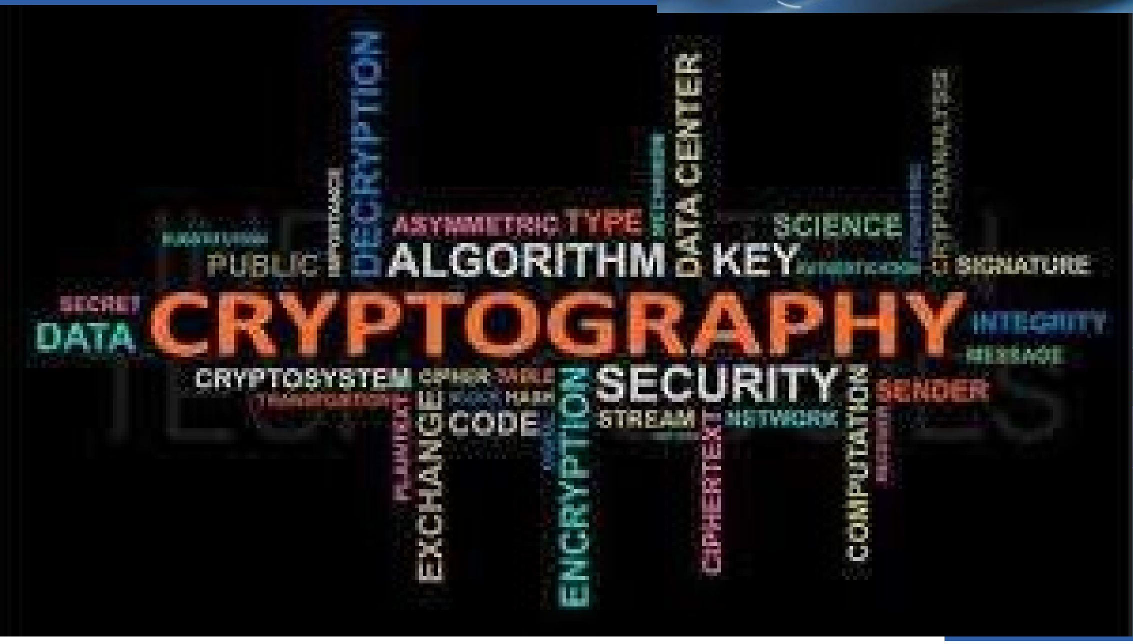
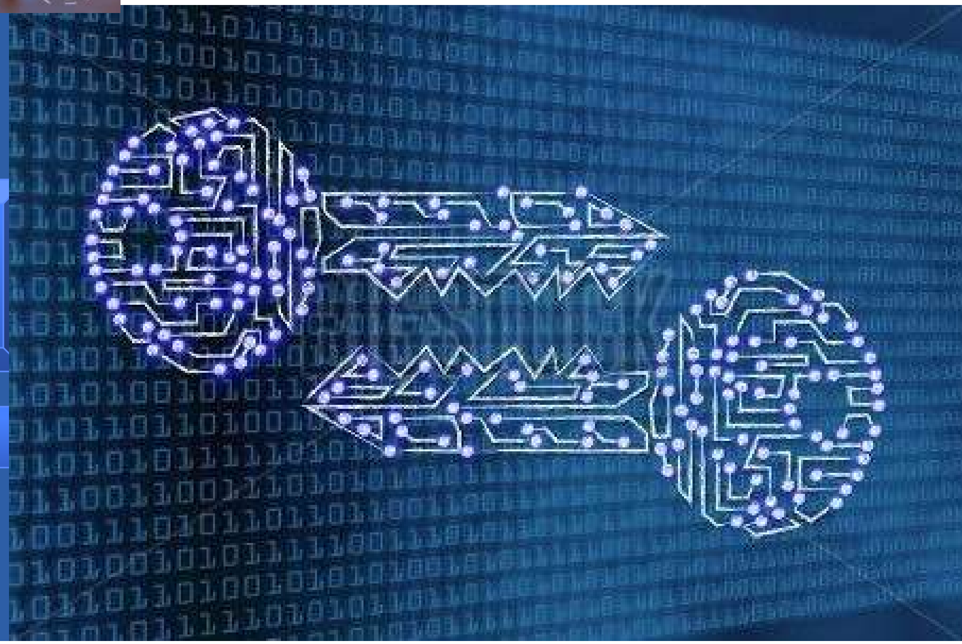
Criptografía

