Module 11

Digital signatures

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

- 11. Digital signatures
  - Digital signature schemes
  - RSA (digital signature)
  - El Gamal (digital signature)
  - Attacks
  - Digital signature and encryption

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

OUTLINE

- 11. Digital signatures
  - **Digital signature schemes**
  - RSA (digital signature)
  - El Gamal (digital signature)
  - Attacks
  - Digital signature and encryption

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

Digital signature schemes

- [ISO-7498-2]
  - Data appended to, or a cryptographic transformation of, a data unit that allows a recipient of the data unit to prove the source and integrity of the data unit and protect against forgery e.g. by the recipient.
- [NIST SP 800-57 Pt. 1 Rev. 5: 2020]
  - The result of a cryptographic transformation of data that, when properly implemented with a supporting infrastructure and policy, provides the services of:
    - 1. Source/identity authentication,
    - 2. Data integrity authentication, and/or
    - 3. Support for signer non-repudiation.

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

Digital signature schemes

- Concept introduced by Diffie and Hellman in 1976
- Somehow, it is the digital equivalent to a handwritten signature
- Properties of handwritten signatures:
  - Easy and cheap to produce
  - Easy to recognize (for verification)
  - Signer cannot reject (repuadiate) the signature
  - Unforgeable (theoretically)
- Digital signatures should satisfy the same properties, but:
  - Digital signature cannot be the same for all documents as it could be easily forged

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

Digital signature schemes. Security properties

- Authenticates the signer of a message
- Prevents unauthorized message modifications (i.e., allows message integrity verification)
- Prevents non-repudiation: it can be used in dispute resolution

It does NOT provide ~~confidentiality~~

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

Digital signature schemes. Components

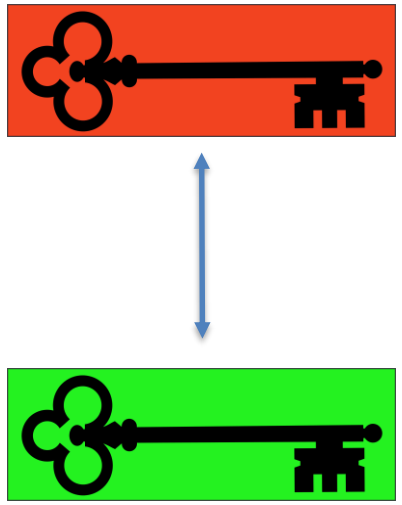
- A digital signature scheme is composed by three parts:
  - Key generation algorithm G
  - Signature generation algorithm S
  - Signature verification algorithm V

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

Digital signature schemes

Each user has a key pair:

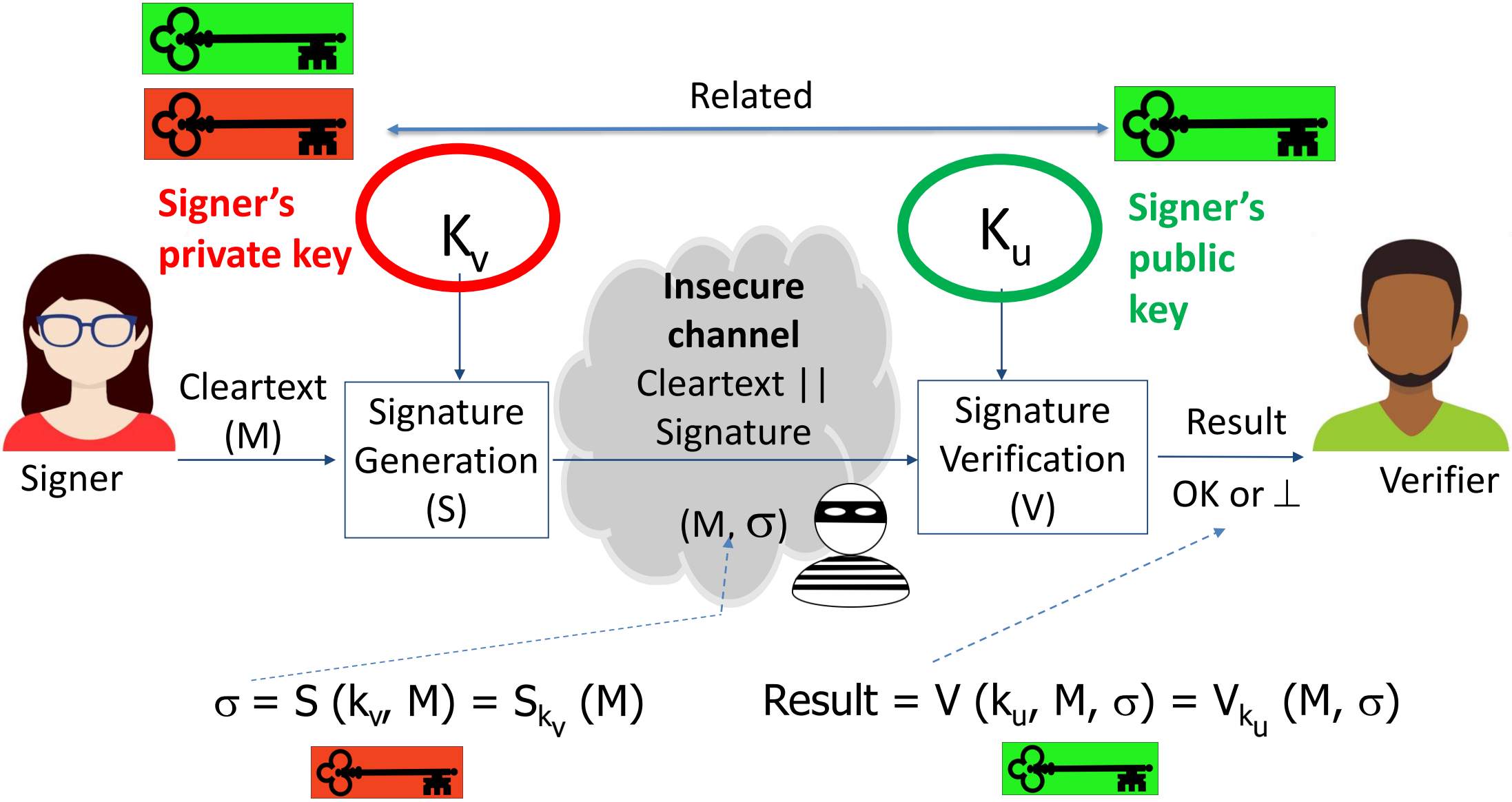
- **private key**
  - Known only by the owner
  - Used to generate signatures



- **Public key**
  - Known by everyone
  - Used to verify signatures: the verifier uses the signer's public key to verify the signatures (generated by the signer)

