Tema 7

Criptosistemas asimétricos

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

CC BY NC SA

ÍNDICE

- 7. Criptosistemas asimétricos
  - Contexto histórico e impacto
  - Modelo de criptosistema asimétrico
  - RSA (cifrado)
  - El Gamal (cifrado)
  - Ataques específicos

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

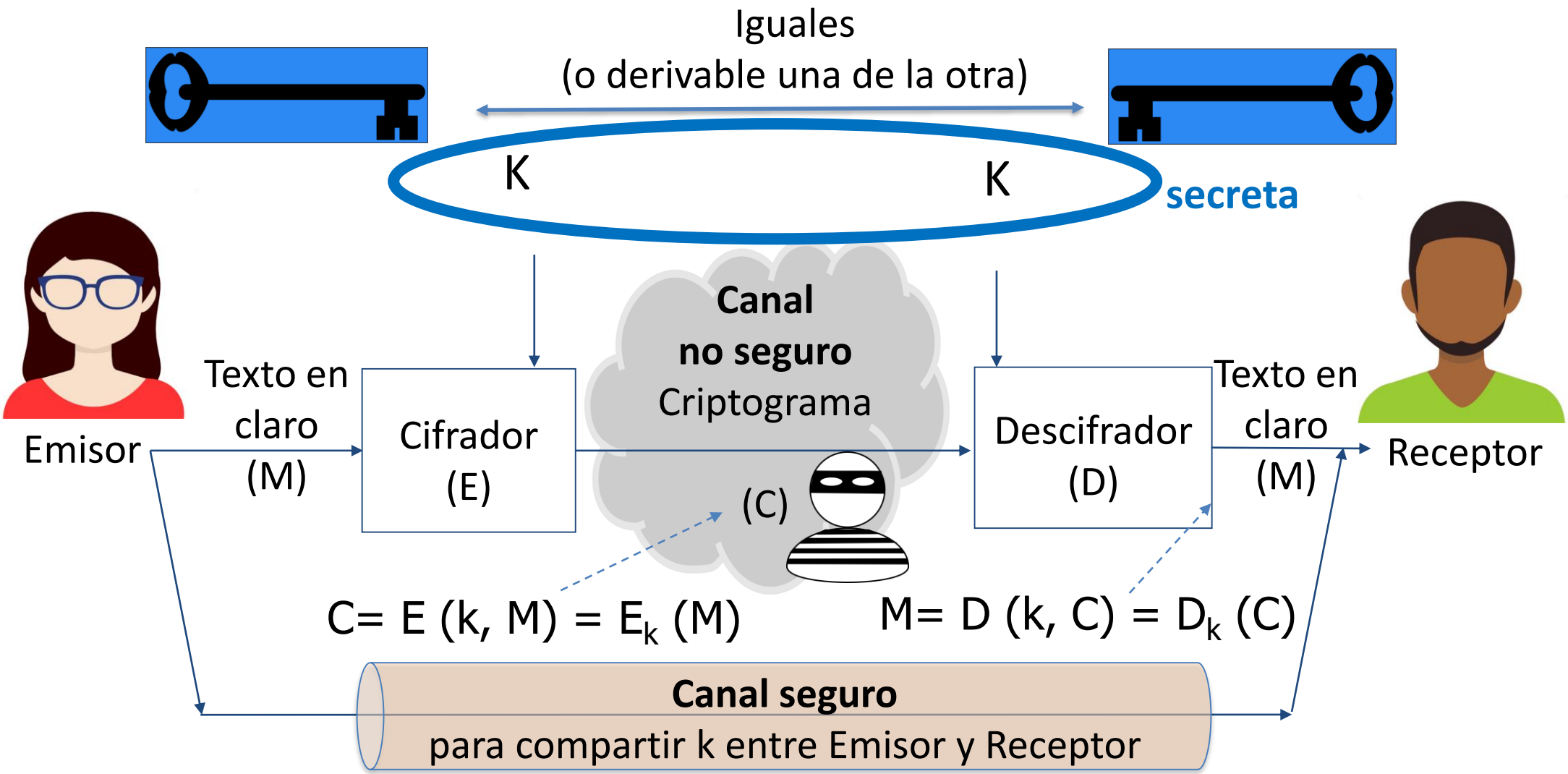
ÍNDICE

- 7. Criptosistemas asimétricos
  - **Contexto histórico e impacto**
  - Modelo de criptosistema asimétrico
  - RSA (cifrado)
  - El Gamal (cifrado)
  - Ataques específicos

BY NC SA

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

Contexto histórico e impacto
Recordatorio: Modelo de criptosistema simétrico



BY NC SA

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

Contexto histórico e impacto

- Problema:
  - Dos personas, que previamente no han intercambiado ningún secreto, deben intercambiar una clave secreta sobre un canal inseguro
  - Los criptosistemas de clave simétrica necesitan un canal seguro para convenir (intercambiar) la clave secreta entre los interlocutores
  - Durante más de 3.000 años se pensó que no tenía solución

