Module 7

Asymmetric Encryption

CRYPTOGRAPHY AND COMPUTER SECURITY COURSE

Ana I. González-Tablas Ferreres
José María de Fuentes García-Romero de Tejada
Lorena González Manzano
Pablo Martín González
Sergio Pastrana Portillo

uc3m | Universidad Carlos III de Madrid

COSEC

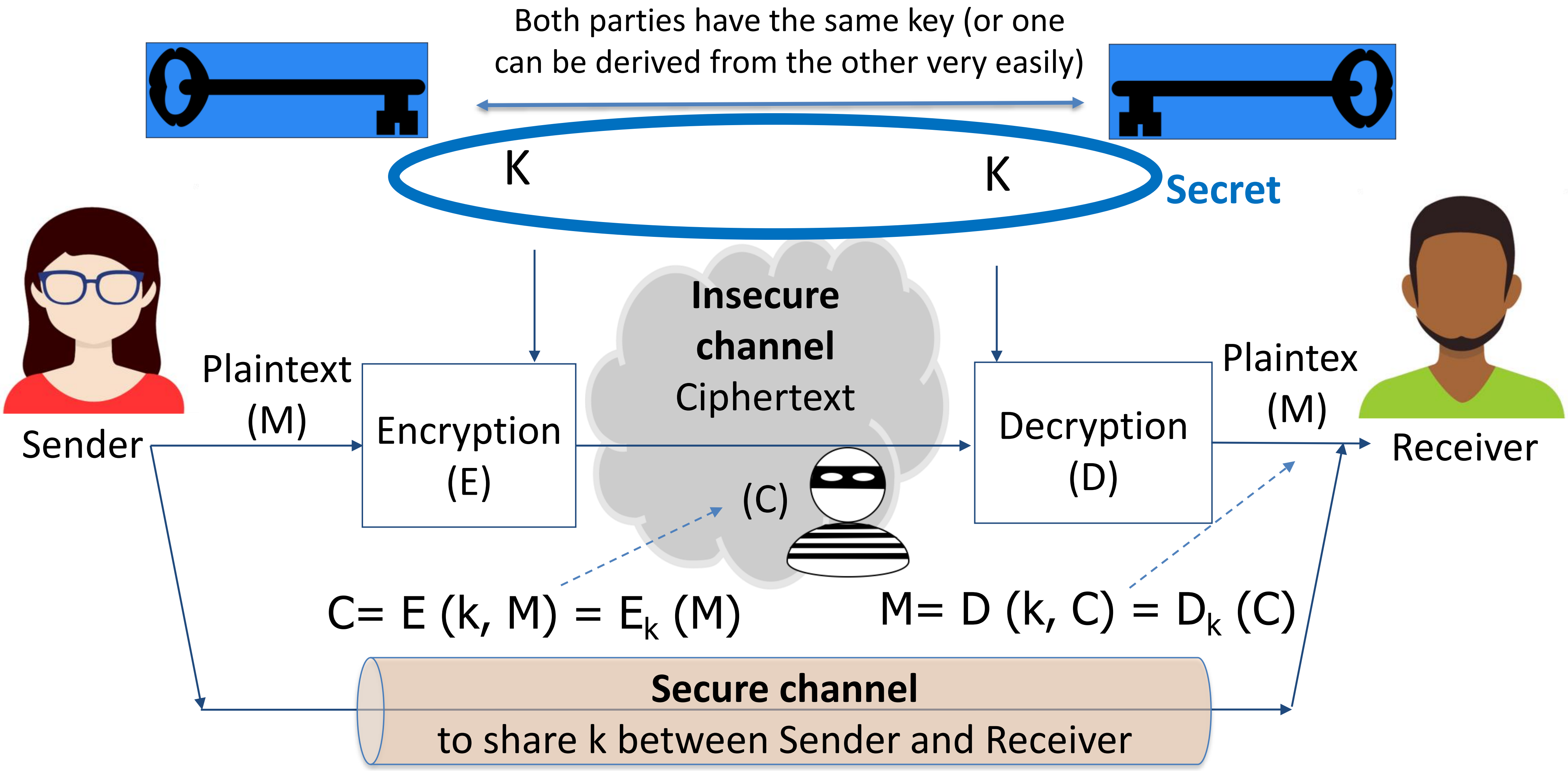
OUTLINE

- 7. Key distribution and asymmetric encryption
  - Asymmetric encryption
    - Historical context and impact
    - Asymmetric encryption model
    - RSA (cipher)
    - El Gamal (cipher)
    - Specific attacks