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

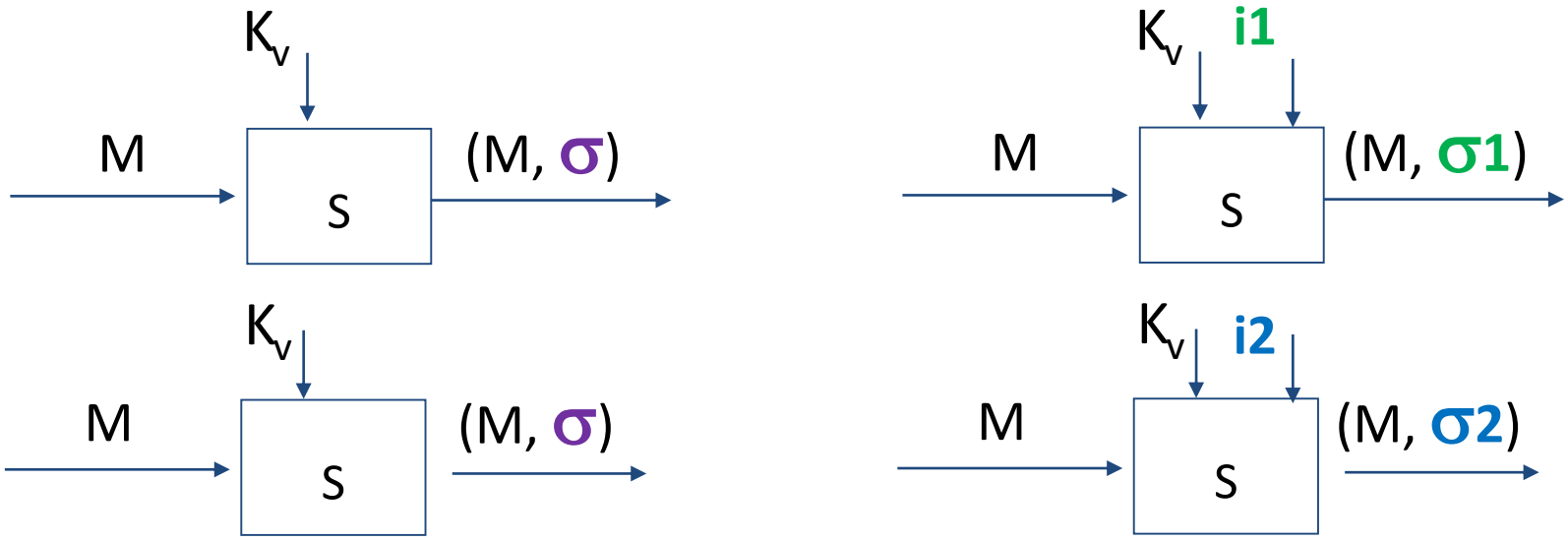
Digital signature schemes



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

Digital signature schemes. Deterministic vs Randomized

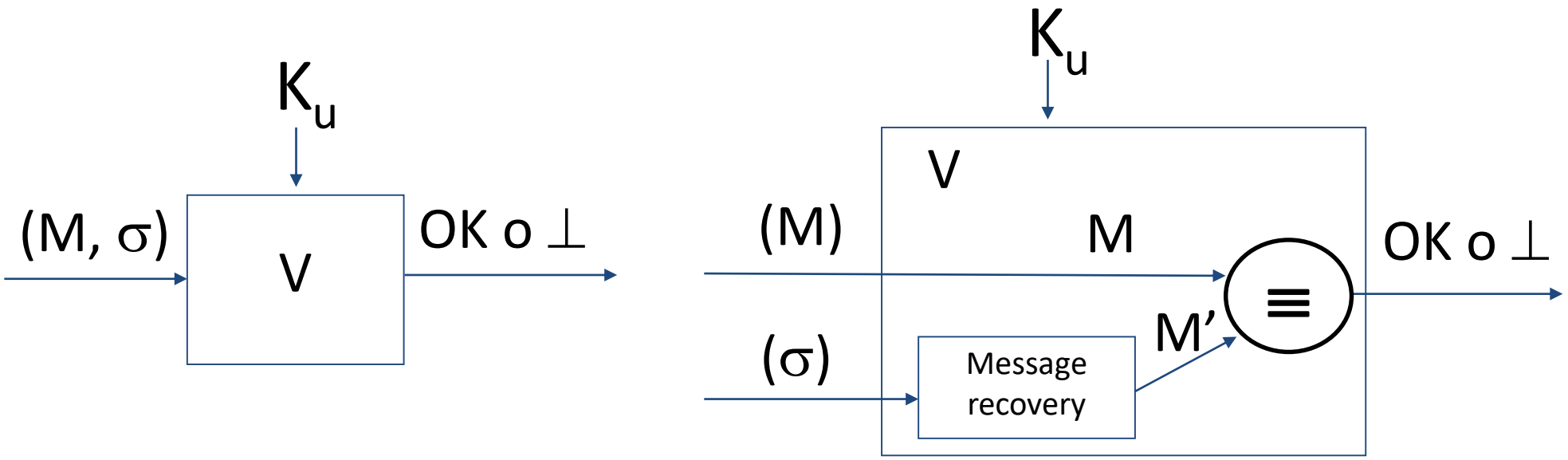
- Digital signature schemes can be:
  - Deterministic: Signatures generated over the same message are equal (eg, "naïve" RSA signatures)
  - Randomized: Signatures generated over the same message are different as they depend on an index (eg, El Gamal signatures)



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

Digital signature schemes. With appendix vs Message recovery

- Digital signatures schemes can be:
  - With appendix or separated from the message: The signature is a value that is appended to the message (e.g., El Gamal digital signatures)
  - With message recovery: The signature is the transformation produced on the message (e.g., "naïve" RSA signatures)



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

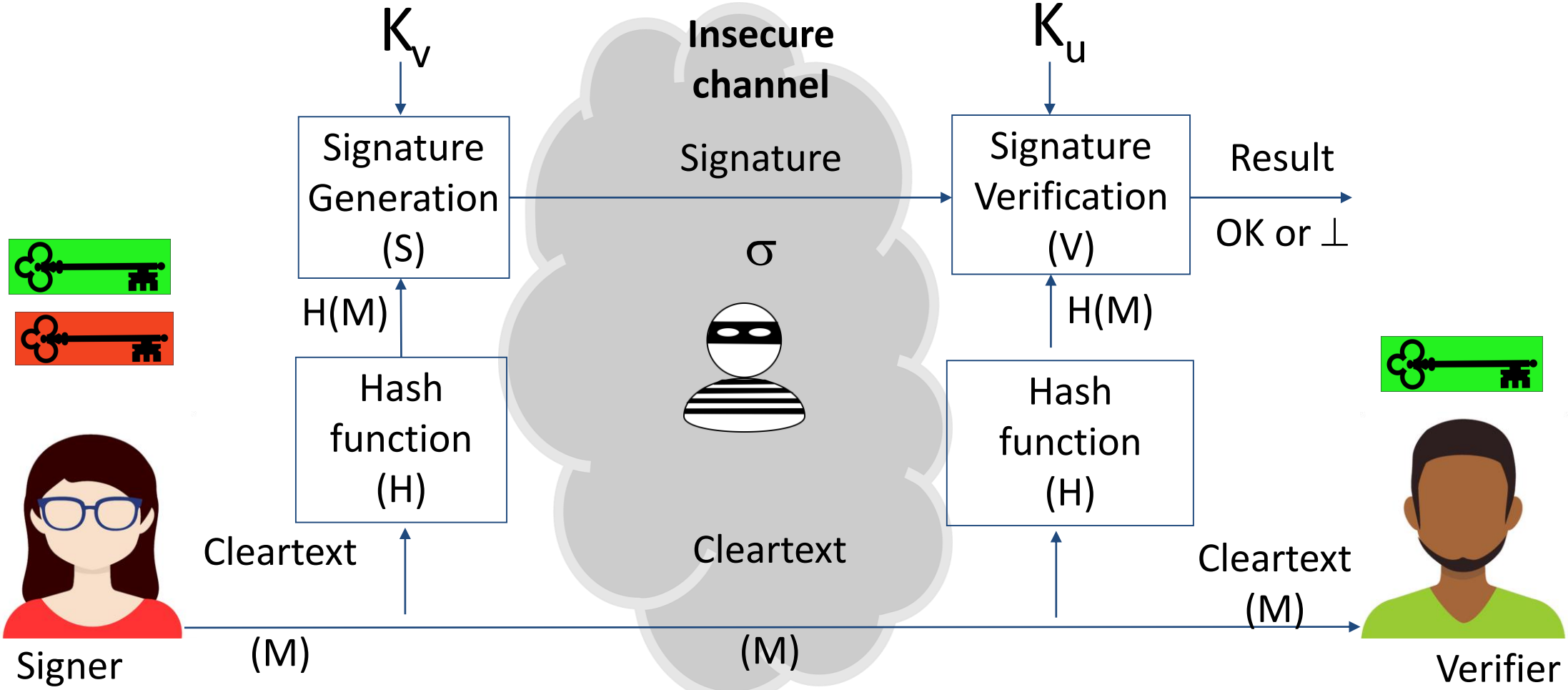
Digital signature schemes. Hash-then-sign