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

Contexto histórico e impacto

- Whitfield Diffie, Martin E. Hellman. ***New Directions in Cryptography***. IEEE Transactions in Information Theory, v. IT-22, pp 664-654. Noviembre de 1976.
  - Artículo revolucionario que creó la criptografía de clave pública
  - Probablemente es el mayor hito criptográfico en 3000 años
  - Descubierto anteriormente por los servicios de inteligencia británicos
  - Propone de forma teórica los criptosistemas asimétricos y el algoritmo de Diffie-Hellman, un algoritmo de intercambio de clave secreta basado en criptografía asimétrica

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

Contexto histórico e impacto

- Whitfield Diffie, Martin E. Hellman. ***New Directions in Cryptography***. IEEE Transactions in Information Theory, v. IT-22, pp. 664-654. Noviembre de 1976.
  - **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.
  - https://www-ee.stanford.edu/~hellman/publications/24.pdf

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

Contexto histórico e impacto

- A continuación veremos los criptosistemas asimétricos

- En un tema posterior veremos:
  - El algoritmo de Diffie-Hellman, como algoritmo de intercambio de clave,
  - Las principales aproximaciones para la distribución de claves, basadas tanto en criptografía simétrica como en asimétrica

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

ÍNDICE

- 7. Criptosistemas asimétricos
  - Contexto histórico e impacto
  - **Modelo de criptosistema asimétrico**
  - RSA (cifrado)
  - El Gamal (cifrado)
  - Ataques específicos

BY NC SA

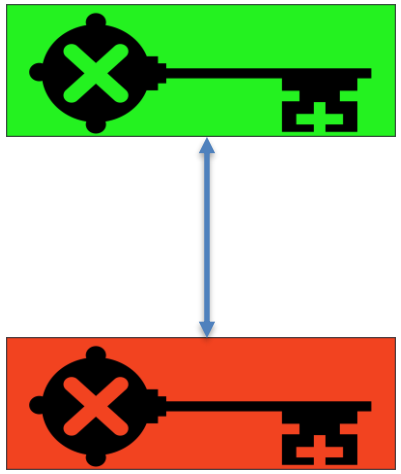
Ana I. González-Tablas Ferreres, José M. de Fuentes García-Romero de Tejada, Lorena González Manzano, Pablo Martín González

Modelo de criptosistema asimétrico

- Criptosistemas de clave pública o asimétricos

  Emplea pares de claves:

  - **clave pública**
    - Conocida por todos
    - El Emisor usa la clave pública del Receptor para cifrar mensajes para éste (el Receptor)
  - **clave privada relacionada**
    - Conocida sólo por el propietario
    - Usada para descifrar por el Receptor