OUTLINE

- 7. Key distribution and asymmetric encryption
  - Asymmetric encryption
    - **Historical context and impact**
    - Asymmetric encryption model
    - RSA (cipher)
    - El Gamal (cipher)
    - Specific attacks

Historical context and impact
Recalling symmetric encryption model



Both parties have the same key (or one can be derived from the other very easily)

$C= E\ (k, M) = E_k\ (M)$

$M= D\ (k, C) = D_k\ (C)$

Secure channel

to share k between Sender and Receiver

Historical context and impact

- Problem:
  - Two parties, who have not shared any secret a priori, need to exchange a message using an insecure channel
  - In symmetric cryptosystems, communicating parties need a secure channel to exchange or agree on the secret key
  - For more than 3,000 years it was thought that there was no solution

Historical context and impact

- Whitfield Diffie, Martin E. Hellman. ***New Directions in Cryptography***. IEEE Transactions in Information Theory, v. IT-22, pp 664-654. November 1976.
  - Seminal article that proposed public key cryptography
  - Probably the biggest cryptographic milestone in 3,000 years
  - It was previously discovered by British Intelligence Services
  - It proposes asymmetric cryptosystems --- in a theoretical way --- and the Diffie-Hellman key exchange algorithm, based also in asymmetric cryptography

Historical context and impact

- Whitfield Diffie, Martin E. Hellman. ***New Directions in Cryptography***. IEEE Transactions in Information Theory, v. IT-22, pp 664-654. November 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

Historical context and impact

- Next we'll see asymmetric cryptosystems

- Later we'll see:
  - The Diffie-Hellman key exchange algorithm,
  - Main approaches to key distribution, based on symmetric cryptography or on asymmetric one

OUTLINE

- 7. Key distribution and asymmetric encryption
  - Asymmetric encryption
    - Historical context and impact
    - **Asymmetric encryption model**
    - RSA (cipher)
    - El Gamal (cipher)
    - Specific attacks

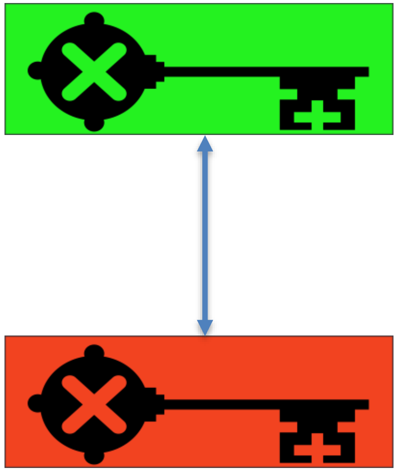
Asymmetric encryption model

- Asymmetric cryptosystesm (aka public key)

  Uses key pairs:

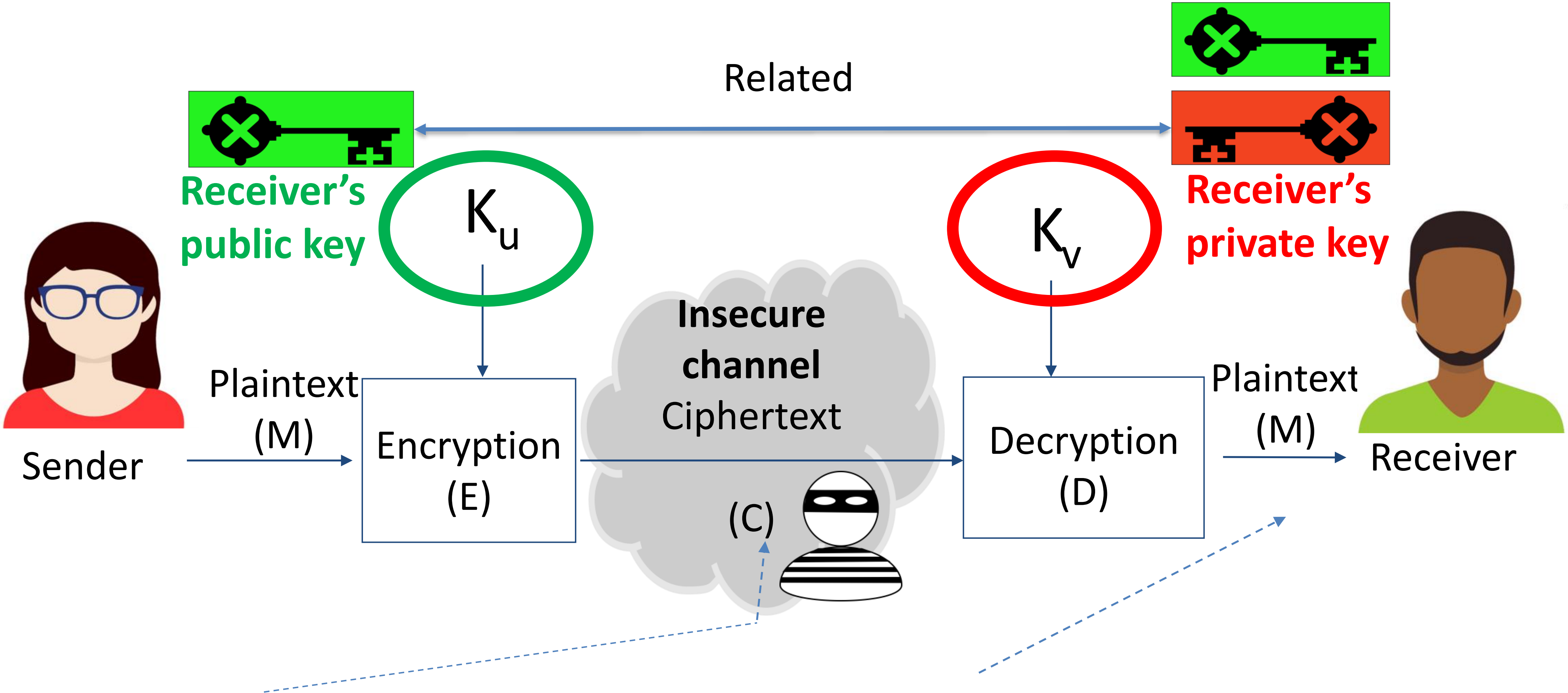
  – **public key**
    - Known by everybody
    - The sender of a message uses the receiver’s public key to encrypt the message for him/her

  – **related private key**
    - Known by the owner (only)
    - The receiver of an encrypted message uses his/her private key to decrypt ciphertexts sent to him/her



Unfeasible to determine the private key from the public one

Asymmetric encryption model



$C= E (k_u, M) = E_{k_u} (M)$

$M= D (k_v, C) = D_{k_v} (C)$

Asymmetric encryption model

- **Computational security**
  - Brute-force search is possible in theory
  - Keys must be large enough
  - Security of public key encryption is based on *hard* problems → Trapdoor one-way function
    - Integer factorization (for large numbers)
    - Discrete logarithm (for large numbers)

- **Slower than symmetric algorithms**

OUTLINE

- 7. Key distribution and asymmetric encryption
  - Asymmetric encryption
    - Historical context and impact
    - Asymmetric encryption model
    - **RSA (cipher)**
    - El Gamal (cipher)
    - Specific attacks

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. February 1978.
  - First public key cryptosystem, the well-known RSA
  - Based on the difficulty of factoring a number product of two large primes of similar bit-length (integer factoring is a *hard problem*)
  - More public key cryptosystems have been proposed (some of them are broken). RSA is still robust considering some modifications

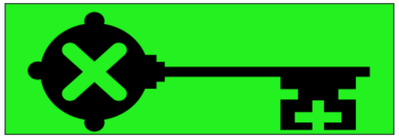
RSA

- 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. February 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 · d ≡ 1 (mod (p − 1) · (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

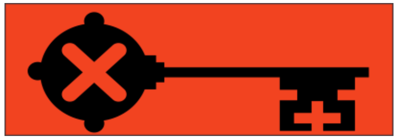
RSA (cipher)

- **B's key pair generation**
  - B chooses p_B, q_B (very large primes, private)
  - B computes $n_B = p_B \cdot q_B$
  - B computes $\phi(n_B) = \phi(p_B) \cdot \phi(q_B)$
  - B chooses $e_B \in Z+ \;/\; \text{m.c.d.}\,(e_B, \phi(n_B))=1$
  - B computes $d_B \;/\; e_B \cdot d_B = 1 \quad \text{mod.}\ \phi(n_B)$

