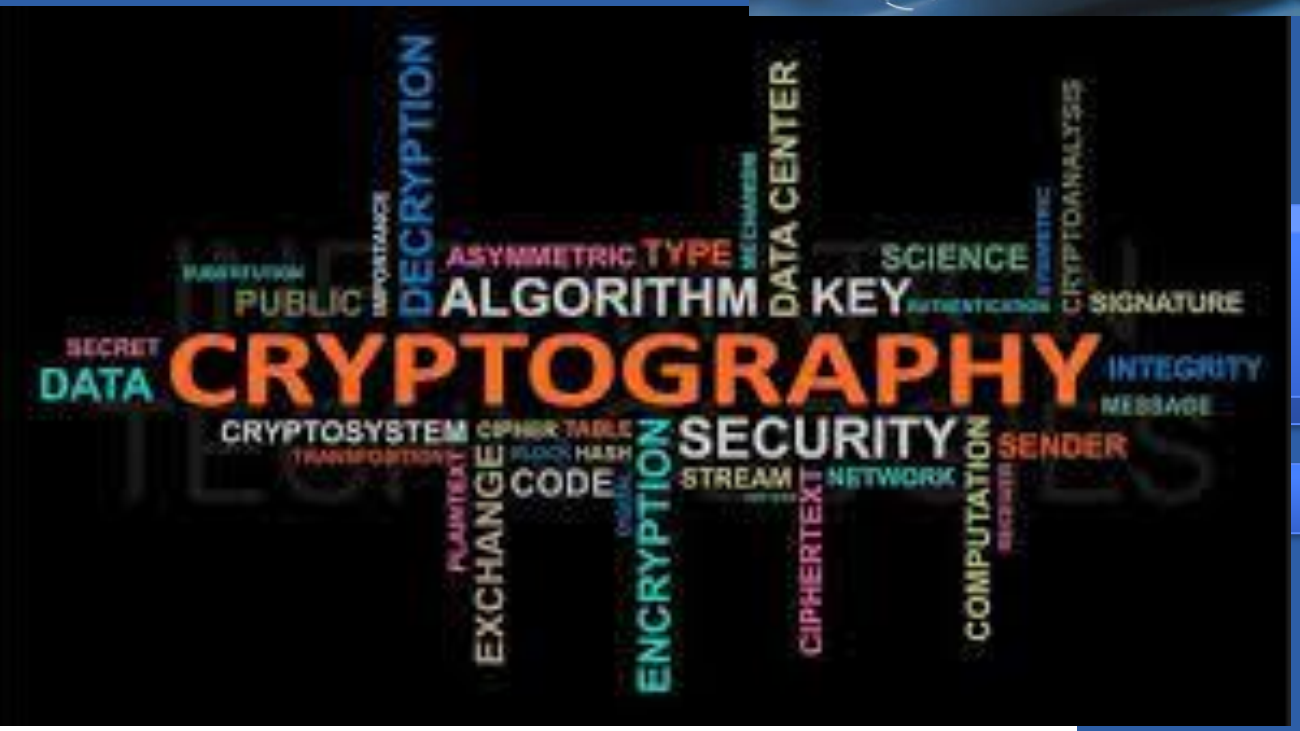
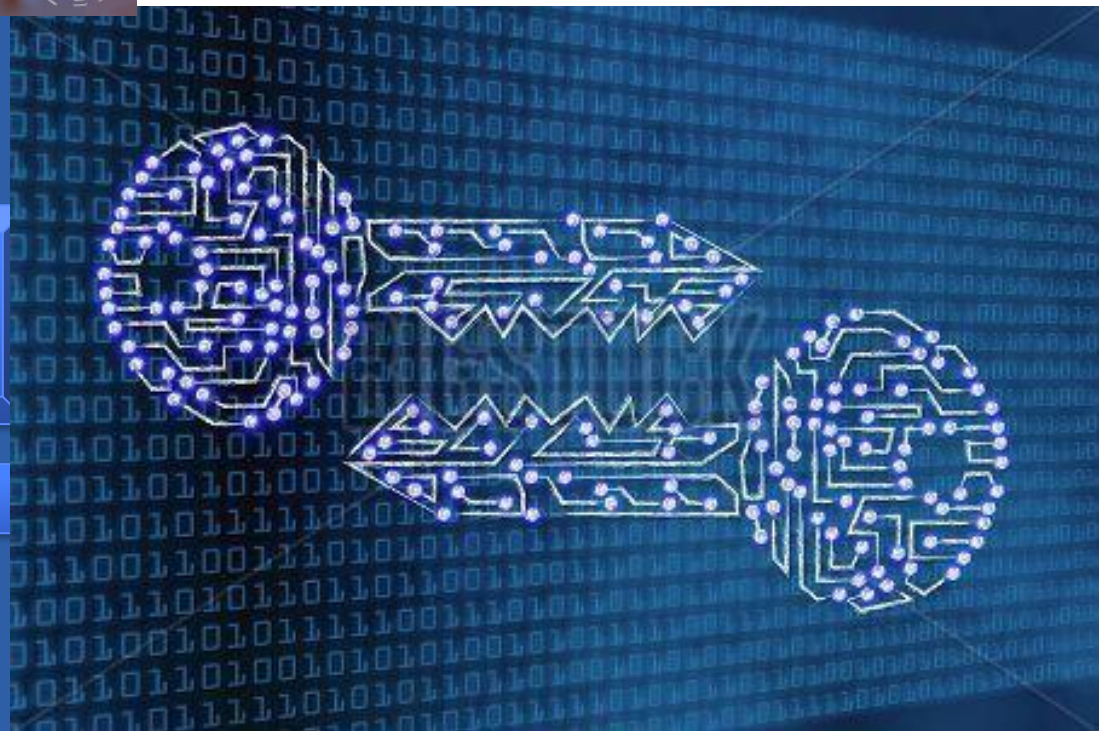
Criptografía

Universidad Francisco de Vitoria
UFV Madrid

Tema 4
Criptografía de Clave Pública





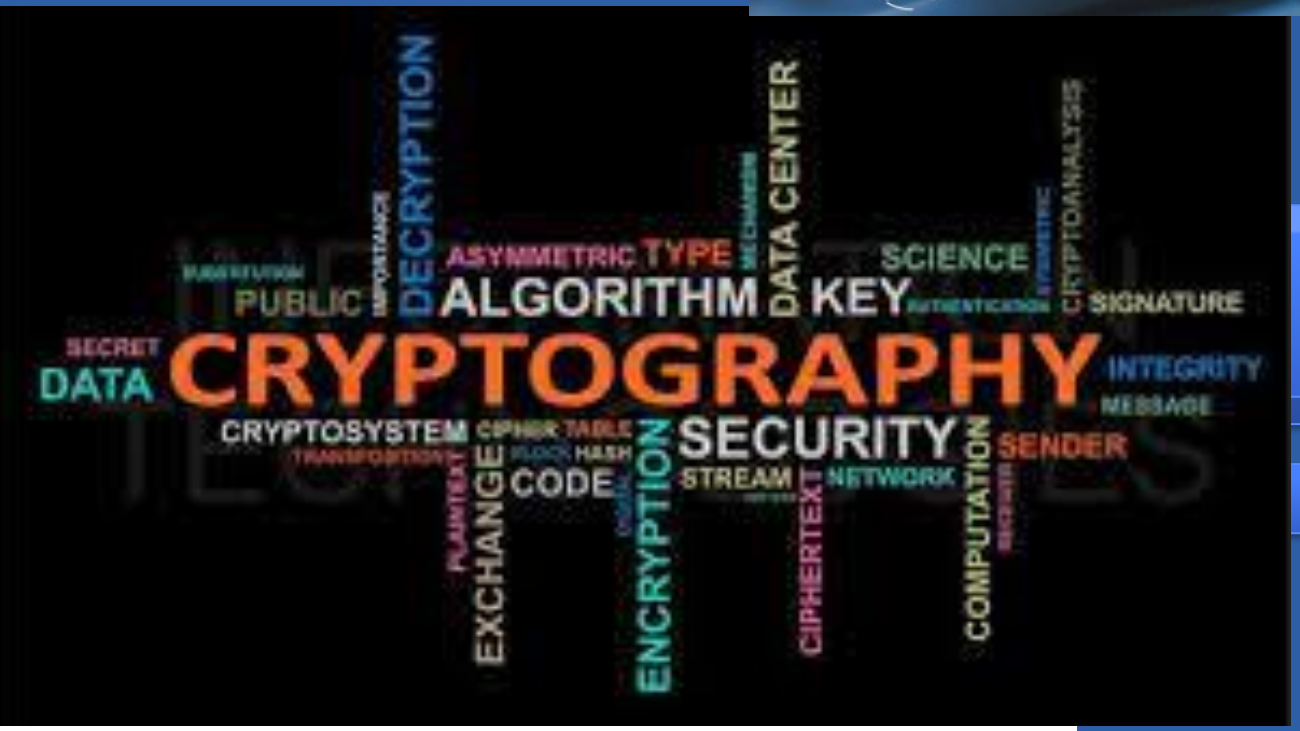
Sistemas de Clave Pública

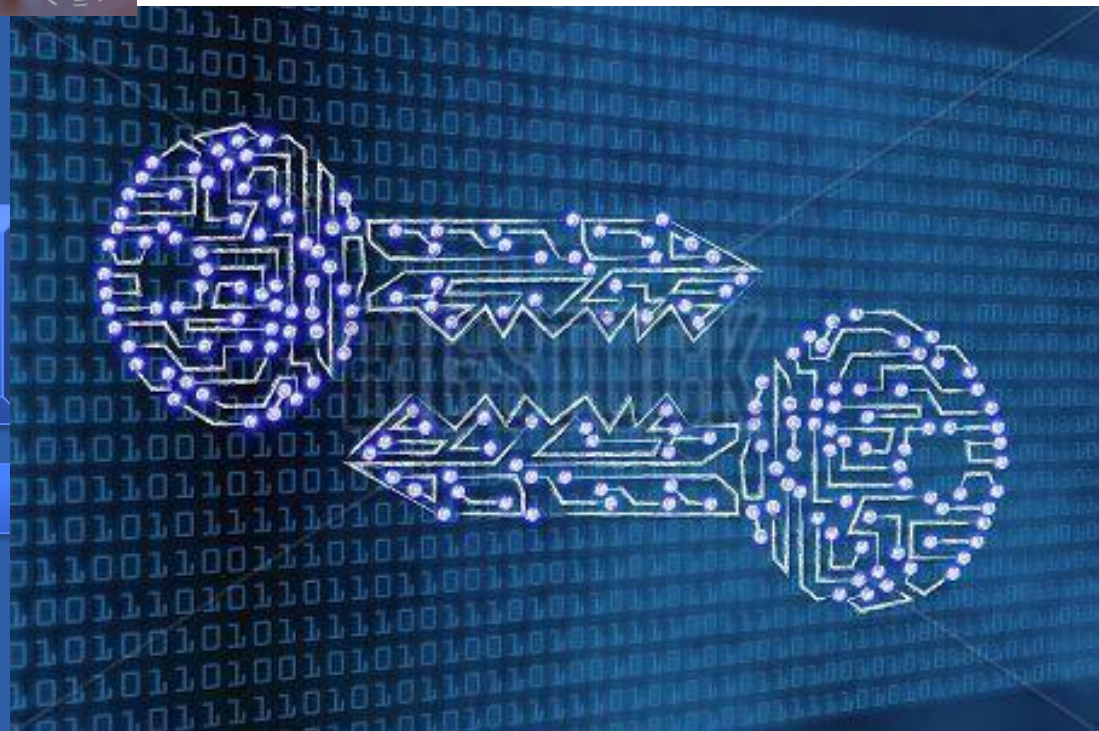
- Introducción
- Distribución de claves
- Cifrado asimétrico
- Firma Digital
- Modelos Híbridos
- Certificados Digitales

Criptografía

Universidad Francisco de Vitoria
UFV Madrid

Tema 4.1
Introducción





Problemas del cifrado simétrico

Distribución de claves

- Dos entidades, que no han hablado previamente, tienen que intercambiarse mensajes cifrados a través de un canal inseguro
- Para los algoritmos de cifrado simétrico, es necesario intercambiar la clave (simétrica) mediante un **canal seguro**.

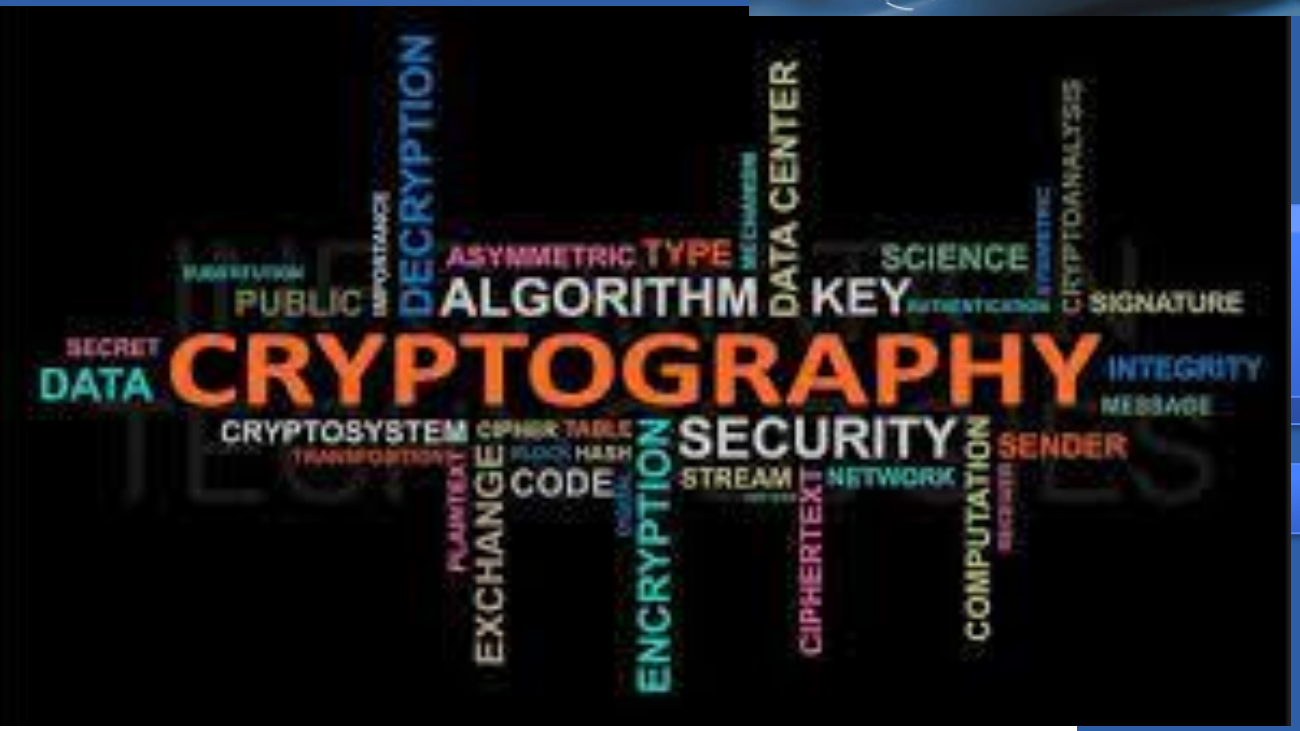
  - Pero…¿por qué no utilizar ese canal seguro para enviar los mensajes?
    - Distancia
    - Reutilización del canal seguro da pistas a los espías
    - Etc
  - Durante miles de años ha sido un problema sin solución

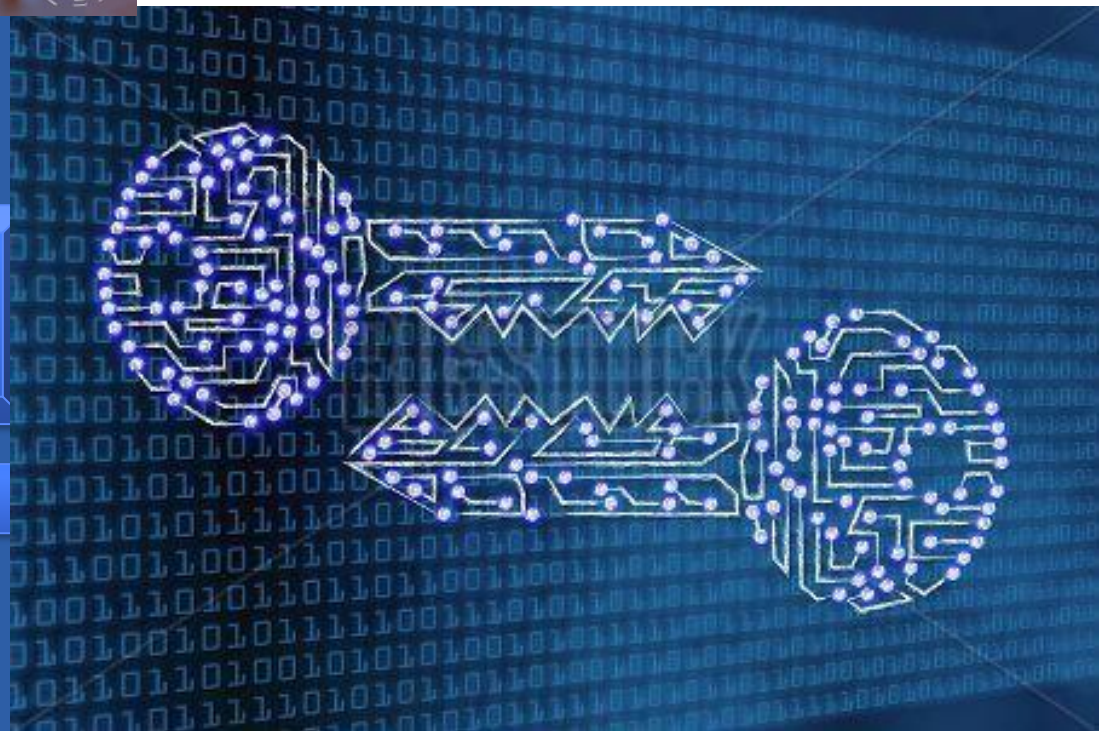
.

