Message Authentication Codes

CRYPTOGRAPHY AND COMPUTER SECURITY

Ana I. González-Tablas Ferreres

José María de Fuentes García-Romero de Tejada

Lorena González Manzano

Sergio Pastrana Portillo

uc3m | Universidad Carlos III de Madrid

COSEC

ÍNDICE

- 10. Message Authentication Codes (MAC)
  - Overview
  - Security requirements
  - MAC based on hash functions
  - MAC based on block ciphers
  - Authenticated encryption

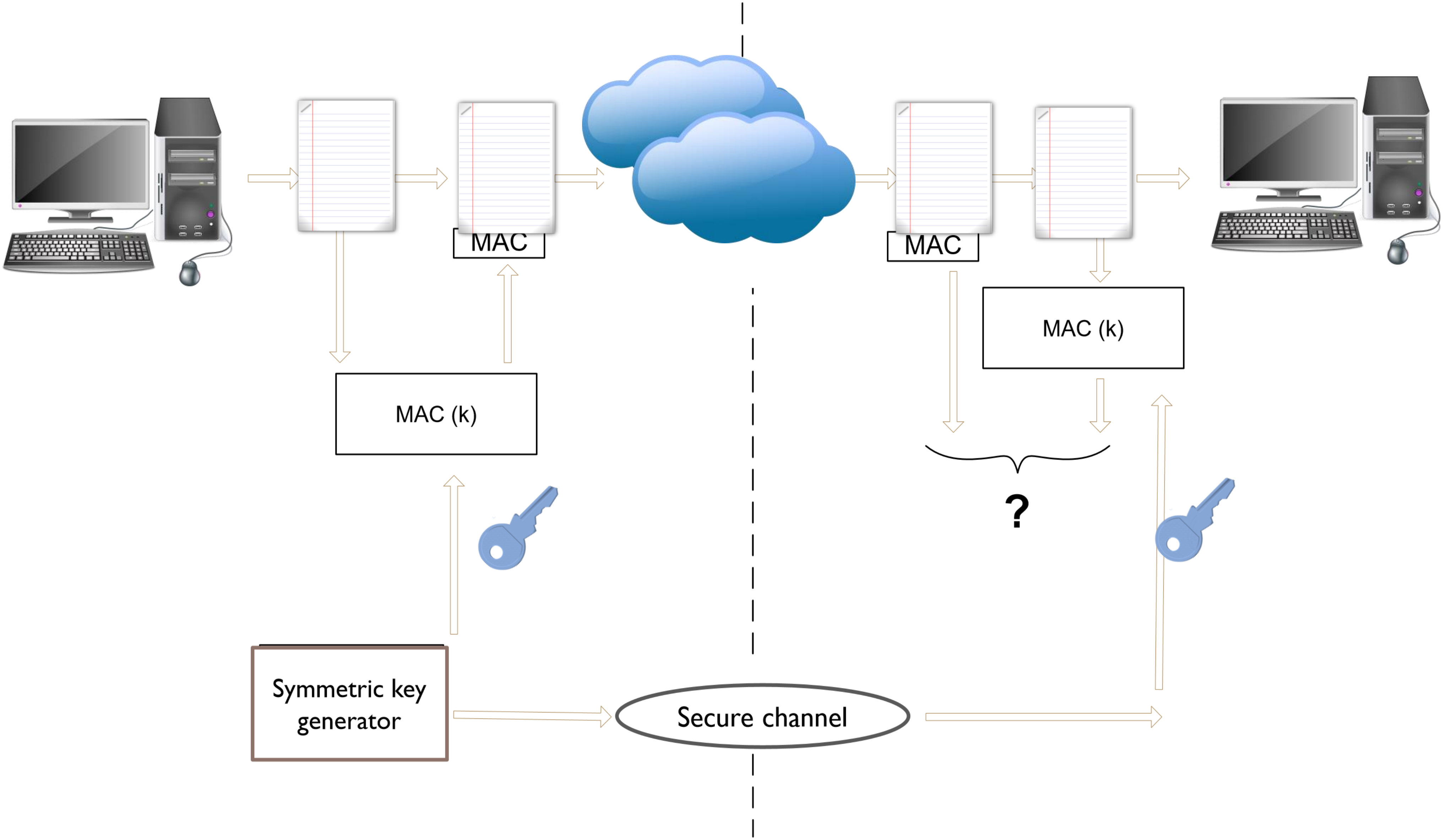
ÍNDICE

- 10. Message Authentication Codes (MAC)
  - Overview
  - Security requirements
  - MAC based on hash functions
  - MAC based on block ciphers
  - Authenticated encryption