Universidad
Francisco de Vitoria
UFV Madrid

Tema 1
Introducción a la Criptografía

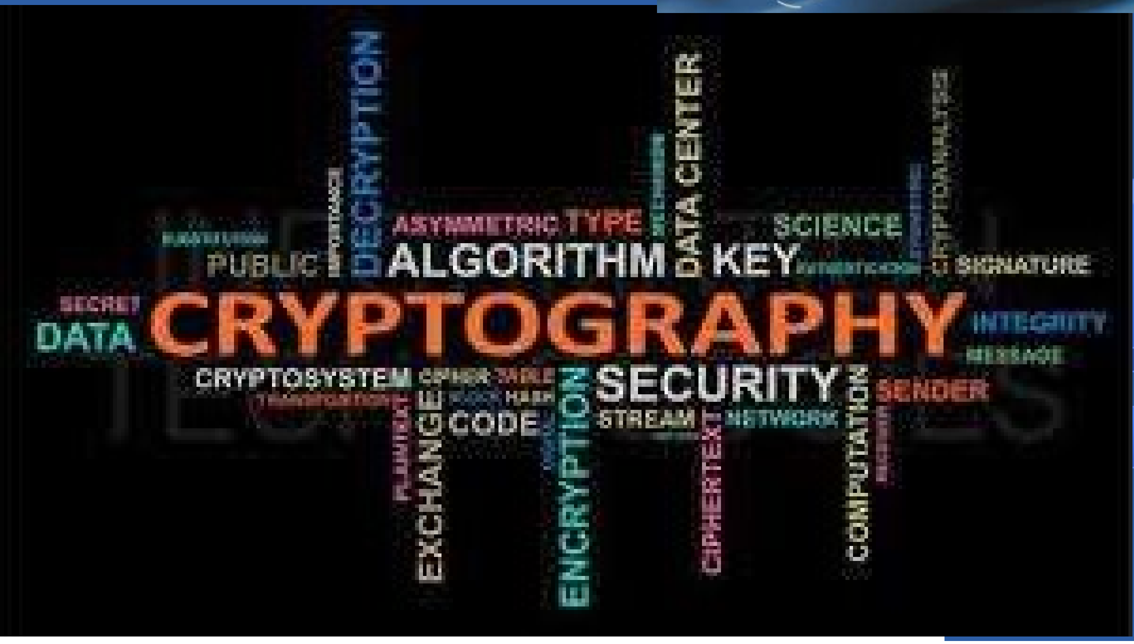


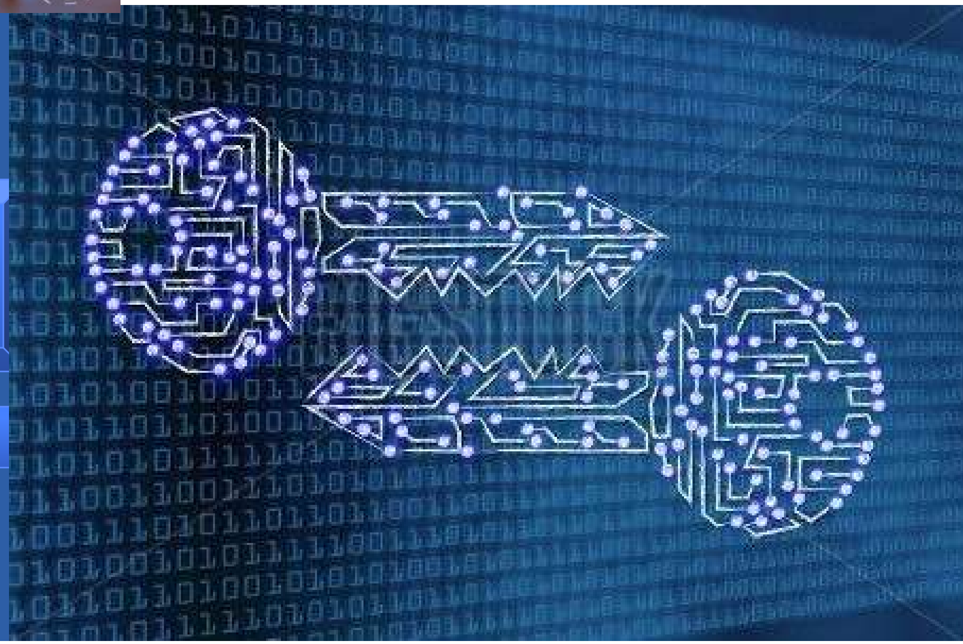


Criptografía

Universidad Francisco de Vitoria UFV Madrid

Tema 1.1 Criptografía y Seguridad Informática





¿Qué es la Criptografía ?

- Puede definirse como

El conjunto de ***conocimientos científicos, métodos y técnicas*** que hacen posible la transformación de los datos para:

- **ocultar su información (confidencialidad),**
- **garantizar su integridad**
- **garantizar su autenticidad**

¿Qué es la Seguridad Informática ?

- Puede definirse como

La capacidad de un sistema para proteger la información y los recursos del propio sistema aplicando ***conocimientos científicos, métodos y técnicas*** que hacen posible la transformación de los datos para:

- **ocultar su información (confidencialidad),**
- **garantizar su integridad**
- **garantizar su disponibilidad**

OBJETIVOS

- **Confidencialidad:** Garantizar que personas no autorizadas no accedan a la información
- **Integridad:** Garantizar que la información no sea alterada por personas no autorizadas de forma que no sea detectable por los usuarios autorizados
- **Disponibilidad:** Garantizar que un sistema es operativo y funcional en un momento dado, generalmente proporcionado a través de la redundancia; la pérdida de disponibilidad se conoce a menudo como "denegación de servicio“
- **Autenticidad**: Garantizar que los usuarios son las personas que dicen ser
- **Responsabilidad**: Propiedad que garantiza que las acciones de una entidad pueden ser rastreadas de forma exclusiva hasta esa entidad.

Mapa de ciberamenazas **en tiempo real**

https://cybermap.kaspersky.com

Seguridad Informática *vs* Criptografía

La Seguridad Informática es mucho más que la Criptografía…

https://www.ccn-cert.cni.es/informes/informes-ccn-cert-publicos/6338-ccn-cert-ia-13-21-ciberamenazas-y-tendencias-edicion-2021-1/file.html

… pero es difícil construir un sistema seguro sin emplear Criptografía.