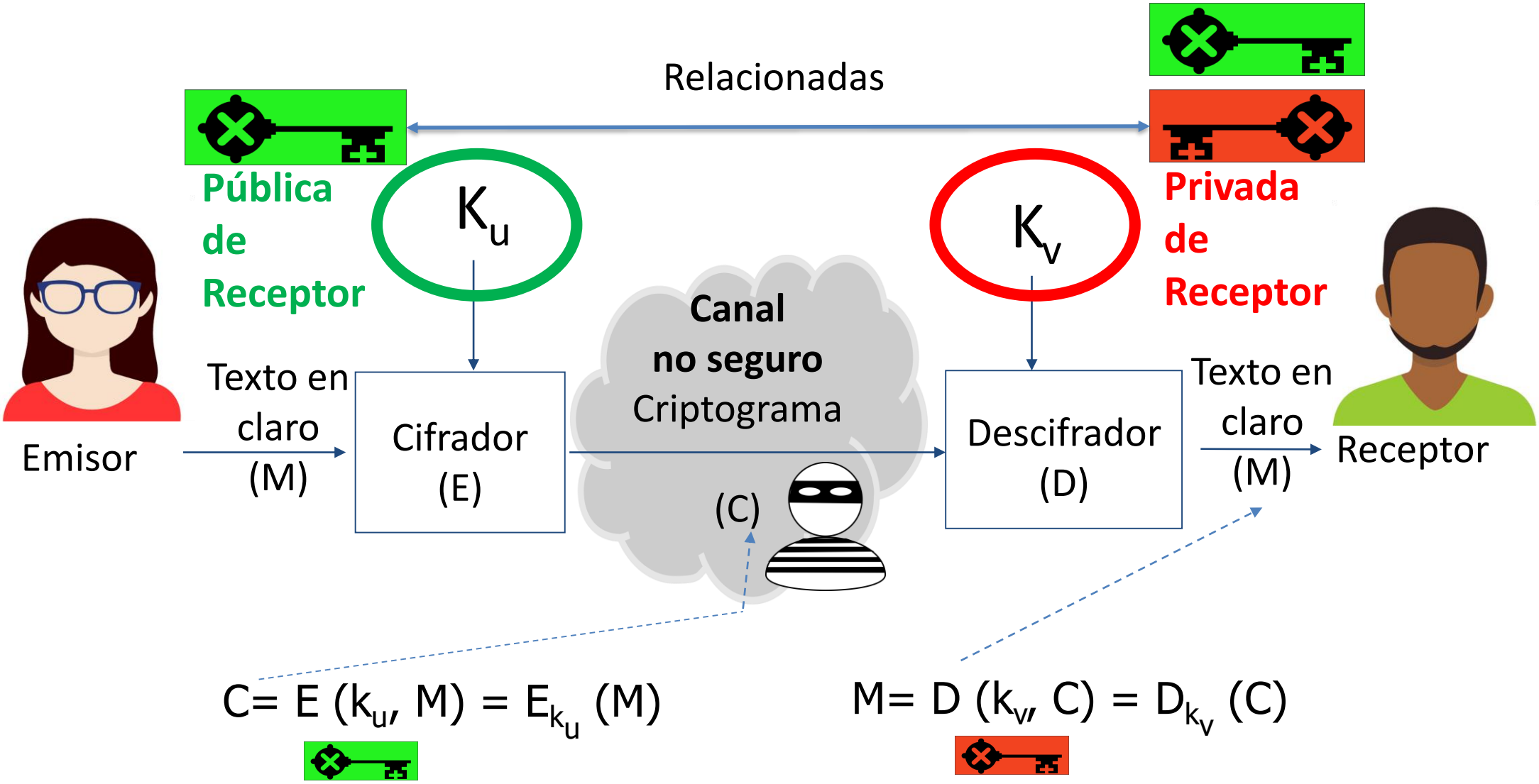


Inviable determinar clave privada a partir de la pública

BY NC SA

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

Modelo de criptosistema asimétrico



BY NC SA

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

Modelo de criptosistema asimétrico

- **Seguridad computacional**
  - La búsqueda exhaustiva es posible en teoría
  - Las claves usadas han de ser suficientemente grandes
  - Los problemas matemáticos en que se basan son difíciles (*hard*) → Funciones unidireccionales con trampa
    - Factorización de números grandes
    - Logaritmo discreto

- **Lentos en comparación con criptosistemas simétricos**

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

ÍNDICE

- 7. Criptosistemas asimétricos
  - Contexto histórico e impacto
  - Modelo de criptosistema asimétrico
  - **RSA (cifrado)**
  - El Gamal (cifrado)
  - Ataques específicos

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

RSA

- R. L. Rivest, A. Shamir, L. Adleman. ***A Method for Obtaining Digital Signature and Public-Key Cryptosystems***. Communications of the ACM, v. 21, nº 2, pp 120-126. Febrero de 1978.
  - Primer criptosistema de clave pública, el famoso RSA
  - Basado en la dificultad de factorizar un número producto de dos primos grandes de similar longitud
  - Luego hubo otros, algunos rotos, pero RSA permanece

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

RSA

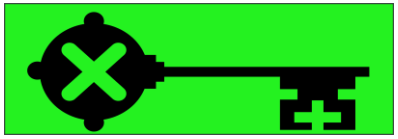
- R. L. Rivest, A. Shamir, L. Adleman. ***A Method for Obtaining Digital Signature and Public-Key Cryptosystems***. Communications of the ACM, v. 21, nº 2, pp 120-126. Febrero de 1978.
  - **Abstract** An encryption method is presented with the novel property that publicly revealing an encryption key 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.
  - https://people.csail.mit.edu/rivest/Rsapaper.pdf

COSEC uc3m
BY NC SA
Ana I. González-Tablas Ferreres, José M. de Fuentes García-Romero de Tejada, Lorena González Manzano, Pablo Martín González

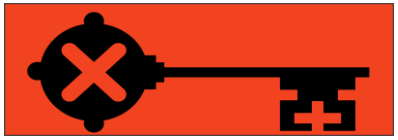
RSA (cifrado)

- **Generación del par de claves por B**
  - B elige p_B, q_B (primos muy grandes, no públicos)
  - B obtiene $n_B = p_B \cdot q_B$
  - B calcula $\phi(n_B) = \phi(p_B) \cdot \phi(q_B)$
  - B escoge $e_B \in Z+ \,/\, \text{m.c.d.}\,(e_B, \phi(n_B))=1$
  - B calcula $d_B \,/\, e_B \cdot d_B = 1 \quad \text{mód.}\ \phi(n_B)$