- Generally, signatures are not generated over messages directly but on the message's hash value
  - It is more efficient (especially for long messages - message should be split in blocks if greater than the modulo)
  - It is more secure, both for RSA and El Gamal based signatures

- To verify hash-then-sign signatures, the verifier first must compute the message's hash

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

Digital signature schemes. Hash-then-sign



$\sigma = S(k_v, H(M)) = S_{k_v}(H(M))$

$Result = V(k_u, H(M), \sigma) = V_{k_u}(H(M), \sigma)$

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

OUTLINE

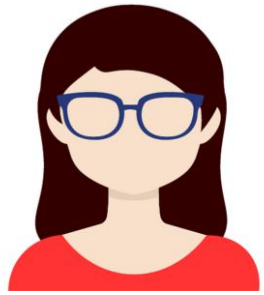
- 11. Digital signatures
  - Digital signature schemes
  - **RSA (digital signature)**
  - El Gamal (digital signature)
  - Attacks
  - Digital signature and encryption

RSA (digital signature)

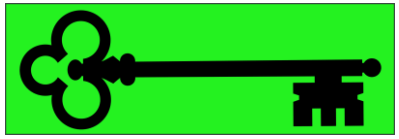
- Digital signature scheme
  - Deterministic
  - With message recovery
- Security based on the problem of integer factorization
  - Recommended key sizes are similar to those recommended for encryption

RSA (digital signature)

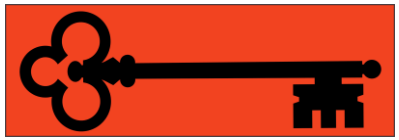
- **A's key pair generation**
  - A chooses p_A, q_A (big integers, private)
  - A computes $n_A = p_A \cdot q_A$
  - A computes $\phi(n_A) = \phi(p_A) \cdot \phi(q_A)$
  - A chooses $e_A \in Z+ / \text{m.c.d.}(e_A, \phi(n_A))=1$
  - A computes $d_A / e_A \cdot d_A = 1 \quad \text{mod. } \phi(n_A)$



- A's public key: $k_{U,A} = (e_A, n_A)$



- A's private key: $k_{V,A} = (d_A, n_A)$

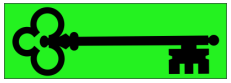


Ana I. González-Tablas Ferreres, José M. de Fuentes García-Romero de Tejada, Lorena González Manzano, Pablo Martín González, Sergio Pastrana Portillo

RSA (digital signature)

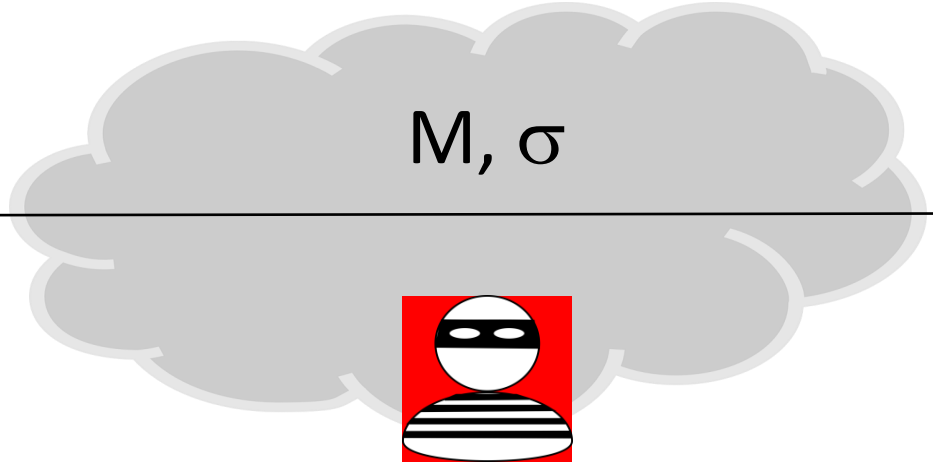
- **A sends a signed message M $\in Z_{n_A}$ to B** (part 1)

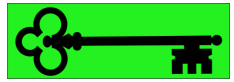
A knows her public and private keys, and the message



(e_A, n_A)

(d_A, n_A)





(e_A, n_A)

B knows A's public key

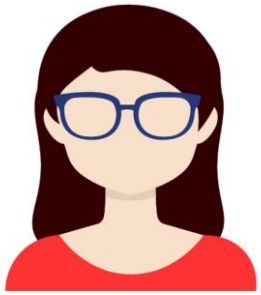
A computes the signature on M using (d_A, n_A), her private key, and sends to B the message M and the signature σ

$$(M, \sigma = M^{d_A} \bmod n_A)$$

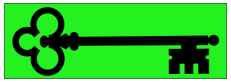
Ana I. González-Tablas Ferreres, José M. de Fuentes García-Romero de Tejada, Lorena González Manzano, Pablo Martín González, Sergio Pastrana Portillo

RSA (digital signature)

- **A sends a signed message M $\in Z_{n_A}$ to B** (part 2)

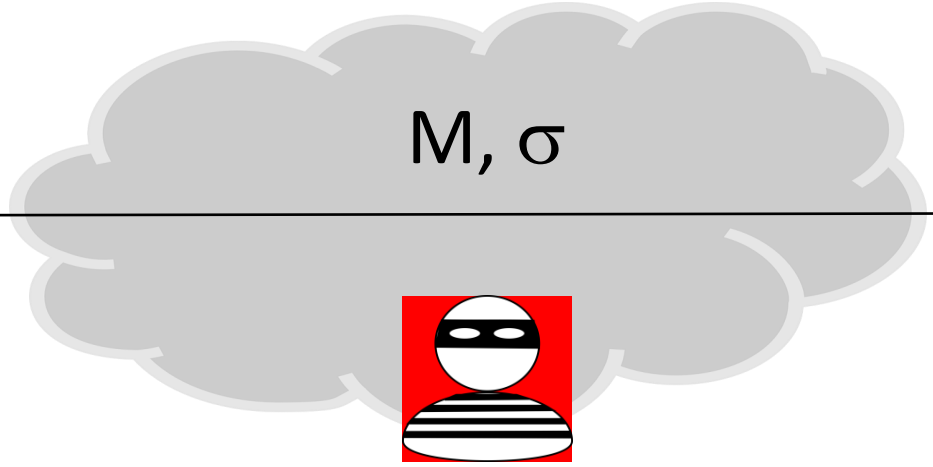


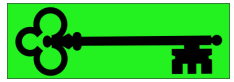
A knows her public and private keys, and the message



(e_A, n_A)

(d_A, n_A)



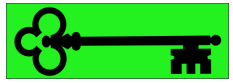


(e_A, n_A)

B knows A's public key

B verifies signature σ on M using (e_A, n_A), A's public key, and accepts the message only if result of the verification is OK

$M' = \sigma^{e_A} \bmod n_A$; if $M' \equiv M \rightarrow$ OK, otherwise, $\perp$



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

OUTLINE

- 11. Digital signatures
  - Digital signature schemes
  - RSA (digital signature)
  - **El Gamal (digital signature)**
  - Attacks
  - Digital signature and encryption