Criptografía

Universidad Francisco de Vitoria
UFV Madrid

Tema 4.2
Diffie-Hellman





Distribución de claves

- Dos entidades, que no han hablado previamente, tienen que intercambiarse mensajes cifrados a través de un canal inseguro
- Para los algoritmos de cifrado simétrico, es necesario intercambiar la clave (simétrica) mediante un **canal seguro**.

  - Pero…¿por qué no utilizar ese canal seguro para enviar los mensajes?
    - Distancia
    - Reutilización del canal seguro da pistas a los espías
    - …
  - Durante miles de años ha sido un problema sin solución
    - Hasta….

Diffie - Hellman

New Directions in Cryptography

Invited Paper

WHITFIELD DIFFIE AND MARTIN E. HELLMAN, MEMBER, IEEE

***Abstract*—Two kinds of contemporary developments in cryptography are examined. Widening applications of teleprocessing have given rise to a need for new types of cryptographic systems, which minimize the need for secure key distribution channels and supply the equivalent of a written signature. This paper suggests ways to solve these currently open problems. It also discusses how the theories of communication and computation are beginning to provide the tools to solve cryptographic problems of long standing.**

I. Introduction

WE STAND TODAY on the brink of a revolution in cryptography. The development of cheap digital hardware has freed it from the design limitations of mechanical computing and brought the cost of high grade cryptographic devices down to where they can be used in

The best known cryptographic problem is that of privacy: preventing the unauthorized extraction of information from communications over an insecure channel. In order to use cryptography to insure privacy, however, it is currently necessary for the communicating parties to share a key which is known to no one else. This is done by sending the key in advance over some secure channel such as private courier or registered mail. A private conversation between two people with no prior acquaintance is a common occurrence in business, however, and it is unrealistic to expect initial business contacts to be postponed long enough for keys to be transmitted by some physical means. The cost and delay imposed by this key distribution problem is a major barrier to the transfer of business communications to large teleprocessing networks.

Section III proposes two approaches to transmitting

Diffie - Hellman

Abstract

Two kinds of contemporary developments in cryptography are examined. Widening applications of teleprocessing have given rise to a **need for new types of cryptographic systems**, which minimize the need for secure key distribution channels and supply the equivalent of a written signature. This paper suggests ways to solve these currently open problems. It also discusses how the theories of communication and computation are beginning to provide the tools to solve cryptographic problems of long standing.

Diffie - Hellman

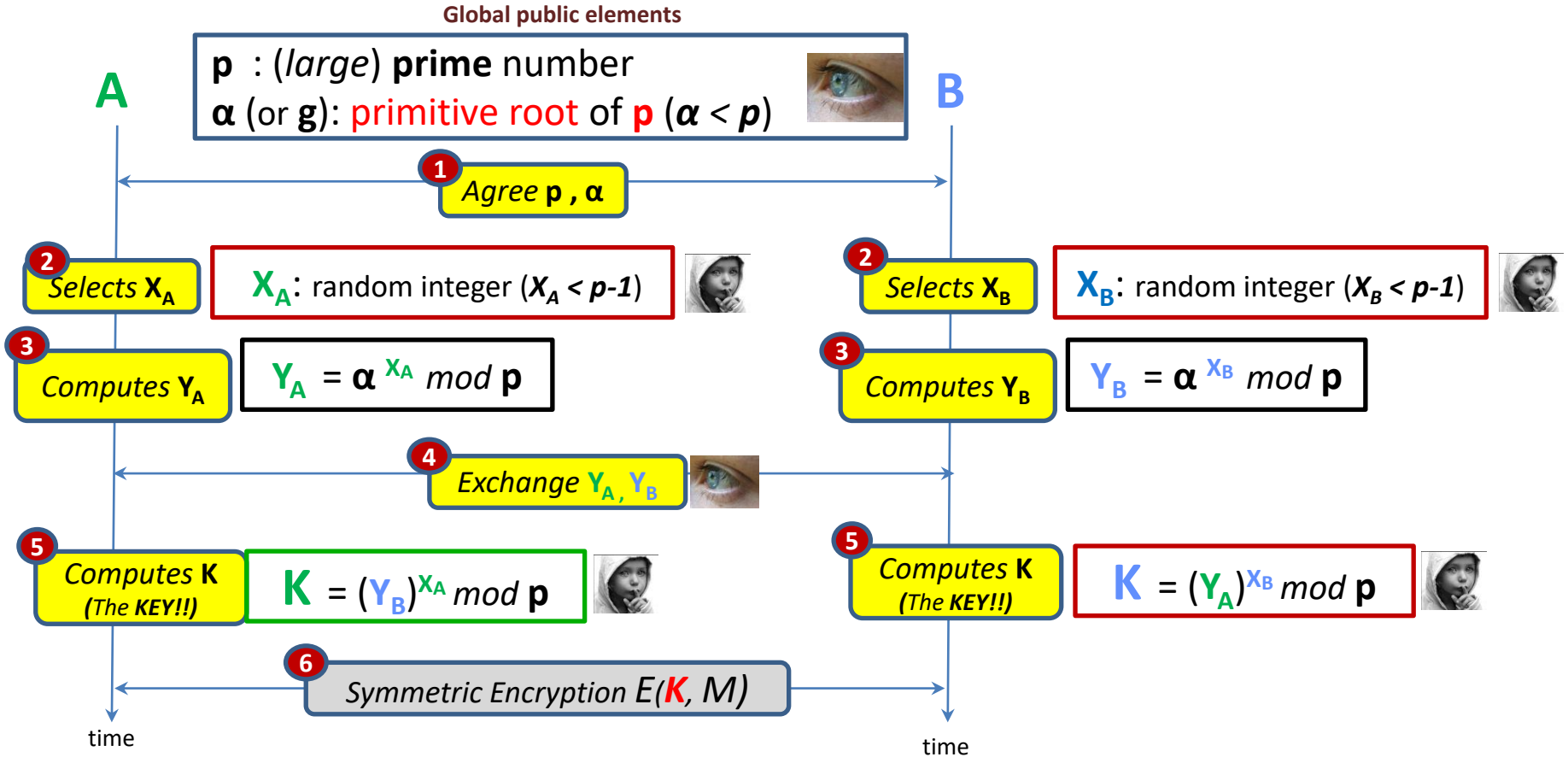
- Introduce el concepto de **sistema de clave pública**
  - Dos valores relacionados:
    - Una **clave pública**, conocida por todos.
    - Una **clave privada**, mantenida secreta.
  - Fundamentos de seguridad:
    - Es sencillo derivar la pública a partir de la privada
    - Pero **casi imposible obtener la privada a partir de la pública**
  - Además…
    - Base para la **firma digital**

Diffie - Hellman

- **Propósito**: permite a dos usuarios (*A y B*) **intercambiar una clave**, de manera segura, **sobre un canal inseguro**
  - *Esa clave puede ser utilizada para cifrado simétrico posterior.*

- **Efectividad** basada en:
  - Es poco costoso **calcular exponentes** de manera modular, **PERO**
  - Es muy costoso **calcular logaritmos en un campo discreto.**

Diffie - Hellman

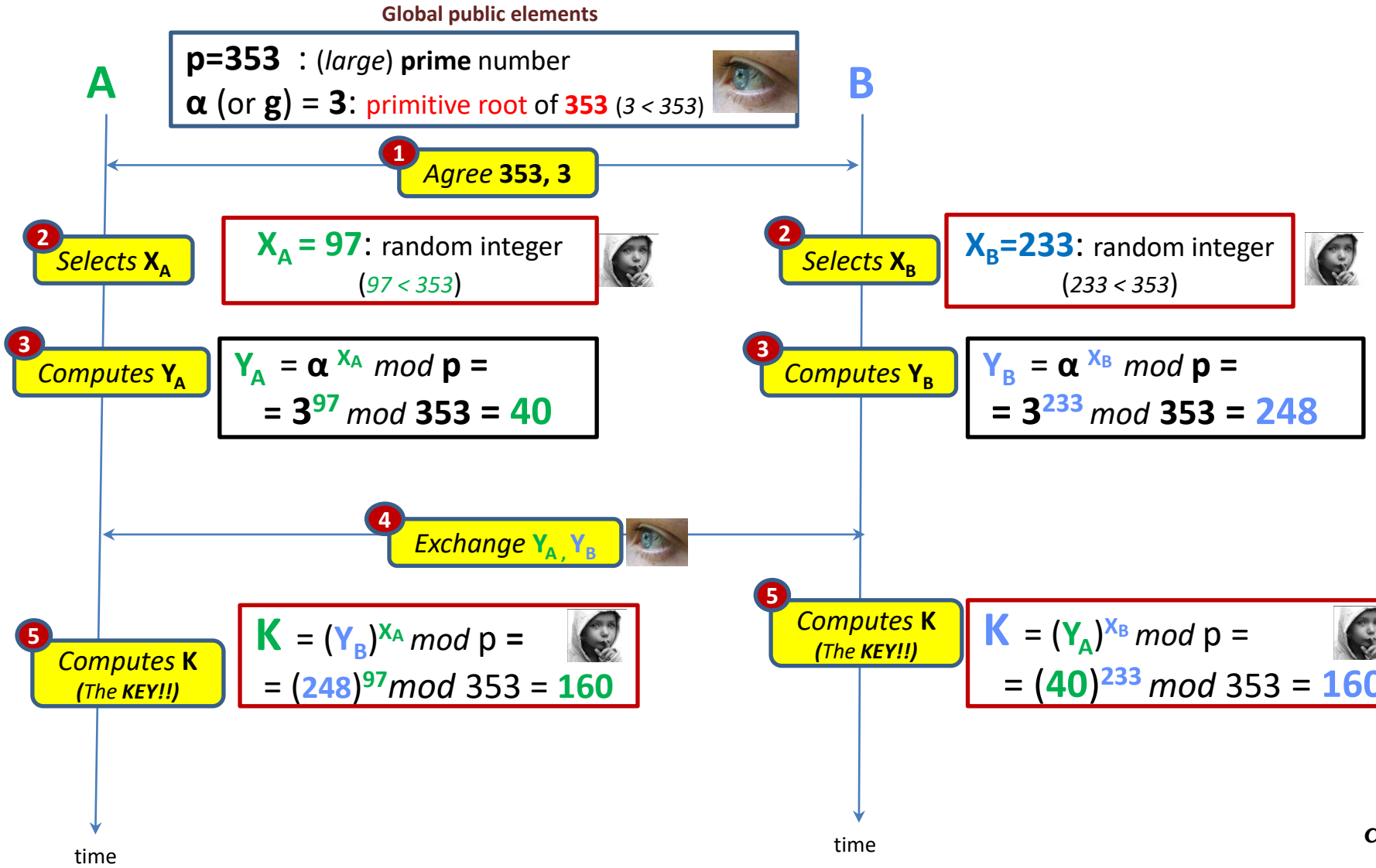


Diffie-Hellman

(modular arithmetic demonstration)

$$
\begin{aligned}
K &= (Y_B)^{X_A} \bmod p = \\
&= (\alpha^{X_B} \bmod p)^{X_A} \bmod p = \\
&= (\alpha^{X_B})^{X_A} \bmod p = \\
&= (\alpha^{X_A})^{X_B} \bmod p = \\
&= (\alpha^{X_A} \bmod p)^{X_B} \bmod p = \\
&= (Y_A)^{X_B} \bmod p = \\
&= K
\end{aligned}
$$

Diffie – Hellman: Ejemplo



Diffie – Hellman: Criptoanálisis

p=353 prime number
α (or **g**) = **3**: primitive root of **353**

$Y_A = 40$
$Y_B = 248$

BRUTE FORCE ATTACK:

$3^{Xb} \bmod 353 = 248$
$3^{Xa} \bmod 353 = 40$

$3^0 \bmod 353 = 1$
$3^1 \bmod 353 = 3$
...
$3^{97} \bmod 353 = 40 \Rightarrow X_a = 97$
...
$3^{233} \bmod 353 = 248 \Rightarrow X_b = 233$

For large (& prime) p, problem becomes impractical

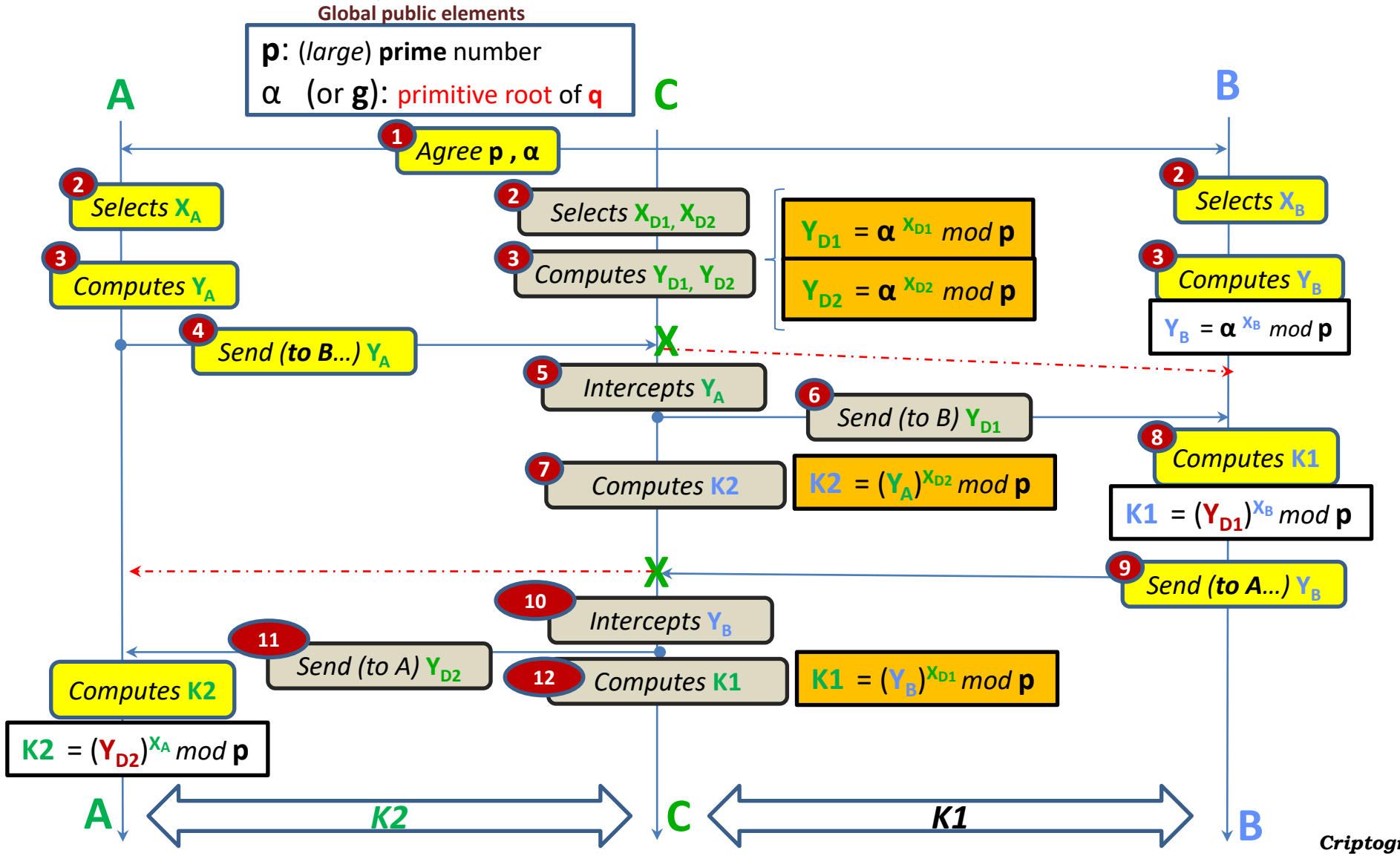
For instance:

p= 283.947.315.571.783.457.402.747.934.850.943.553…

(up to 300 decimal digits or more!)

