Introducción a la criptografía

CURSO CRIPTOGRAFÍA Y SEGURIDAD INFORMÁTICA

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

uc3m | Universidad Carlos III de Madrid

COSEC

ÍNDICE

- 2. Introducción a los criptosistemas
  - Criptografía
    - Definición
    - Modelo de criptosistema
    - Características de los sistemas criptográficos
    - Codificadores vs cifradores
  - Criptoanálisis

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

ÍNDICE

- 2. Introducción a los criptosistemas
  - **Criptografía**
    - **Definición**
    - Modelo de criptosistema
    - Características de los sistemas criptográficos
    - Codificadores vs cifradores
  - Criptoanálisis

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

Definición de criptografía

- Definición clásica (2000 a.c – 1949)

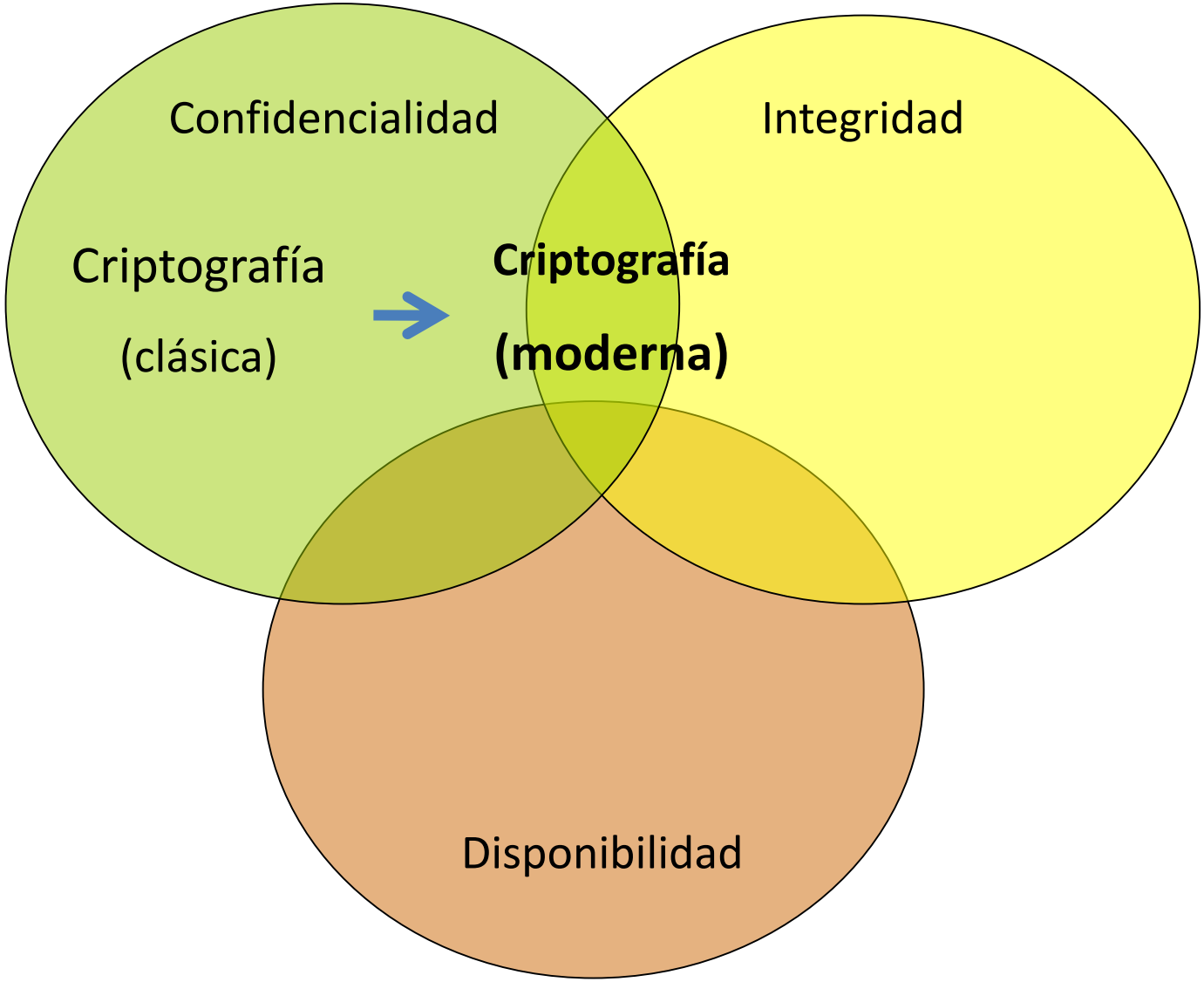
> Disciplina que estudia los principios, métodos y medios de transformar los datos para ocultar su significado