- Clave pública de B: $k_{U,B} = (e_B, n_B)$



- Clave privada de B: $k_{V,B} = (d_B, n_B)$

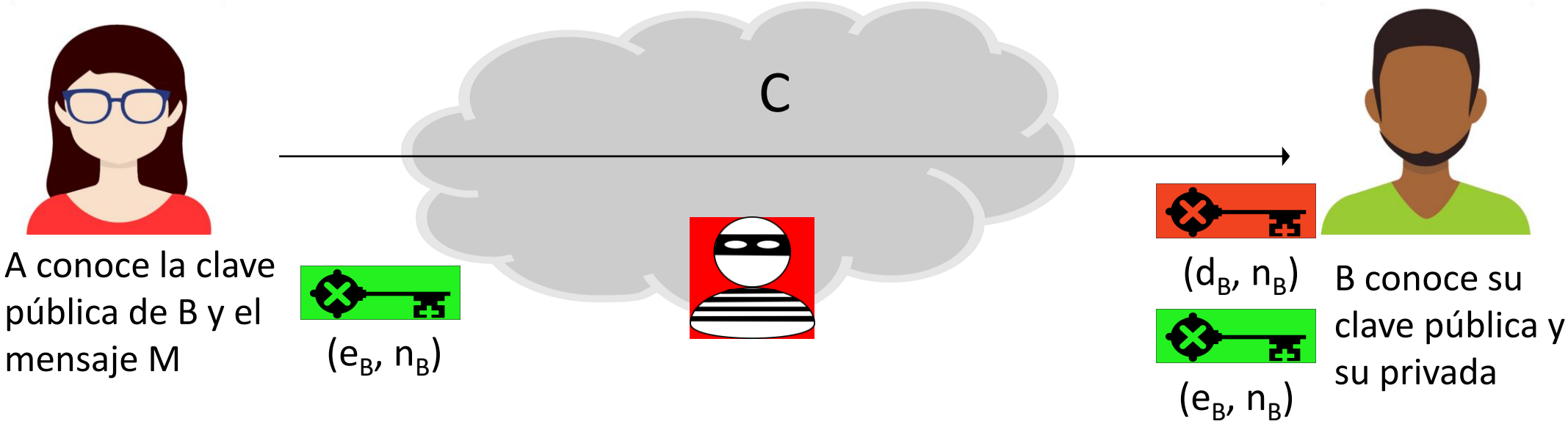


BY NC SA

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

RSA (cifrado)

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



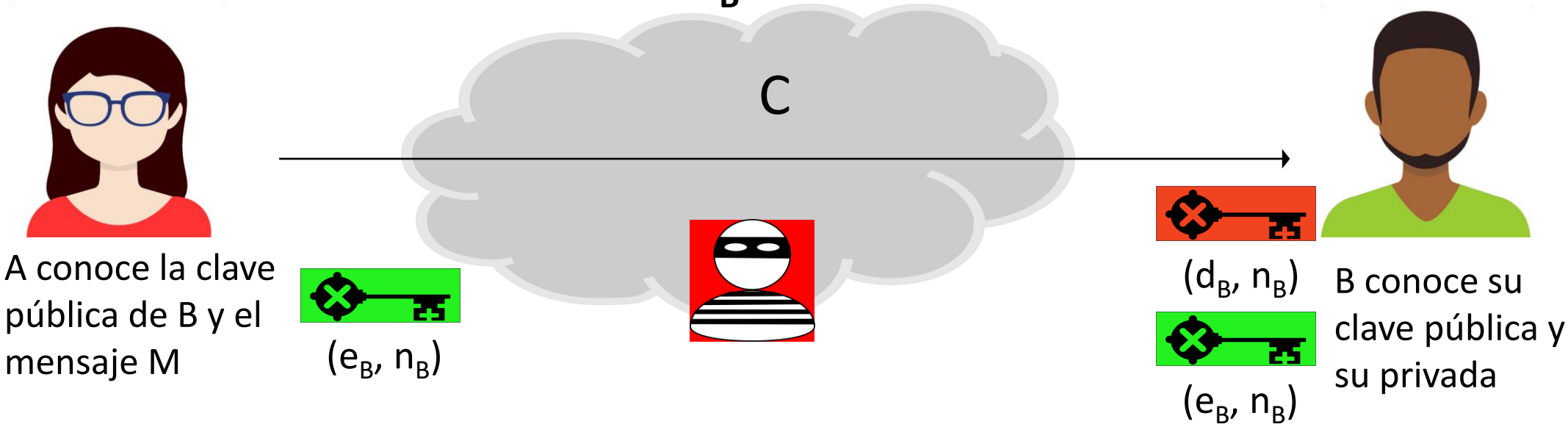
A cifra M usando (e_B, n_B), la clave pública de B, y se la envía a B

$$C = M^{e_B} \text{ mód. } n_B$$

COSEC uc3m
BY NC SA
Ana I. González-Tablas Ferreres, José M. de Fuentes García-Romero de Tejada, Lorena González Manzano, Pablo Martín González