Diffie – Hellman: Vulnerabilidades

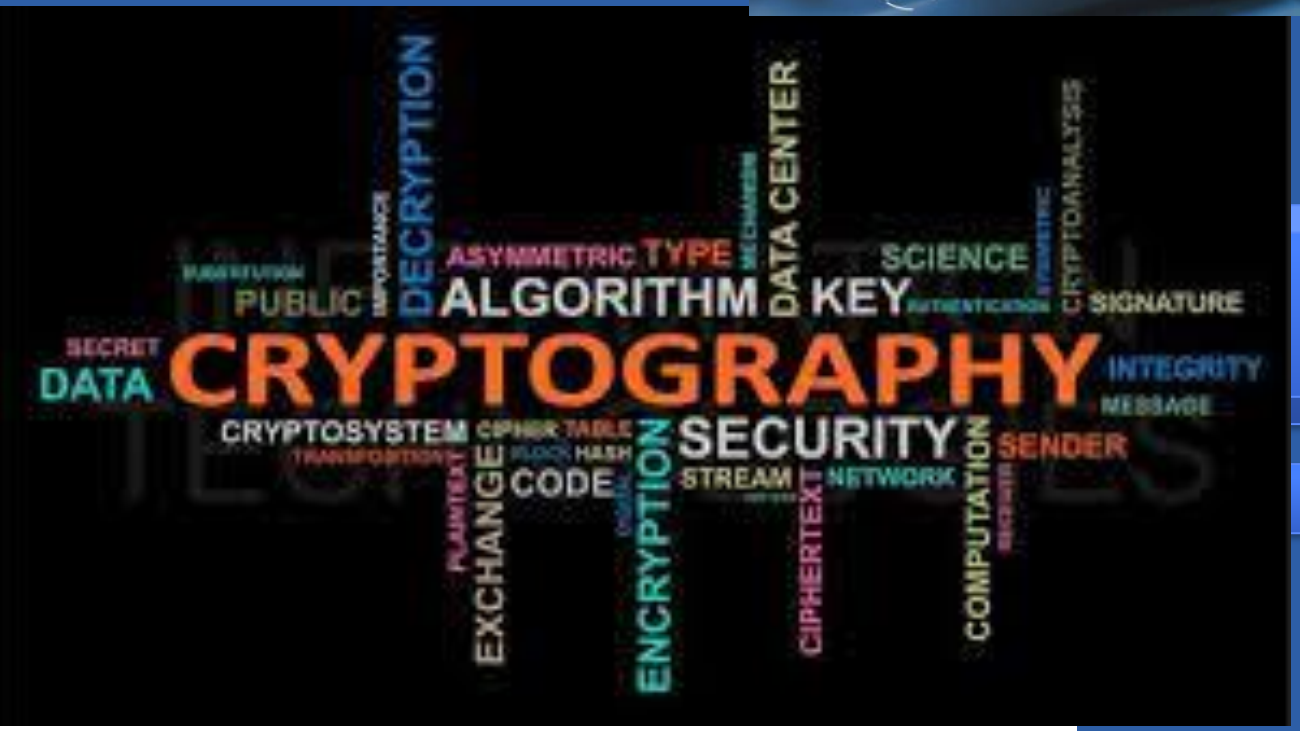
NO AUTHENTICATION: ⇨ *(Vulnerability: Man-in-the-middle Attack)*

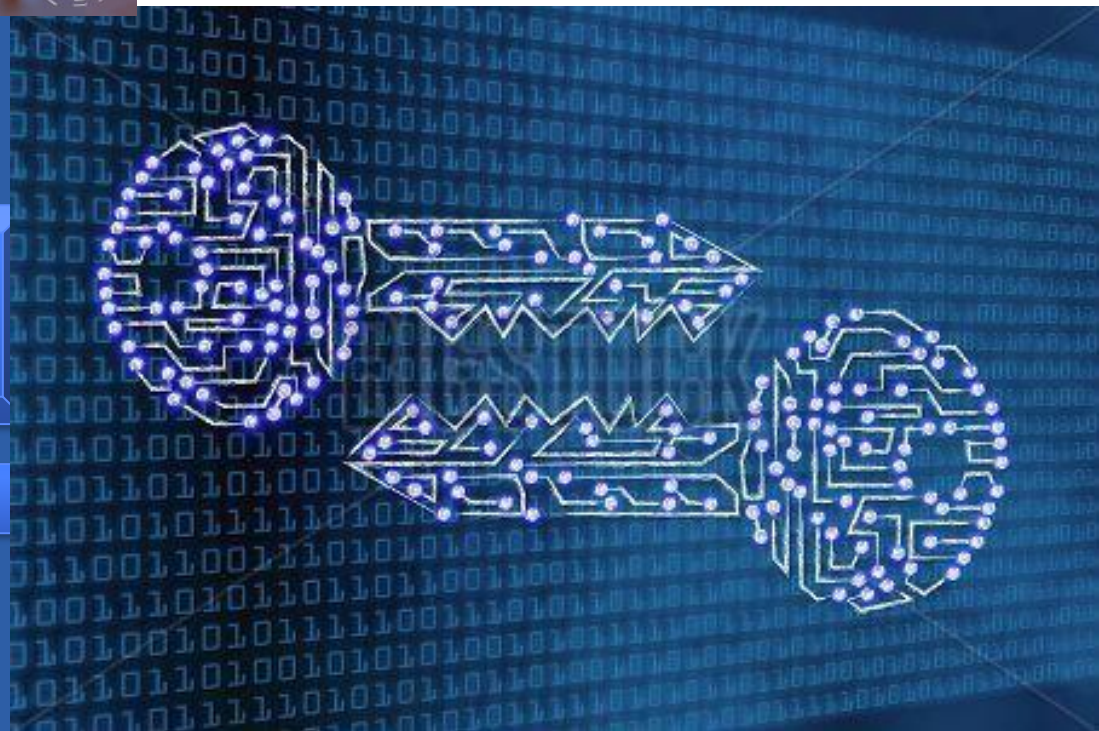


Criptografía

Universidad Francisco de Vitoria
UFV Madrid

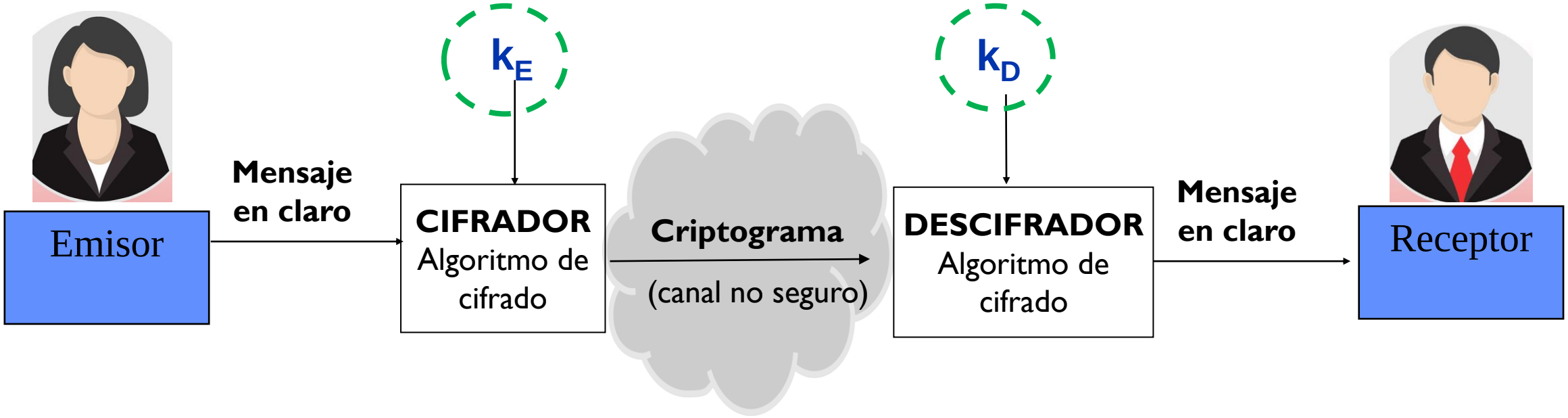
Tema 4.3
Algoritmos de cifrado asimétrico





Modelo de Criptosistema

ASIMÉTRICOS: Una clave (k_E) para cifrar y otra (k_D) para descifrar



- Base de los sistemas de clave pública

RSA

"A Method for Obtaining Digital Signature and Public-Key Cryptosystems."

R. L. **R**ivest, A. **S**hamir, L. **A**dleman.

Communications of the ACM, v. 21, nº 2, pp 120-126.

February 1978

- Primer **sistema de cifrado basado en clave pública**

- **Seguridad** basada en la **dificultad de factorizar** un número obtenido como producto de dos números primos muy grandes

A Method for Obtaining Digital Signatures and Public-Key Cryptosystems

R.L. Rivest, A. Shamir, and L. Adleman*

Abstract

An encryption method is presented with the novel property that publicly revealing an encryption key does not thereby reveal the corresponding decryption key. This has two important consequences:

1. Couriers or other secure means are not needed to transmit keys, since a message can be enciphered using an encryption key publicly revealed by the intended recipient. Only he can decipher the message, since only he knows the corresponding decryption key.
2. A message can be "signed" using a privately held decryption key. Anyone can verify this signature using the corresponding publicly revealed encryption key. Signatures cannot be forged, and a signer cannot later deny the validity of his signature. This has obvious applications in "electronic mail" and "electronic funds transfer" systems.

RSA

Abstract

- An encryption method is presented with the novel property that publicly **revealing an encryption key does not thereby reveal the corresponding decryption key**. This has two important consequences:
  - Couriers or other secure means are not needed to transmit keys, since a message can be enciphered using an encryption key publicly revealed by the intended recipient. Only he can decipher the message, since only he knows the corresponding decryption key.
  - (…)
- A **message is encrypted** by representing it as a number M, **raising M to** a publicly specified **power e**, and then taking the **remainder** when the result is **divided by** the publicly specified product, **n**, of two large secret prime numbers p and q.
- **Decryption** is similar; only a different, **secret, power d is used**, where $e \cdot d \equiv 1 \pmod{(p-1) \cdot (q-1)}$. **The security of the system rests in part on the difficulty of factoring the published divisor, n**.

Abstract (II)

- **Además** de cifrado asimétrico, especifica un protocolo para **Firma Digital**:
  - A message can be "**signed**" using a privately held decryption key.
  - **Anyone can verify this signature** using the corresponding publicly revealed encryption key.
  - Signatures cannot be forged, and a signer cannot later deny the validity of his signature. This has obvious applications in "electronic mail" and "electronic funds transfer" systems..

RSA

Proceso de generación de parejas de claves (pública / privada).

Cada usuario debe:

1. **Seleccionar** dos números primos muy grandes **p** y **q**
2. **Calcular n = p·q**
3. **Calcular phi(n) = phi(p)· phi(q)**
4. **Elegir** el exponente público **"e", tal que:**
   1. e > 0
   2. e, phi(n) son coprimos
5. **Calcular d,** tal que ***e·d = 1 mod (phi(n))***

⇨ **PU = (e, n)**

PR = (d, n)

Proceso de cifrado

$PU = (e_B, n_B)$

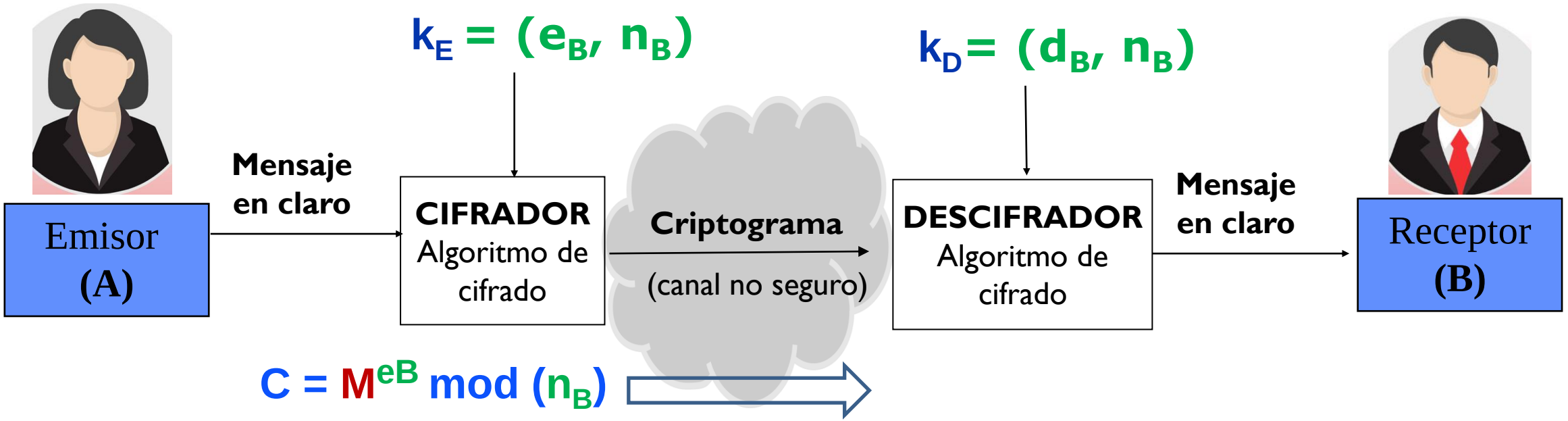
$PR = (d_A, n_A)$

El usuario (A) que envía el mensaje (cifrado) (a B) debe:

1. **Codificar** cada parte del mensaje en un número entero **M**
2. **Obtener la clave pública del receptor:** $PU_B = (e_B, n_B)$
3. **Calcular** $C = M^{eB} \bmod (n_B)$

Modelo de Criptosistema

ASIMÉTRICOS: Una clave (k_E) para cifrar y otra (k_D) para descifrar



- Se cifra con la **clave pública del receptor**

Proceso de descifrado

El usuario (B) que recibe el mensaje (cifrado) (de A) debe:

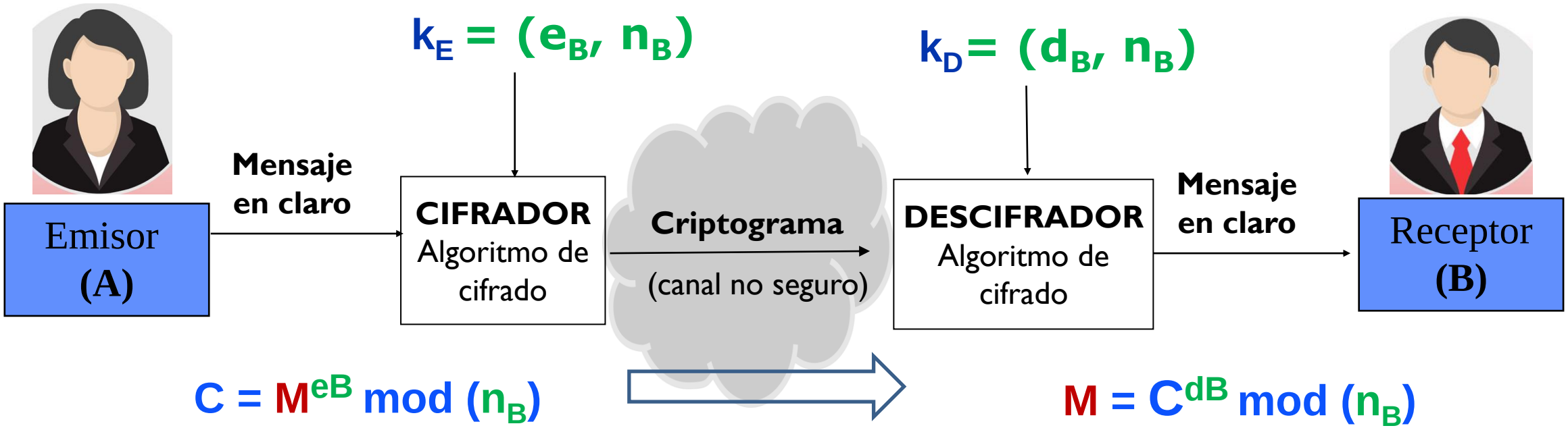
$PU = (e_B, n_B)$

$PR = (d_A, n_A)$

1. **Calcular** $M = C^{dB} \bmod (n_B)$
2. **Decodificar** el número entero **M** al alfabeto del mensaje