- Definición moderna (desde 1976)

> Disciplina que estudia los principios, métodos y medios de transformar los datos para ocultar su significado, garantizar su integridad, establecer su autenticidad y prevenir su repudio

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

Definición de criptografía



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

ÍNDICE

- 2. Introducción a los criptosistemas
  - **Criptografía**
    - Definición
    - **Modelo de criptosistema**
    - Características de los sistemas criptográficos
    - Codificadores vs cifradores
  - Criptoanálisis

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

Modelo de criptosistema

- Espacio de mensajes

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

- Espacio de cifrados

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

- Espacio de claves

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

- Familia de transformaciones de cifrado

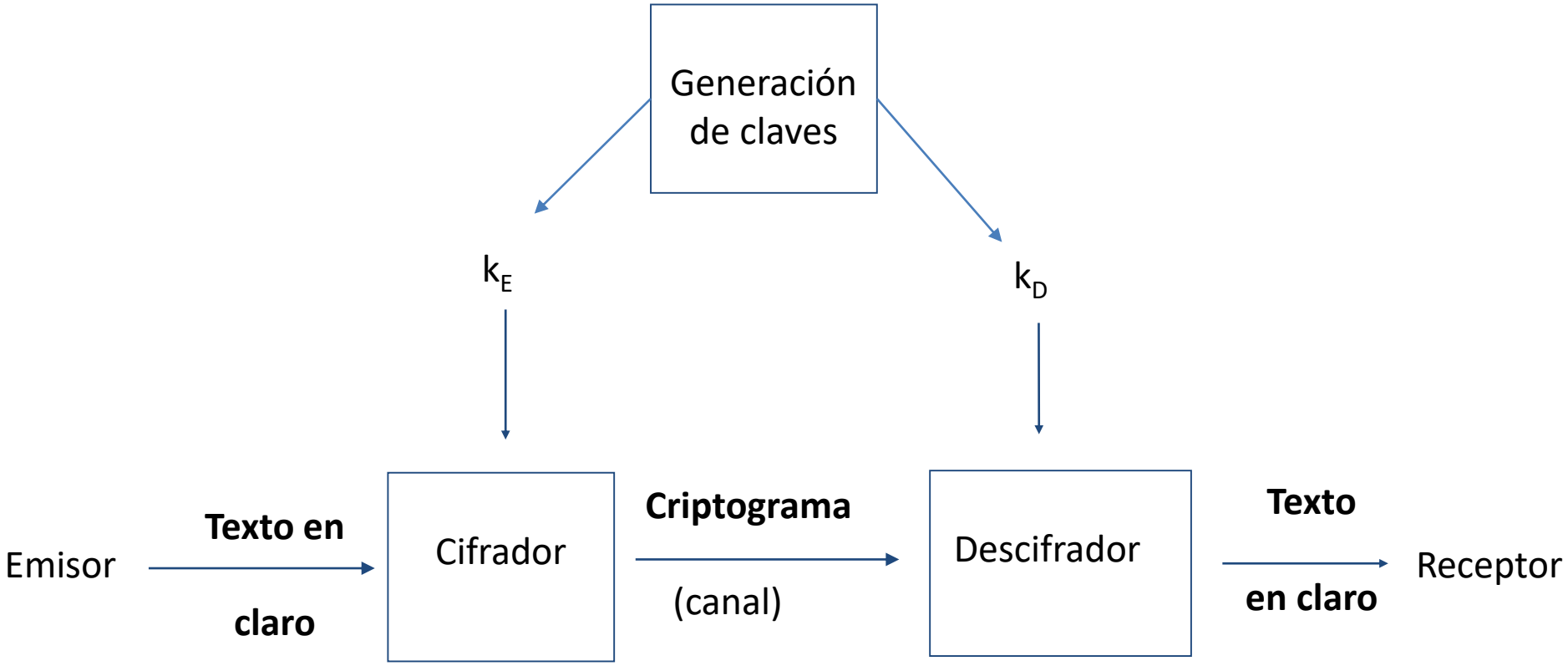
  $E_k : M \rightarrow C$

- Familia de transformaciones de descifrado

  $D_k : C \rightarrow M$

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

Modelo de criptosistema



k_E y k_D pueden o no ser iguales

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

ÍNDICE

- 2. Introducción a los criptosistemas
  - **Criptografía**
    - Definición
    - Modelo de criptosistema
    - **Características de los sistemas criptográficos**
    - Codificadores vs cifradores
  - Criptoanálisis

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

Características de los sistemas criptográficos