Objetivos de Seguridad de la Información

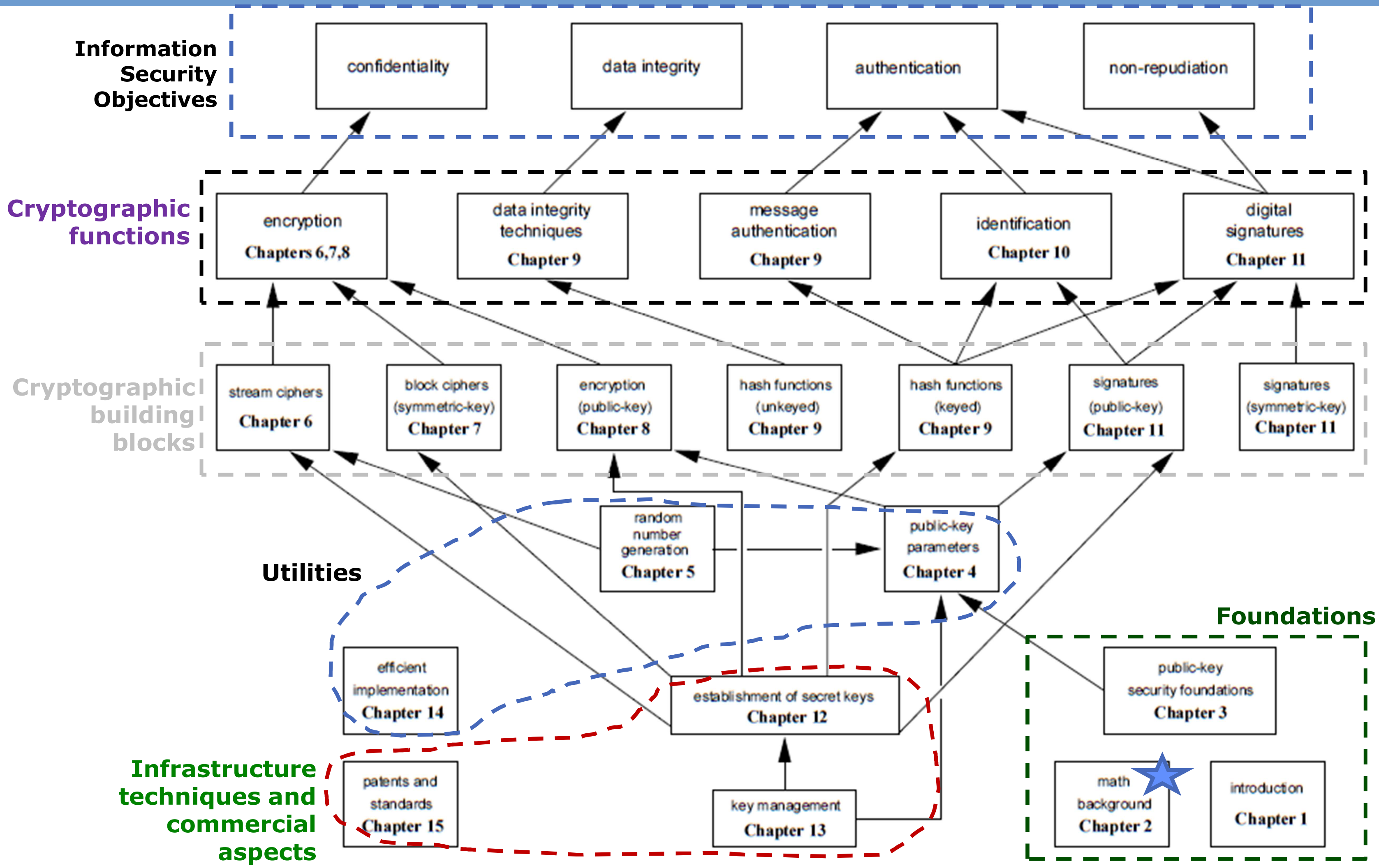
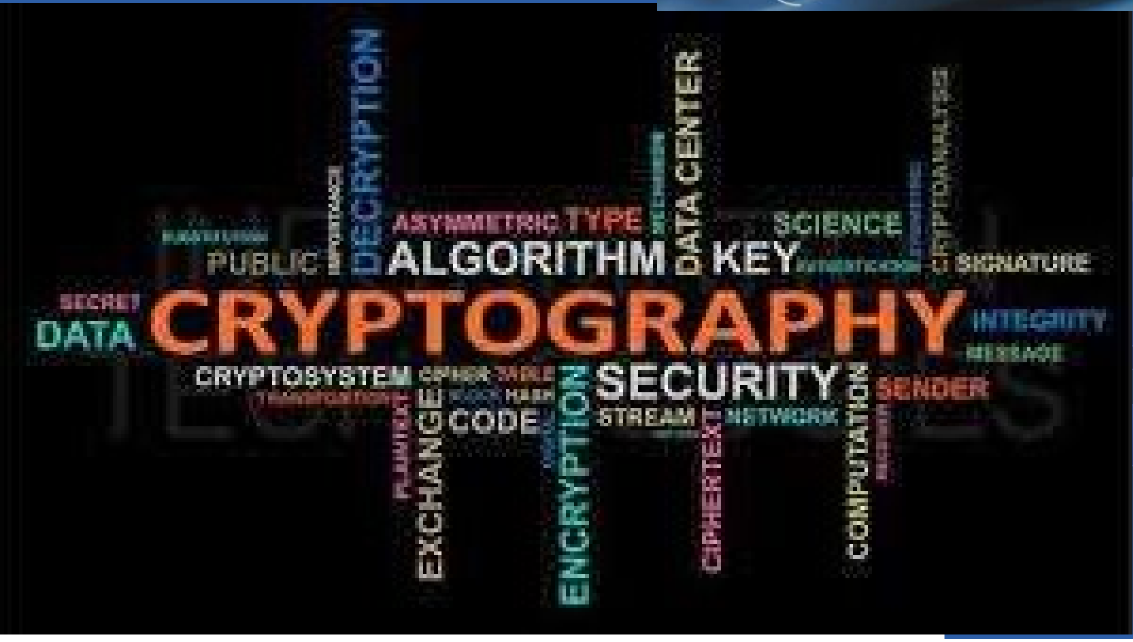