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

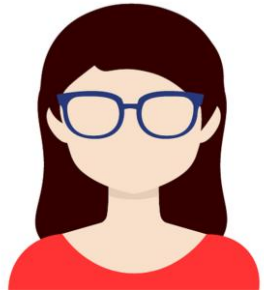
El Gamal (digital signature)

- Digital signature scheme
  - Randomized
  - With appendix

- Security based on the problem of computing the discrete logarithm
  - Recommended key sizes are similar to those recommended for encryption
- Instead of using El Gamal digital signature scheme, it is more common to use DSA (*Digital Signature Algorithm*), which is a variant derived from El Gamal, or ECDSA, its elliptic curve version

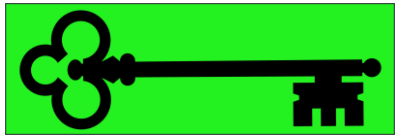
Ana I. González-Tablas Ferreres, José M. de Fuentes García-Romero de Tejada, Lorena González Manzano, Pablo Martín González, Sergio Pastrana Portillo

El Gamal (digital signature)

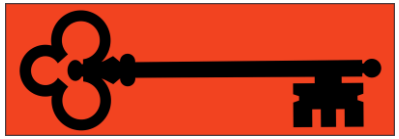


- **A's key pair generation**
  - A chooses p_A, large prime number
  - A selects g_A, generator of a cyclic group G of order p_A
  - A chooses x_A , private key such as $1 < x_A < p_A - 1$
  - A computes y_A , public key ($y_A = g^{x_A} \mod p_A$)

- A's private key: $k_{V,A} = (x_A)$



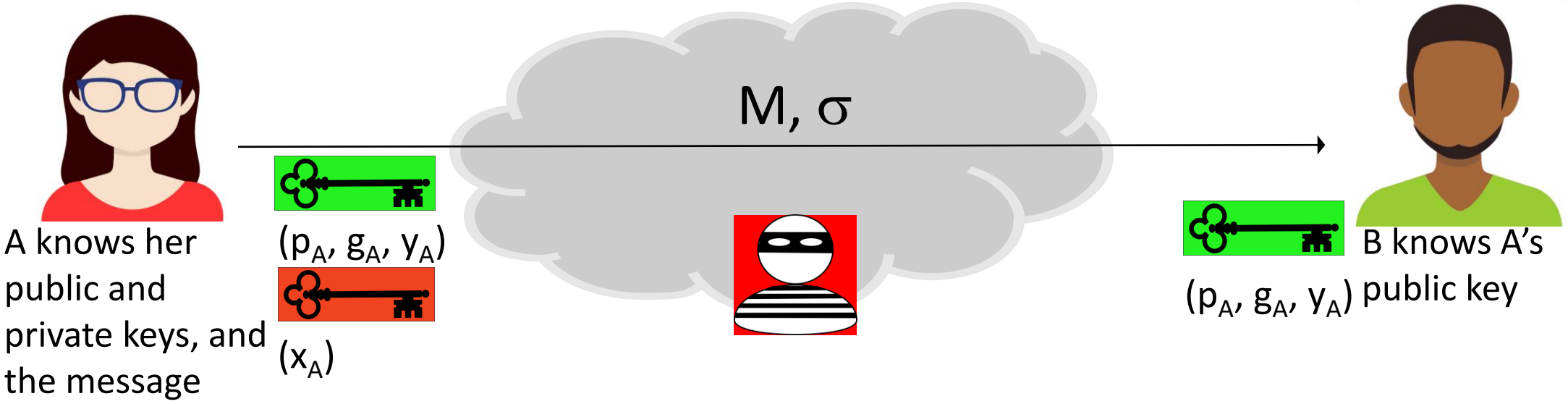
- A's public key: $k_{U,A} = (p_A, g_A, y_A)$



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

El Gamal (digital signature)

- **A sends a signed message M $\in G(p_A)$ to B** (part 1)



A chooses an ephemeral key k_s s.t. $0 < k_s < p_A$ and computes $\mathbf{r} = g^{k_s} \pmod{p_A}$

A, using her private key (x_A), computes $\mathbf{s} = (M - x_A . r) \cdot k_s^{-1} \bmod (p_A - 1)$

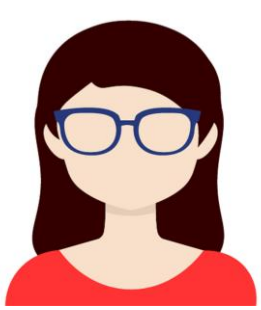
A sends to B message M and its signature, $\boldsymbol{\sigma = (r, s)}$

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

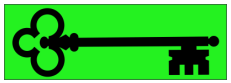
Ana I. González-Tablas Ferreres, José M. de Fuentes García-Romero de Tejada, Lorena González Manzano, Pablo Martín González, Sergio Pastrana Portillo

El Gamal (digital signature)

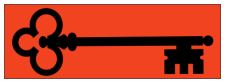
- **A sends a signed message M $\in G(p_A)$ to B** (part 2)



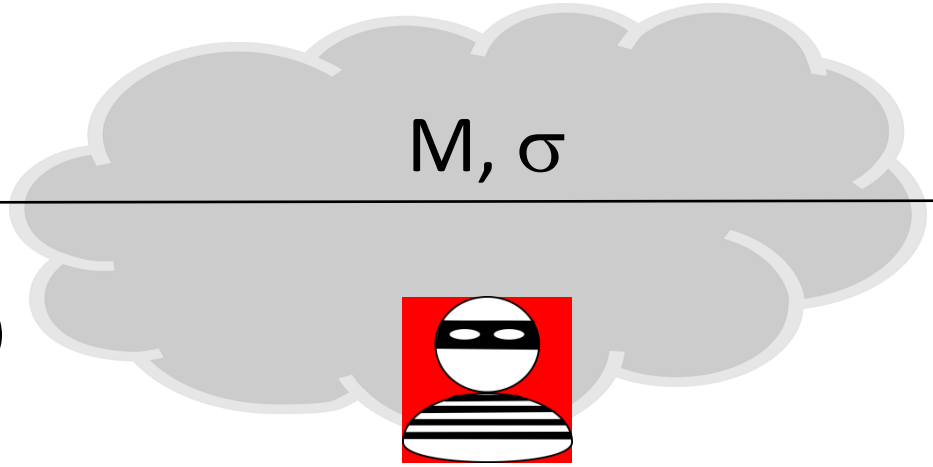
A knows her public and private keys, and the message

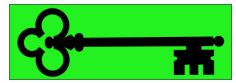


(p_A, g_A, y_A)



(x_A)



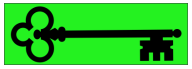


(p_A, g_A, y_A)

B knows A's public key

B verifies M's signature using (p_A, g_A, y_A), A's public key, and accepts the message only if verification result is OK

$V_1 = y_A^{\,r} \cdot r^{s} \pmod{p_A}$; $V_2 = g_A^{\,M} \pmod{p_A}$; if $V_1 \equiv V_2 \rightarrow$ OK, otherwise, $\perp$



OUTLINE

- 11. Digital signatures
  - Digital signature schemes
  - RSA (digital signature)
  - El Gamal (digital signature)
  - **Attacks**
  - Digital signature and encryption

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

Attacks

- Adversary's goal is to forge valid signatures
  - Total break: The adversary determines A's private key
  - Universal forgery: The adversary has a signing algorithm functionally equivalent to the A's one
  - Selective forgery: The adversary forges a signature on a message chosen by the adversary
  - Existential forgery: The adversary can forge a signature for at least one message, but the adversary has no control over this message