RSA (cifrado)

- **Envío de un mensaje M $\in Z_{n_B}$ cifrado de A para B** (parte 2)



B descifra C usando (d_B, n_B), su clave privada

$$M = C^{d_B} \text{ mód. } n_B$$

COSEC uc3m
Ana I. González-Tablas Ferreres, José M. de Fuentes García-Romero de Tejada, Lorena González Manzano, Pablo Martín González

RSA (cifrado)

- Demostración cifrado/descifrado RSA:
  - Como $C = M^{e_B}$ mód. $n_B \Rightarrow C^{d_B}$ mód. $n_B = M^{e_B \cdot d_B}$ mód. n_B
  - Por hipótesis $e_B \cdot d_B = 1$ mód. $\phi(n_B) \Rightarrow e_B \cdot d_B = 1 + k \cdot \phi(n_B)$
  - Por Teo. de Euler, $M^{\phi(n_B)}$ mód. $n_B = 1$
  - Luego $M^{e_B \cdot d_B}$ mód. $n_B = M^{1 + k \cdot \phi(n_B)}$ mód. $n_B = M$
  - Así pues C^{d_B} mód. $n_B = M$

COSEC uc3m
BY NC SA
Ana I. González-Tablas Ferreres, José M. de Fuentes García-Romero de Tejada, Lorena González Manzano, Pablo Martín González

RSA (cifrado)

- La seguridad del RSA se basa en el problema de la factorización de números grandes
  - Para calcular $d = \text{inv}\,[e, \phi(n)]$
    - Hay que calcular $\phi(n) = (p - 1) \cdot (q - 1)$
    - Para realizar el cálculo de $\phi(n)$ de forma eficiente, hay que conocer p y q
    - $O(e^{\ln(n) \cdot \ln \ln(n)})$
- Reto de factorización de RSA (*RSA factoring challenge*)
  - https://web.archive.org/web/20130507091636/http://www.rsa.com/rsalabs/node.asp?id=2092
  - RSA-768 (768 bits, 232 dígitos decimales) roto el 12/12/2009
  - RSA-230 (762 bits, 230 dígitos decimals) roto el 15/08/2018
- Recomendación de módulos n de longitud
  - Al menos de 2048 bits (NIST 2016) o de 3072 bits (ECRYPT-CSA 2018)

COSEC uc3m
BY NC SA
Ana I. González-Tablas Ferreres, José M. de Fuentes García-Romero de Tejada, Lorena González Manzano, Pablo Martín González

ÍNDICE

- 7. Criptosistemas asimétricos
  - Contexto histórico e impacto
  - Modelo de criptosistema asimétrico
  - RSA (cifrado)
  - **El Gamal (cifrado)**
  - Ataques específicos

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

El Gamal (cifrado)

- Taher ElGamal. ***A Public Key Cryptosystem and a Signature Scheme Based on Discrete Logarithms***. IEEE Transactions in Information Theory, vol. IT-31, nº 4, pp. 4569-472, Julio de 1985.
  - Criptosistema de clave pública basado en problemas relacionados con la dificultad de calcular de forma eficiente el logaritmo discreto
  - http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.476.4791&rep=rep1&type=pdf

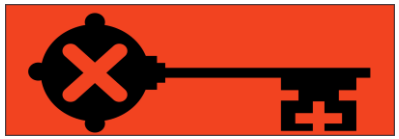
BY NC SA

El Gamal (cifrado)

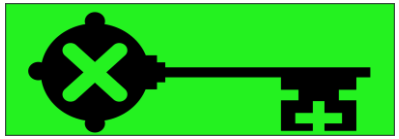
- **Generación del par de claves por B**
  - B elige p_B, primo muy grande
  - B elige g_B, generador de grupo cíclico G de orden p_B
  - B elige x_B , clave privada de B,

    $1 < x_B < p_B - 1$
  - B calcula y_B , clave pública de B ($y_B = g^{x_B}$ mód. p_B)

