Introduction to cryptosystems

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

OUTLINE

- 2. Introduction to cryptosystems
  - Cryptography
    - Definition
    - Cryptosystem model
    - Characteristics of cryptosystems
    - Codes vs Ciphers
  - Cryptanalysis

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

OUTLINE

- 2. Introduction to cryptosystems
  - Cryptography
    - Definition
    - Cryptosystem model
    - Characteristics of cryptosystems
    - Codes vs Ciphers
  - Cryptanalysis

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

Definition

– Classic definition (2000 b.c. – 1949)

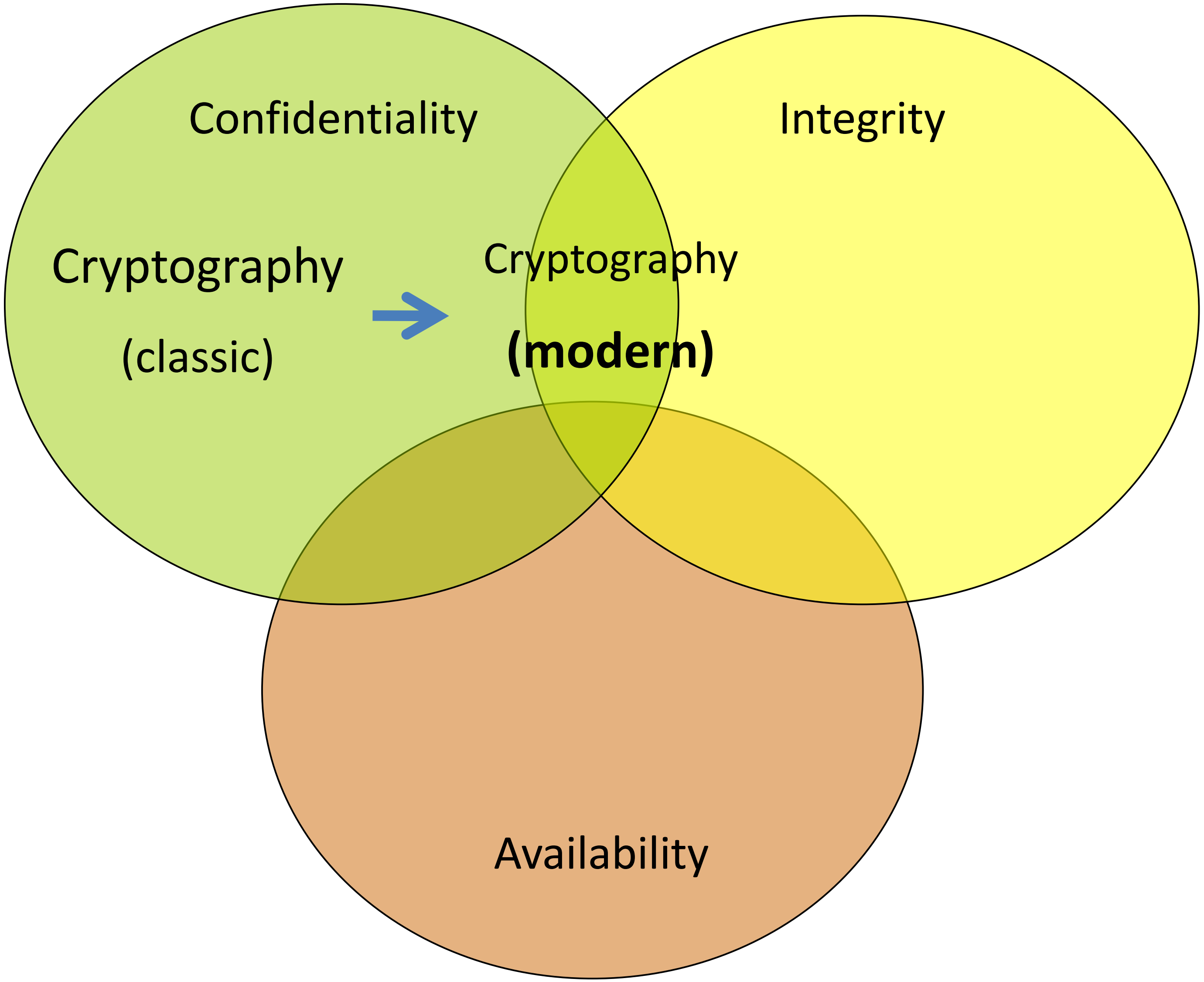
The discipline which embodies principles, means and methods for the **transformation of data** in order to **hide** its information **content**