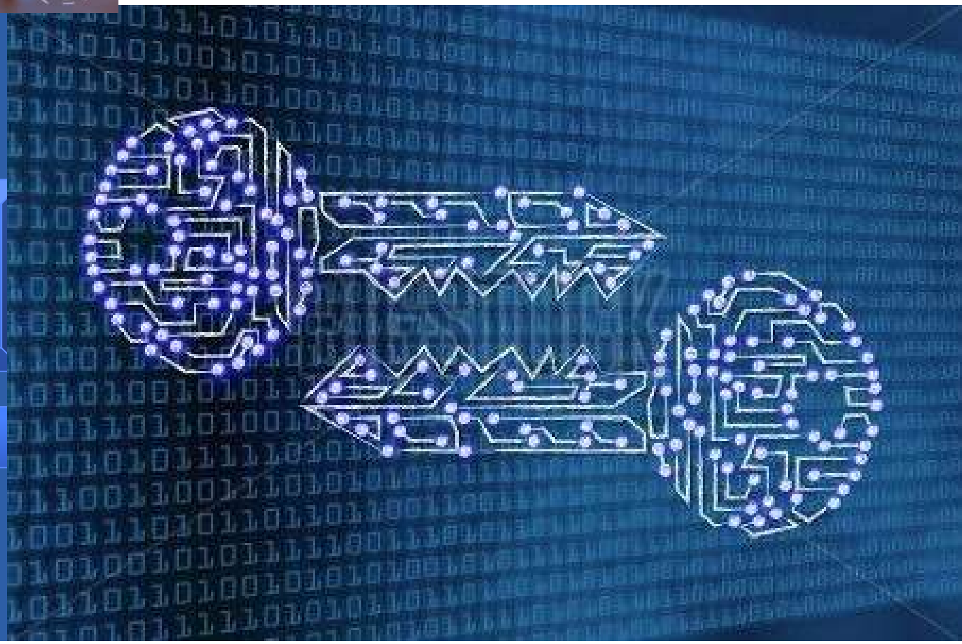
Image Source: HANDBOOK of APPLIED CRYPTOGRAPHY Alfred J. Menezes

Criptografía

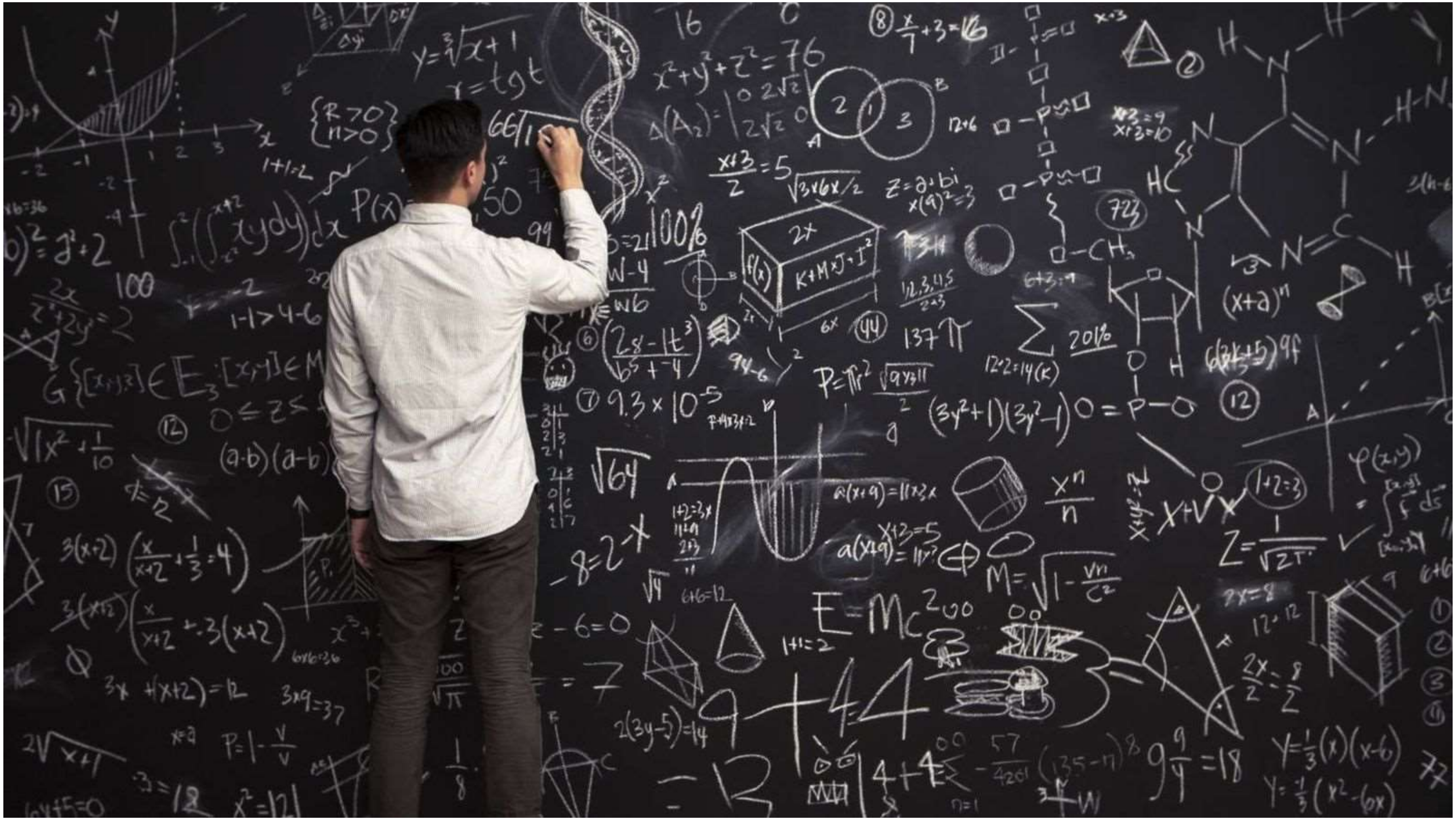
Universidad
Francisco de Vitoria
UFV Madrid