- Clave privada de B: $k_{V,B} = (x_B)$



- Clave pública de B: $k_{U,B} = (p_B, g_B, y_B)$

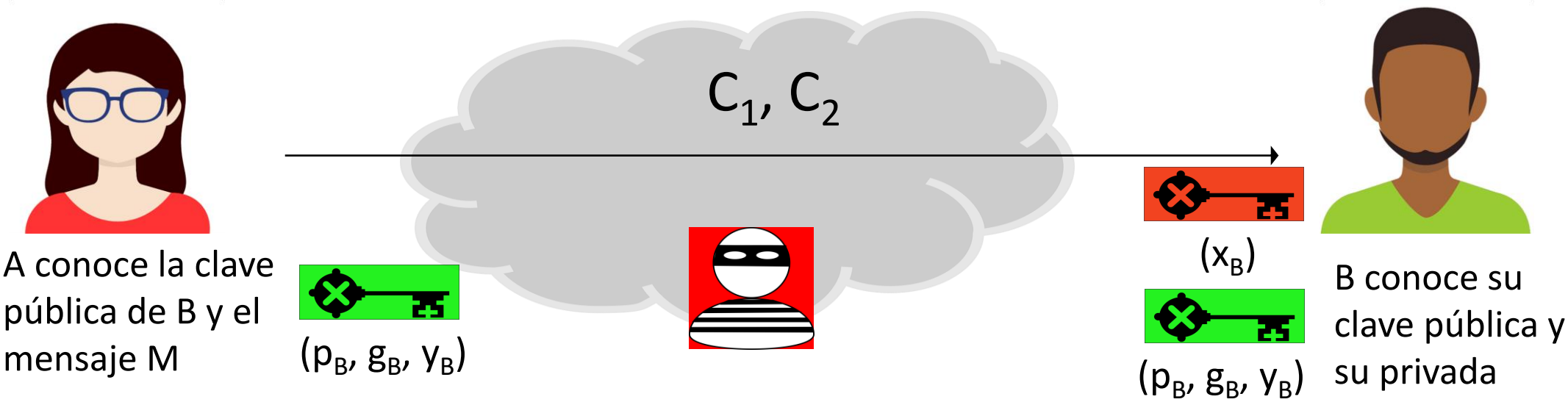


BY NC SA

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

El Gamal (cifrado)

- **Envío de un mensaje $M \in G(p_B)$ cifrado de A para B** (parte 1)



A elige k_e (aleatorio) | $1 < k_e < p_B - 1$

A calcula $C_1 = g_B^{k_e}$ mód. p_B

A calcula la clave temporal usando la clave pública de B: $K_T = y_B^{k_e}$ mód. p_B

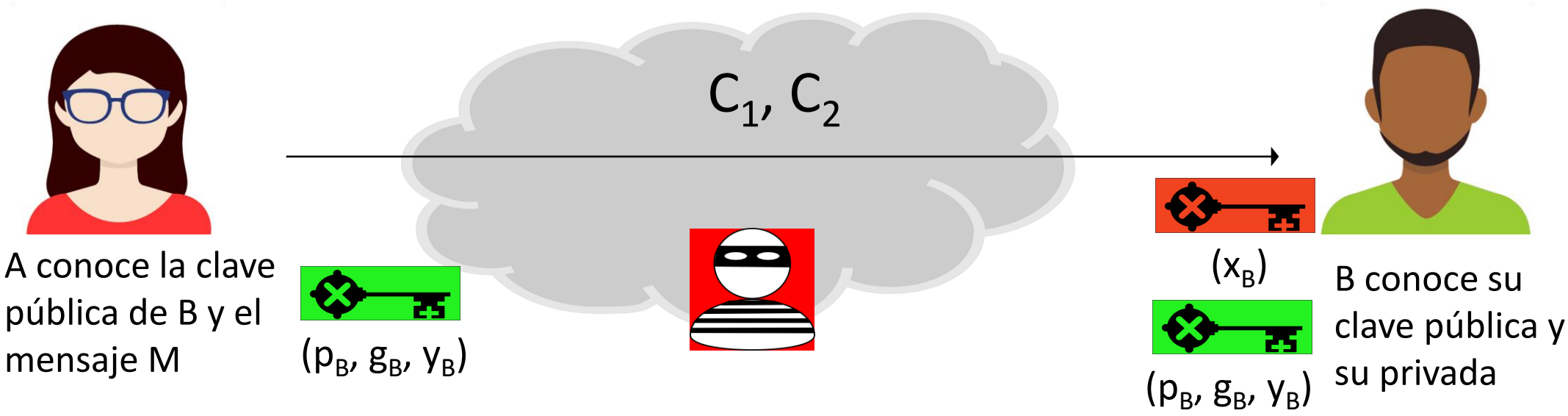
A calcula el cifrado de M como $C_2 = K_T \cdot M$ mód. p_B

BY NC SA

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

El Gamal (cifrado)

- **Envío de un mensaje $M \in G(p_B)$ cifrado de A para B** (parte 2)