– Modern definition (desde 1976)

The discipline which embodies principles, means and methods for the **transformation of data** in order to **hide** its information **content**, establish its **authenticity** and **prevent** it from **unauthorised modification** and **repudiation**

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

Definition



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

OUTLINE

- 2. Introduction to cryptosystems
  - Cryptography
    - Definition
    - Cryptosystem model
    - Characteristics of cryptosystems
    - Codes vs Ciphers
  - Cryptanalysis

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

Cryptosystem model

- Message space

  $M = \{m_1, m_2, \ldots\}$

- Ciphertext space

  $C = \{c_1, c_2, \ldots\}$

- Key space

  $K = \{k_1, k_2, \ldots\}$

- Set of encryption functions

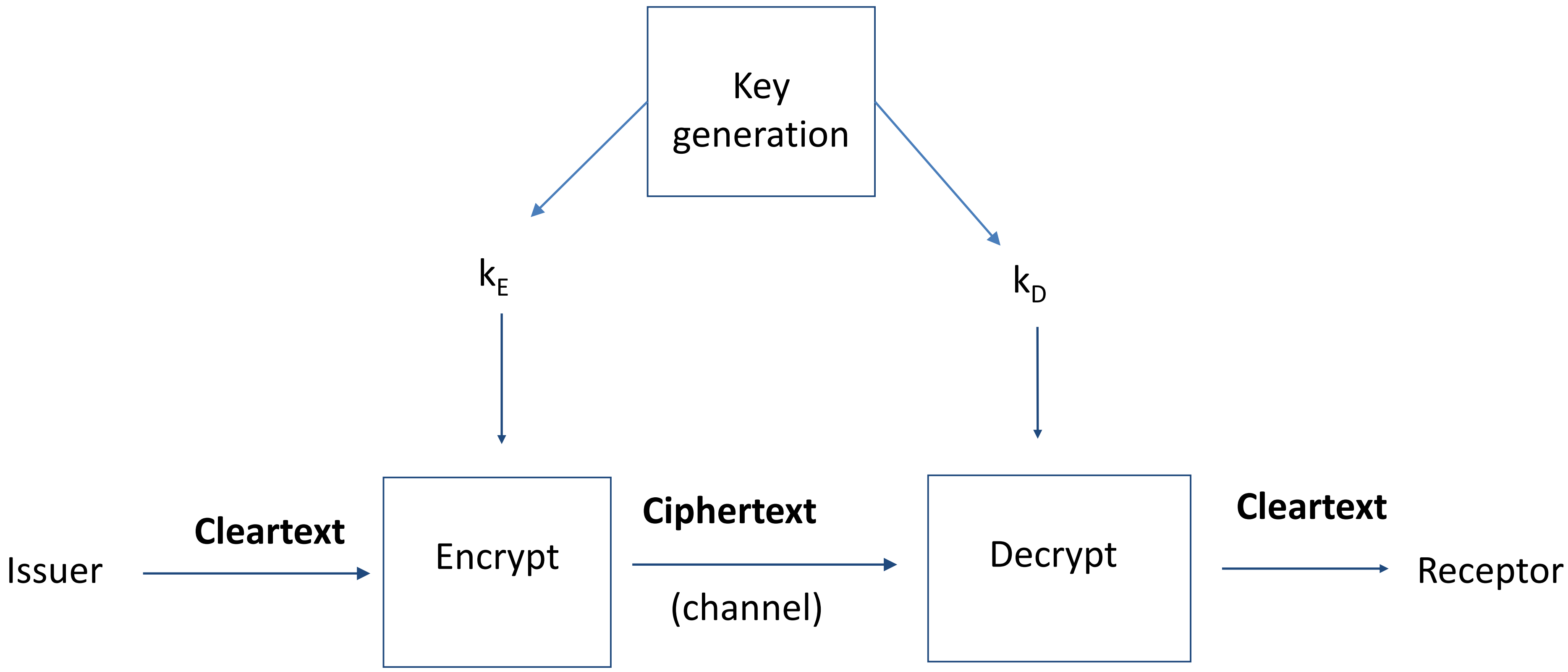
  $E_k : M \rightarrow C$

- Set of encryption functions

  $D_k : C \rightarrow M$

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

Cryptosystem model



k_E and k_D can be equal or not

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

OUTLINE

- 2. Introduction to cryptosystems
  - Cryptography
    - Definition
    - Cryptosystem model
    - Characteristics of cryptosystems
    - Codes vs Ciphers
  - Cryptanalysis

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

Characteristics of cryptosystems

- Type of operations used for transforming PT to CT
  - Generally, substitutions and transpositions without information loss. Combinations using product operations are common.