Modelo de Criptosistema

ASIMÉTRICOS: Una clave (k_E) para cifrar y otra (k_D) para descifrar

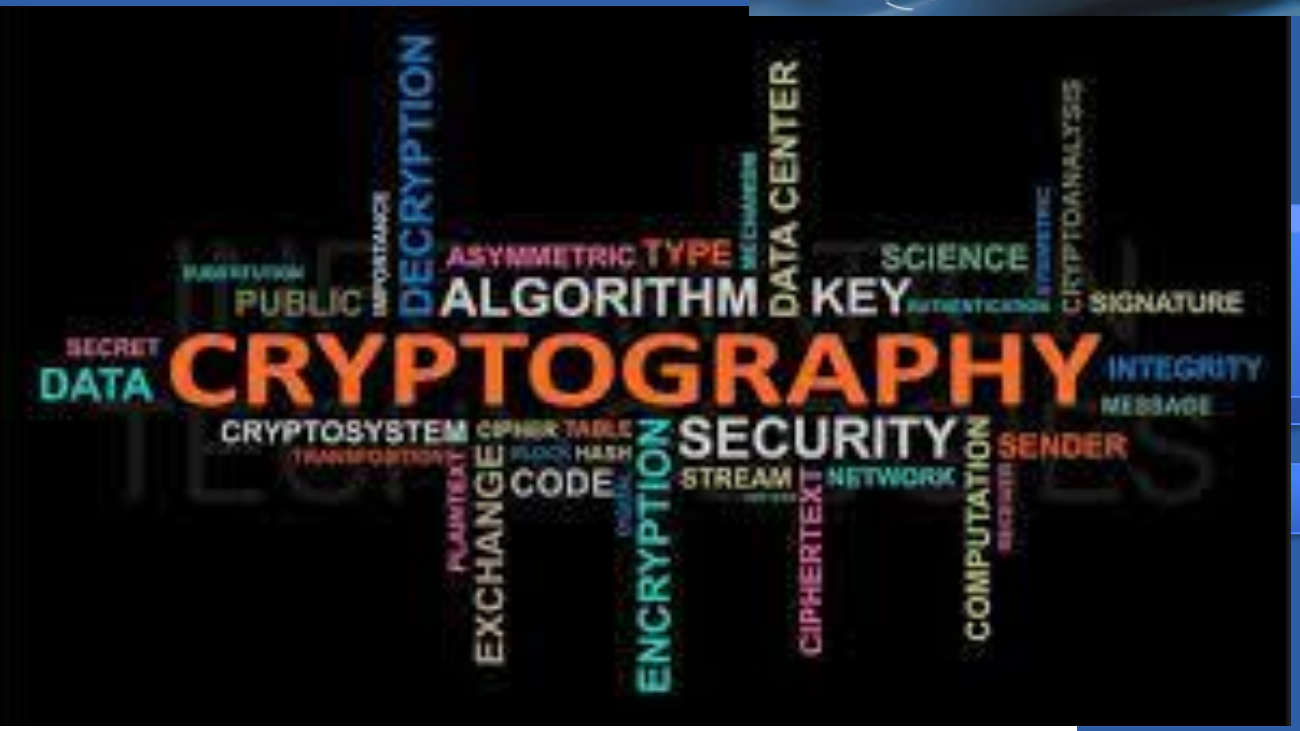


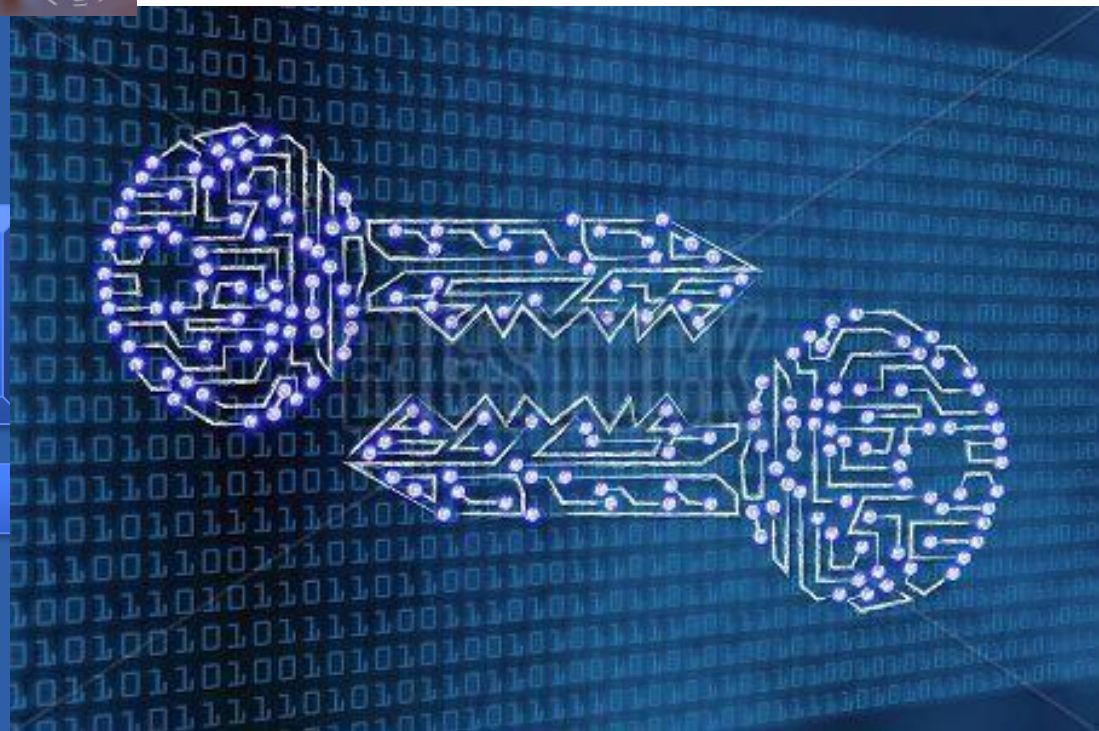
- Se descifra con la **clave <u>privada</u> del receptor**

Criptografía

Universidad Francisco de Vitoria
UFV Madrid

Tema 4.4
Firma Digital





Objetivos de Seguridad de la Información

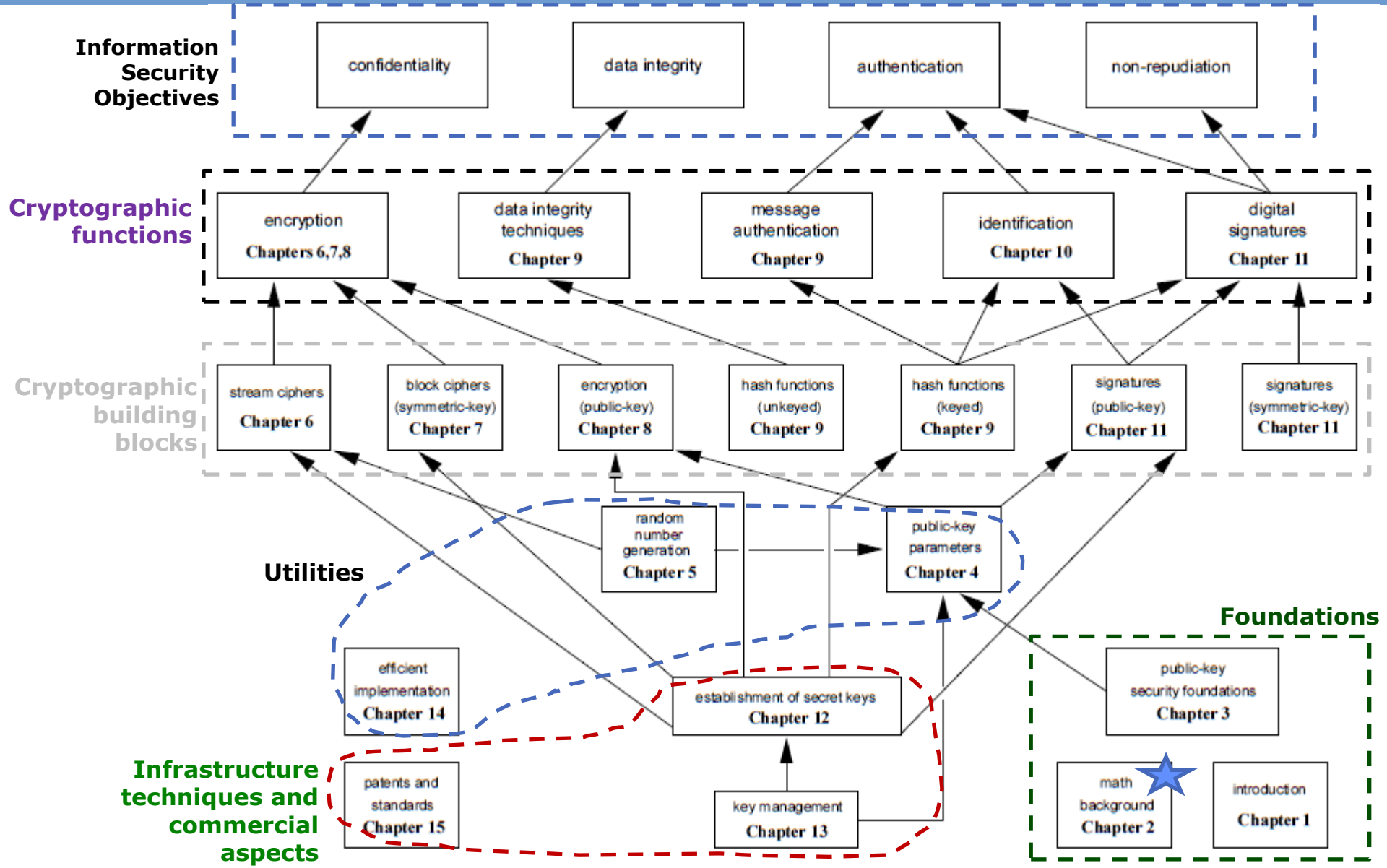
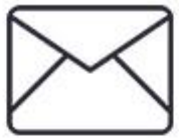


Image Source: HANDBOOK of APPLIED CRYPTOGRAPHY Alfred J. Menezes

Funciones Hash

¿Qué son y qué hacen las funciones Hash?

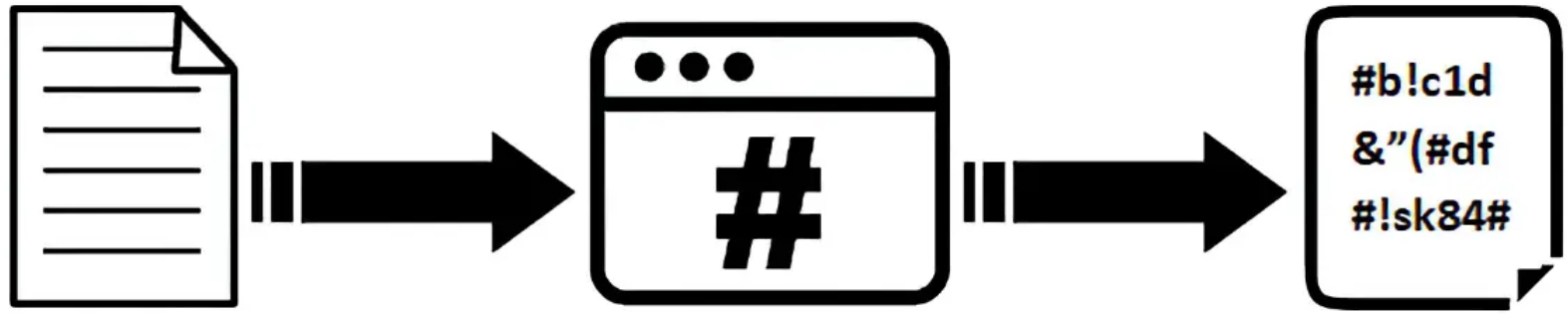


Longitud variable

Longitud fija

Funciones Hash

¿Qué son y qué hacen las funciones Hash?



Longitud variable

Longitud fija

https://www.youtube.com/watch?v=2BldESGZKB8

Funciones Hash: SHA-1 y SHA-2

FIPS 180-4 Secure Hash Standard

https://csrc.nist.gov/publications/detail/fips/202/final

FIPS 180-4 especifica siete algoritmos hash:

- ***SHA-1*** (Secure Hash Algorithm-1),

- **SHA-2 family** of hash algorithms:
  - ***SHA-224,***
  - ***SHA-256,***
  - ***SHA-384,***
  - ***SHA-512,***
  - ***SHA-512/224,*** and
  - ***SHA-512/256***.

Funciones Hash: SHA-1 y SHA-2

FIPS 180-4 Secure Hash Standard

When a **message** of
- **any length** less than 2^{64} bits (for SHA-1, SHA-224 and SHA-256) or
- less than 2^{128} bits (for SHA-384,, SHA-512/224 and SHA-512/256)

is **input** to a **hash algorithm**, the result is an **output** called a **message digest**.

The **message digests range in length from 160 to 512 bits**, depending on the algorithm.

Secure hash algorithms are typically used with other cryptographic algorithms, such as digital signature algorithms and keyed-hash message authentication codes, or in the generation of random numbers (bits).

Funciones Hash: SHA-3

SHA-3 Standard: Permutation-Based Hash and Extendable-Output Functions

This Standard specifies the **Secure Hash Algorithm-3 (SHA-3)** family of functions on binary data. Each of the SHA-3 functions is based on an instance of the **KECCAK** algorithm that **NIST** selected as the winner of the SHA-3 Cryptographic Hash Algorithm Competition.

The **SHA-3 family** consists of four cryptographic hash functions, called **SHA3-224, SHA3-256, SHA3-384, and SHA3-512**, and two extendable-output functions (XOFs), called SHAKE128 and SHAKE256.
Hash functions are **components for** many important information **security applications**, including

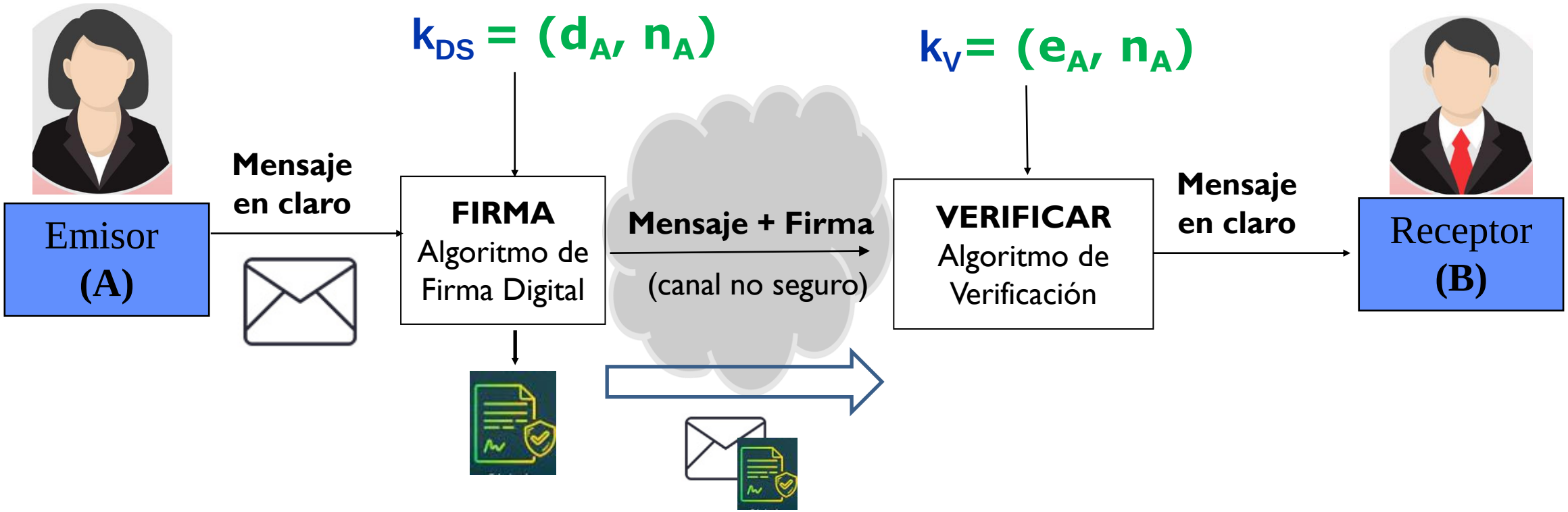
1) the generation and verification of **digital signatures**,
2) **key derivation**, and
3) **pseudorandom** bit generation.