- B's public key: $k_{U,B} = (e_B, n_B)$

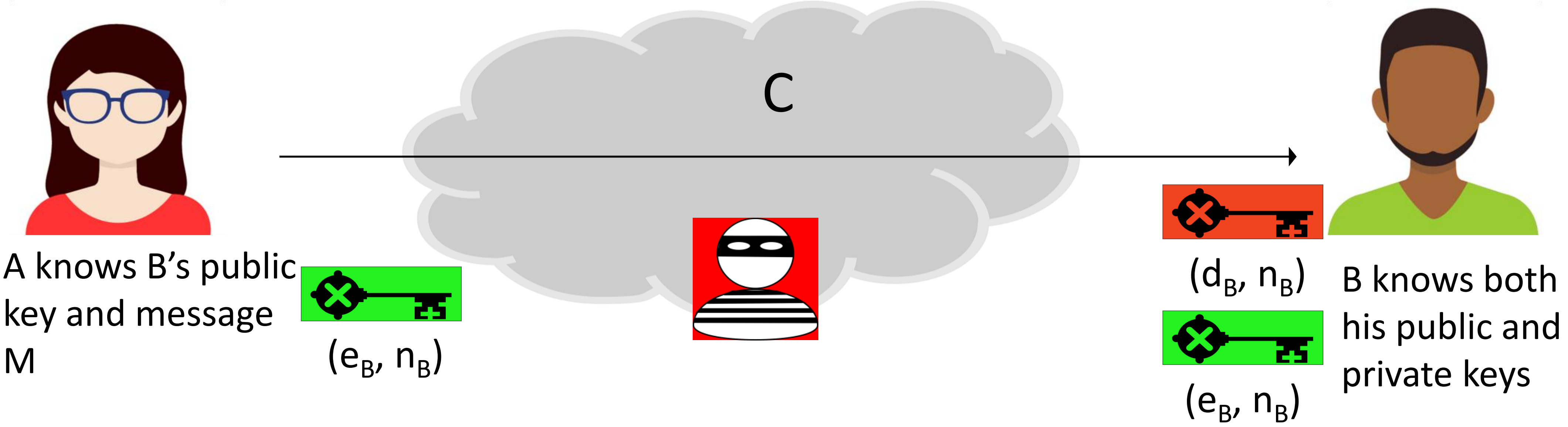


- B's private key: $k_{V,B} = (d_B, n_B)$



RSA (cipher)

- **A sends an encrypted message M $\in Z_{n_B}$ to B** (part 1)



C

A knows B's public key and message M

(e_B, n_B)

(d_B, n_B)

(e_B, n_B)

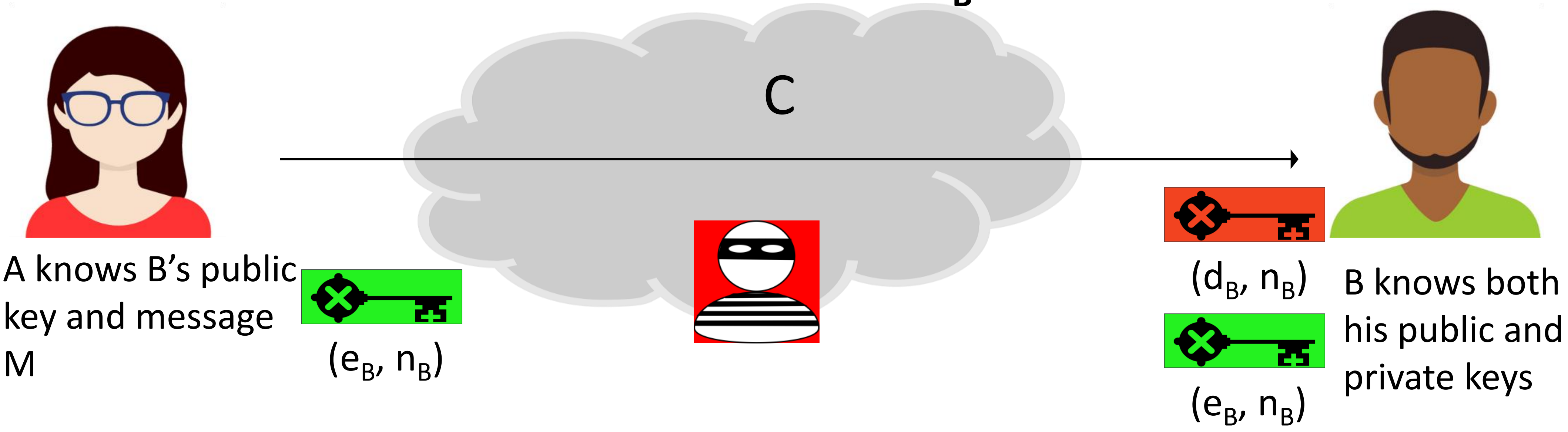
B knows both his public and private keys

