Tema 11

Esquemas de firma digital

CURSO CRIPTOGRAFÍA Y SEGURIDAD INFORMÁTICA

Ana I. González-Tablas Ferreres
José M. de Fuentes García-Romero de Tejada
Lorena González Manzano
Pablo Martín González

uc3m | Universidad Carlos III de Madrid

COSEC

Índice

- 11. Esquemas de firma digital
  - Esquemas de firma digital
  - RSA (firma)
  - El Gamal (firma)
  - Ataques
  - Firma digital y cifrado

Ana I. González-Tablas Ferreres, José M. de Fuentes García-Romero de Tejada, Lorena González Manzano, Pablo Martín González

Índice

- 11. Esquemas de firma digital
  - **Esquemas de firma digital**
  - RSA (firma)
  - El Gamal (firma)
  - Ataques
  - Firma digital y cifrado

Ana I. González-Tablas Ferreres, José M. de Fuentes García-Romero de Tejada, Lorena González Manzano, Pablo Martín González

Esquemas de firma digital

- [Ribagorda:1997] (ISO-7498-2)
  - Datos añadidos a un conjunto de datos, o transformación de éstos, que permite al receptor probar el origen e integridad del conjunto de datos recibidos, así como protegerlos contra falsificaciones; por ejemplo, del propio receptor.
- [NIST SP 800-57 Pt. 1 Rev. 4:2016]
  - El resultado de una transformación criptográfica de datos que, si se aplica correctamente, según la infraestructura y políticas, proporciona los servicios de:
    - Autenticación del origen,
    - Integridad de los datos, y
    - No repudio del firmante

Ana I. González-Tablas Ferreres, José M. de Fuentes García-Romero de Tejada, Lorena González Manzano, Pablo Martín González

Esquemas de firma digital

- Concepto introducido por Diffie y Hellman en 1976
- Analogía electrónica de la firma manual
- Propiedades de una firma manual:
  - Fácil y barata de producir
  - Fácil de reconocer
  - Imposible de rechazar por el propietario
  - Infalsificable (teóricamente)
- La firma digital debería cumplir las mismas propiedades, pero:
  - No puede ser siempre la misma ya que sería fácilmente falsificable

Esquemas de firma digital. Propiedades de seguridad

- Autentica indubitablemente al signatario de una información
- Garantiza la integridad del mensaje recibido al imposibilitar su modificación fraudulenta
- Garantiza el no repudio (del firmante): medio de prueba en la resolución de disputas

NO asegura la ~~confidencialidad~~

Ana I. González-Tablas Ferreres, José M. de Fuentes García-Romero de Tejada, Lorena González Manzano, Pablo Martín González

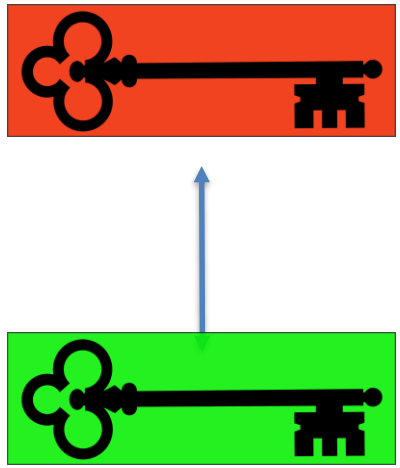
Esquema de firma digital. Componentes

- Un esquema de firma digital comporta tres partes:
  - Algoritmo de generación de claves G
  - Algoritmo de firma S
  - Algoritmo de verificación de la firma V

Esquemas de firma digital

Emplea pares de claves:

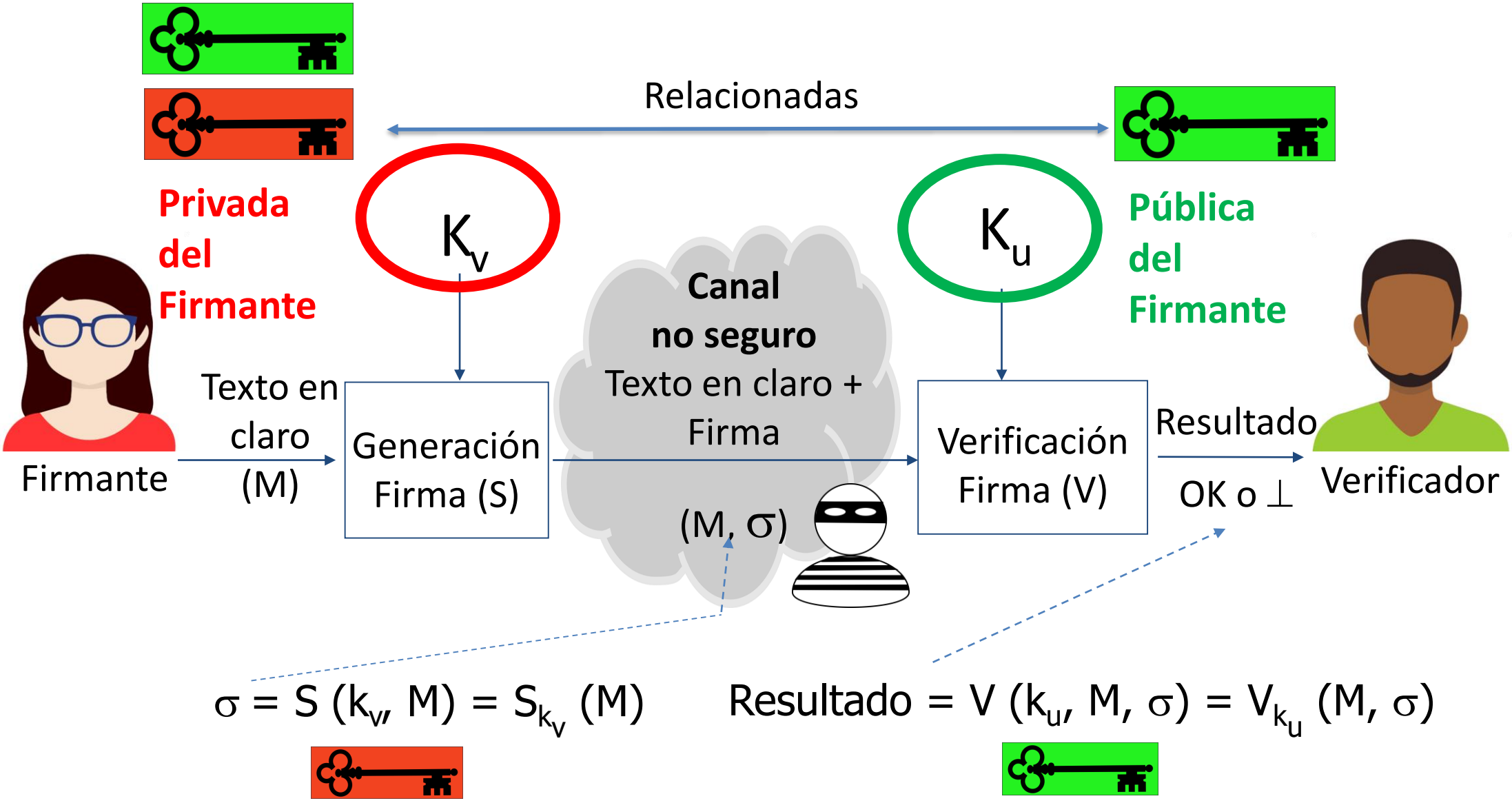
- **clave privada**
  - Conocida sólo por el propietario
  - Usada para firmar por el Firmante



- **clave pública**
  - Conocida por todos
  - El Verificador usa la clave pública del Firmante para verificar las firmas emitidas por éste (el Firmante)

Ana I. González-Tablas Ferreres, José M. de Fuentes García-Romero de Tejada, Lorena González Manzano, Pablo Martín González

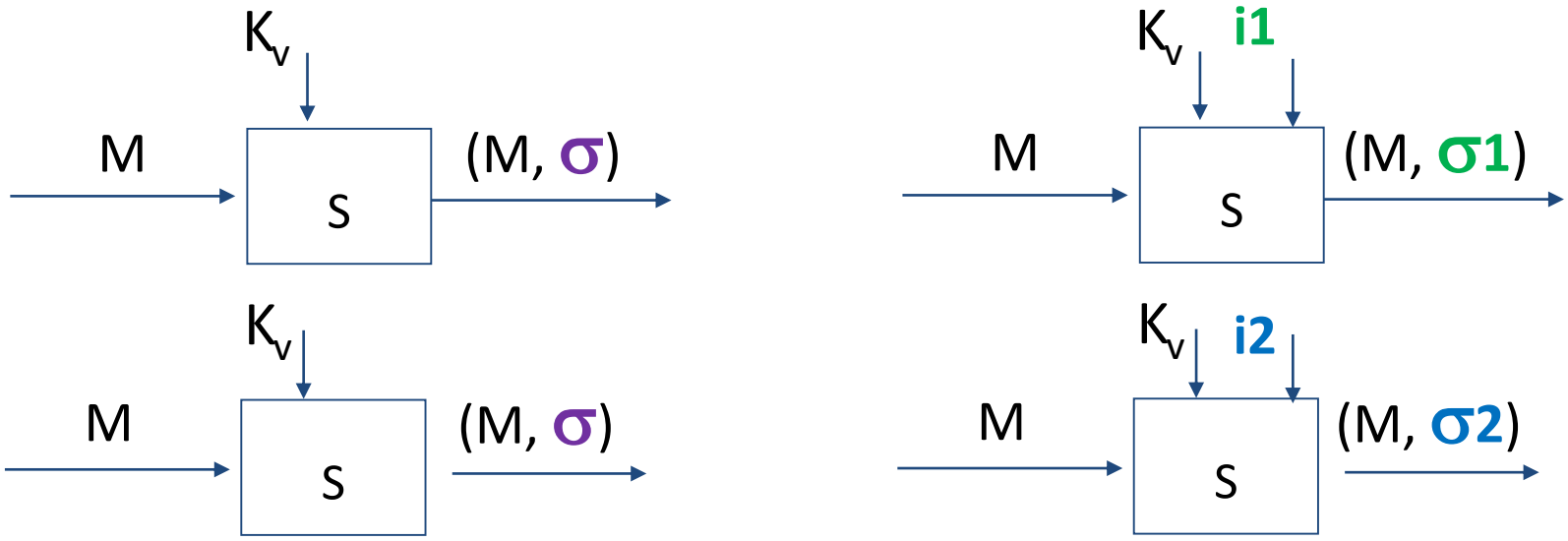
Esquemas de firma digital



Ana I. González-Tablas Ferreres, José M. de Fuentes García-Romero de Tejada, Lorena González Manzano, Pablo Martín González