The hash functions specified in this Standard **supplement the SHA-1** hash function **and the SHA-2** family of hash functions that are specified in FIPS 180-4, the Secure Hash Standard.

https://csrc.nist.gov/publications/detail/fips/202/final

Firma Digital

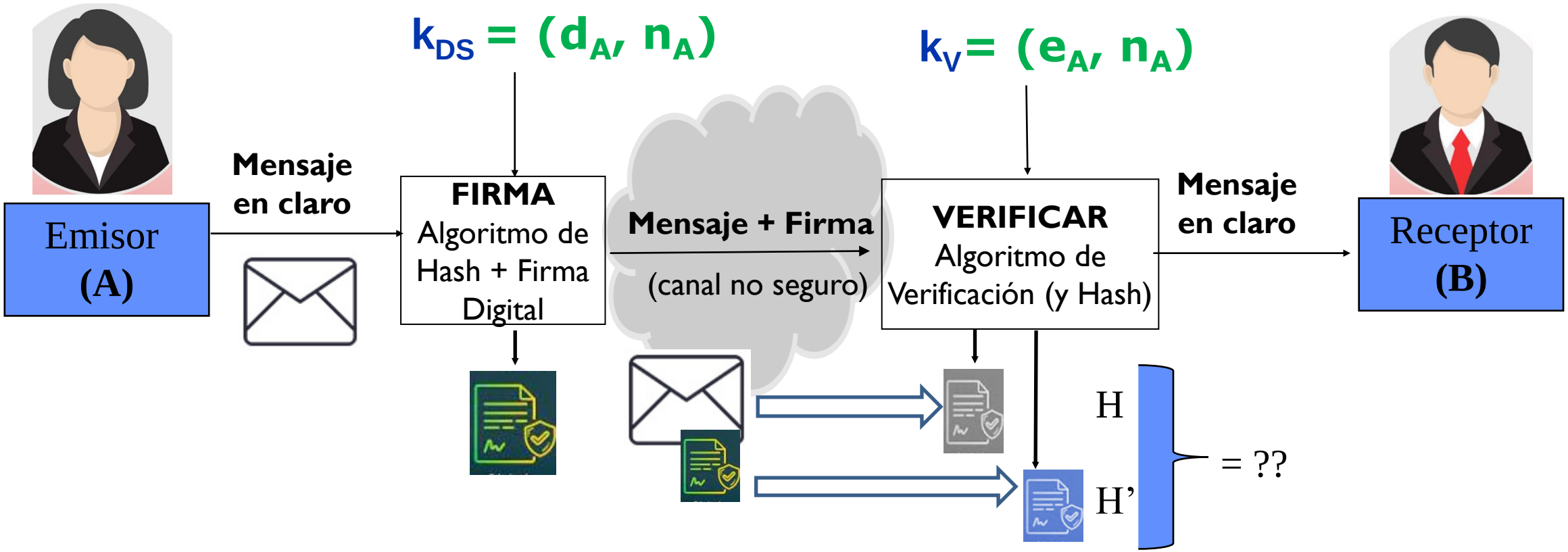
ASIMÉTRICOS: Una clave (k_{DS}) para firmar y otra (k_V) para verificar



- Se **firma** con la **clave privada del emisor**

Firma Digital

ASIMÉTRICOS: Una clave (k_{DS}) para firmar y otra (k_V) para verificar



- Se **verifica** con la **clave pública del emisor**

Firma Digital con RSA

Proceso de generación de parejas de claves (pública / privada).

(igual que para cifrado / descifrado)

Cada usuario debe:

1. **Seleccionar** dos números primos muy grandes **p** y **q**
2. **Calcular n = p·q**
3. **Calcular phi(n) = phi(p)· phi(q)**
4. **Elegir** el exponente público "**e**", **tal que:**
   1. e > 0
   2. e, phi(n) son coprimos
5. **Calcular d,** tal que ***e·d = 1 mod (phi(n))***

⇨ **PU = (e, n)**

PR = (d, n)

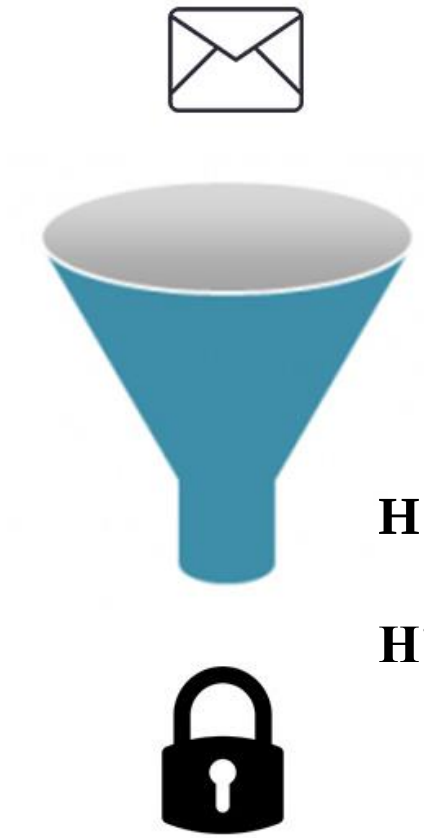
Y además…

Firma Digital con RSA

Utilización de la misma función Hash en emisión (firma) y en recepción (verificación de la firma)

H = Hash (M)

S = DS (H)



H = Hash (M)

H’ = V (S)

H = H’ ??

Firma Digital con RSA

Proceso de firma digital

El usuario (A) que envía el mensaje (cifrado) (a B) debe:

$PU = (e_B, n_B)$

$PR = (d_A, n_A)$

1. **Codificar** cada parte del mensaje en un número entero **M**
2. **Acceder a su clave privada (del emisor: $PR = (d_A, n_A)$)**
3. **Calcular H = Hash (M)**
4. **Calcular $S = H^{dA} \bmod (n_A)$**

Proceso de verificación

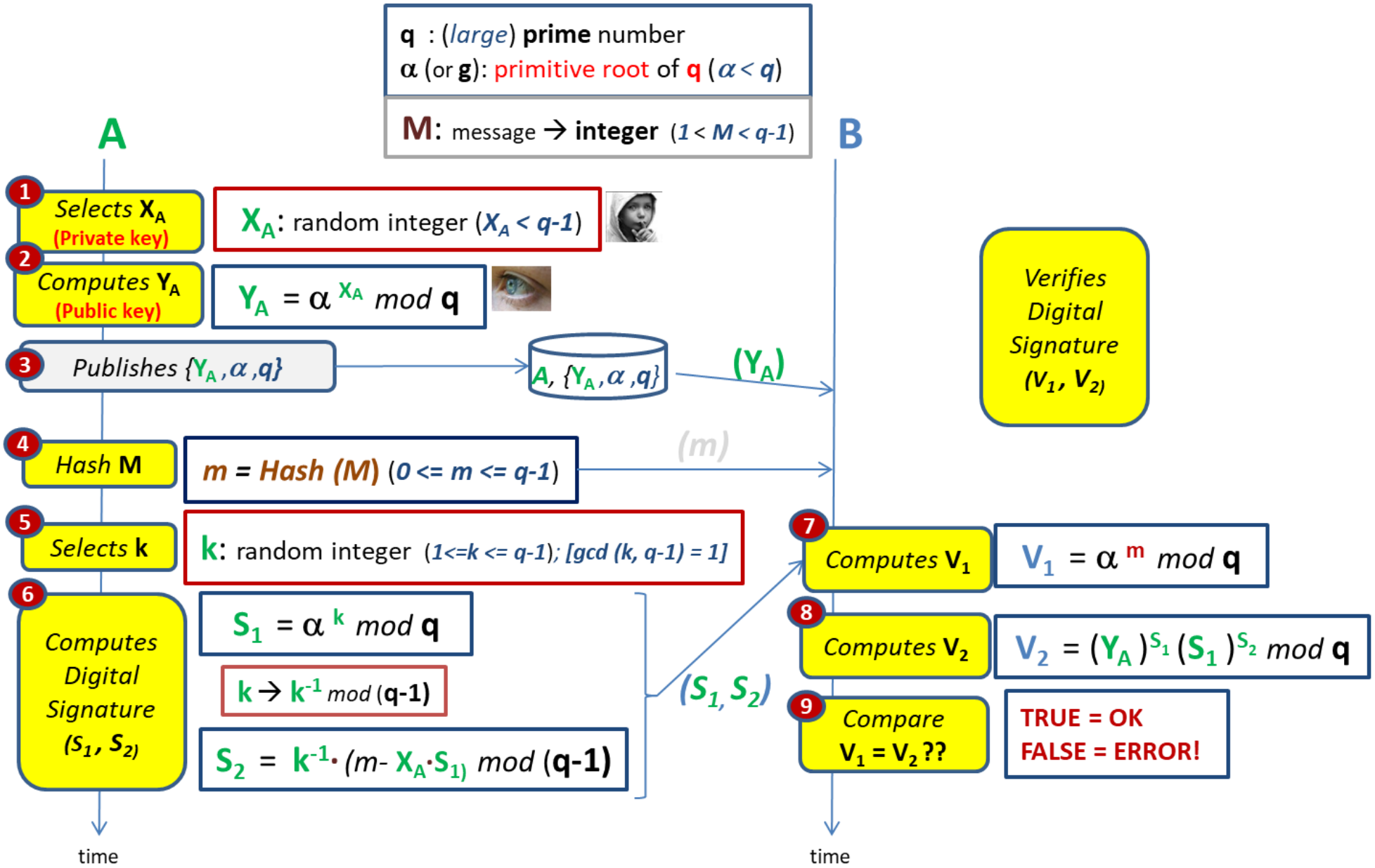
El usuario (B) que recibe el mensaje (cifrado) (de A) debe:

$PU = (e_B, n_B)$

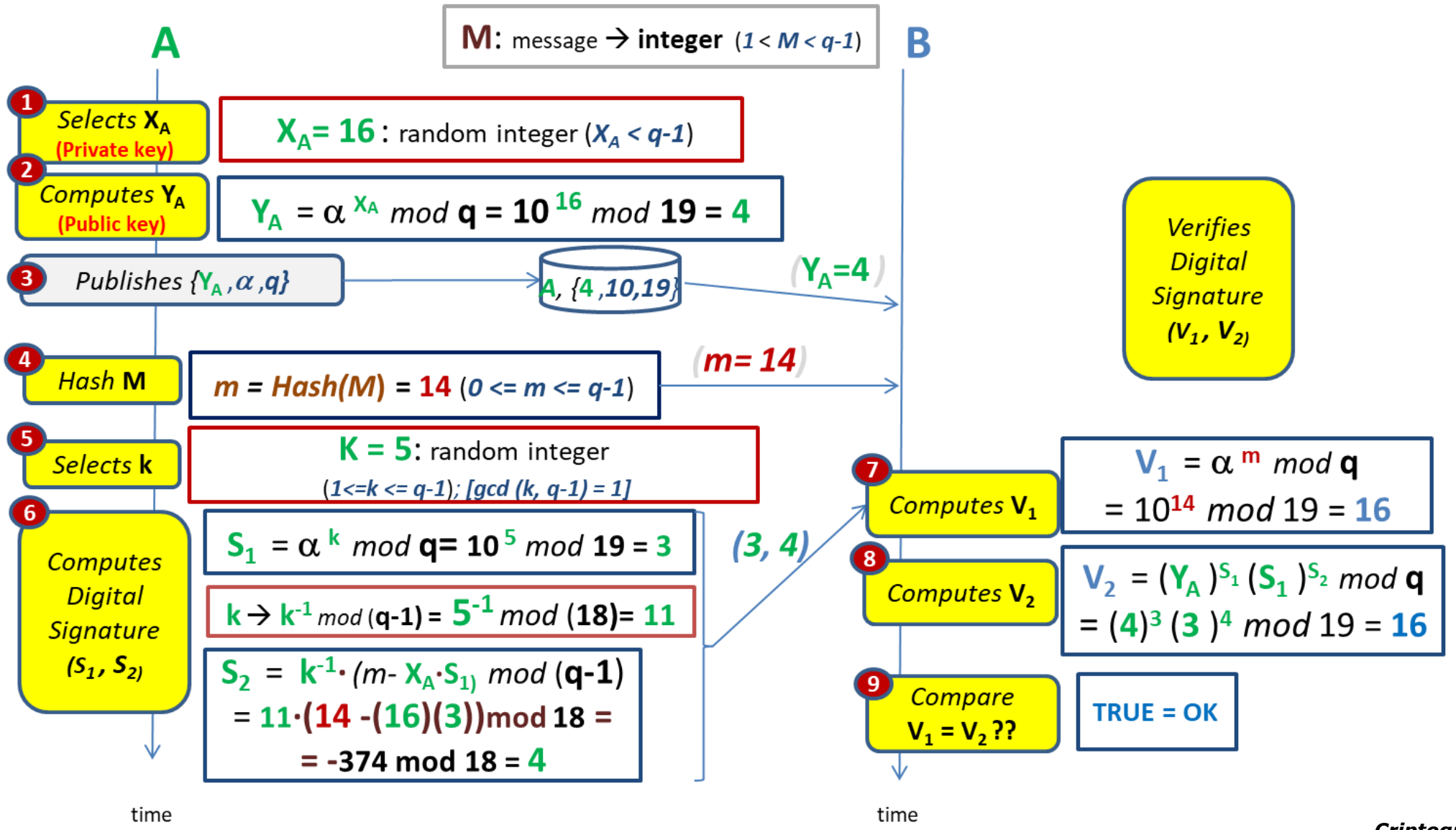
$PR = (d_A, n_A)$

1. **Obtener la clave pública del emisor $PU_A = (e_A, n_A)$**
2. **Recibir el mensaje original M, y la firma asociada S**
3. **Calcular el Hash H = Hash(M)**
4. **Calcular $H' = S^{eA} \bmod (n_A)$**
5. **Comparar H y H'**
   1. **Si son iguales → mensaje válido y corresponde efectivamente al emisor.**