A encrypts M using (e_B, n_B), B's public key, and sends ciphertext to B

$$C = M^{e_B} \bmod. n_B$$

RSA (cifrado)

- **A sends an encrypted message M $\in Z_{n_B}$ to B** (part 2)



C

A knows B's public key and message M

(e_B, n_B)

(d_B, n_B)

(e_B, n_B)

B knows both his public and private keys

B decrypts C using (d_B, n_B), his private key

$$M = C^{d_B} \text{ mod. } n_B$$

RSA (cipher)

- Proof of correcteness:

$$C = M^{e_B} \text{ mod. } n_B \Rightarrow C^{d_B} \text{ mod. } n_B = M^{e_B \cdot d_B} \text{ mod. } n_B$$

$$e_B \cdot d_B = 1 \text{ mod. } \phi(n_B) \Rightarrow e_B \cdot d_B = 1 + k \cdot \phi(n_B)$$

By Euler's Theo.(*),

$$M^{\phi(n_B)} \text{ mod. } n_B = 1$$

$$M^{e_B \cdot d_B} \text{ mod. } n_B = M^{1 + k \cdot \phi(n_B)} \text{ mod. } n_B = M$$

$$C^{d_B} \text{ mod. } n_B = M$$

(*) Note that this demonstration as provided here only works for M such that gcd(M,n_B)=1. RSA correctness can be proved as well for M that are not relatively prime to n_B .
https://en.wikipedia.org/wiki/RSA_(cryptosystem)#Proof_using_Euler's_theorem

RSA (cipher)

- RSA's security is shown to be as hard as the integer factorization problem
  - To compute d = inv [e, ϕ(n)]
    - You need to compute $\phi(n) = (p - 1) \cdot (q - 1)$
    - To efficiently compute ϕ(n), it is necessary to know p and q
    - $O(e^{\ln(n) \cdot \ln \ln(n)})$
- RSA factoring challenge
  - https://en.wikipedia.org/wiki/RSA_Factoring_Challenge
  - RSA-768 (768 bits, 232 decimal digits) was factorized on 2009/12/12
  - RSA-230 (762 bits, 230 decimal digits) was factorized on 2018/08/15
- Recommended modulo bit-length
  - At least 2048 bits (NIST 2016) or 3072 bits (ECRYPT-CSA 2018)
  - https://www.keylength.com/en/

OUTLINE

- 7. Key distribution and asymmetric encryption
  - Asymmetric encryption
    - Historical context and impact
    - Asymmetric encryption model
    - RSA (cipher)
    - **El Gamal (cipher)**
    - Specific attacks

El Gamal (cipher)

- 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, July 1985.
  - Public key cryptosystem based on hard problems related to the difficulty of efficiently computing the discrete logarithm
  - http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.476.4791&rep=rep1&type=pdf

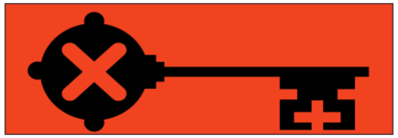
El Gamal (cipher)

- **B's key pair generation**
  - B chooses p_B, very large prime
  - B chooses g_B, generator of cyclic group G of order p_B
  - B selects x_B as B's private such that

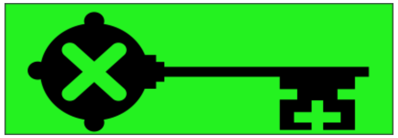
    $$1 < x_B < p_B - 1$$

  - B computes y_B , s B's public key ($y_B = g^{x_B}$ mod. p_B)