Esquema de firma digital. Determinista vs Aleatorio

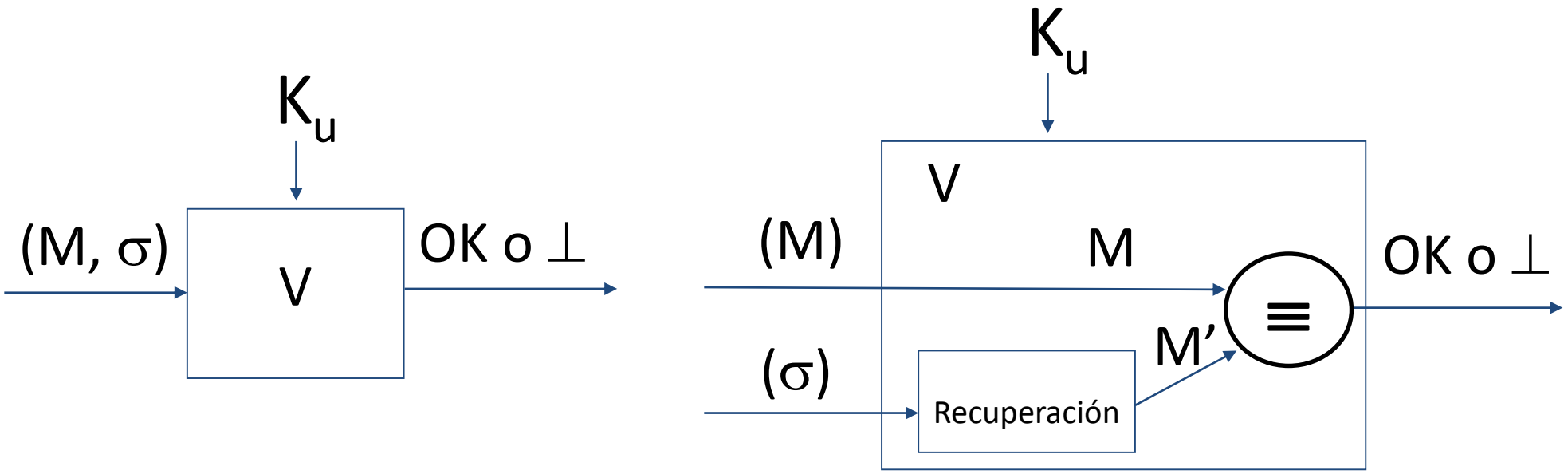
- El esquema de firma puede ser:
  - Determinista: Dos firmas del mismo mensaje producen el mismo resultado (por ejemplo, las firmas basadas en el algoritmo RSA)
  - Aleatorio: Las firmas de un mismo mensaje dependen de un conjunto de índices (por ejemplo, las basadas en el algoritmo El Gamal)



Ana I. González-Tablas Ferreres, José M. de Fuentes García-Romero de Tejada, Lorena González Manzano, Pablo Martín González

Esquema de firma digital. Con apéndice vs Recuperación del mensaje

- El esquema de firma puede ser:
  - Con apéndice o separada del mensaje: La firma se vuelca en un apéndice (e.g., firmas basadas en el algoritmo El Gamal)
  - Con recuperación del mensaje: La firma está integrada en el propio mensaje transformado (e.g., firmas basadas en el algoritmo RSA)



Ana I. González-Tablas Ferreres, José M. de Fuentes García-Romero de Tejada, Lorena González Manzano, Pablo Martín González