Firma Digital con Elgamal



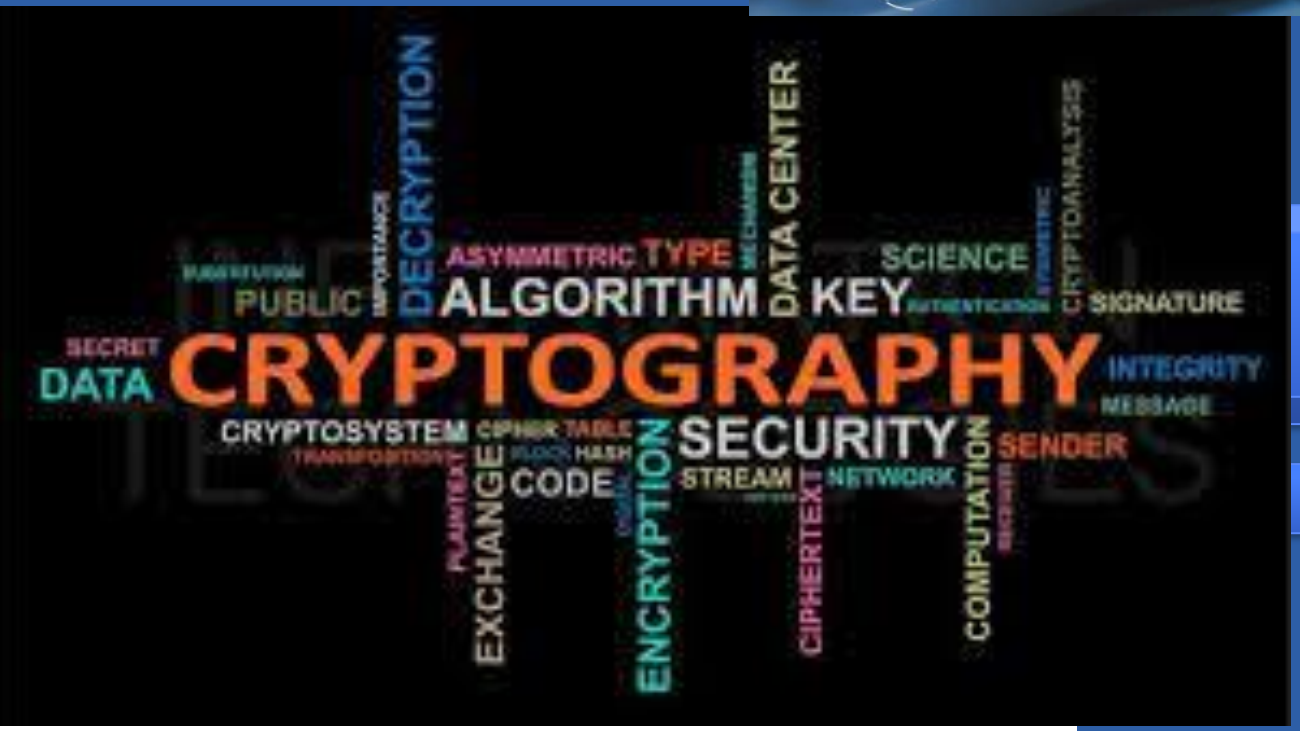
Firma Digital con Elgamal

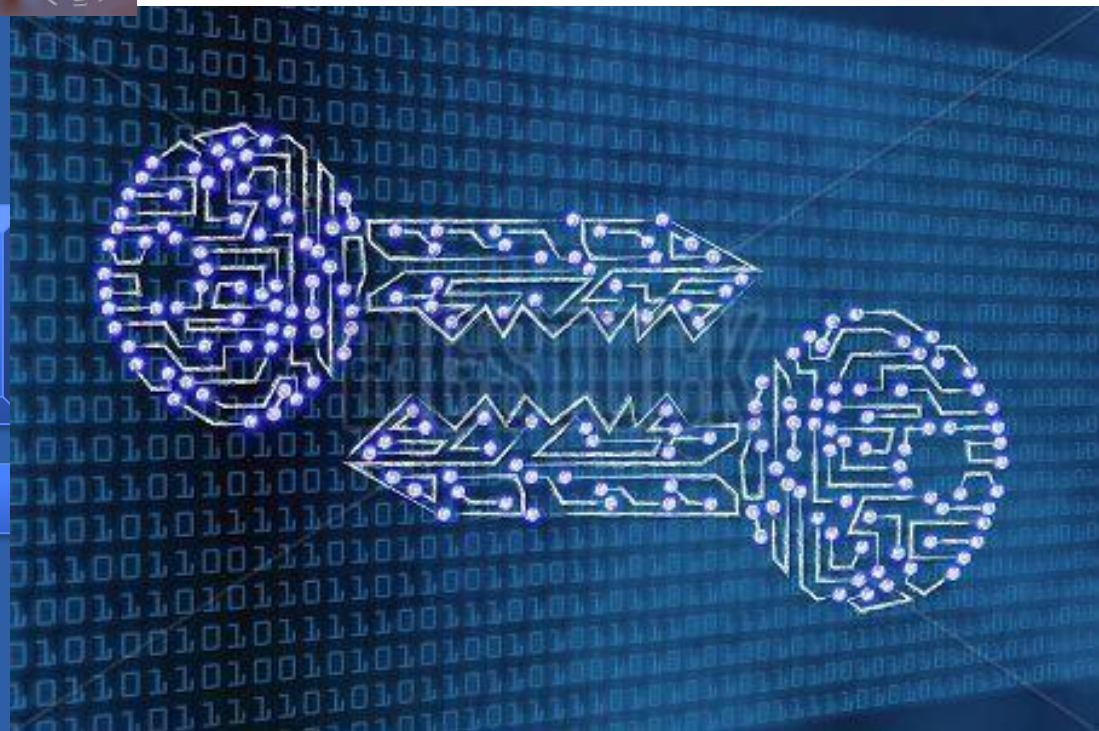


Criptografía

Universidad Francisco de Vitoria
UFV Madrid

Tema 4.5
Modelos Híbridos





Modelo de Criptosistema

- Hasta ahora hemos visto…
  - **CONFIDENCIALIDAD**
    - **Cifrado simétrico**
      - ✓ **Eficiente para grandes volúmenes de datos**
    - **Cifrado asimétrico**
      - ✓ **Eficiente para intercambio de claves de manera segura y cifrado en canales no seguros**
  - **INTEGRIDAD Y AUTENTICACIÓN**
    - **Firma digital**

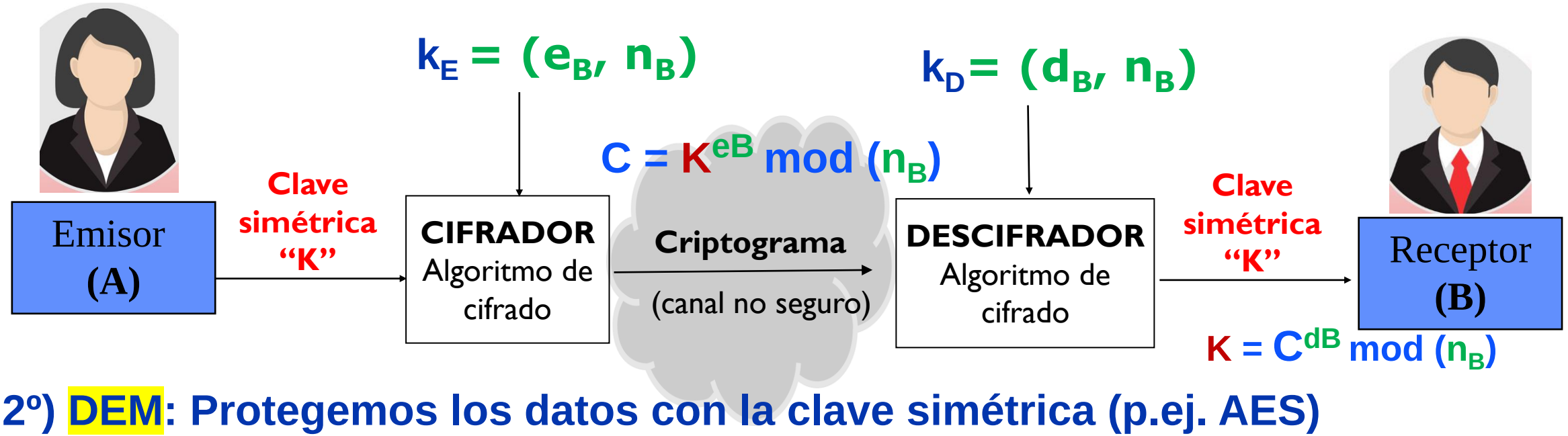
Modelo de Criptosistema

- Hasta ahora hemos visto…
  - **CONFIDENCIALIDAD**
    - **Cifrado simétrico**
      - ✓ **Eficiente para grandes volúmenes de datos**
    - **Cifrado asimétrico**
      - ✓ **Eficiente para intercambio de claves de manera segura y cifrado en canales no seguros**
  - **INTEGRIDAD Y AUTENTICACIÓN**
    - **Firma digital**

¿Y si los combinamos?

Modelo de Criptosistema: KEM/DEM

1º) KEM: Protegemos la clave simétrica con cifrado asimétrico



2º) DEM: Protegemos los datos con la clave simétrica (p.ej. AES)

Modelo de Criptosistema

CIFRADO + FIRMA DIGITAL: ¡¡Múltiples combinaciones!!

Emisor
(A)

Mensaje en claro

CIFRADOR
Algoritmo de cifrado

FIRMA
Algoritmo de Firma Digital

(canal no seguro)

DESCIFRADOR
Algoritmo de cifrado

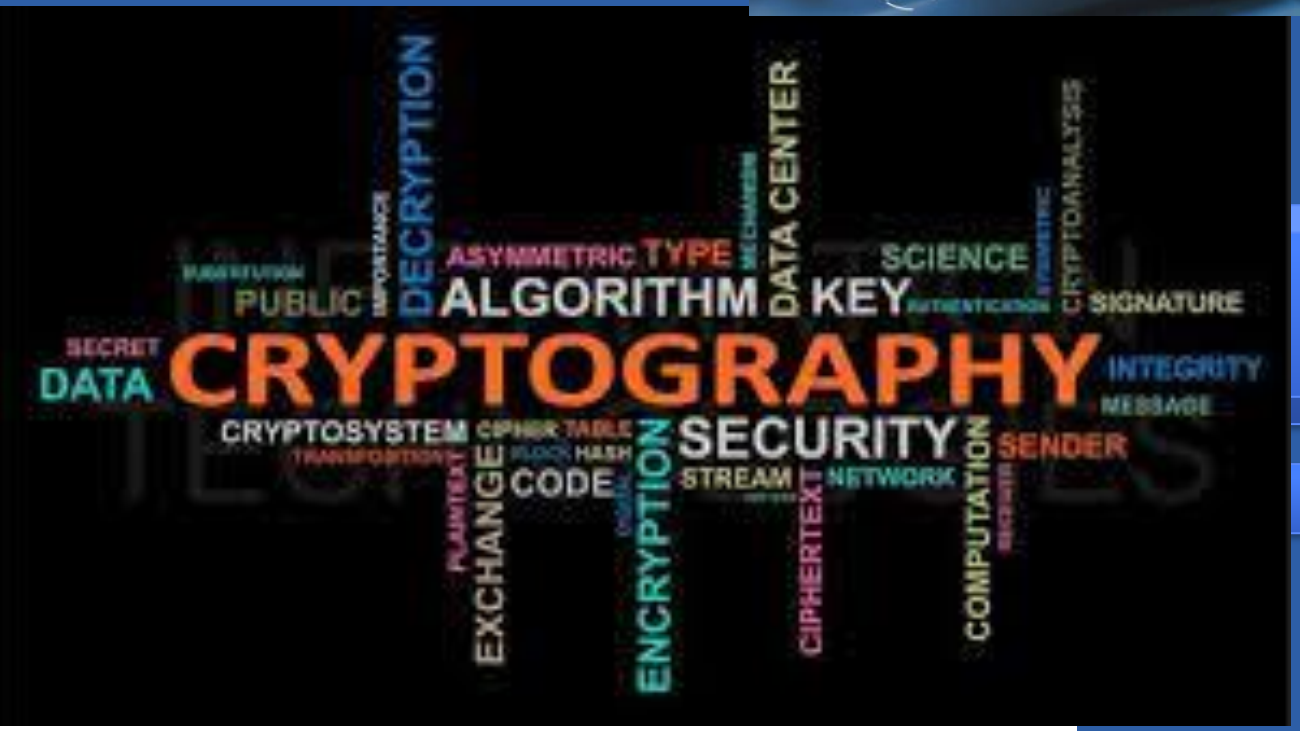
VERIFICACION
Algoritmo de Firma Digital

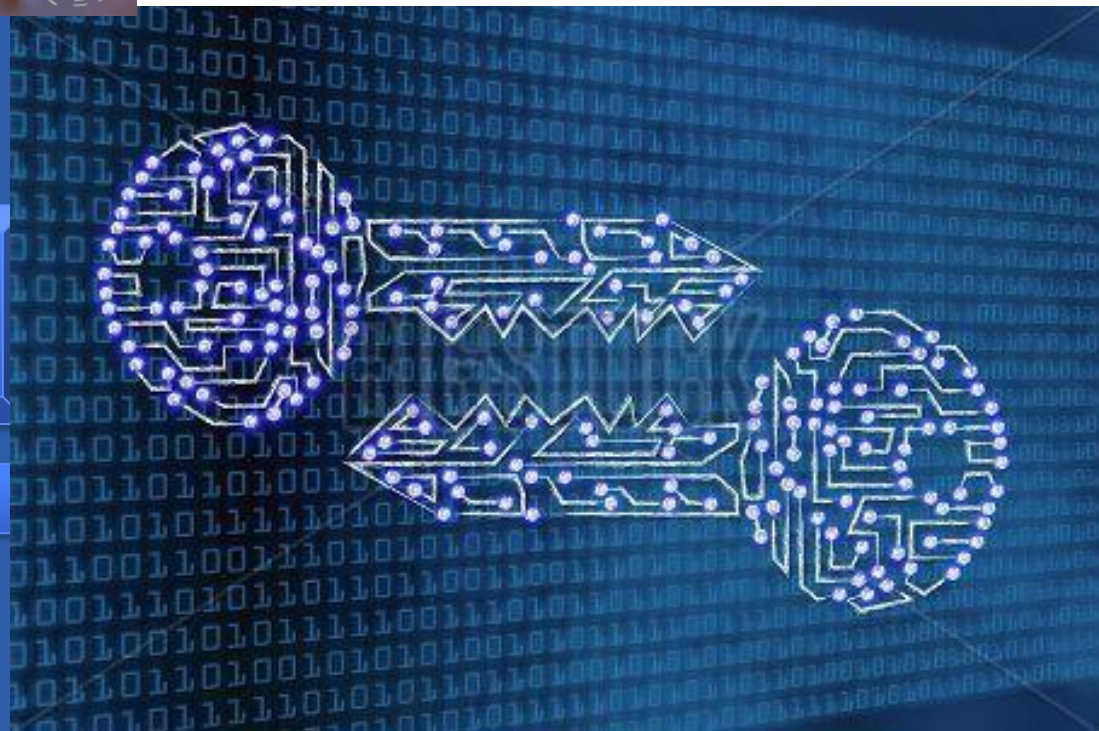
Receptor
(B)

Criptografía

Universidad Francisco de Vitoria
UFV Madrid

Tema 4.6
PKI





Sistemas de Clave Pública

- Introducción
- Distribución de claves
- Cifrado asimétrico
- Firma Digital
- Modelos Híbridos
- **Certificados Digitales y PKI**

Necesidad de algo más que algoritmos

- Los sistemas de clave asimétrica no garantizar la vinculación entre el usuario y las claves públicas asociadas
- Confidencialidad ¿Cómo podemos garantizar que la clave pública del receptor realmente corresponde a ese usuario?
- Firma digital ¿Cómo podemos garantizar que la clave pública del firmante realmente corresponde a ese usuario?

- Necesitamos algo más que meros algoritmos para garantizar el funcionamiento adecuado:
  - **Infraestructura de Clave Pública (PKI)**

Certificados Digitales

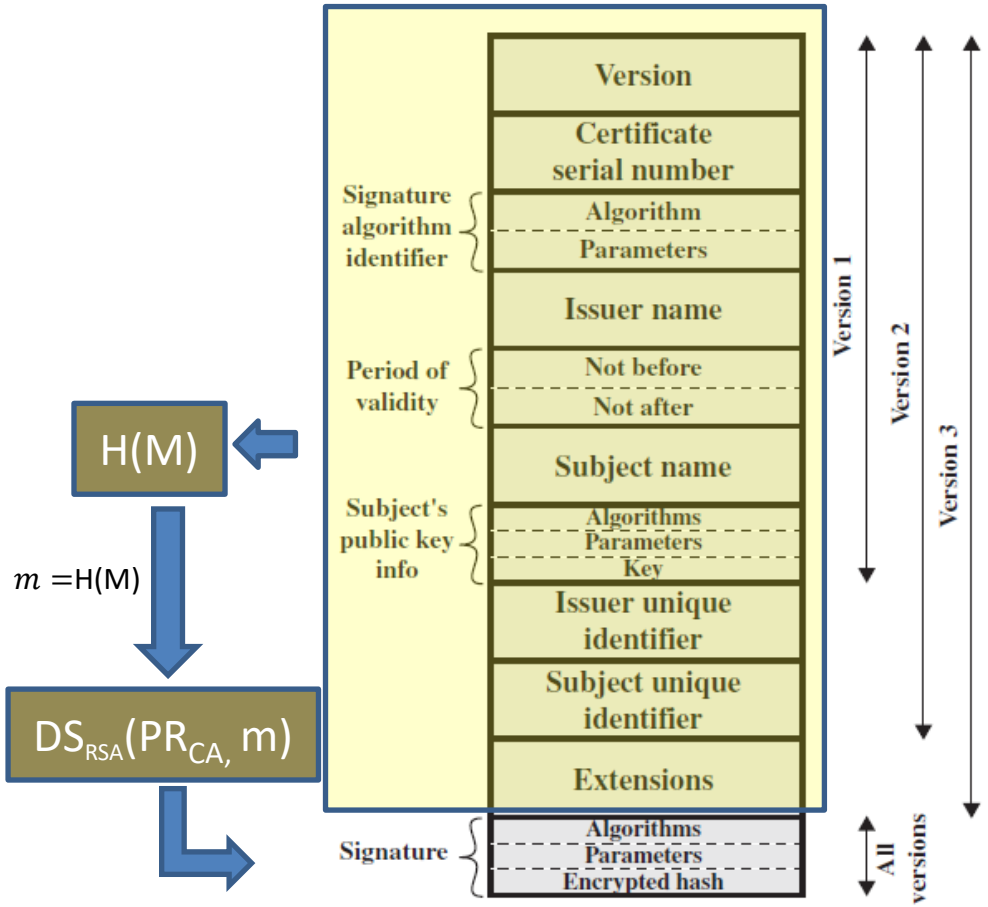
- Vinculan la identidad de un sujeto, con su clave pública
- Además, permiten determinar información adicional:
  - Fecha de validez
  - Parámetros públicos de la clave pública
    - Algoritmo
    - Parámetros comunes
    - Uso esperado (para cifrar, para firma personal, para firma delegada…)
- Van firmados digitalmente por el emisor del certificado
  - E indican los parámetros para poder verificar dicha firma

Certificados Digitales: ITU-T recomendación X.509:

- **ITU-R X.509**
  - Es **parte de la familia de normas X.500** que definen un **Servicio de Directorio.**
  - Define **protocolos de autenticación** basados en el empleo de **Certificados de Clave Pública**
    - basados en el uso de **criptografía de clave pública** y **firma digital**

https://www.itu.int/rec/T-REC-X.509/es

Certificados Digitales: Formato X.509:

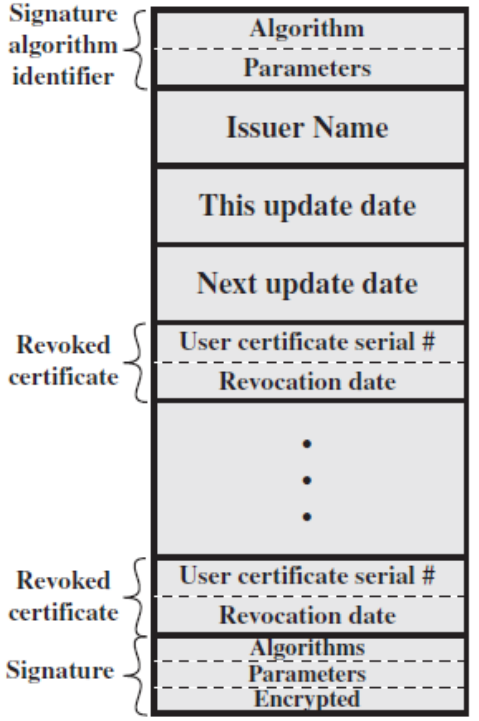


(a) X.509 certificate

Figure 14.14 X.509 Formats

Need to revoke before it expires when:

- user's private key compromised
- Name changed, CA's policies…
- CA's certificate compromised



(b) Certificate revocation list

Certificados Digitales: Operación X.509

Escenario: "A" necesita enviar un mensaje cifrado "M" (según esquema calve public) a "B"
→ "A" necesita $\mathbf{PU_B}$

1. "A" request "$\mathbf{PU_B}$" to directory service
2. "A" is certified by "X": **X <<A>>**
3. "X" is certified by "W": **W <<X>>**
4. "W" is certified by "V": **V <<W>>**
5. "Y" is certified by "V": **V <<Y>>**
6. "Z" is certified by "Y": **Y <<Z>>**
7. "B" is certified by "Z": **Z <<B>>** → $\mathbf{PU_B}$
8. Directory service returns $\mathbf{PU_B}$ **to "A"**
9. "A" send encrypt messages to B: $E(PU_B, M)$

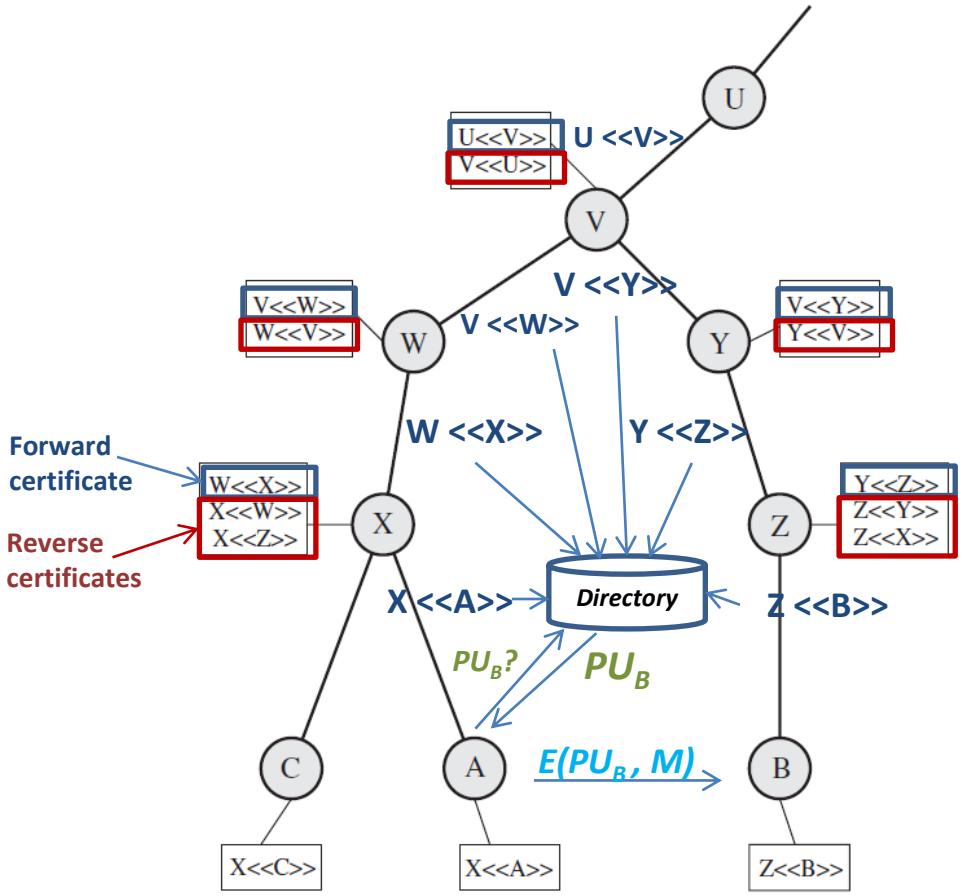
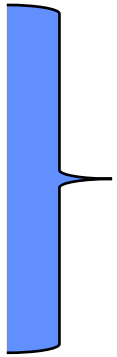


Figure 14.15 X.509 Hierarchy: A Hypothetical Example

Necesidad de algo más que algoritmos: PKI

- La **RFC 2828** (*Internet Security Glossary*) define la **Infraestructura de Clave Pública (PKI)** como el **conjunto de:**
  - HW
  - SW
  - Personas
  - Políticas
  - y Procedimientos
- **Necesarios para:**
  - Crear
  - Gestionar
  - Almacenar
  - Distribuir y Revocar



Certificados digitales basados en criptografía asimétrica.

https://www.rfc-editor.org/rfc/pdfrfc/rfc2828.txt.pdf

Necesidad de algo más que algoritmos: PKI

- El principal objetivo para desarrollar una **Infraestructura de Clave Pública (PKI)** es permitir la adquisición y distribución de claves públicas de una manera:
  - Segura,
  - Adecuada, y
  - Eficiente.

PKI X.509 (PKIX)

➢ PKIX elements:

- ✓ **End entity:** A generic term used to denote end users, routers, servers, devices, etc.
- ✓ **Certification authority (CA):** The issuer of certificates and (usually) certificate revocation lists (CRLs)
- ✓ **Registration authority (RA):** (*optional*) administrative functions from the CA.
- ✓ **CRL issuer:** (*optional*) CA can delegate to publish CRLs.
- ✓ **Repository:** A generic term used to denote any method for storing certificates and CRLs so that they can be retrieved by end entities.

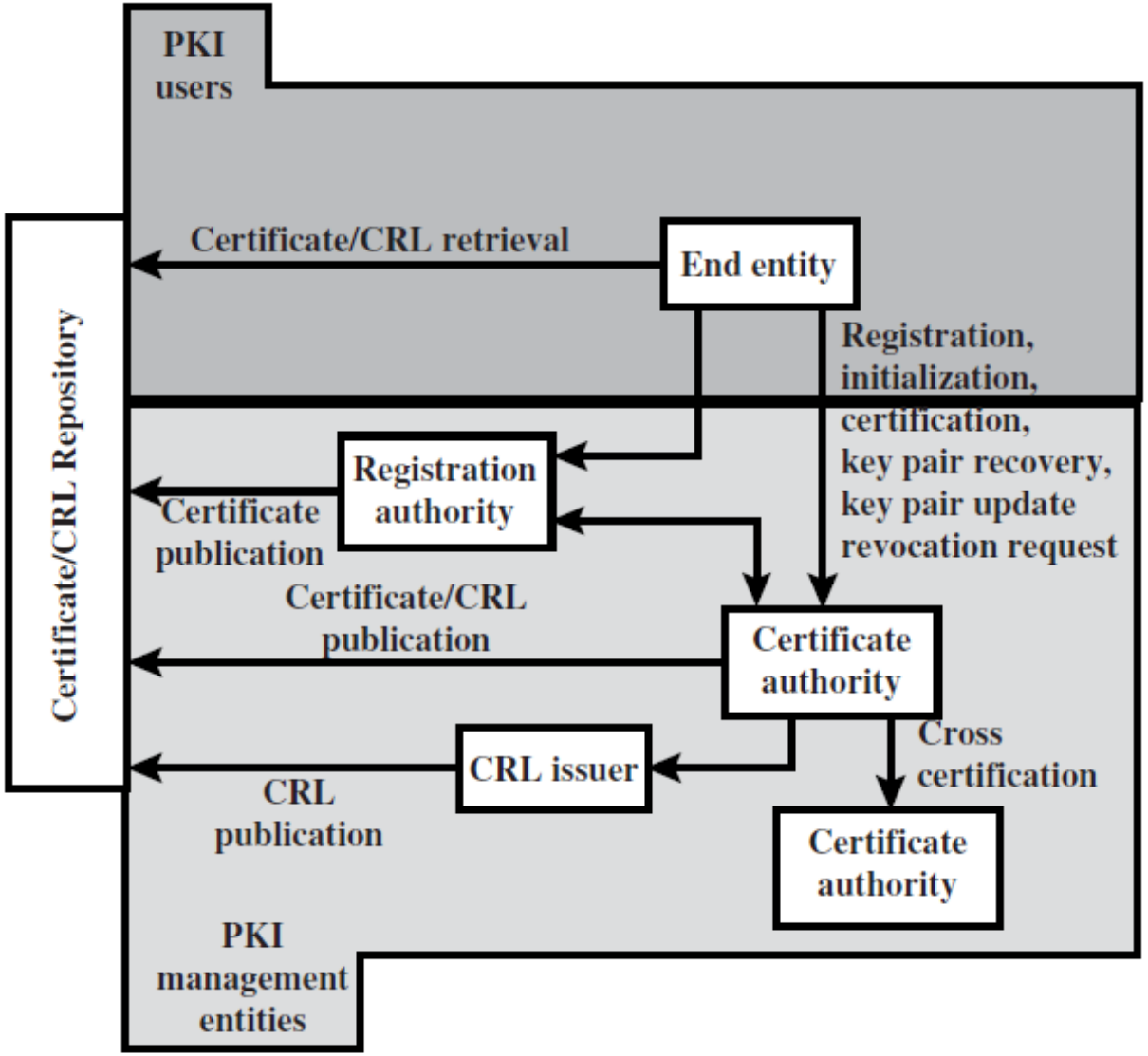
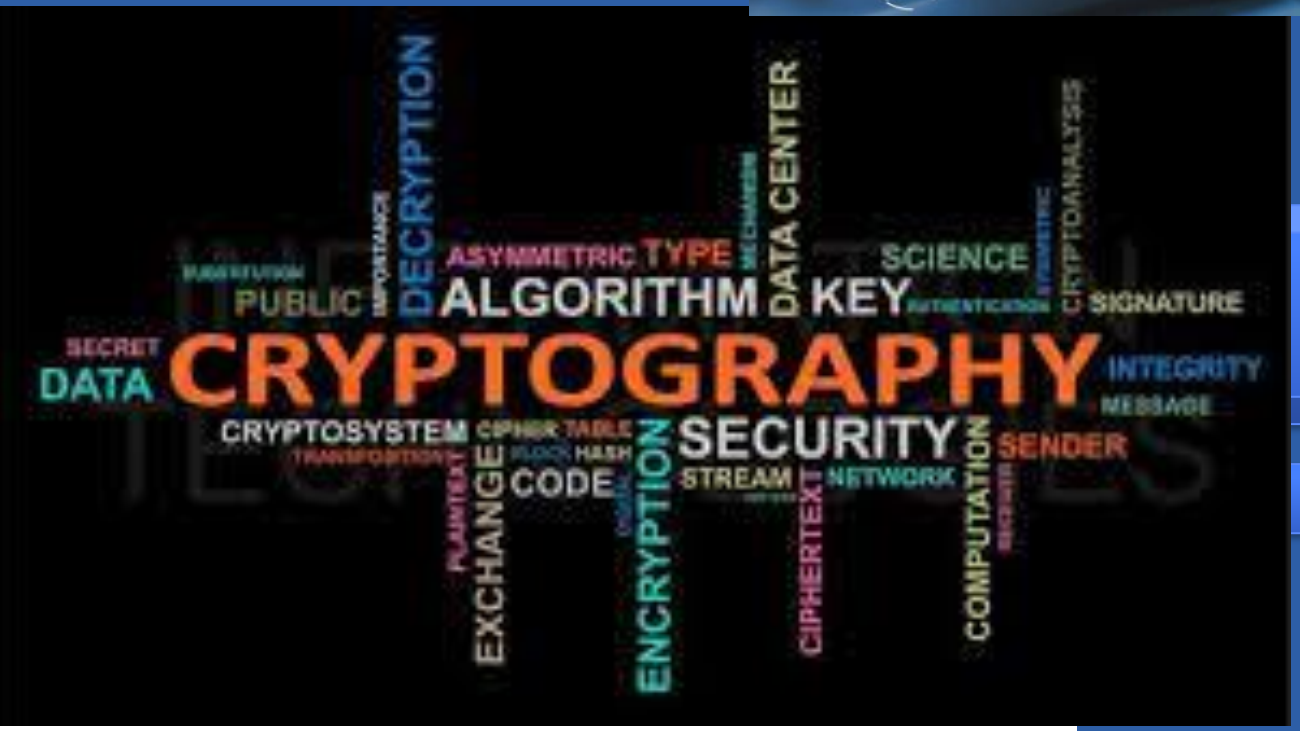


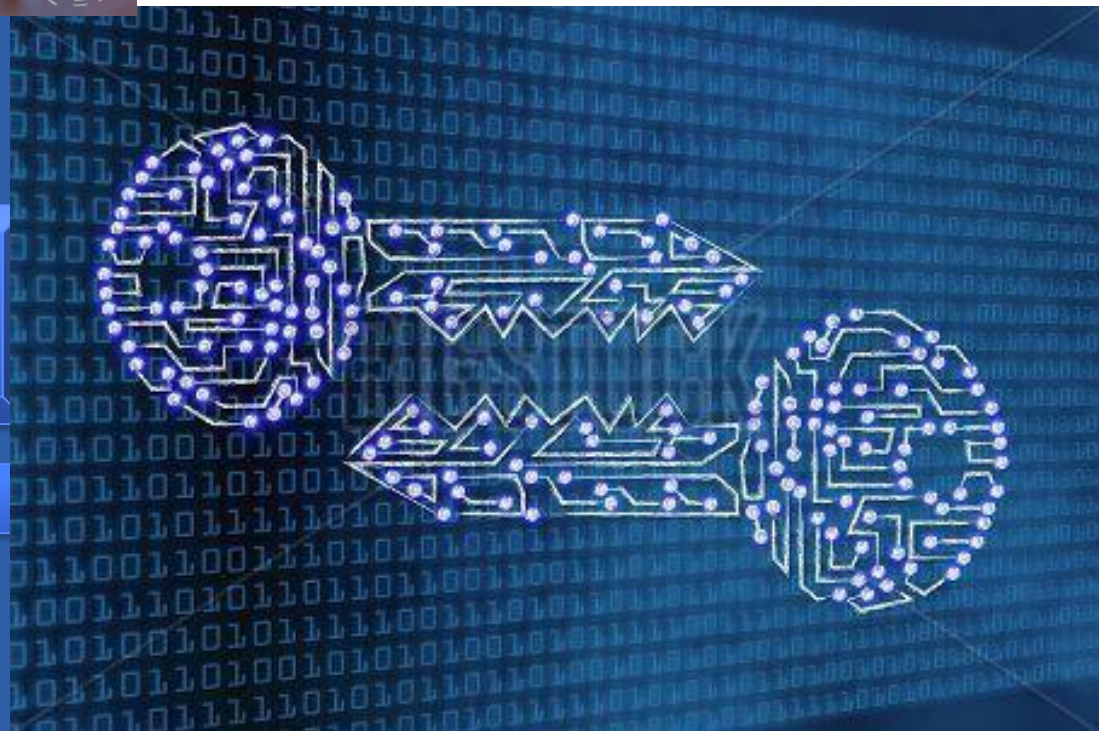
Figure 14.16 PKIX Architectural Model

Criptografía

Universidad Francisco de Vitoria
UFV Madrid

MATERIAL ADICIONAL: ECC





ECC
Additional slides

José Luis de Miguel Álvarez

Curvas Elípticas

¿Qué es una curva elíptica?