- Number of keys used
  - Symmetric or with one key (also known as secret key algorithms)
  - Asymmetric or with two keys (also known as public key algorithms)
- Way of processing PT
  - Block of elements at a time (block cipher algorithms)
  - Stream of byte or bit elements (stream cipher algorithms)

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

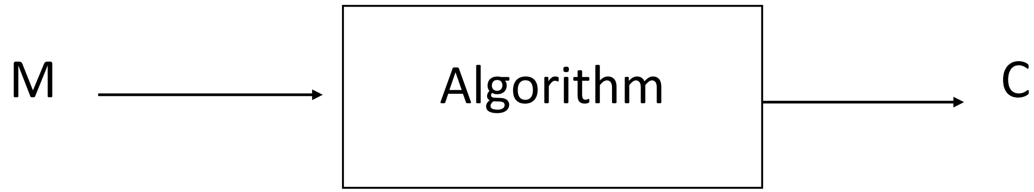
OUTLINE

- 2. Introduction to cryptosystems
  - Cryptography
    - Definition
    - Cryptosystem model
    - Characteristics of cryptosystems
    - Codes vs Ciphers
  - Cryptanalysis

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

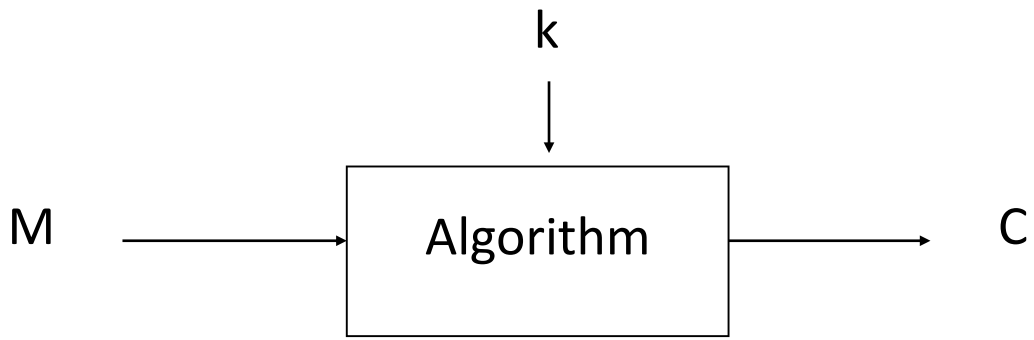
Coders vs Ciphers

– Coder



$C=f(M)$

– Cipher



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

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

OUTLINE

- 2. Introduction to cryptosystems
  - – Cryptography
    - Definition
    - Cryptosystem model
    - Characteristics of cryptosystems
    - Codes vs Ciphers
  - – Cryptanalysis

COSEC uc3m

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

Cryptanalysis

- Methods for obtaining the meaning of encrypted information, without access to the secret information
- Kerckoffs's principle:

A cryptosystem should be secure even if everything about the system, except the key, is public knowledge

La cryptographie militaire, 1883.
Auguste Kerckhoffs von Nieuwenhof (1835-1903)

- No to 'security through obscurity'.