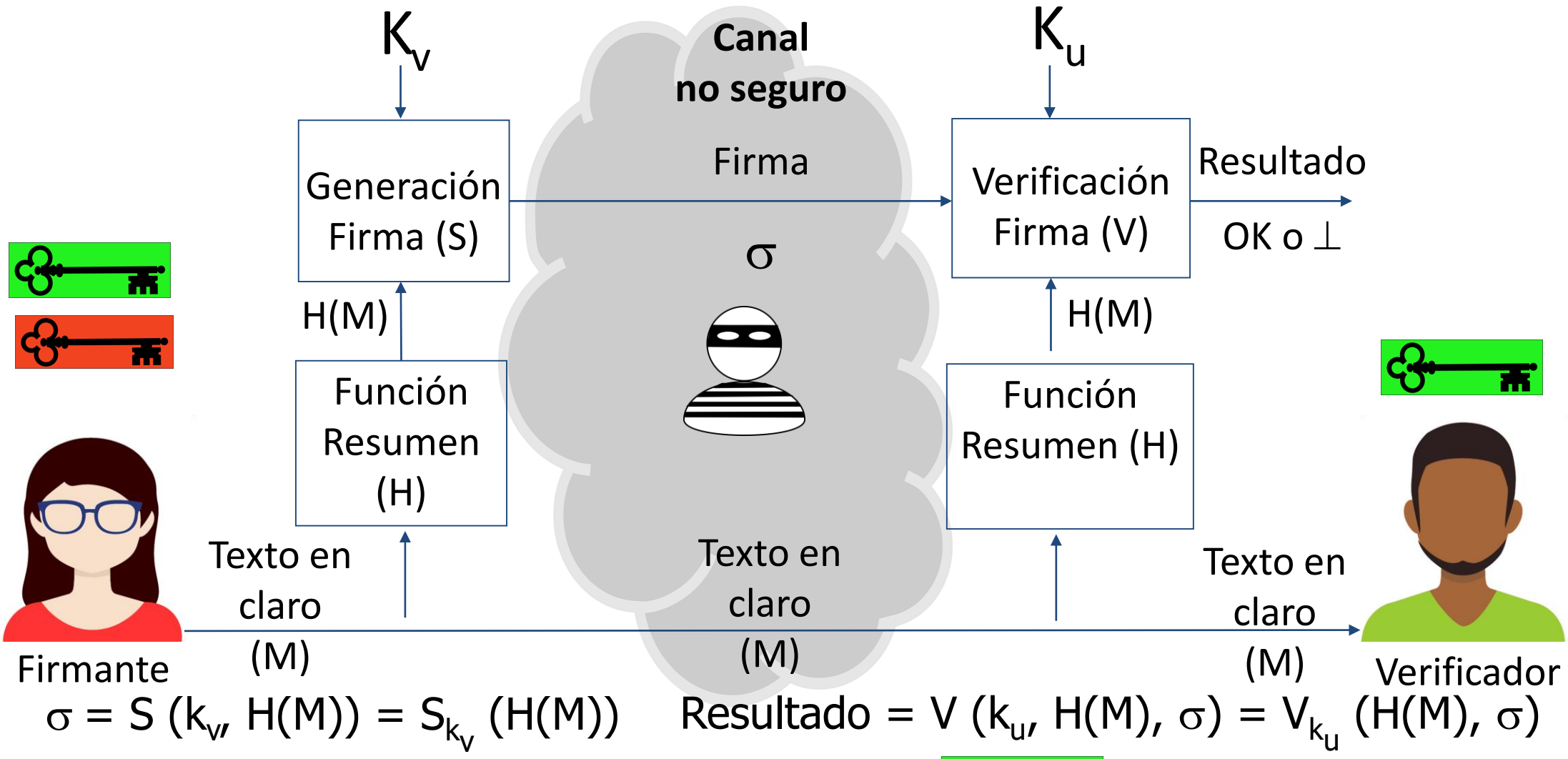
Esquemas de firma digital. Paradigma “resume y firma”

- En general se aplica primero una función resumen al mensaje antes de firmar
  - Por eficiencia, sobre todo si se debe firmar mensajes muy largos
  - Por seguridad, en esquemas basados tanto en El Gamal como en RSA

- En verificación, se debe también aplicar la función resumen sobre el mensaje antes de verificar

Ana I. González-Tablas Ferreres, José M. de Fuentes García-Romero de Tejada, Lorena González Manzano, Pablo Martín González

Esquemas de firma digital. Paradigma "resume y firma"



Ana I. González-Tablas Ferreres, José M. de Fuentes García-Romero de Tejada, Lorena González Manzano, Pablo Martín González

Índice

- 11. Esquemas de firma digital
  - Esquemas de firma digital
  - **RSA (firma)**
  - El Gamal (firma)
  - Ataques
  - Firma digital y cifrado

Ana I. González-Tablas Ferreres, José M. de Fuentes García-Romero de Tejada, Lorena González Manzano, Pablo Martín González

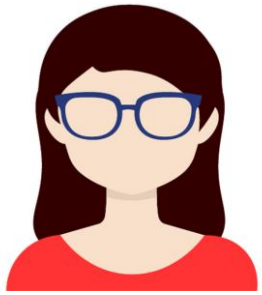
RSA (firma)

- Esquema de firma
  - Determinista
  - Con recuperación del mensaje

- Seguridad basada en la factorización de los números enteros
  - Se recomiendan los mismos tamaños de clave que para el cifrado

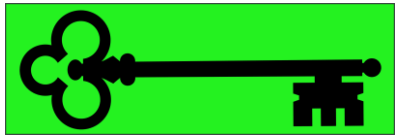
Ana I. González-Tablas Ferreres, José M. de Fuentes García-Romero de Tejada, Lorena González Manzano, Pablo Martín González

RSA (firma)

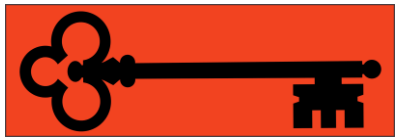


- **Generación del par de claves por A**
  - A elige p_A, q_A (primos muy grandes, no públicos)
  - A obtiene $n_A = p_A \cdot q_A$
  - A calcula $\phi(n_A) = \phi(p_A) \cdot \phi(q_A)$
  - A escoge $e_A \in Z+ / \text{m.c.d.}(e_A, \phi(n_A))=1$
  - A calcula $d_A / e_A \cdot d_A = 1 \quad \text{mód. } \phi(n_A)$