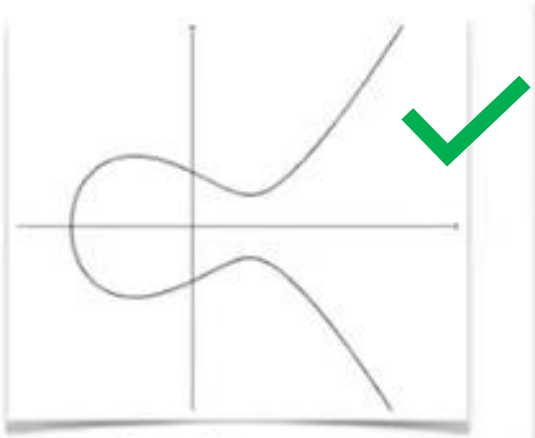
Una curva elíptica es el conjunto de todos los puntos (x, y) tales que

$$y^2 = x^3 + ax + b$$

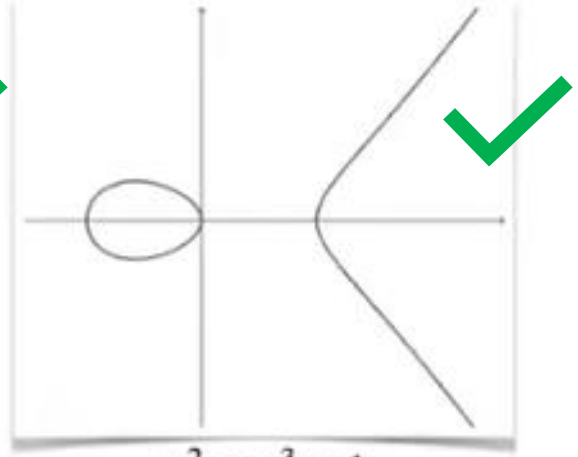
+ un punto "al infinito" $\mathcal{O}$.

La curva debe ser suave, eso es equivalente a $4a^3 + 27b^2 \neq 0$.

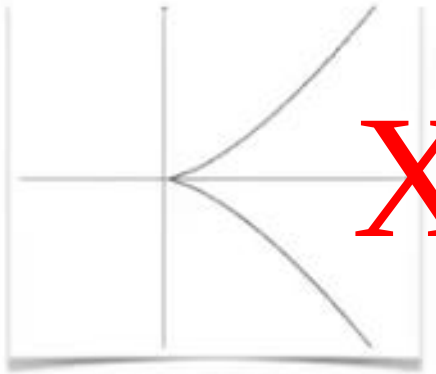
Determinante de la curva debe ser **distinto de cero**



$y^2 = x^3 - 3x + 3$



$y^2 = x^3 + 1$



$y^2 = x^3$

X → ¡No es CE!

Curvas Elípticas

La curva, además de objeto geométrico, es un objeto algebraico: **Grupo Abeliano**

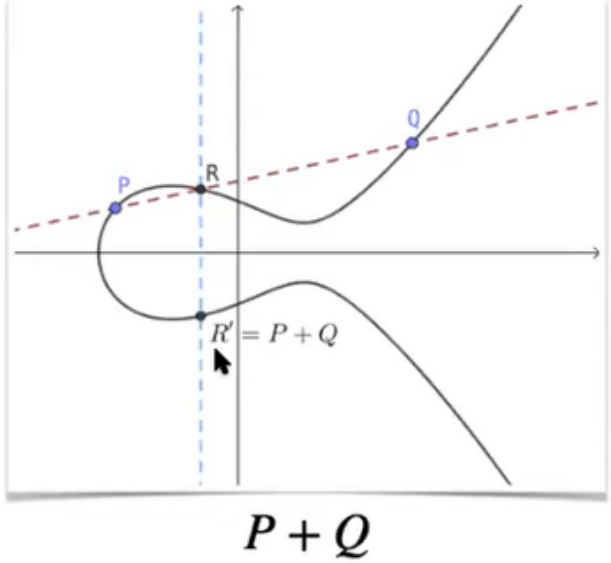
Curvas elípticas

La curva elíptica E tiene una estructura de grupo abeliano.

Grupo

Conjunto → Puntos de E

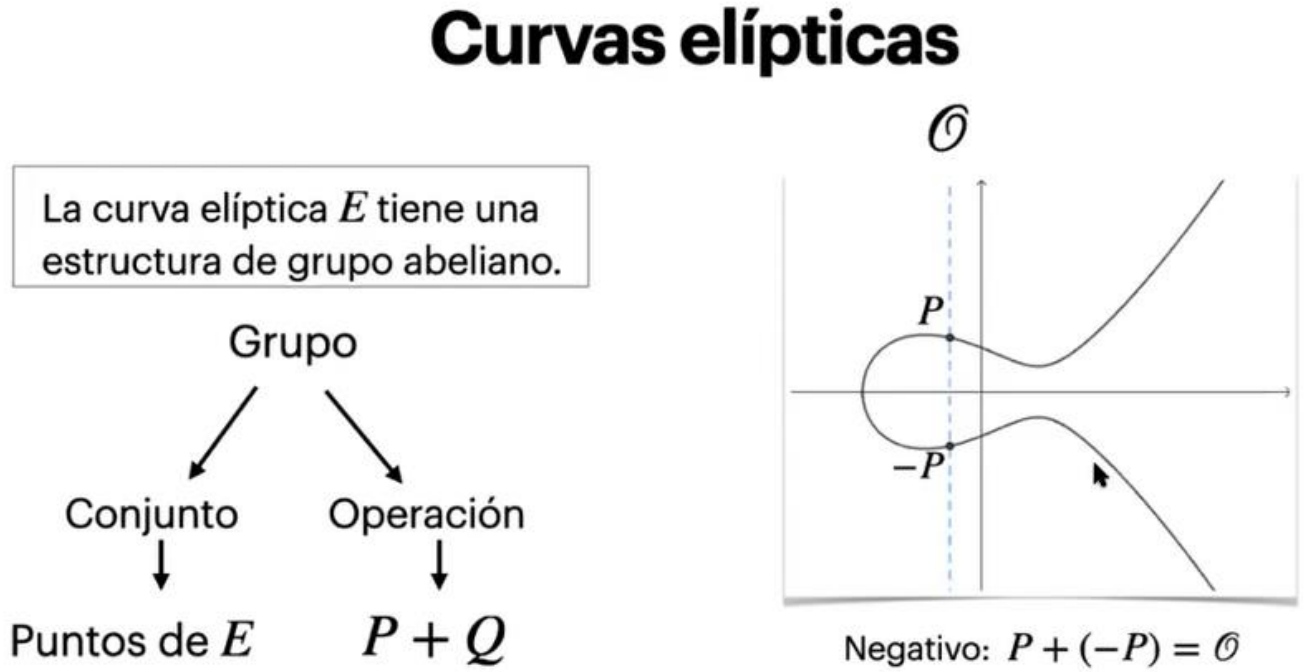
Operación → $P + Q = ?$



Se define la "**suma**" como el punto **reflejado** ***(R')*** de la intersección (R) de la **secante** entre los dos puntos a "sumar" (P y Q)

Curvas Elípticas

La curva, además de objeto geométrico, es un objeto algebraico: **Grupo Abeliano**



Se define "**cero**" (***O***) como el punto **infinito** resultante la intersección de la operación ***P + (-P)***

→ Al sumar puntos en vertical, la intersección es el infinito, por eso hay que añadirle al grupo abeliano para que todos los resultados de sumas pertenezcan al grupo.

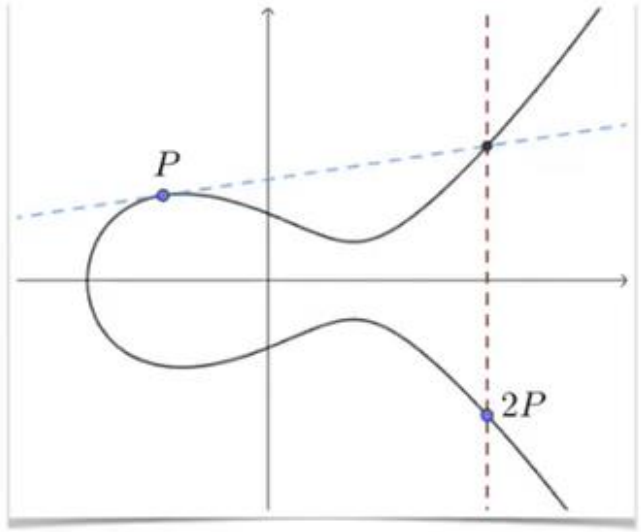
Curvas Elípticas

La curva, además de objeto geométrico, es un objeto algebraico: **Grupo Abeliano**

Calculando

$$2P = P + P$$

Tangente de la curva sobre P



Se define la "**suma**" (***2P***) la suma del valor del **punto P consigo mismo**

→ **Al sumar P consigo mismo, se aplica la tangente de la curva en P, y se coge la reflexión (2P) del corte de esa tangente sobre la curva**

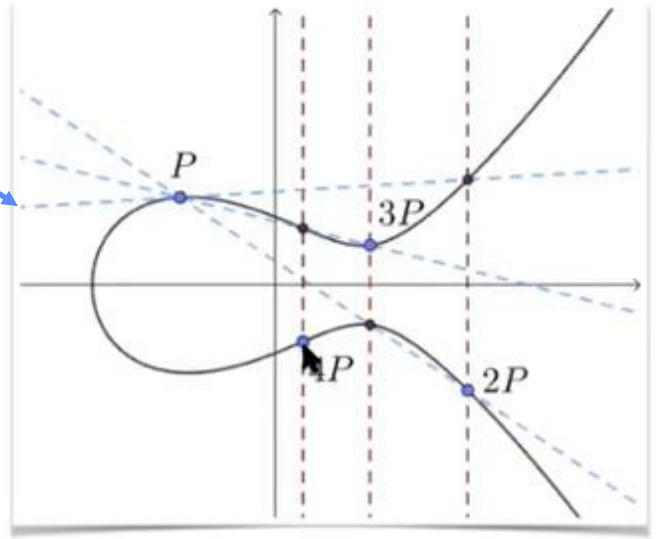
Curvas Elípticas

La curva, además de objeto geométrico, es un objeto algebraico: **Grupo Abeliano**

Calculando

$$kP = P + P + \cdots + P$$

Tangente de la curva sobre P



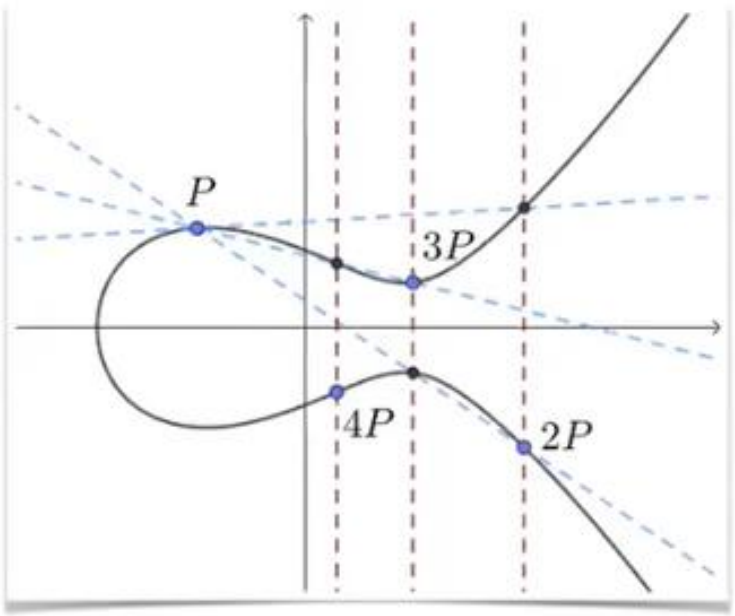
Se define la "**suma**" (***kP***) la suma de "**k" veces** el valor del **punto P**

→ **Combinamos las propiedades anteriores (P+Q, siendo Q=k·P)**

Curvas elípticas

Calculando

$$kP = P + P + \cdots + P$$



Si conocemos el resultado

$$Q = kP$$

¿podemos encontrar k?

Problema del logaritmo discreto elíptico

¡No existen algoritmos eficientes para resolverlo!

Curvas Elípticas → Aplicación para D-H

Clave: n

Público

$E : y^2 = x^3 + ax + b$

P un punto base

Clave: m

$nP = Q_A$

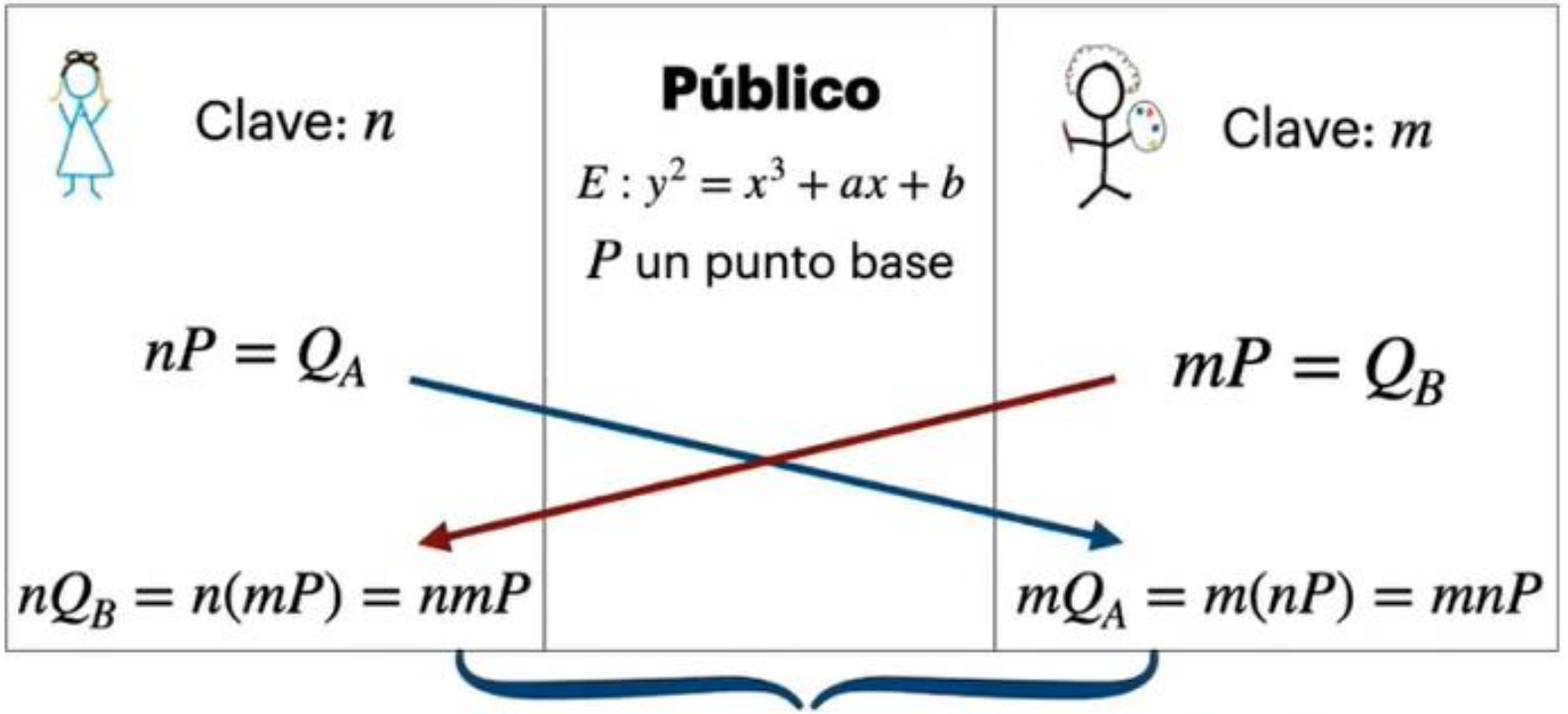
$mP = Q_B$

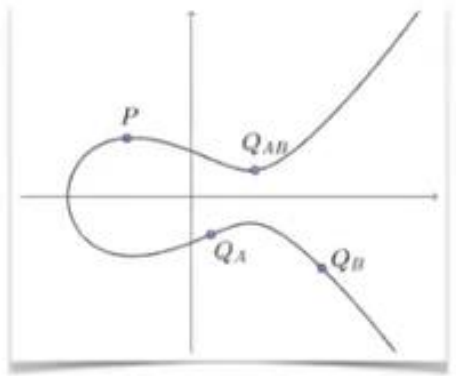
$nQ_B = n(mP) = nmP$

$mQ_A = m(nP) = mnP$

Curvas Elípticas → Aplicación para D-H

Alice y Bob 2.1: DH + Curvas Elípticas





Clave secreta compartida: $nmP = mnP = Q_{AB}$

Criptografía

Universidad Francisco de Vitoria
UFV Madrid

Tema 4
Criptografía de Clave Pública