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

Attacks. RSA

- "Text-book" RSA is vulnerable to existential forgery attacks

  Attack 1:

  C wants to create a valid signature, as A would have generated it

  Let's assume that C knows A's public key (e_A, n_A)

  C randomly chooses $\sigma \in Z_{n_A}$ and computes $M = \sigma^{e_A} \bmod n_A$

  C sends to B the computed message M and its "forged" signature:

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

  B verifies the message and its signature as correct, as

  $$M \equiv M' = \sigma^{e_A} \bmod n_A \rightarrow OK$$

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

Attacks. RSA

Attack 2:

C can forge a valid signature from two valid signatures generated by A

C gets two valid (message, signature) pairs:

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

C can create a valid signature σ' for message $M' = M_1 \cdot M_2 \bmod n_A$

$$\sigma' = \sigma_1 \cdot \sigma_2 \bmod n_A$$

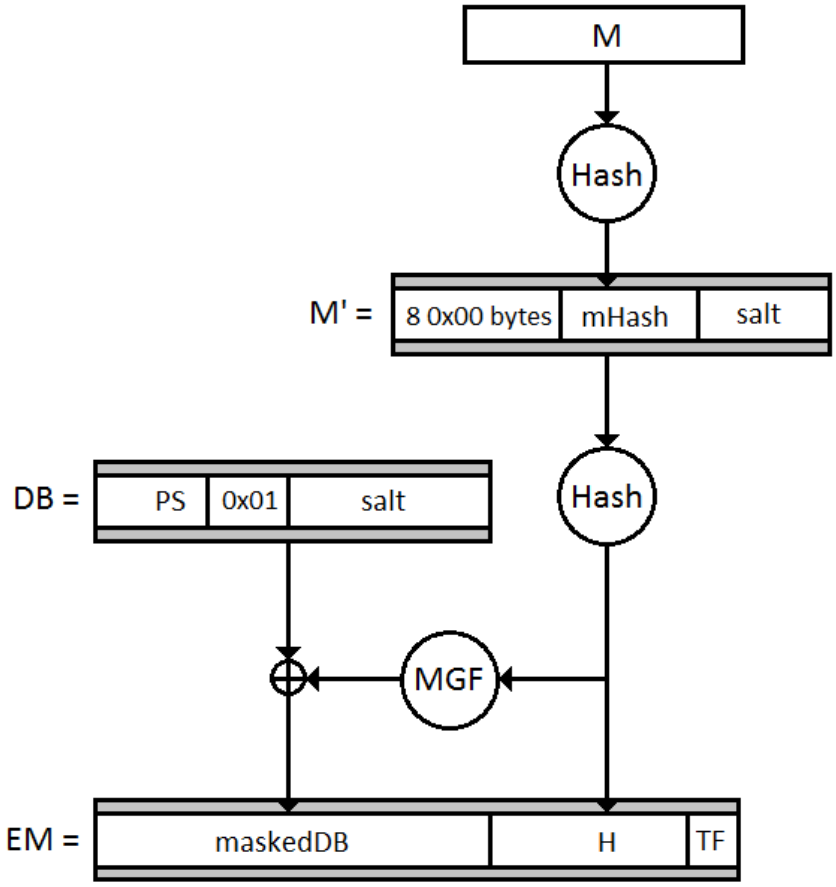
B verifies as correct the signature σ' on M', as

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

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

Attacks. RSA

- Solution:
  - Attacks are prevented if the message's hash value is signed instead of the message itself
  - However, this is not enough to satisfy all modern security requirements. It is desirable to transform deterministic RSA to a randomized scheme
  - RSA-PSS (*Probabilistic Signature Scheme*)
    - Specific padding and random values (*salt*) are added and random values in a way similar to the shown figure



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

Attacks. El Gamal

- Similarly to RSA, “text-book” El Gamal is vulnerable to existential forgery attacks
  - We’ll not see their details
- Solution:
  - Similarly to RSA, the message’s hash value is signed instead of directly signing the message

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

OUTLINE

- 11. Digital signatures
  - Digital signature schemes
  - RSA (digital signature)
  - El Gamal (digital signature)
  - Attacks
  - **Digital signature and encryption**

Digital signature and encryption

- To build a secure channel (message confidentiality and authentication) using public key cryptography, it is necessary to combine a public key cryptosystem and a digital signature scheme
- In the last decades, the security properties of different ways of combining both constructions have been discussed
  - *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

Digital signature and encryption

- Finally, a new cryptographic scheme has been defined, named ***signcryption***, that has to satisfy:
  - If A sends to B a "*signcrypted*" message,
  - only B can decrypt the message, and
  - B can verify that the message's origin was A

- Combinations *sign-then-encrypt* and *encrypt-then-sign* are considered secure if the identities of both the receiver and the sender are included in the signature and the ciphertext, respectively, among other requirements

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

CRYPTOGRAPHY AND COMPUTER SECURITY COURSE

COSEC

uc3m | Universidad Carlos III de Madrid

OUTLINE

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

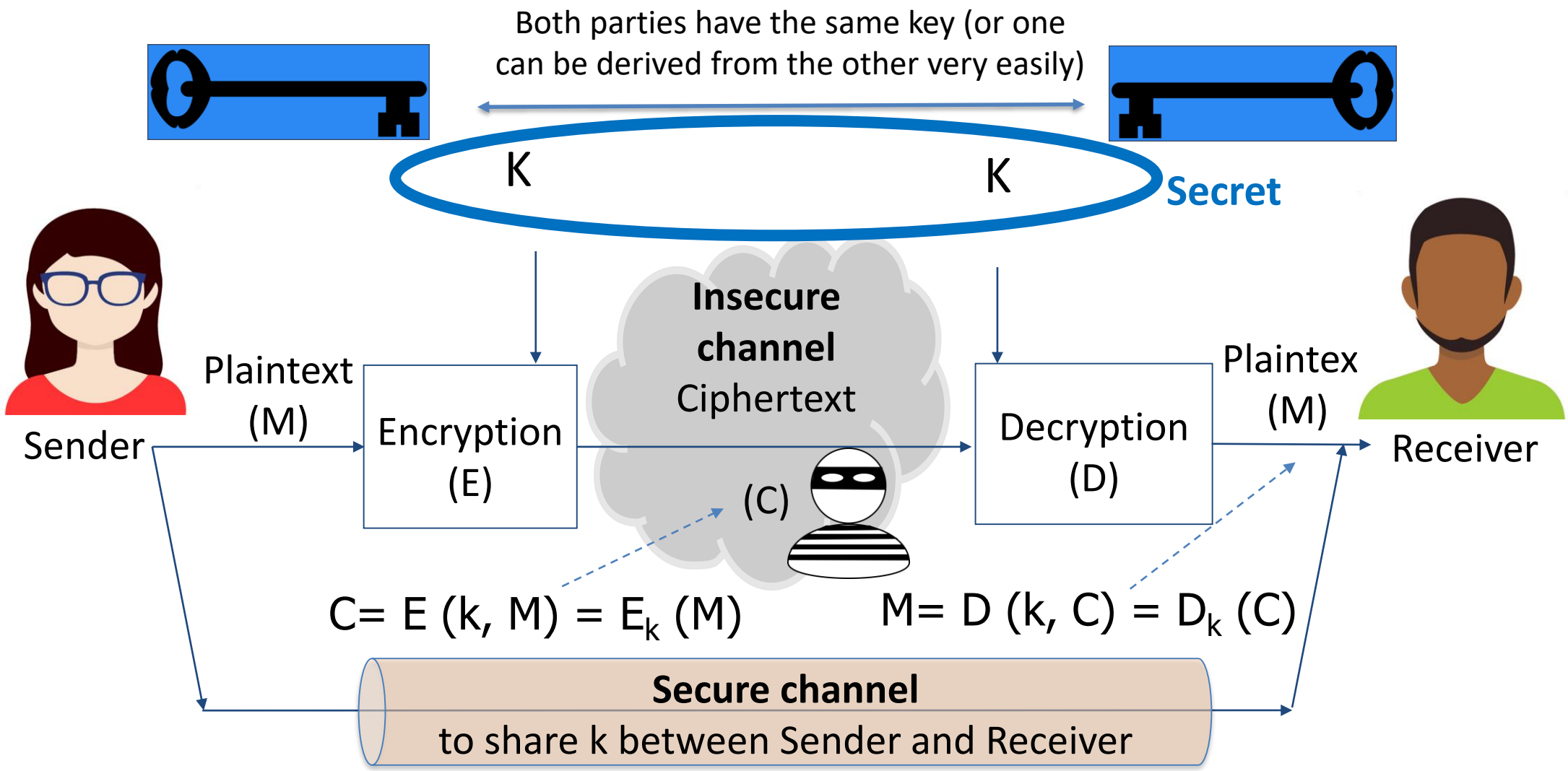
Ana I. González-Tablas Ferreres, José M. de Fuentes García-Romero de Tejada, Lorena González Manzano, Pablo Martín González, Sergio Pastrana Portillo