- Clave pública de A: $k_{U,A} = (e_A, n_A)$



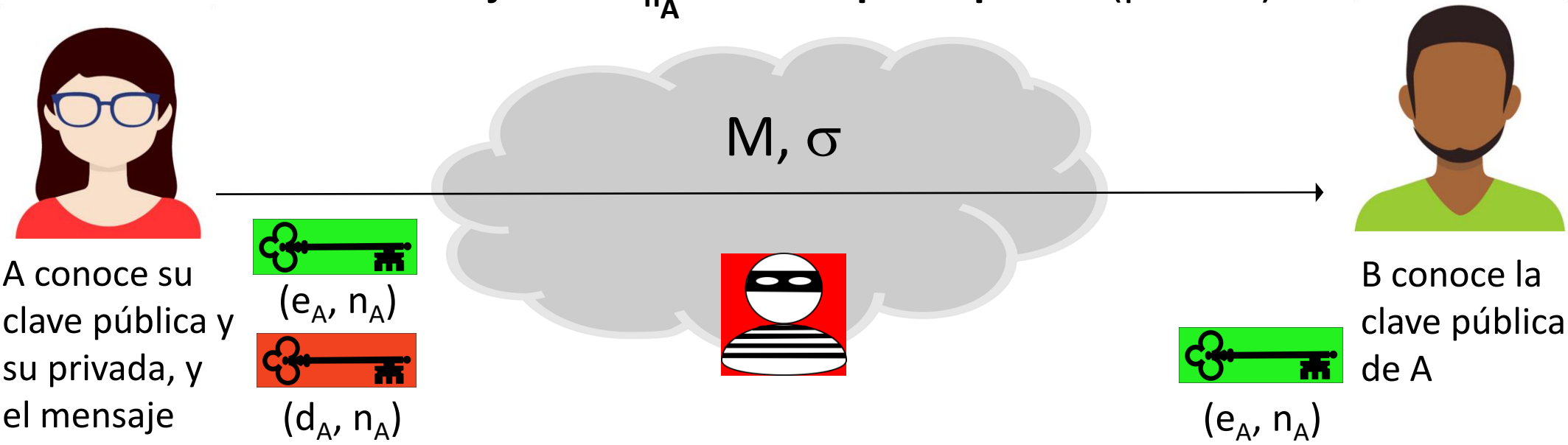
- Clave privada de A: $k_{V,A} = (d_A, n_A)$



Ana I. González-Tablas Ferreres, José M. de Fuentes García-Romero de Tejada, Lorena González Manzano, Pablo Martín González

RSA (firma)

- **Envío de un mensaje M $\in Z_{n_A}$ firmado por A para B** (parte 1)



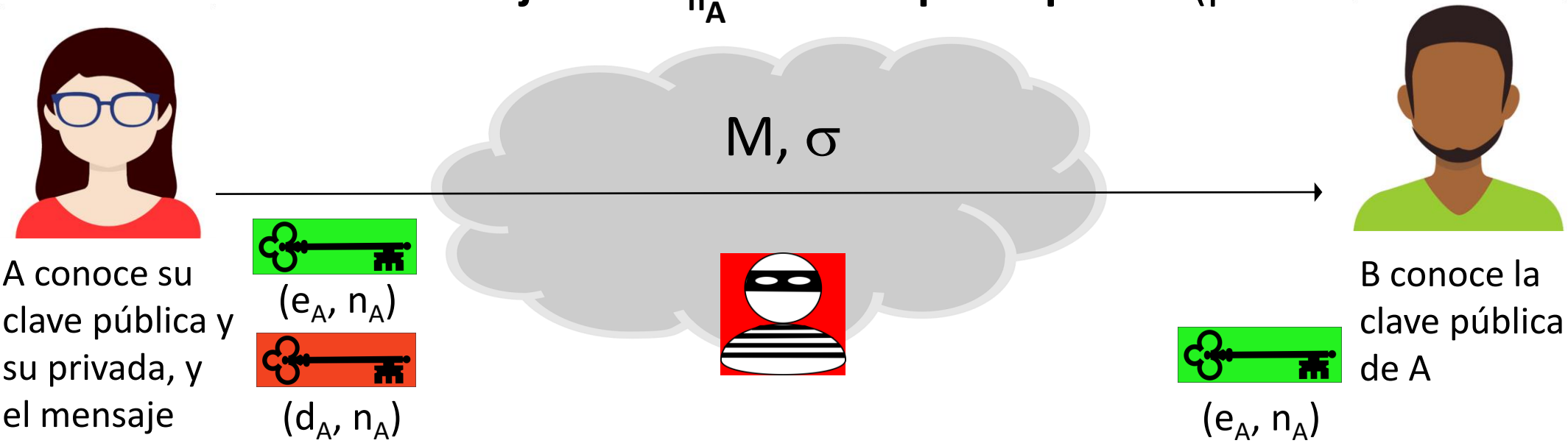
A obtiene la firma sobre M usando (d_A, n_A), su clave privada, y envía a B el mensaje M y la firma σ

$$(M, \sigma = M^{d_A} \text{ mód. } n_A)$$

Ana I. González-Tablas Ferreres, José M. de Fuentes García-Romero de Tejada, Lorena González Manzano, Pablo Martín González

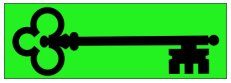
RSA (firma)

- **Envío de un mensaje M $\in Z_{n_A}$ firmado por A para B** (parte 1)



B verifica la firma sobre M usando (e_A, n_A), la clave pública de A, y acepta el mensaje firmado solo si el resultado es OK

$M' = \sigma^{e_A}$ mód. n_A; si $M' \equiv M \rightarrow$ OK, si no, $\perp$



Ana I. González-Tablas Ferreres, José M. de Fuentes García-Romero de Tejada, Lorena González Manzano, Pablo Martín González

Índice

- 11. Esquemas de firma digital
  - Esquemas de firma digital
  - RSA (firma)
  - **El Gamal (firma)**
  - Ataques
  - Firma digital y cifrado