- B's private key: $k_{V,B} = (x_B)$

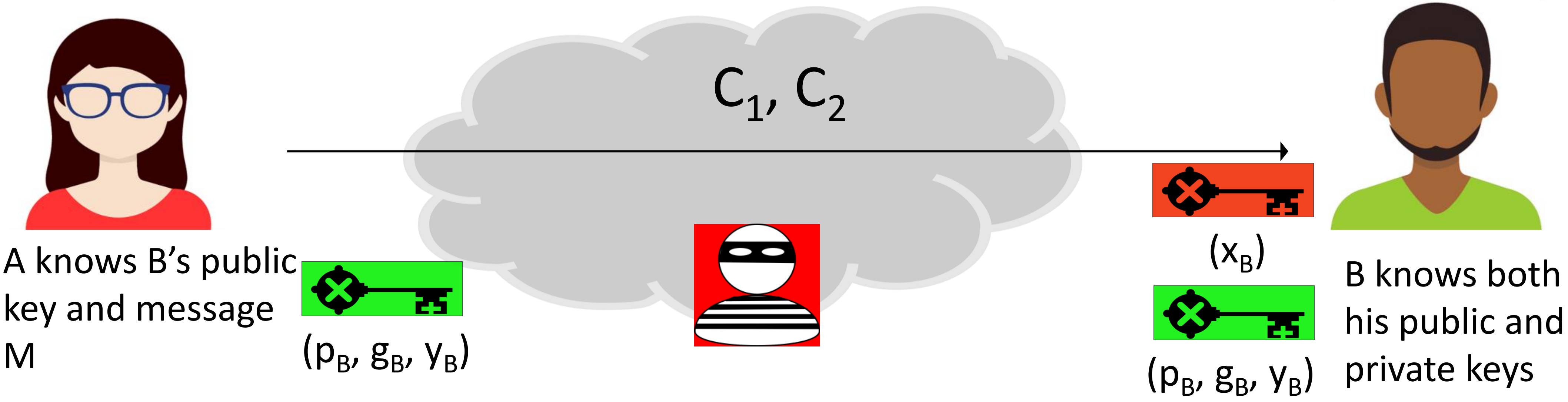


- B's public key: $k_{U,B} = (p_B, g_B, y_B)$



El Gamal (cipher)

- **A sends message M$\in$G(p_B) encrypted to B** (part 1)



C_1, C_2

A knows B's public key and message M

(p_B, g_B, y_B)

(x_B)

(p_B, g_B, y_B)

B knows both his public and private keys

A chooses k_e (random) | $1 < k_e < p_B - 1$

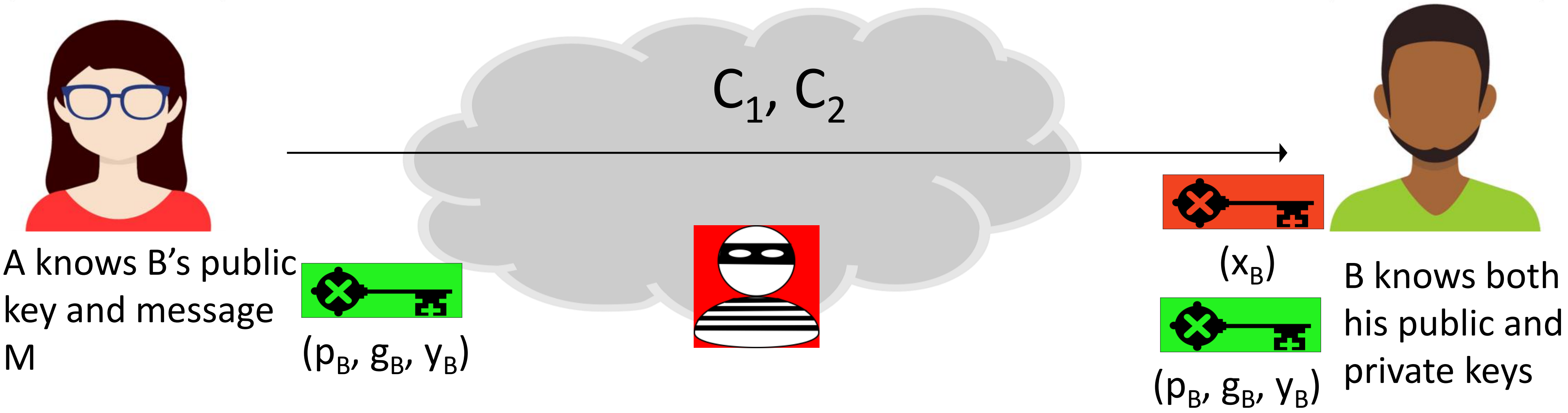
A computes $C_1 = g_B^{k_e} \bmod. p_B$

A computes ephemeral key using B's public key: $K_T = y_B^{k_e} \bmod. p_B$

A computes M's ciphertext as $C_2 = K_T \cdot M \bmod. p_B$

El Gamal (cipher)

