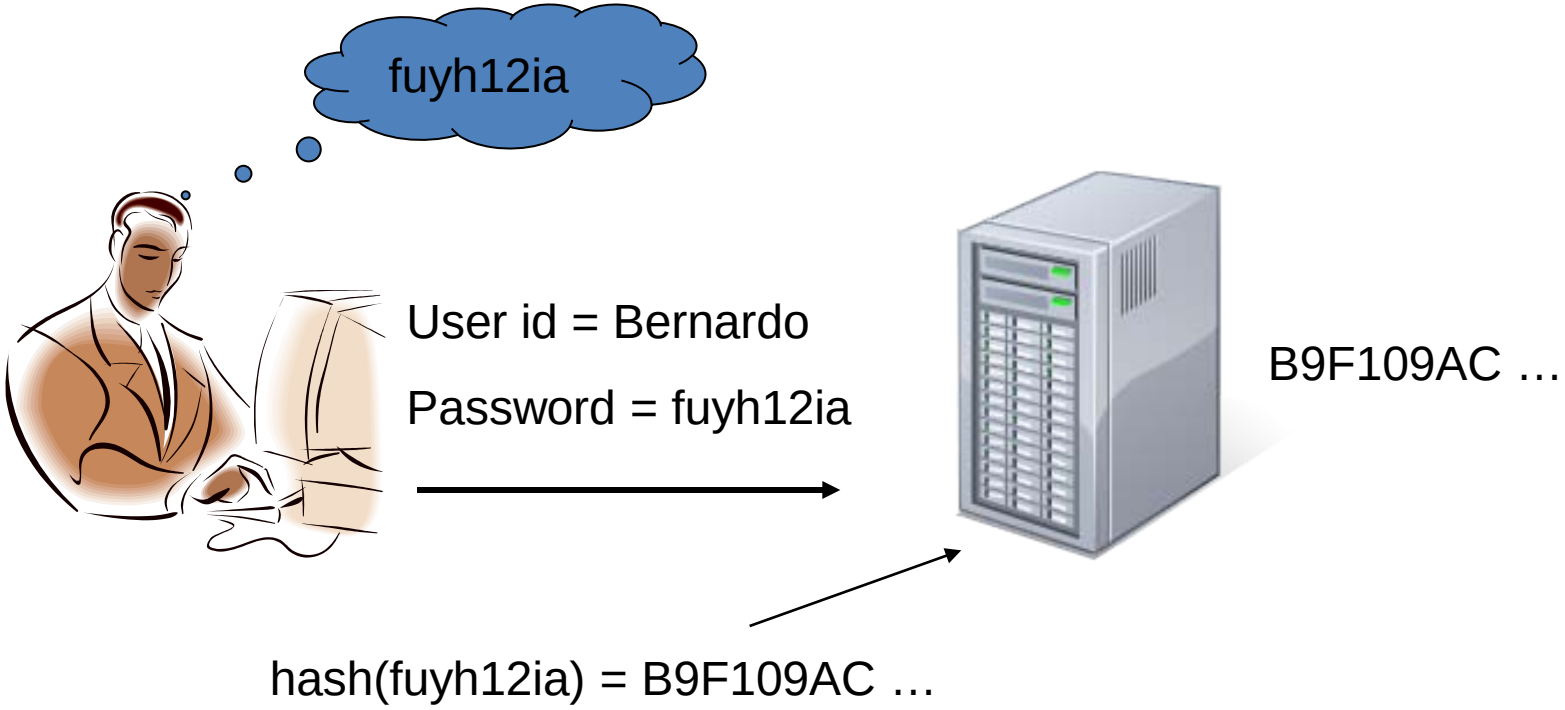
Segunda pre-imagen



Ejemplo. Fichero en red

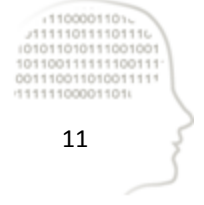


Ejemplo. Autenticación de usuario y credenciales almacenadas



Algunos algoritmos de hash

- MD5: Ron Rivest 1992. Mejoras al MD4 y MD2 (1990). Resumen de 128 bits. Se recomienda no usar desde 2004.
- SHA-1: Del NIST, National Institute of Standards and Technology, 1995. Similar a MD5 pero con un resumen de 160 bits.
- Otras propuestas: SHA-256 y SHA-512 de familia SHA-2.
- Concurso NIST nuevo estándar: pendiente en mayo 2012 …
  http://csrc.nist.gov/groups/ST/hash/sha-3/index.html
- Otros hash:
- N-Hash: Nippon Telephone and Telegraph, 1990. Resumen de 128 bits.
- RIPEMD: Comunidad Europea, RACE, 1992. Resumen de 160 bits.
- Tiger: Ross Anderson, Eli Biham, 1996. Resúmenes de hasta 192 bits. Optimizado para máquinas de 64 bits.



intypedia

INFORMATION SECURITY ENCYCLOPEDIA

Contacto: info@intypedia.com