Ana I. González-Tablas Ferreres, José M. de Fuentes García-Romero de Tejada, Lorena González Manzano, Pablo Martín González

El Gamal (firma)

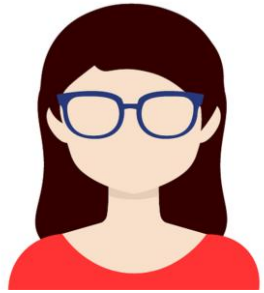
- Esquema de firma
  - Aleatorio
  - Con apéndice

- Seguridad basada en el cálculo del logaritmo discreto
  - Se recomiendan los mismos tamaños de clave que para el cifrado

- Habitualmente no se usa el esquema de El Gamal, si no esquemas derivados de una variante estandarizada de El Gamal, conocida como DSA (*Digital Signature Algorithm*)

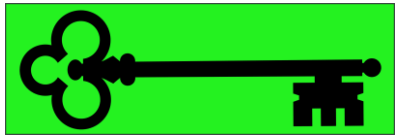
Ana I. González-Tablas Ferreres, José M. de Fuentes García-Romero de Tejada, Lorena González Manzano, Pablo Martín González

El Gamal (firma)

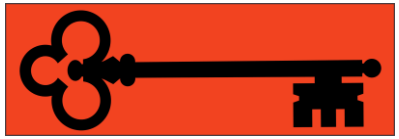


- **Generación del par de claves por A**
  - A elige p_A, primo muy grande
  - A elige g_A, generador de grupo cíclico G de orden p_A
  - A elige x_A , clave privada de A | $1 < x_A < p_A - 1$
  - A calcula y_A , clave pública de B ($y_A = g^{x_A}$ mód. p_A)

- Clave privada de A: $k_{V,A} = (x_A)$



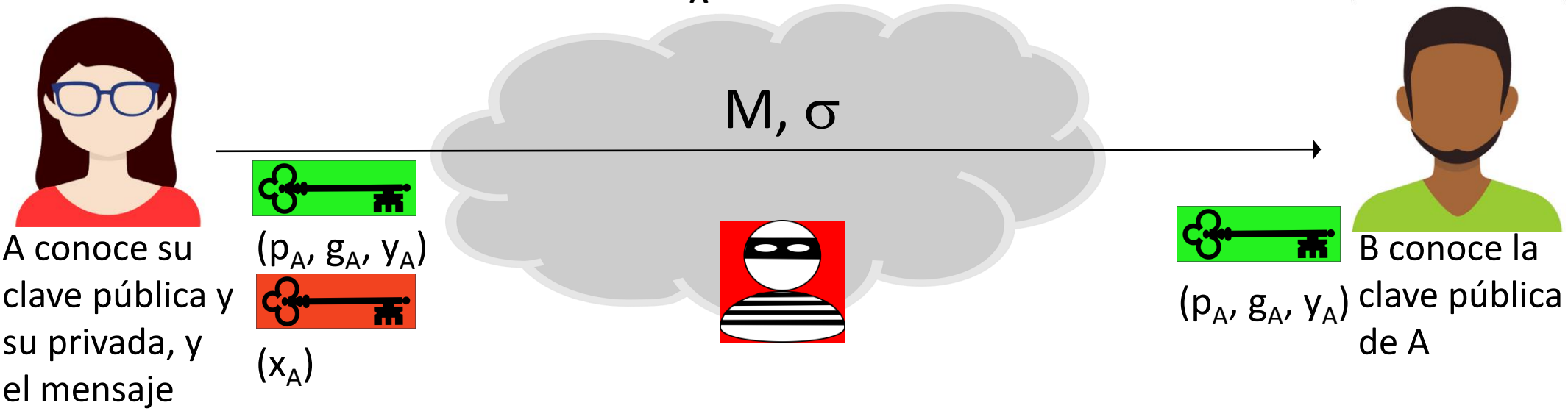
- Clave pública de A: $k_{U,A} = (p_A, g_A, y_A)$



Ana I. González-Tablas Ferreres, José M. de Fuentes García-Romero de Tejada, Lorena González Manzano, Pablo Martín González

El Gamal (firma)

- **Envío de un mensaje M $\in G(p_A)$ firmado por A para B** (parte 1)



A elige una clave temporal k_s | $0 < k_s < p_A$ y calcula $\mathbf{r} = g^{k_s} \text{ (mód. } p_A)$

A, usando su clave privada (x_A), calcula $\mathbf{s} = (M - x_A . r) \cdot k_s^{-1} \text{ mód. } (p_A - 1)$