OUTLINE

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

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

Historical context and impact
Recalling symmetric encryption model



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

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

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

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

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

OUTLINE

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

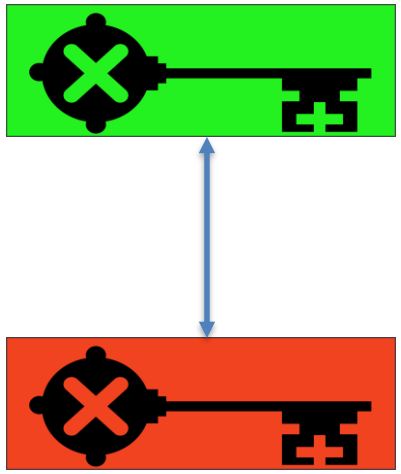
Ana I. González-Tablas Ferreres, José M. de Fuentes García-Romero de Tejada, Lorena González Manzano, Pablo Martín González, Sergio Pastrana Portillo

Asymmetric encryption model

- Asymmetric cryptosystesm (aka public key)

  Uses key pairs:

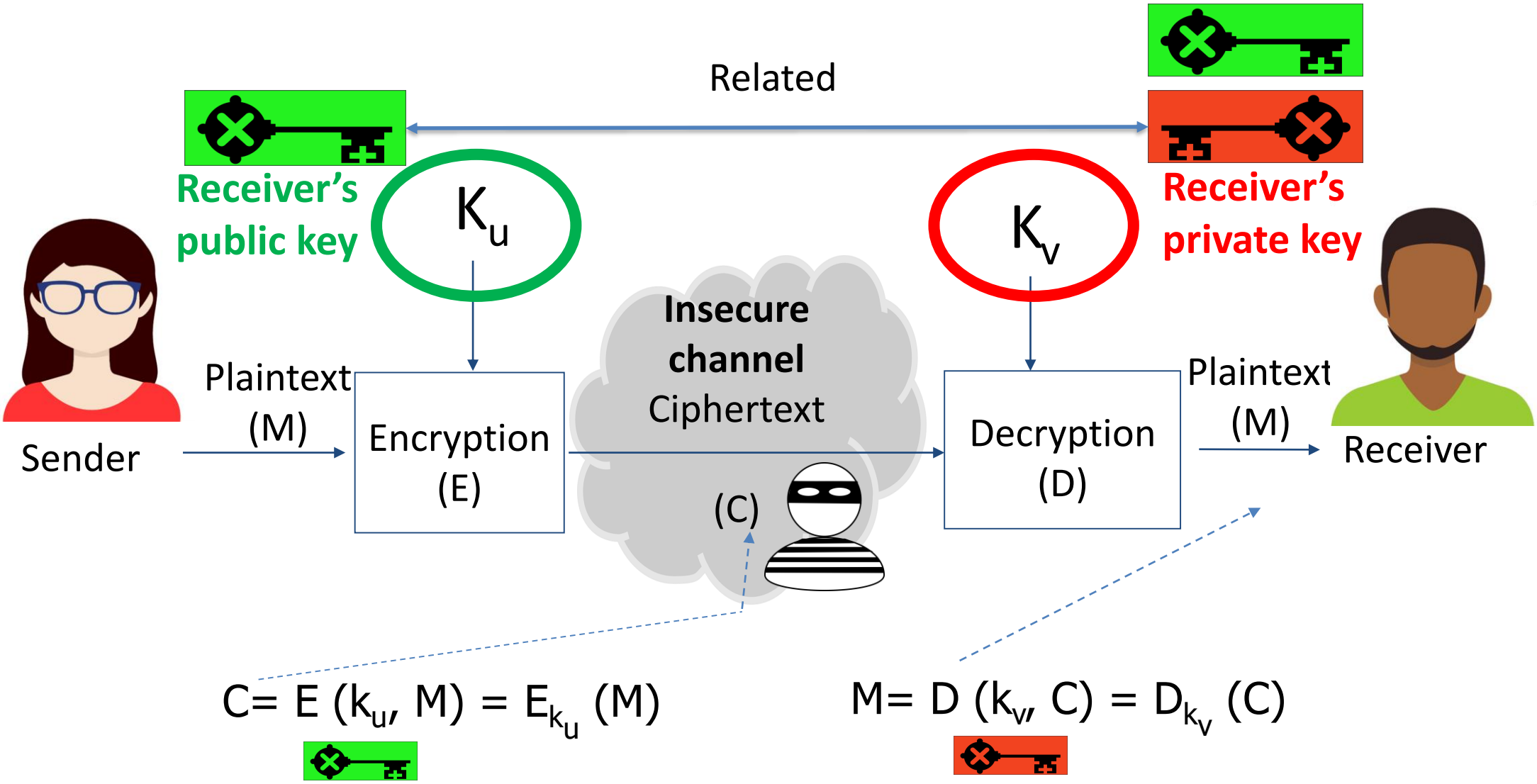
  - **public key**
    - Known by everybody
    - The sender of a message uses the receiver's public key to encrypt the message for him/her
  - **related private key**
    - Known by the owner (only)
    - The receiver of an encrypted message uses his/her private key to decrypt ciphertexts sent to him/her



Unfeasible to determine the private key from the public one

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

Asymmetric encryption model



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

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**

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

OUTLINE

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

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

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

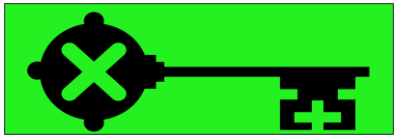
- R. L. Rivest, A. Shamir, L. Adleman. ***A Method for Obtaining Digital Signature and Public-Key Cryptosystems***. Communications of the ACM, v. 21, nº 2, pp 120-126. February 1978.
  - **Abstract** An encryption method is presented with the novel property that publicly revealing an encryption key does 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 $e \cdot d \equiv 1 \pmod{(p-1)\cdot(q-1)}$. 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

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

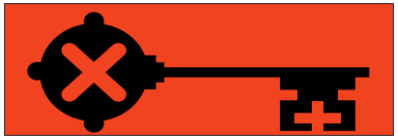
RSA (cipher)

- **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: $k_{U,B} = (e_B, n_B)$