- Se caracterizan con tres dimensiones independientes:
  - Tipo de operaciones realizadas
    - En general, sustituciones y transposiciones. No puede perderse información. Los más comunes usan el producto de varias operaciones
  - Número de claves usadas
    - Simétricos o con una clave (también conocido como algoritmos de clave secreta)
    - Asimétricos o con dos claves (también conocido como algoritmos de clave pública)
  - Tipo de procesamiento del texto en claro
    - Por bloques (algoritmos de cifrado en bloque)
    - Como un flujo continuo de bytes o de bits (algoritmos de cifrado en flujo)

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

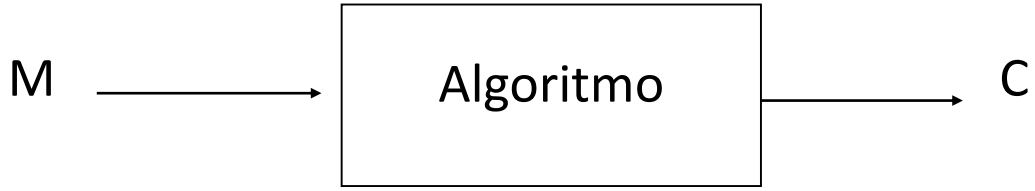
ÍNDICE

- 2. Introducción a los criptosistemas
  - **Criptografía**
    - Definición
    - Modelo de criptosistema
    - Características de los sistemas criptográficos
    - **Codificadores vs cifradores**
  - Criptoanálisis

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

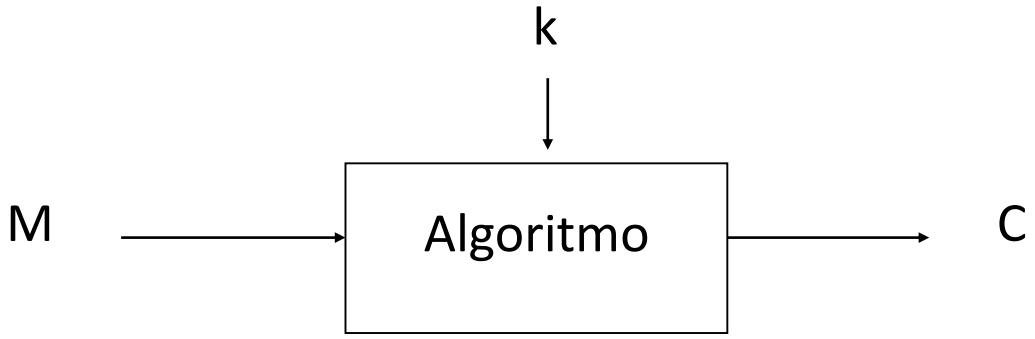
Codificadores vs Cifradores

- Codificador



C=f(M)

- Cifrador



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

ÍNDICE

- 2. Introducción a los criptosistemas
  - Criptografía
    - Definición
    - Modelo de criptosistema
    - Codificadores vs cifradores
  - **Criptoanálisis**

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

Criptoanálisis

- Ciencia que trata de frustrar las técnicas criptográficas
  - Principio de Kerckhoffs

> La seguridad del cifrado debe residir, exclusivamente, en el secreto de la clave