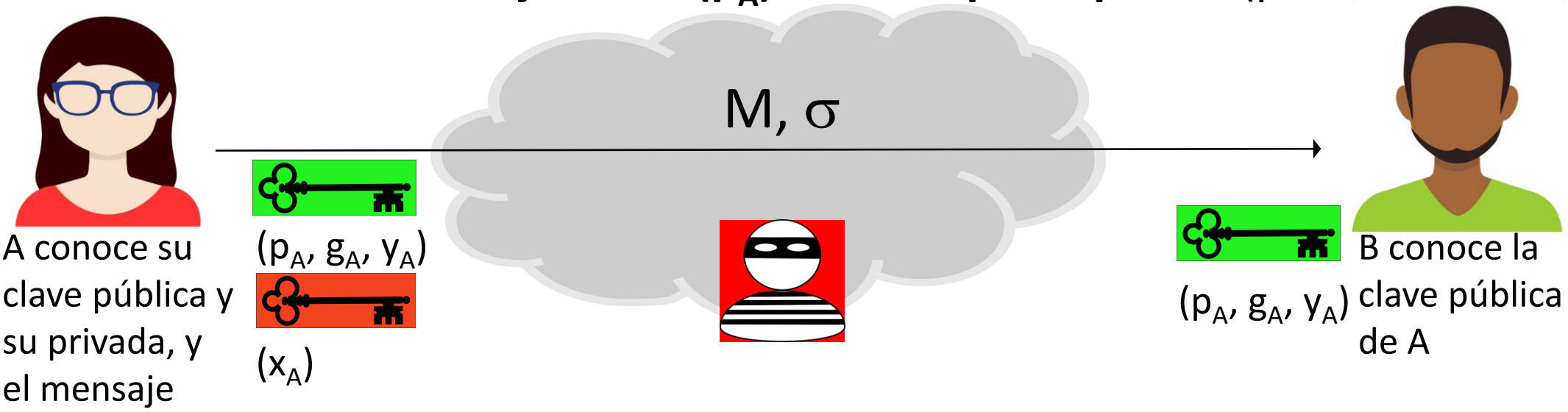
A envía a B el mensaje M y la firma sobre éste, $\boldsymbol{\sigma = (r, s)}$

$$(M, \sigma) = (M, r, s) = (M, g^{k_s} \text{ (mód. } p_A), (M - x_A . r) \cdot k_s^{-1} \text{ mód. } (p_A - 1))$$

Ana I. González-Tablas Ferreres, José M. de Fuentes García-Romero de Tejada, Lorena González Manzano, Pablo Martín González

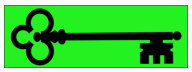
El Gamal (firma)

- **Envío de un mensaje M $\in G(p_A)$ firmado por A para B** (parte 2)



B verifica la firma sobre M usando (p_A, g_A, y_A), la clave pública de A, y acepta el mensaje firmado solo si el resultado es OK

$V_1 = y_A^{\,r} \cdot r^{s} \pmod{p_A}$; $V_2 = g_A^{\,M} \pmod{p_A}$; si $V_1 \equiv V_2 \rightarrow$ OK, si no, $\perp$



Ana I. González-Tablas Ferreres, José M. de Fuentes García-Romero de Tejada, Lorena González Manzano, Pablo Martín González

Índice

- 11. Esquemas de firma digital
  - Esquemas de firma digital
  - RSA (firma)
  - El Gamal (firma)
  - **Ataques**
  - Firma digital y cifrado

Ana I. González-Tablas Ferreres, José M. de Fuentes García-Romero de Tejada, Lorena González Manzano, Pablo Martín González

Ataques

- El objetivo para un atacante a un proceso de firma digital es crear firmas que sean aceptadas como válidas.
  - Rotura total: El atacante posee un algoritmo de firma funcionalmente equivalente al auténtico.
  - Rotura selectiva: El atacante es capaz de forjar una firma para un tipo particular de mensaje.
  - Rotura existencial: El atacante es capaz de forjar una firma para al menos un mensaje.

Ana I. González-Tablas Ferreres, José M. de Fuentes García-Romero de Tejada, Lorena González Manzano, Pablo Martín González

Ataques.
RSA

- RSA de “libro-de-texto” es vulnerable a ataques de rotura existencial

Ataque 1:

C quiere crear una firma válida, como si la hubiese generado A

Supongamos que C conoce clave pública de A (e_A, n_A)

C escoge $\sigma \in Z_{n_A}$ aleatoriamente y calcula $M = \sigma^{e_A}$ mód. n_A

C envía a B el mensaje M y la firma “ficticia” sobre éste:

$$C \rightarrow B: (M, \sigma)$$

B verifica el mensaje recibido como efectivamente firmado por A, pues

$$M \equiv M' = \sigma^{e_A} \text{ mód. } n_A \rightarrow OK$$

Ana I. González-Tablas Ferreres, José M. de Fuentes García-Romero de Tejada, Lorena González Manzano, Pablo Martín González

Ataques.
RSA

Ataque 2:

C puede crear una firma válida, a partir de 2 generadas por A

C obtiene dos pares de mensaje con su firma:

$$(M_1, \sigma_1); (M_2, \sigma_2)$$

escoge $\sigma \in Z_{n_A}$ aleatoriamente y calcula $M = \sigma^{e_A}$ mód. n_A

C puede crear una firma válida σ' para el mensaje $M' = M_1 \cdot M_2$ mód. n_A

$$\sigma' = \sigma_1 \cdot \sigma_2 \text{ mód. } n_A$$

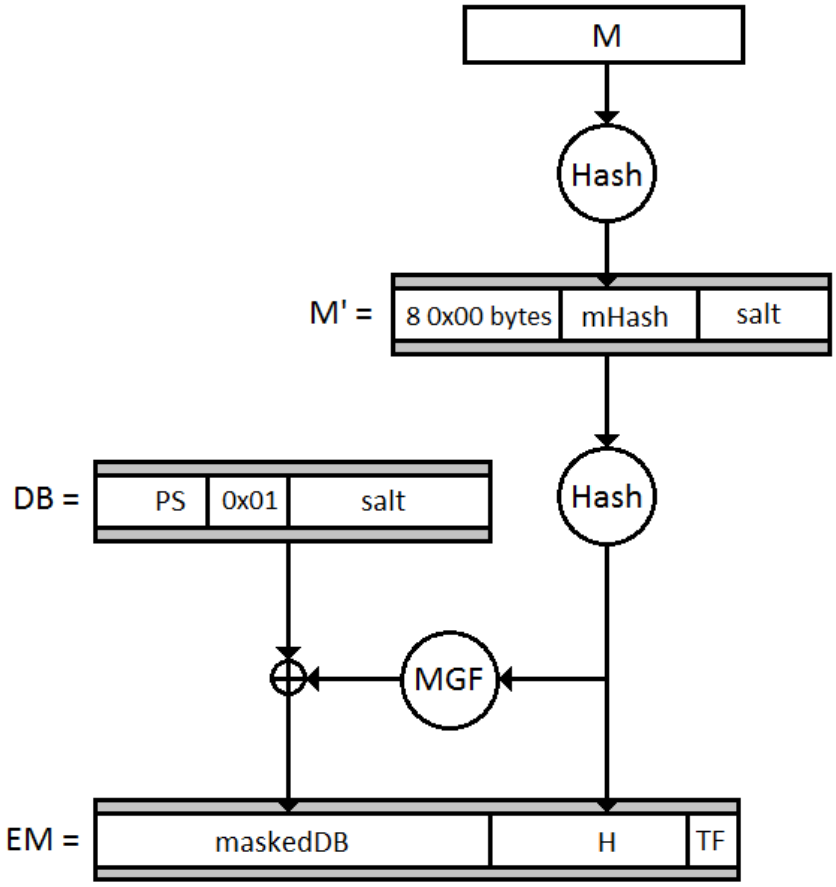
B verifica el mensaje recibido como efectivamente firmado por A, pues

$$M' \equiv \sigma'^{e_A} \text{ mód. } n_A = \sigma_1^{e_A} \cdot \sigma_2^{e_A} \text{ mód. } n_A = M_1 \cdot M_2 \text{ mód. } n_A \rightarrow \text{OK}$$

Ana I. González-Tablas Ferreres, José M. de Fuentes García-Romero de Tejada, Lorena González Manzano, Pablo Martín González

Ataques.
RSA

- Solución:
  - Aplicar una función resumen al mensaje antes de firmar previene el éxito de estos ataques
  - Sin embargo, esto no es suficiente para los estándares requeridos de seguridad. Es necesario convertir RSA en un esquema aleatorio
  - RSA-PSS (*Probabilistic Signature Scheme*)
    - Se añaden unos rellenos (*paddings*) específicos y un valor aleatorio (*salt*) de forma parecida a la Figura adjunta



Ataques.
El Gamal

- Al igual que con RSA, El Gamal de “libro-de-texto” es vulnerable a ataques de rotura existencial
  - No veremos los detalles
- Solución:
  - Igual que con RSA, es necesario aplicar una función resumen al mensaje antes de firmar
  - Comúnmente se utiliza DSA o ECDSA (DSA sobre curvas elípticas escogidas cuidadosamente), aunque no todas las variantes ofrecen los niveles de seguridad requeridos en la actualidad

Ana I. González-Tablas Ferreres, José M. de Fuentes García-Romero de Tejada, Lorena González Manzano, Pablo Martín González

Índice

- 11. Esquemas de firma digital
  - Esquemas de firma digital
  - RSA (firma)
  - El Gamal (firma)
  - Ataques
  - **Firma digital y cifrado**

Ana I. González-Tablas Ferreres, José M. de Fuentes García-Romero de Tejada, Lorena González Manzano, Pablo Martín González

Firma digital y cifrado

- Para construir un canal seguro (confidencialidad, autenticación e integridad) con criptografía de clave pública es necesario combinar un criptosistema de clave pública y un esquema de firma digital seguros
- Durante las últimas décadas se ha estado discutiendo sobre las propiedades de seguridad de diversas construcciones
  - *Sign-then-encrypt*
  - *Sign-and-encrypt*
  - *Encrypt-then-sign*

Davis, D. (2001, June). Defective Sign & Encrypt in S/MIME, PKCS# 7, MOSS, PEM, PGP, and XML. In *USENIX Annual Technical Conference, General Track* (pp. 65-78). https://pdfs.semanticscholar.org/3de0/d2e8d6a46c07264bbe1cacefc446b35b2b7e.pdf

Firma digital y cifrado

- Finalmente se ha definido un nuevo esquema, denominado ***signcryption***, y que debe garantizar que:
  - Si A envía un mensaje a B cifrado con uno de estos esquemas,
  - solo el receptor B puede acceder al mensaje, y
  - el receptor tiene garantías de que el mensaje proviene del emisor A

- Se admiten como combinaciones seguras *sign-then-encrypt* y *encrypt-then-sign* si se referencian las identidades del receptor (en la firma) y del emisor (en el cifrado), entre otras consideraciones

Ana I. González-Tablas Ferreres, José M. de Fuentes García-Romero de Tejada, Lorena González Manzano, Pablo Martín González

CURSO CRIPTOGRAFÍA Y SEGURIDAD INFORMÁTICA

COSEC

uc3m | Universidad Carlos III de Madrid