Tema 1.2 Repaso matemático





Repaso de matemáticas para criptografía



Repaso de matemáticas para criptografía

TEORÍA DE NÚMEROS (Repaso)

- **Números Primos:** sólo divisibles entre 1 y sí mismos.
  - Son la base de la Teoría de Números
  - Ejemplo: primos inferiores de 200:

    2 3 5 7 11 13 17 19 23 29 31 37 41 43 47 53 59 61 67 71 73 79 83 89 97 101 103 107 109 113 127 131 137 139 149 151 157 163 167 173 179 181 191 193 197 199
- **Factorización de Números Primos :** expresar un número *n* como producto de números primos ($n = a \cdot b \cdot c$)
  - Es más complejo factorizar, que calcular *n* en base a sus números primos.
  - Ejemplo: $3600 = 2^4 x 3^2 x 5^2$:

Repaso de matemáticas para criptografía

TEORÍA DE NÚMEROS (Repaso)

- **Números Co-primos:** sólo tienen como divisor común al 1.
  - Ejemplo: 6 y 35 son co-primos:

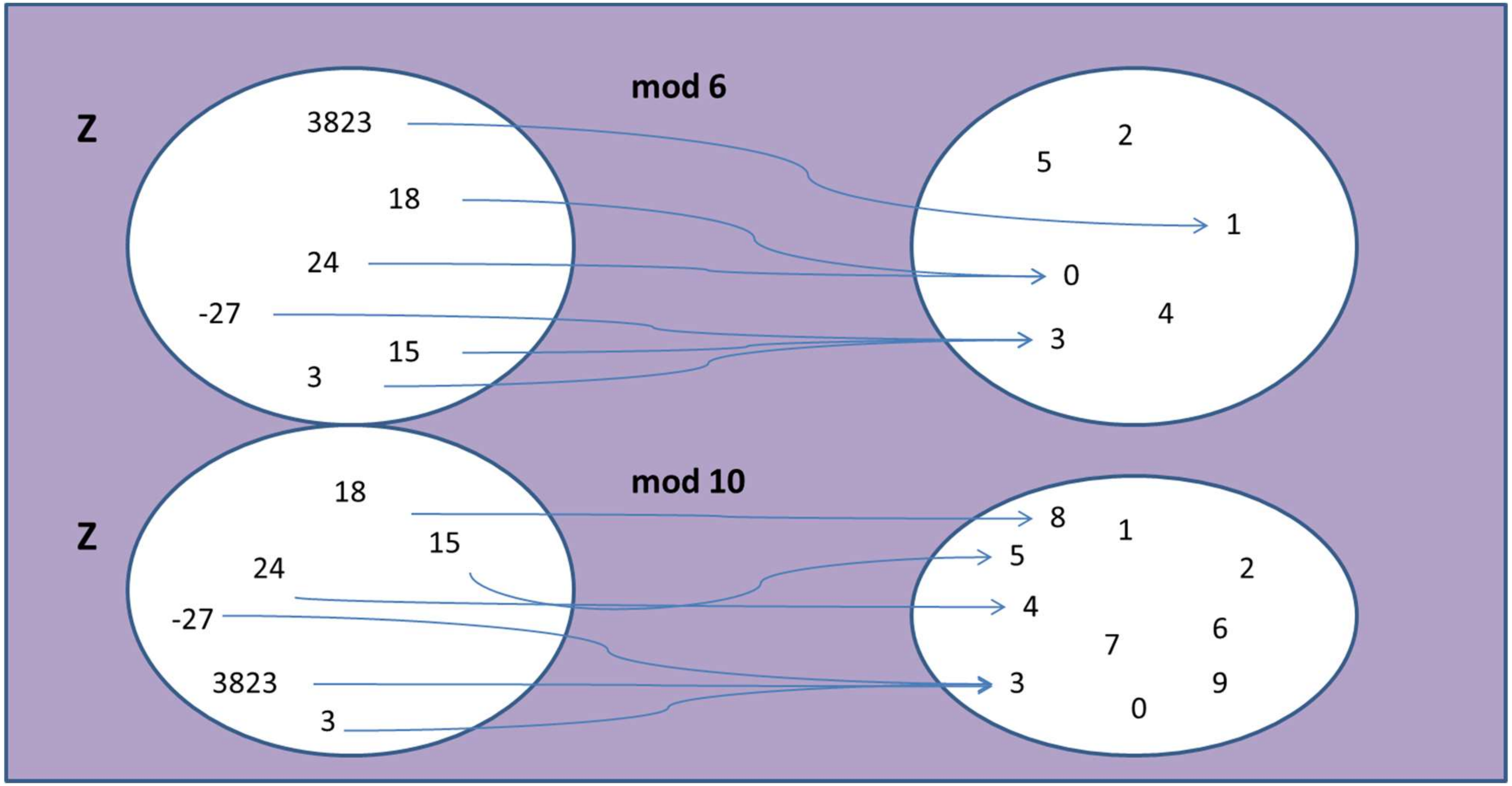
$$6 = 2 \cdot 3$$
$$35 = 5 \cdot 7$$

- **Máximo Común Divisor:** se cogen los divisores comunes con el menor exponente.
  - Ejemplo:

$$180 = 2^2 \cdot 3^2 \cdot \mathbf{5}$$
$$150 = \mathbf{2} \cdot \mathbf{3} \cdot 5^2$$

$$\Rightarrow \quad mcd = 30 = 2 \cdot 3 \cdot 5$$

Operación Módulo (mod)



Repaso de matemáticas para criptografía

Y TODO ESTO… PARA QUÉ??

Repaso de matemáticas para criptografía

VARIOS ALGORITMOS CRIPTOGRÁFICOS SÓLO FUNCIONAN CON AQUELLOS ELEMENTOS QUE TENGAN INVERSO MULTIPLICATIVO.

- Si $a \cdot b = 1 \bmod n$, entonces b es el **inverso multiplicativo** de a módulo n
  - Ejemplo:

```
a = 3
b = 4
n = 11
```

$$3 \cdot 4 = 12 = 1 \bmod 11$$

- Por tanto, necesitamos conocer **técnicas** para **calcular inversos multiplicativos** de un número módulo n**:**
  - **Fermat**
  - **Euler**
  - **Algoritmo Euclídeo Extendido**

Repaso de matemáticas para criptografía

1. TEOREMA DE FERMAT

- $\forall\, a \in \mathbf{Z}$, p primo, siendo $\mathrm{mcd}(a,p)=1$, entonces:

$$a^{p-1} = 1 \pmod{p}$$

- Equivalente:

$$a^{p} = a \pmod{p}$$

EJERCICIO (Enunciado)