- **A sends message M∈G(p_B) encrypted to B** (part 2)



C_1, C_2

A knows B's public key and message M

(p_B, g_B, y_B)

(x_B)

(p_B, g_B, y_B)

B knows both his public and private keys

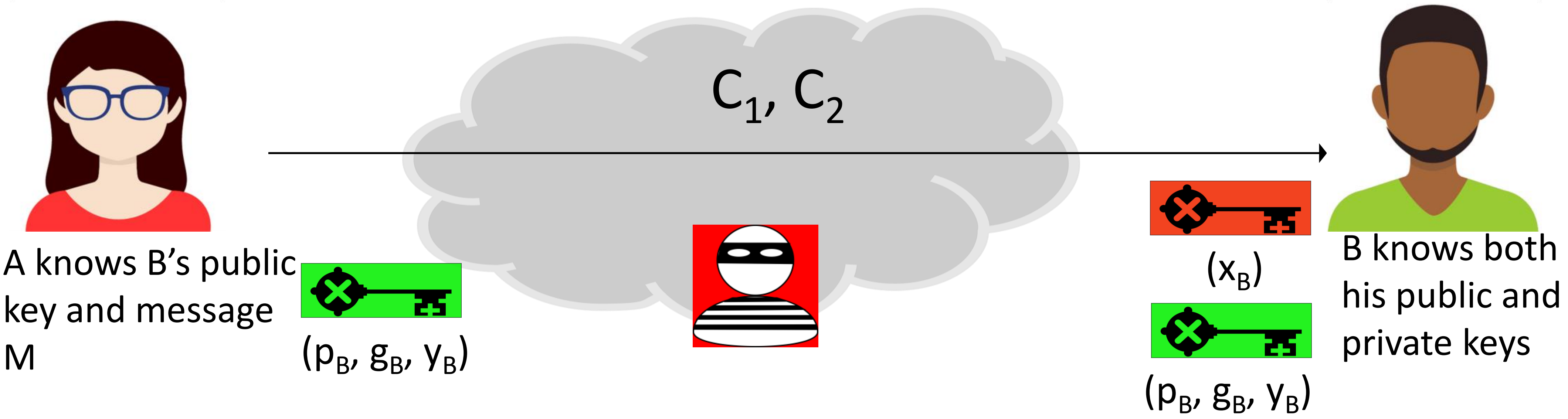
A sends to B C = C_1, C_2

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

If $C_2 = K_T \cdot M$ mod. p_B , M and $K_T \in G(p_B)$ → $M = C_2 \cdot K_T^{-1}$ mod. p_B

El Gamal (cipher)

- **A sends message $M \in G(p_B)$ encrypted to B** (part 3)



A knows B's public key and message M

(p_B, g_B, y_B)

C_1, C_2

(x_B)

(p_B, g_B, y_B)

B knows both his public and private keys

B first recovers ephemeral key and then decrypts C:

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

As for Fermat's Theorem

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

El Gamal (cipher)

- El Gamal security is based on the discrete logarithm problem
  - Given a cyclic group of order p with a generator g, once selected y $\in$ G(p), there is a unique x | g^x = y mod. p
  - Computing x = $\log_g$ y mod. p is a hard problem

- Recommended length for primes p
  - At least 2048 bits (NIST 2016) or 3072 bits (ECRYPT-CSA 2018)
  - If cyclic groups are defined over elliptic curves, they should have at least 224 bits (NIST 2016) or 256 bits (ECRYPT-CSA 2018)

El Gamal (cipher)

- In practice
  - Group and parameters p and g are standardized and are publicly known
  - K_T is not used directly as the symmetric key but another symmetric key K_T' is derived from it, e.g, using a hash function, to encrypt the message M (hybrid encryption)

$$K_T' = H(K_T)$$

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

OUTLINE

- 7. Key distribution and asymmetric encryption
  - Asymmetric encryption
    - Historical context and impact
    - Asymmetric encryption model
    - RSA (cipher)
    - El Gamal (cipher)
    - **Specific attacks**