OVERVIEW

- A message Authentication Code (MAC) is a secret key algorithm that computes a fixed length value (authentication code) from a variable length message
- Any entity having the secret key is able to **verify the message integrity**
- A receiver sharing the secret key can **authenticate the message origin**
- Replay attacks can be avoided by including sequence numbers into the messages

OVERVIEW



OVERVIEW

- A MAC function needs not to be reversible

- Similarly as hash functions,collisions can be produced

$|k| = 2^k$

$|MAC| = 2^n$

$|M|$ = any

ÍNDICE

- 10. Message Authentication Codes (MAC)
  - Overview
  - Security requirements
  - MAC based on hash functions
  - MAC based on block ciphers
  - Authenticated encryption

SECURITY REQUIREMENTS

- Given M and its MAC(K, M) value, it is computationally unfeasible to find a message M’ with the same MAC

$$\text{MAC}(K,M') = \text{MAC}\ (K,M)$$

- MAC(K,M) must be uniformly distributed; thus the probability of finding 2 messages M and M’ with the same MAC value is:

- Let M’ be the output message of a transformation to M [M’ = f(M)]. In this case, it must be satisfied the following:

$$\Pr[\text{MAC}(K, M) = \text{MAC}(K, M')] = \frac{1}{2^n}$$

SECURITY REQUIREMENTS

- MAC functions attacks
  - Given a set Mi, MAC(K,Mi), the attacker wishes to generate M', MAC(K,M'),with M'≠Mi ∀ i=0…n
  - Brute force

    Key space attack $(\frac{1}{2^k})$ versus MAC value attack $(\frac{1}{2^n})$

    Computational complexity is *Min* $(\frac{1}{2^k}, \frac{1}{2^n})$
  - Cryptanalysis

    Requires the existence of vulnerabilities in the algorithm design or implementation (it will depend on internal structure)

ÍNDICE

- 10. Message Authentication Codes (MAC)
  - Overview
  - Security requirements
  - MAC based on hash functions
  - MAC based on block ciphers
  - Authenticated encryption

MAC BASED ON HASH FUNCTIONS

- HMAC (Hash-MAC)
- Use known hash functions
- Hash function upon a message with some bits appended (obtained from the key)

$$\mathbf{HMAC(K, M) = H[(K' \oplus opad) \,||\, H[(K' \oplus ipad) \,||\, M]]}$$

K': K *padded* with 0's on the left until reaching a length b

b: Processed block length in bits

ipad: 00110110 (0x36) repeated b/8 times

opad:01011100 (0x5C) repeated b/8 times

||: concatenation operator

ÍNDICE

- 10. Message Authentication Codes (MAC)
  - Overview
  - Security requirements
  - MAC based on hash functions
  - MAC based on block ciphers
  - Authenticated encryption

MAC BASED ON BLOCK CIPHERS

- Symmetric block encryption of the message, using CBC mode
- The MAC value is the result of the last encrypted block
- The MAC value depends on every bit of the message

ÍNDICE

- 10. Message Authentication Codes (MAC)
  - Overview
  - Security requirements
  - MAC based on hash functions
  - MAC based on block ciphers
  - Authenticated encryption

AUTHENTICATED ENCRYPTION

- Provide confidentiality, integrity and authenticity of communications
- In other words: privacy and authenticity is provided

- Symmetric encryption and MAC are used
  - MAC provides integrity and authentication
  - Encryption provides confidentiality