A envía a B $C = C_1, C_2$

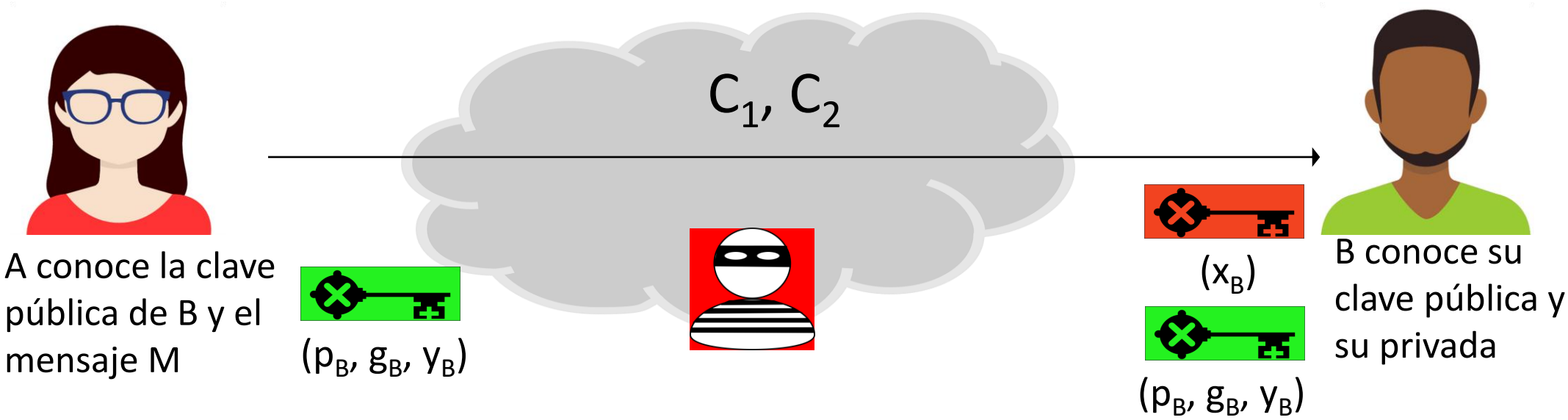
$$C_1 = g_B^{k_e} \text{ mód. } p_B \text{ , } C_2 = K_T \cdot M \text{ mód. } p_B$$

Si $C_2 = K_T \cdot M$ mód. p_B , M y $K_T \in G(p_B) \rightarrow M = C_2 \cdot K_T^{-1}$ mód. p_B

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

El Gamal (cifrado)

- **Envío de un mensaje $M \in G(p_B)$ cifrado de A para B** (parte 3)



B primero recupera la clave temporal y luego descifra C:

$$K_T = C_1^{x_B} \text{ mód. } p_B, \text{ pues } (g_B^{x_B})^{k_e} \text{ mód. } p_B = (g_B^{k_e})^{x_B} \text{ mód. } p_B$$

Por Teorema de Fermat

$$M = C_2 \cdot K_T^{-1} \text{ mód. } p_B = C_2 \cdot C_1^{-x_B} \text{ mód. } p_B = C_2 \cdot C_1^{p_B - 1 - x_B} \text{ mód. } p_B$$

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

El Gamal (cifrado)

- La seguridad de El Gamal se basa en la dificultad de calcular el logaritmo discreto
  - Suponiendo un grupo cíclico de orden p con un generador g, conocido $y \in G(p)$, sabemos que existe un único $x \mid g^x = y$ mód. p
  - Calcular $x = \log_g y$ mód. p se asume difícil

- Recomendación de primos p de longitud
  - Al menos de 2048 bits (NIST 2016) o de 3072 bits (ECRYPT-CSA 2018)
  - Si grupos definidos sobre curvas elípticas, al menos de 224 bits (NIST 2016) o de 256 bits (ECRYPT-CSA 2018)

COSEC uc3m
BY NC SA
Ana I. González-Tablas Ferreres, José M. de Fuentes García-Romero de Tejada, Lorena González Manzano, Pablo Martín González

El Gamal (cifrado)

- En la práctica
  - El grupo, y los parámetros p y g están estandarizados y son conocidos por todos
  - No se utiliza K_T directamente como clave para cifrar M sino que se deriva otra clave simétrica K_T' a partir de K_T, e.g, con una función resumen

$$K_T' = H(K_T)$$

$$C_1 = g_B^{k_e} \text{ mód. } p_B \text{ , } C_2' = E_{SIM}(K_T', M)$$

  - Esencialmente lo que se conoce como cifrado híbrido, que veremos en un tema posterior

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

ÍNDICE

- 7. Criptosistemas asimétricos
  - Contexto histórico e impacto
  - Modelo de criptosistema asimétrico
  - RSA (cifrado)
  - El Gamal (cifrado)
  - **Ataques específicos**