- Demostrar que se cumple el teorema de Fermat para $p = 7$ y los siguientes valores de a (analizar el resultado en cada caso):
  - a = 6
  - a = 11
  - a = 21

Recuerda: $a^{p-1} = 1 \pmod{p}$

$a^p = a \pmod{p}$

Repaso de matemáticas para criptografía

EJERCICIO (Solución)

- Demostrar que se cumple el teorema de Fermat para $p = 7$ y los siguientes valores de a (analizar el resultado en cada caso):
  - **a = 6**
    - 6 y 7 son coprimos → se puede aplicar Fermat
    - $a^{p-1} = 6^{7-1} = 6^6 = 46.656 \pmod{7} = \mathbf{1} \pmod{7}$
  - Equivalente:
    - $a^p = 6^7 = 279.936 \pmod{7} = 6 \pmod{7}$

Recuerda: $a^{p-1} = 1 \pmod{p}$

$a^p = a \pmod{p}$

Repaso de matemáticas para criptografía

EJERCICIO (Solución)

- Demostrar que se cumple el teorema de Fermat para $p = 7$ y los siguientes valores de a (analizar el resultado en cada caso):
  - **a = 11**
    - 11 y 7 son coprimos → se puede aplicar Fermat
    - $a^{p-1} = 11^{7-1} = 11^6 = 1.771.561 \pmod{7} = 1 \pmod{7}$
  - Equivalente:
    - $a^p = 11^7 = 19.487.171 \pmod{7} = 11 \pmod{7} = 4$

Recuerda: $a^{p-1} = 1 \pmod{p}$

$a^p = a \pmod{p}$

EJERCICIO (Solución)

- Demostrar que se cumple el teorema de Fermat para $p = 7$ y los siguientes valores de a (analizar el resultado en cada caso):
  - **a = 21**
    - 21 y 7 **no son coprimos** → **no se puede aplicar Fermat**
    - $a^{p-1} = 21^{7-1} = 21^6 = 85.766.121 \pmod{7} = 0$

Recuerda: $a^{p-1} = 1 \pmod{p}$

$a^{p} = a \pmod{p}$

Sólo si: $\mathrm{mcd}(a,p) = 1$

2. TEOREMA DE EULER. Introducción.

- En aritmética modulo **n**:
  - **Conjunto completo de residuos** es: { 0..n−1 }
  - **Conjunto reducido de residuos** contiene los **residuos (> 0) co-primos con n**

***Ejemplo*: n=10,**

Conjunto completo de residuos:
{0,1,2,3,4,5,6,7,8,9}

Conjunto reducido de residuos:
{1,3,7,9}

r	r^{-1}	Motivo
0	--	*0 excluido*
1	1	*1·1 = 1 mod 10*
2	--	*2, 10 no coprimos*
3	7	*3·**7** = 21 mod 10 = 1*
4	--	*4, 10 no coprimos*
5	--	*5, 10 no coprimos*
6	--	*6, 10 no coprimos*
7	3	*7·**3** = 21 mod 10 = 1*
8	--	*8, 10 no coprimos*
9	9	*9·**9** = 81 mod 10 = 1*