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

Cryptanalysis

- Goal of the cryptanalysist:
  - Main: Recover decryption key
  - Secondary: Decrypt a cypher text

- Approaches of the cryptoanalyst / atacker:

Attacks to the algorithm

Brute force attacks

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

Cryptanalysis

- Attacks to the algorithms

Ataque	Conocido por el atacante (además de algoritmo)	Dificultad
Ciphertext-only (worst case)	The cryptanalist has access only to a collection of ciphertexts	+
Known-plaintext	The attacker has a set of ciphertexts for which he/she knows the corresponding plaintext	
Chosen-plaintext	The attacker can obtain the ciphertexts corresponding to an arbitrary set of plaintexts of his/her own choice	
Chosen-ciphertext	The attacker can obtain the plaintexts corresponding to an arbitrary set of ciphertexts of his/her own choice	-

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

Cryptanalysis

- Unconditionally secure encryption algorithm
  - No additional information is leaked besides that already known by the attacker, independently of the CT length
  - Only Vernam cipher is unconditionally secure

- Encryption algorithm vulnerable to mathematical attacks
  - Additional information is leaked when CT length increases
  - Except Vernam, other encryption algorithms are vulnerable to mathematical attacks

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

Cryptanalysis

Vernam cipher. One-time-pad

- Encryption: $E(M) = M \oplus K = m_1 \oplus k_1, m_2 \oplus k_2, \ldots, m_n \oplus k_n$

```
   1 0 0 1 1 1 0 1   M
⊕  0 0 1 0 0 1 0 1   K
   ---------------
   1 0 1 1 1 0 0 0   C
```

- Decryption: $M = E(M) \oplus K$

- Shannon proved that Vernam cipher is unconditionally secure when the followings conditions on the key K are met:
  - Truly random
  - It is used only once
  - Its length is equal or greater than that of M

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

Cryptanalysis

- Unconditionally secure ciphers, like Vernam, ARE NOT PRACTICAL
- **Computational security** (or“Not vulnerable in a practical way”):
  - Cryptanalysis of the system requires at least t operations
    - Time of cryptanalysis exceeds the useful lifetime of the information
    - Cost of cryptanalysis exceeds the value of encrypted information
- In the case of symmetric ciphers:
  - There is no algorithm that can break the cipher with less complexity of a brute-force attack

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

Cryptanalysis

- Brute-force attack
  - Trying every possible key
  - On average, half of the keys must be tried

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

Cryptanalysis

- Average time required for exhaustive key search

Sensible assumption

Parallel processing assumption

Key length (bits)	Number of posible keys	Time required at 1 decryption/µs	Time required at 10^6 decryptions/µs
32	$2^{32} = 4{,}3 \cdot 10^9$	2^{31}µs = 35,8 min	2,15 ms
56	$2^{56} = 7{,}2 \cdot 10^{16}$	2^{55}µs = 1142 years	10,01 hours
128	$2^{128} = 3{,}4 \cdot 10^{38}$	2^{127}µs = $5{,}4 \cdot 10^{24}$ years	$5{,}4 \cdot 10^{18}$ years
168	$2^{168} = 3{,}7 \cdot 10^{50}$	2^{167}µs = $5{,}9 \cdot 10^{36}$ years	$5{,}9 \cdot 10^{30}$ years
26 characters (permutation)	$26! = 4 \cdot 10^{26}$	$2 \cdot 2^{26}$µs = $6{,}4 \cdot 10^{12}$ years	$6{,}4 \cdot 10^{6}$ years

Fuente: Cryptography and Network Security. Principles and Practice. Stallings

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

CRYPTOGRAPHY AND COMPUTER SECURITY

COSEC

uc3m | Universidad Carlos III de Madrid