BY NC SA

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

Ataques específicos.
RSA

- RSA es determinista
  - Se puede derivar información sobre el mensaje en claro a partir de un conjunto de parejas (mensaje en claro, mensajes cifrado) aplicando técnicas estadísticas
- RSA es maleable
  - Dado mensaje cifrado C correspondiente a un mensaje en claro M, es fácil para un atacante obtener un cifrado C' que se corresponda a un mensaje M' relacionado con M

$$M \rightarrow \quad C = M^e \text{ mód. } n$$

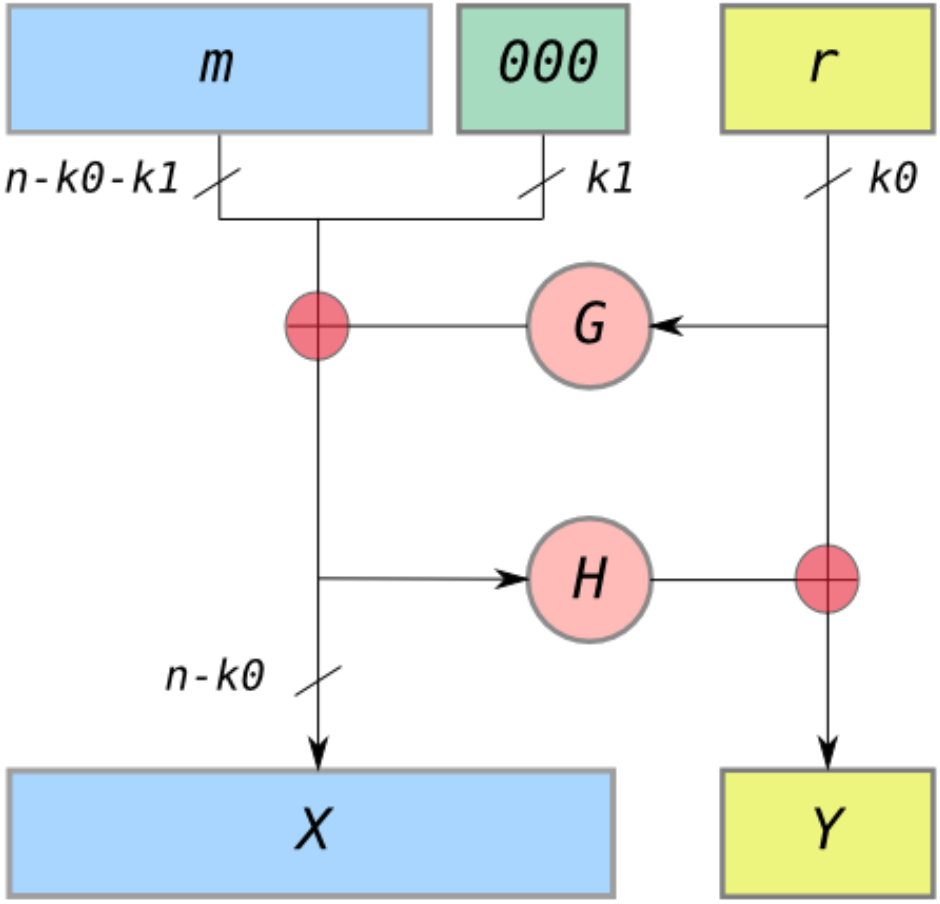
$$C' = C \cdot \alpha^e \text{ mód. } n \quad \rightarrow M' = \alpha \cdot M$$

COSEC uc3m
BY NC SA
Ana I. González-Tablas Ferreres, José M. de Fuentes García-Romero de Tejada, Lorena González Manzano, Pablo Martín González

Ataques específicos.
RSA

- Solución: RSA-OAEP
  - RSA combinado con el relleno (padding) OAEP (*Optimal Asymmetric Encryption Padding*)
    - El actual algoritmo estandarizado es similar al de la Figura
  - Se añade cierta redundancia para que no todos los mensajes posibles sean válidos
  - Supuesto un relleno como el de la Figura, faltaría cifrar:

$$C = (X \,||\, Y)^e \text{ mód. } n$$



COSEC uc3m
BY NC SA
Ana I. González-Tablas Ferreres, José M. de Fuentes García-Romero de Tejada, Lorena González Manzano, Pablo Martín González

Ataques específicos.
El Gamal

- El Gamal es maleable
  - Dado mensaje cifrado $C = (C_1, C_2)$ correspondiente a un mensaje en claro M, es fácil para un atacante obtener un cifrado C' que se corresponda a un mensaje M' relacionado con M

$M \rightarrow C_1 = g_B^{k_e}$ mód. p_B, $C_2 = (y_B^{k_e}) \cdot M$ mód. p_B

$C_1' = C_1$, $C_2' = \alpha \cdot C_2 = (y_B^{k_e}) \cdot (\alpha \cdot M)$ mód. $p_B \rightarrow M' = \alpha \cdot M$

- Solución: Usar una clave simétrica K_T' derivada con una función resumen segura y utilizar un algoritmo de cifrado simétrico robusto (cifrado híbrido)
  - Utilizado así en DHIES (*Diffie-Hellman Integrated Encryption Scheme*) y ECIES (*Elliptic Curve Integrated Encryption Scheme*)

BY NC SA
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

CC BY NC SA