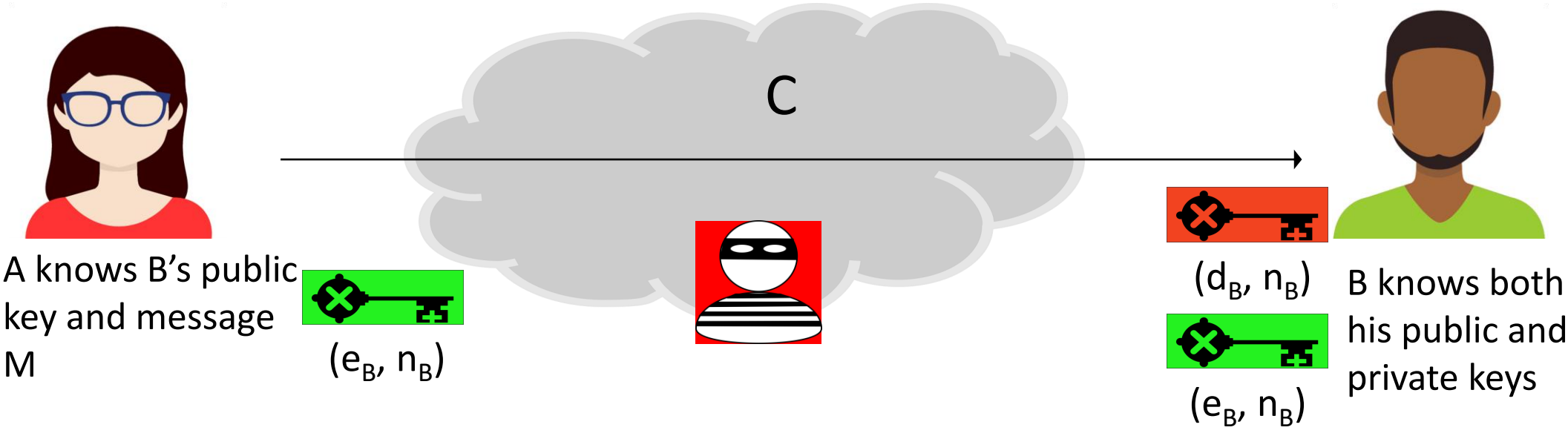
- B's private key: $k_{V,B} = (d_B, n_B)$



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

RSA (cipher)

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



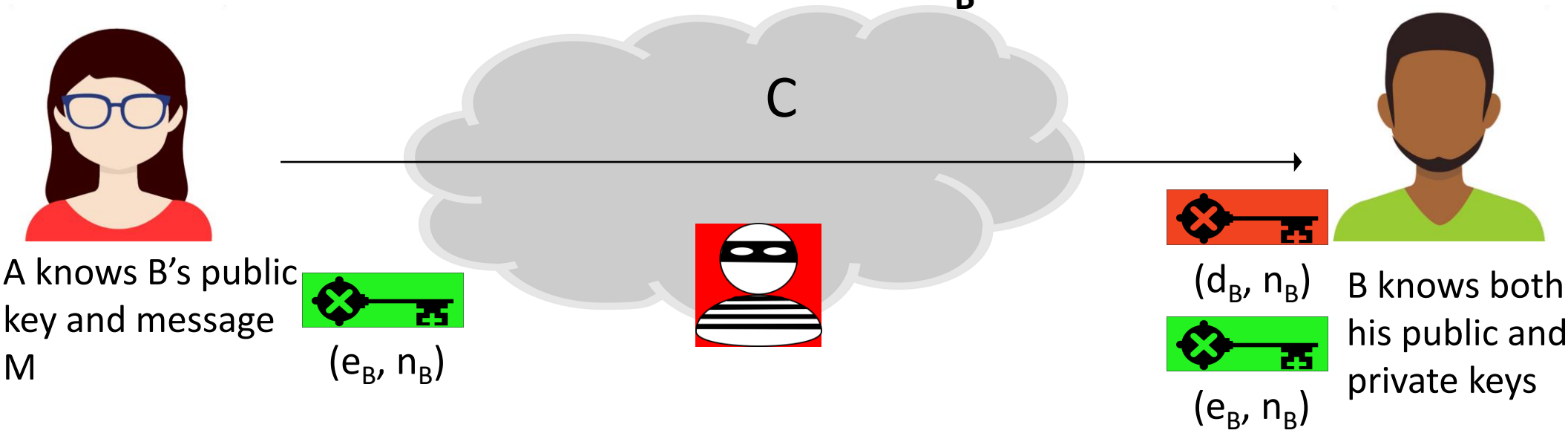
A encrypts M using (e_B, n_B), B's public key, and sends ciphertext to B

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

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

RSA (cifrado)

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



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

$$M = C^{d_B} \bmod n_B$$

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

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

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

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/

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

OUTLINE

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

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

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

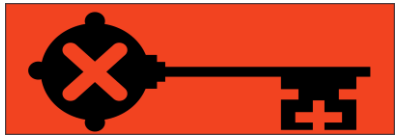
Ana I. González-Tablas Ferreres, José M. de Fuentes García-Romero de Tejada, Lorena González Manzano, Pablo Martín González, Sergio Pastrana Portillo

El Gamal (cipher)

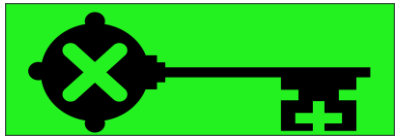
- **B's key pair generation**
  - B chooses p_B, very large prime
  - B chooses g_B, generator of cyclic group G of order p_B
  - B selects x_B as B's private such that

    $1 < x_B < p_B - 1$
  - B computes y_B , s B's public key ($y_B = g^{x_B} \mod p_B$)

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



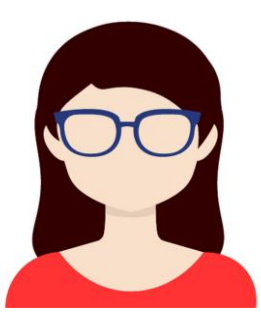
- B's public key: $k_{U,B} = (p_B, g_B, y_B)$



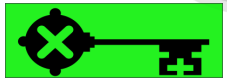
Ana I. González-Tablas Ferreres, José M. de Fuentes García-Romero de Tejada, Lorena González Manzano, Pablo Martín González, Sergio Pastrana Portillo

El Gamal (cipher)

- **A sends message M∈G(p_B) encrypted to B** (part 1)

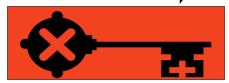


A knows B's public key and message M

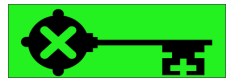


(p_B, g_B, y_B)

C_1, C_2



(x_B)



(p_B, g_B, y_B)

B knows both his public and private keys

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

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

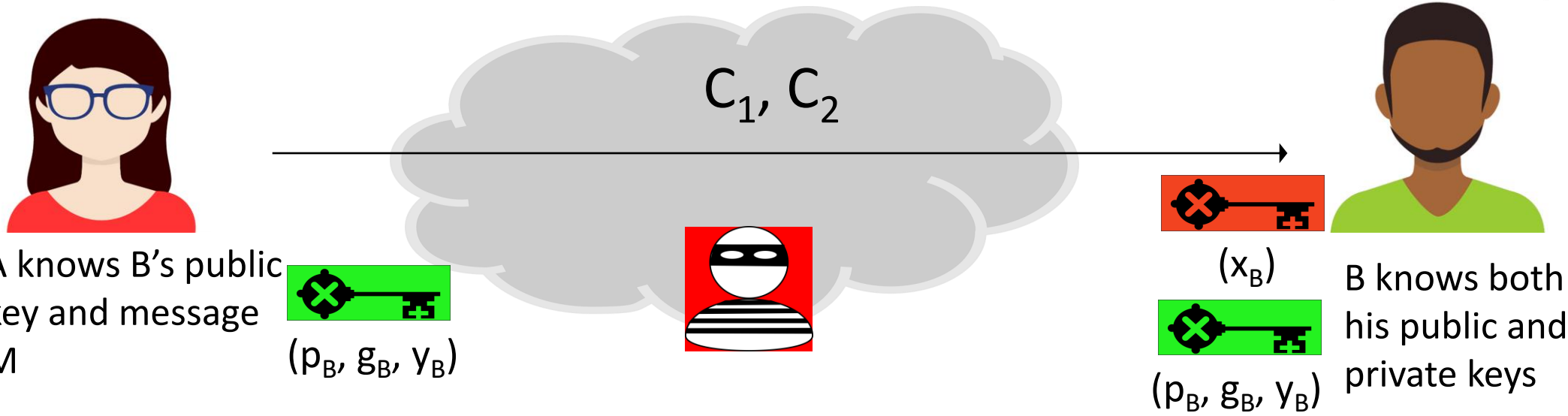
A computes ephemeral key using B's public key: $K_T = y_B^{k_e} \bmod p_B$