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

  - No a la seguridad por falta de claridad (u oscuridad)
  - Los ataques se basan en el conocimiento del algoritmo y, quizá, en información adicional sobre el texto en claro

Criptoanálisis

- Objetivo del criptoanalista:
  - Principal: Recuperar la clave de descifrado
  - Secundario: Descifrar un texto cifrado concreto

- Aproximaciones del criptoanalista/atacante:

Ataques al algoritmo

Ataque de fuerza bruta

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

Criptoanálisis

- Ataques al algoritmo

Ataque	Conocido por el atacante (además de algoritmo)	Dificultad
Texto cifrado	Criptograma	
Texto en claro conocido	Criptograma + uno o más pares (texto en claro, texto cifrado) con la misma clave	
Texto en claro escogido	Criptograma + uno o más pares (texto en claro escogido, texto cifrado) con la misma clave	
Texto cifrado escogido	Criptograma + uno o más criptogramas escogidos por el atacante junto con sus correspondientes textos en claro, con la misma clave	
Texto escogido	Criptograma + uno o más pares (texto en claro escogido, texto cifrado) con la misma clave + uno o más criptogramas escogidos por el atacante junto con sus correspondientes textos en claro, con la misma clave	

Criptoanálisis

- Algoritmo de cifrado incondicionalmente seguro
  - No se filtra información adicional a la conocida por el atacante independientemente de la longitud del texto cifrado C
  - Solo el cifrador de Vernam es incondicionalmente seguro

- Algoritmo de cifrado matemáticamente vulnerable
  - Si al aumentar la longitud de C se filtra información
  - El resto de algoritmos de cifrado excepto Vernam son matemáticamente vulnerables

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

Criptoanálisis

Cifrado de Vernam. One-time-pad

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

```
  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
```

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

- Shannon demostró que el cifrado de Vernam es incondicionalmente seguro si la clave K:
  - Es realmente aleatoria
  - Se usa una sola vez
  - Es de longitud igual o mayor que M

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

Criptoanálisis

- Los cifradores incondicionalmente seguros, como Vernam, NO SON PRÁCTICOS
- **Seguridad computacional** (o "No es vulnerable en la práctica"):
  - El criptoanálisis del sistema requiere al menos *t* operaciones
    - El tiempo de criptoanalizar el algoritmo excede el tiempo de vida útil de la información
    - El coste de criptoanalizar el algoritmo excede el valor de la información
- Para cifradores simétricos
  - No existe un algoritmo capaz de criptoanalizar el cifrador con una complejidad menor que la de un ataque de fuerza bruta

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

Criptoanálisis

- Ataque de fuerza bruta
  - Probar todas las claves posibles
  - En media, se deben probar la mitad de las posibilidades para tener éxito

Criptoanálisis

- Tiempo medio requerido para realizar una búsqueda exhaustiva de la clave (ataque de fuerza bruta)

Suposición razonable

Supuesto procesamiento masivo paralelo

Tamaño de la clave (bits)	Número de claves posibles	Tiempo requerido supuesto 1 descifrado/μs	Tiempo requerido supuesto 10^6 descifrados/μs
32	$2^{32} = 4{,}3 \cdot 10^9$	2^{31}μs = 35,8 minutos	2,15 milisegundos
56	$2^{56} = 7{,}2 \cdot 10^{16}$	2^{55}μs = 1142 años	10,01 horas
128	$2^{128} = 3{,}4 \cdot 10^{38}$	2^{127}μs = $5{,}4 \cdot 10^{24}$ años	$5{,}4 \cdot 10^{18}$ años
168	$2^{168} = 3{,}7 \cdot 10^{50}$	2^{167}μs = $5{,}9 \cdot 10^{36}$ años	$5{,}9 \cdot 10^{30}$ años
26 caracteres (permutación)	$26! = 4 \cdot 10^{26}$	$2 \cdot 2^{26}$μs = $6{,}4 \cdot 10^{12}$ años	$6{,}4 \cdot 10^6$ años

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, Pablo Martín González

CURSO CRIPTOGRAFÍA Y SEGURIDAD INFORMÁTICA

COSEC

uc3m | Universidad Carlos III de Madrid