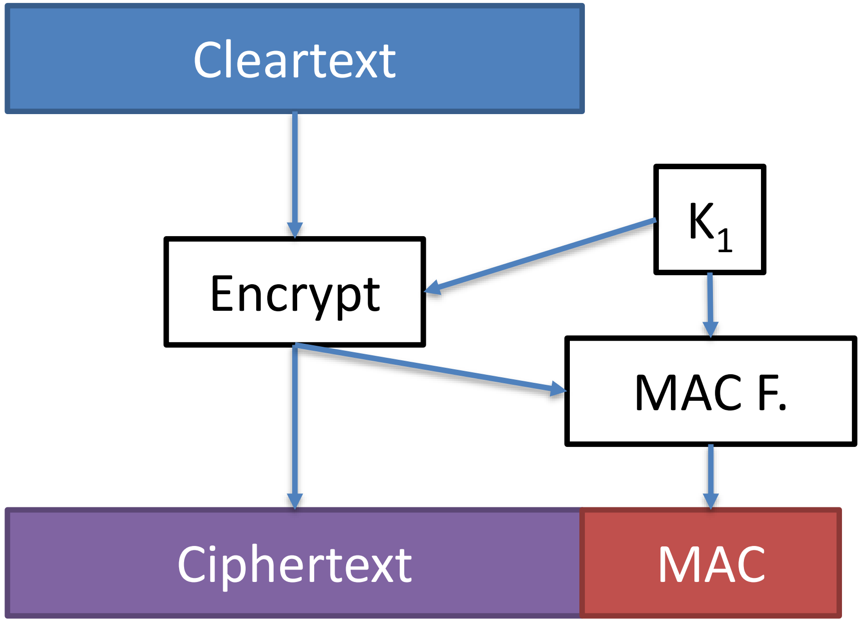
AUTHENTICATED ENCRYPTION

- TYPES
  - Encrypt-then-MAC
  - Encrypt-and-MAC
  - MAC-then-Encrypt

  - For simplicity, in the following a single key is used from encryption adn MAC but…
    - The use of different keys (for encryption and MAC) is a solid way to construct an authenticated encryption scheme

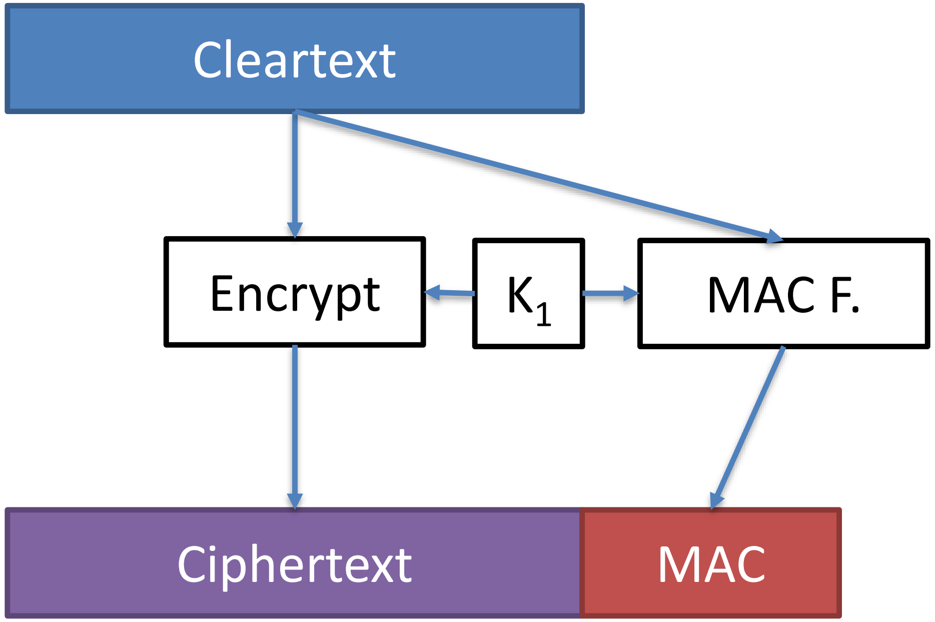
AUTHENTICATED ENCRYPTION

- Types
  - Encrypt-then-MAC
    - High security when using an appropriate MAC function