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

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

El Gamal (cipher)

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



A sends to B C = C_1, C_2

$$C_1 = g_B^{k_e} \bmod p_B \,,\; C_2 = K_T \cdot M \bmod p_B$$

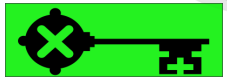
If $C_2 = K_T \cdot M \bmod p_B$, M and $K_T \in G(p_B) \rightarrow M = C_2 \cdot K_T^{-1} \bmod p_B$

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

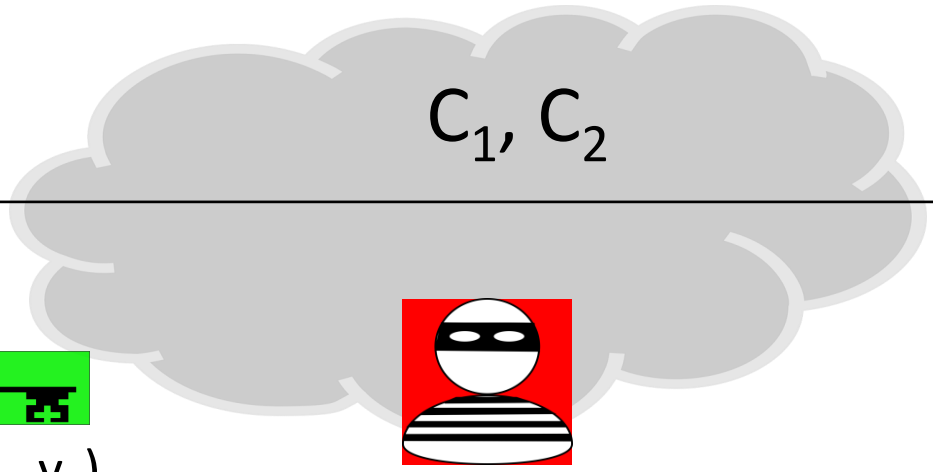
El Gamal (cipher)

- **A sends message M∈G(p_B) encrypted to B** (part 3)

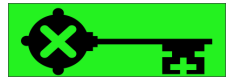
A knows B's public key and message M



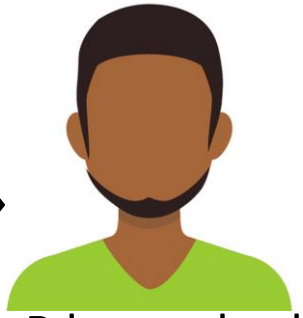
(p_B, g_B, y_B)



(x_B)



(p_B, g_B, y_B)



B knows both his public and private keys

B first recovers ephemeral key and then decrypts C:

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

As for Fermat's Theorem

$M = C_2 \cdot K_T^{-1} \bmod p_B = C_2 \cdot C_1^{-x_B} \bmod p_B = C_2 \cdot C_1^{p_B - 1 - x_B} \bmod p_B$

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

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 $x \mid g^x = y \bmod p$
  - Computing $x = \log_g y \bmod p$ 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)

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

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)

$$K_T' = H(K_T)$$

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

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

OUTLINE

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

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

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

$$M \rightarrow \quad C = M^e \bmod n$$

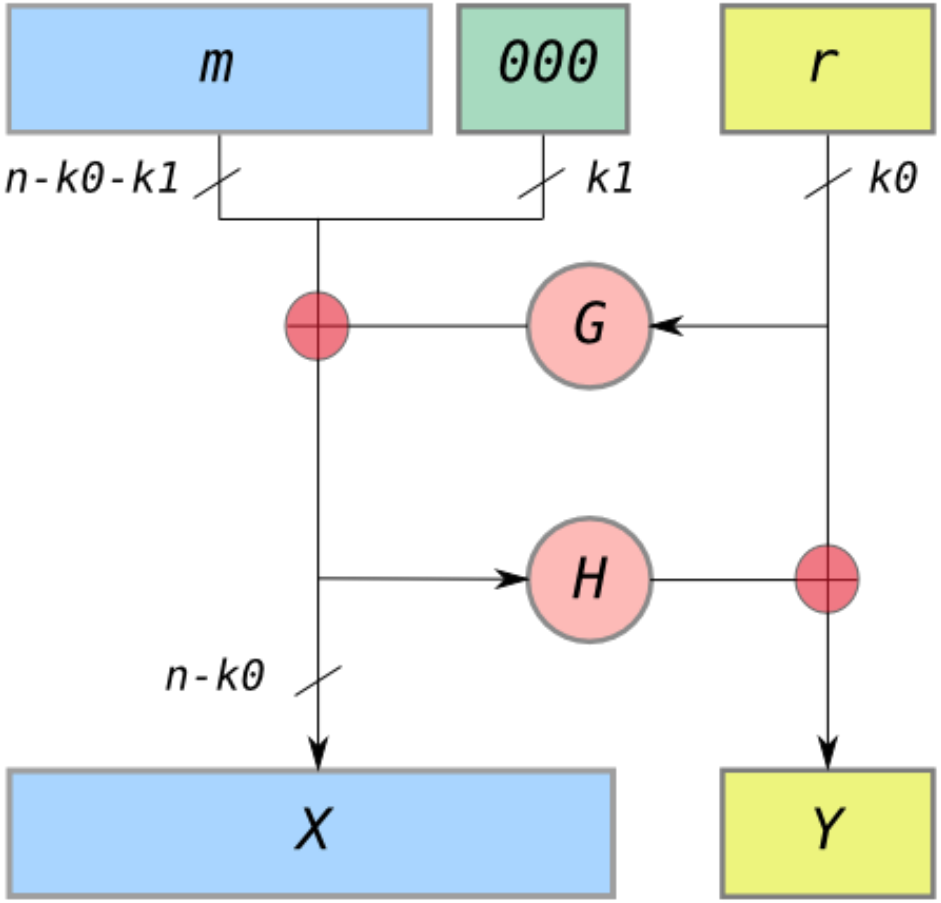
$$C' = C \cdot \alpha^e \bmod n \quad \rightarrow M' = \alpha \cdot M$$

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

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:

$$C = (X \,||\, Y)^e \bmod n$$



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

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 → $C_1 = g_B^{k_e} \bmod p_B$, $C_2 = (y_B^{k_e}) \cdot M \bmod p_B$

$C_1' = C_1$, $C_2' = \alpha \cdot C_2 = (y_B^{k_e}) \cdot (\alpha \cdot M) \bmod p_B$ → $M' = \alpha \cdot M$

- 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*)

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

CRYPTOGRAPHY AND COMPUTER SECURITY COURSE

COSEC

uc3m | Universidad Carlos III de Madrid