Specific attacks on RSA

- *Text-book* RSA encryption is deterministic → it is not IND-CPA secure
  - Adv produces m_0 and m_1
  - Challenger encrypts one of them: $c^* \leftarrow m_b^e \bmod n$
  - Adv computes both $m_0^e \bmod n$ and $m_1^e \bmod n$ being able to distinguish the value of b
- *Text-book* RSA encryption is malleable
  - Given ciphertext C, that decrypts into plaintext M, it is easy to obtain a ciphertext C' that decrypts to a plaintext M' related to M

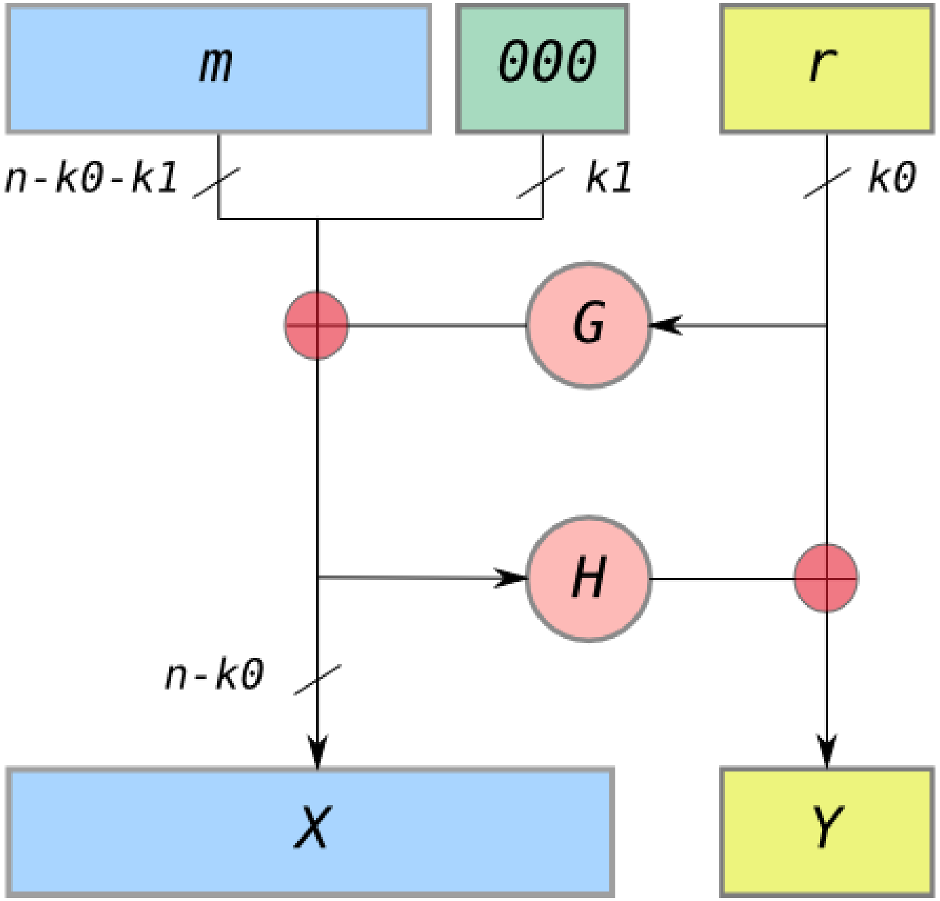
$$M \rightarrow \quad C = M^e \text{ mod. } n$$

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

Specific attacks on RSA. RSA-OAEP

- Fixing *text-book* RSA encryption → RSA-OAEP
  - Padding is added to RSA
    - OAEP (*Optimal Asymmetric Encryption Padding*)
    - Current standardized algorithm is similar to the one in the figure
  - Some redundancy is added so not all messages are valid
  - After padding, padded message is encrypted:

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



Specific attacks on El Gamal

- El Gamal is malleable
  - Given a ciphertext C = (C_1, C_2) that encrypts a cleartext M, it is easy for an adversary to compute a second ciphertext C' that encrypts a message M' related to M

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

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

- Solution: Use a symmetric key K_T' derived with a secure hash function and encrypt the message with a robust symmetric encryption algorithm (hybrid encryption)
  - DHIES (*Diffie-Hellman Integrated Encryption Scheme*) and ECIES (*Elliptic Curve Integrated Encryption Scheme*)

CRYPTOGRAPHY AND COMPUTER SECURITY COURSE

COSEC

uc3m | Universidad Carlos III de Madrid