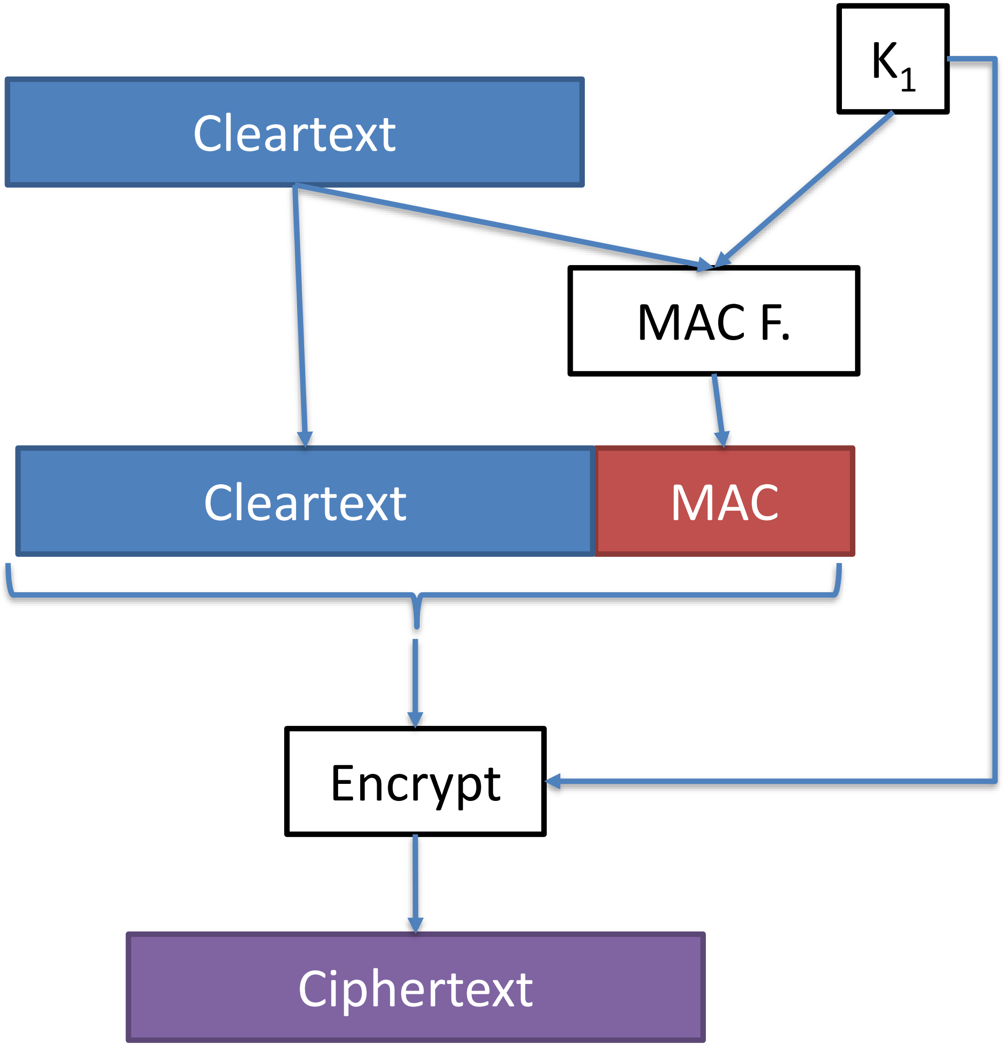
AUTHENTICATED ENCRYPTION

- Types
  - Encrypt-and-MAC
    - Possible problem:
      - The same text-> the same MAC



AUTHENTICATED ENCRYPTION

- Types
  - *M*AC-then-Encrypt
    - Decryption should be carried out after verifying integrity and authenticity



CRYPTOGRAPHY AND COMPUTER SECURITY

COSEC

uc3m | Universidad Carlos III de Madrid