2. TEOREMA DE EULER. Introducción.

- El número de elementos contenidos en el conjunto reducido de residuos se calcula con la **Función de Euler $\Phi(n)$**

  - Para **p primo** → $\Phi(p) = p-1$
  - Si **n factorizable** ($n = a \cdot b$) → $\Phi(n) = \Phi(a) \cdot \Phi(b)$
  - Si **p primo,** y **k** entero >0 → $\Phi(p^k) = p^k - p^{k-1} = p^{k-1} \cdot (p-1)$

  - *Ejemplo:* $\Phi(10) = \Phi(5) \cdot \Phi(2) = 4 \cdot 1 = 4$
    - ***4 elementos en el conjunto reducido de residuos mod 10: {1,3,7,9}***

TEOREMA DE EULER

- Generalización del Teorema de Fermat
- Para todo *a* y *n* enteros, siendo *n* diferente de cero, y **mcd(a,n)=1**

$$a^{\Phi(n)} = 1 \pmod{n}$$

- Equivalente:

$$a \cdot a^{\Phi(n)-1} = 1 \pmod{n}$$

$a \cdot b = 1 \bmod n$, entonces b es el **inverso multiplicativo** de a módulo n

EJERCICIO (Enunciado)

- Calcular, mediante el teorema de Euler, el inverso multiplicativo "***b***"

  $$(a \cdot b = 1 \bmod n)$$

  para `n = 10` y los siguientes valores de `a`:

  - a = 3
  - a = 37

Recuerda: $a \cdot a^{\Phi(n)-1} = 1 \pmod{n}$

EJERCICIO (Enunciado)

- Calcular, mediante el teorema de Euler, el inverso multiplicativo "*b*"

$$(a \cdot b = 1 \bmod n)$$

para $n = 10$ y los siguientes valores de a:

- $a = 3$
- $n = 10 \rightarrow \Phi(n) = \Phi(10) = \Phi(2) \cdot \Phi(5) = 1 \cdot 4 = 4$
- $b = a^{\Phi(n)-1} \pmod{n} = 3^{4-1} \pmod{10} = 3^3 \pmod{10} = 27 \bmod 10 = 7$

$$(3 \cdot 7 = 21 = 1 \bmod 10)$$

Recuerda: $a \cdot a^{\Phi(n)-1} = 1 \pmod{n}$

EJERCICIO (Enunciado)

- Calcular, mediante el teorema de Euler, el inverso multiplicativo "*b*"

$$(a \cdot b = 1 \bmod n)$$

para $n = 10$ y los siguientes valores de a:

- $a = 37$
- $n = 10 \rightarrow \Phi(n) = \Phi(10) = \Phi(2) \cdot \Phi(5) = 1 \cdot 4 = 4$
- $b = a^{\Phi(n)-1} \pmod{n} = 37^{4-1} \pmod{10} = 37^{3} \pmod{10} = 50.653 \bmod 10 = 3$

$$(37 \cdot 3 = 111 = 1 \bmod 10)$$

Recuerda: $a \cdot a^{\Phi(n)-1} = 1 \pmod{n}$

2. Algoritmo Euclídeo Extendido

- Ventaja: no requiere factorizar los números para calcular el mcd

If gcd(a,n)=1

	c_1	c_2	…	…	…	c_n	r_{n-1}
n	a	r_1	r_2	…	…	r_{n-1}	1
r_1	r_2	r_3	…	…	1	0	

$n = c_1 a + r_1$
$a = c_2 r_1 + r_2$
$r_1 = c_3 r_2 + r_3$
…
…
$r_{n-2} = c_n r_{n-1} + 1$
$r_{n-1} = c_{n+1} + 0$

Substituting:

$$1 = k_1\, a + k_2\, n$$

Reducing modulo n:

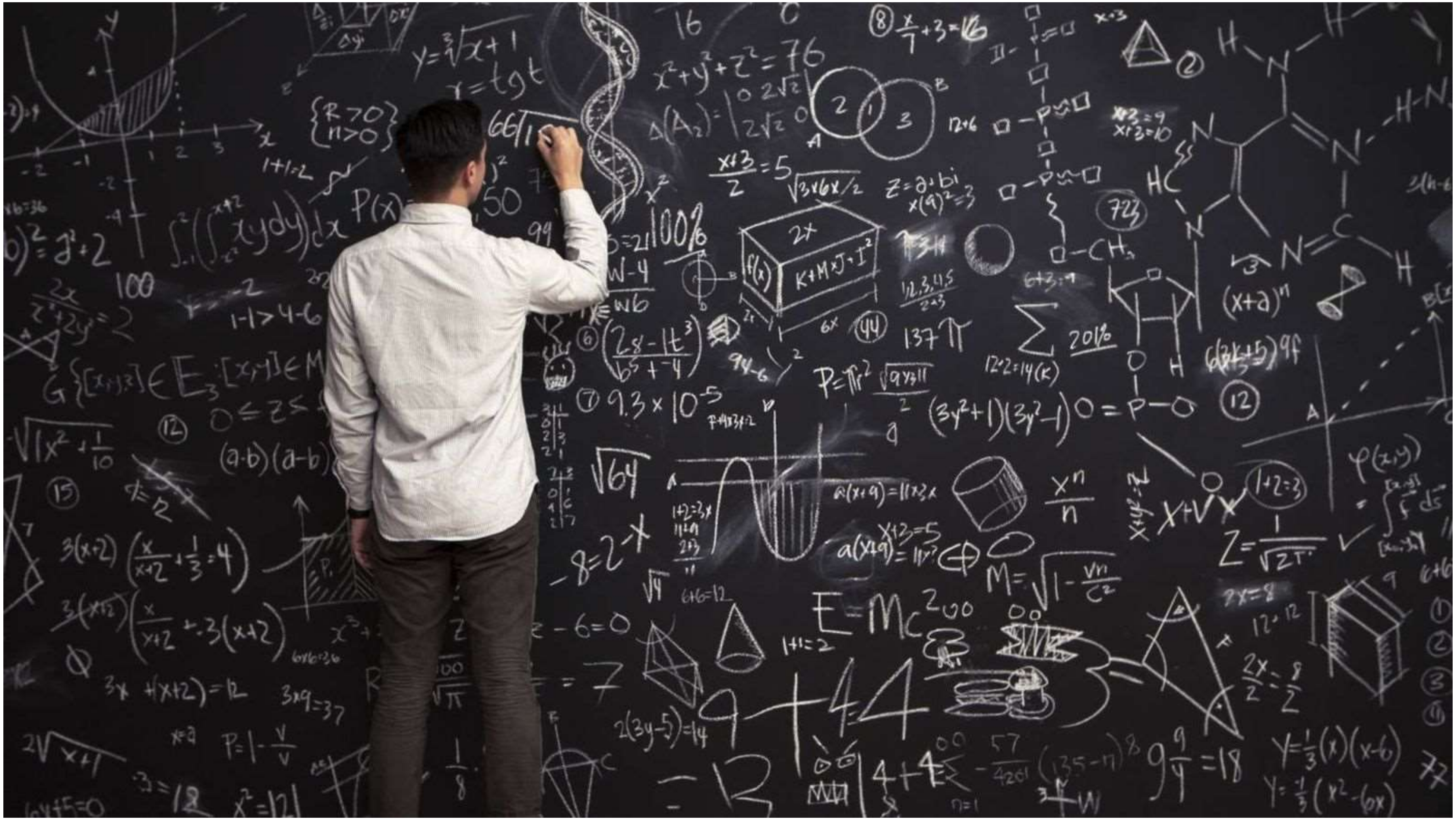
$$1 = k_1\, a \text{ (mód. n)}$$

Then

$$\boxed{k_1 = a^{-1} \text{ (mód. n)}}$$

¡¡No entra en el examen!!

Repaso de matemáticas para criptografía



Repaso de matemáticas para criptografía

CUERPOS DE GALOIS

- Sea *A* el conjunto de polinomios a(x) de grado **n-1** or inferior, cuyos coeficientes están en Z_q (**q** primo)

$$a(x) = a_{n-1}x^{n-1}+a_{n-2}x^{n-2}+\cdots\cdots+a_1x+a_0 \qquad a_i \in Z_q$$

- a(x) son los restos de la division de los polinomios entre el polinomio irreducible **p(x)**, siendo p(x) un polinomio de grado **n**
  - Junto con las operaciones (+, ·) → campo finito **GF(q^n)**
    - Todos los elementos (except el 0) tienen inverso multiplicative
  - *Ejemplo: En AES: q = 2, n=8 → GF(2^8)*

Repaso de matemáticas para criptografía

NOS CENTRAMOS EN: GF(2^8)

- Genérico:
  - $a(x) = a_7x^7 + a_6x^6 + a_5x^5 + a_4x^4 + a_3x^3 + a_2x^2 + a_1x + a_0$ $\quad a_i \in Z_2 = \{0,1\}$
- Ejemplos:

  $a(x) = x^6 + x^4 + x^2 + 1$

  $b(x) = x^7 + x^3 + x^2$

  $p(x) = x^5 + x^2 + 1$
- Caso particular:

  En **AES**: **GF(2^8)** con **$p(x) = x^8 + x^4 + x^3 + x + 1$** → (bin)100011011

Repaso de matemáticas para criptografía

OPERACIONES EN CUERPOS DE GALOIS GF (2^8)

- Suma y Resta:
  - $c_i = (a_i \pm b_i) \bmod 2 = a_i \oplus b_i$ ($\oplus$ == XOR)

- *Ejemplo: calcular c(x) = a(x) + b(x):*

  $a(x) = x^4+x^2+1$ → (bin)10101

  $b(x) = x^4+x^3+x^2$ → (bin)11100

  $c(x) = ?$

SOLUCIÓN:

- Suma y Resta:
  - $c_i = (a_i \pm b_i) \bmod 2 = a_i \oplus b_i$ ($\oplus$ == XOR)

- *Ejemplo: calcular c(x) = a(x) + b(x):*

$a(x) = x^4+x^2+1 \rightarrow 10101$

$b(x) = x^4+x^3+x^2 \rightarrow \oplus\ 11100$

01001

$c(x) = x^3+1$

OPERACIONES EN CUERPOS DE GALOIS GF (2^8)

- Multiplicación:
  - $c(x) = a(x) \cdot b(x) \bmod p(x)$
    - El polinomio resultante se reduce (si es necesario) módulo p(x)
    - Los coeficientes se reducen módulo 2

- *Ejemplo: calcular c(x) = a(x) · b(x) mod p(x), siendo:*

$a(x) = x^4+x^2+1$

$b(x) = x^4+x^3+x^2$

$\mathbf{p(x) = x^8+ x^4+ x^3 + x + 1}$

$c(x) = ?$

Repaso de matemáticas para criptografía

Y TODO ESTO… PARA QUÉ??

Repaso de matemáticas para criptografía

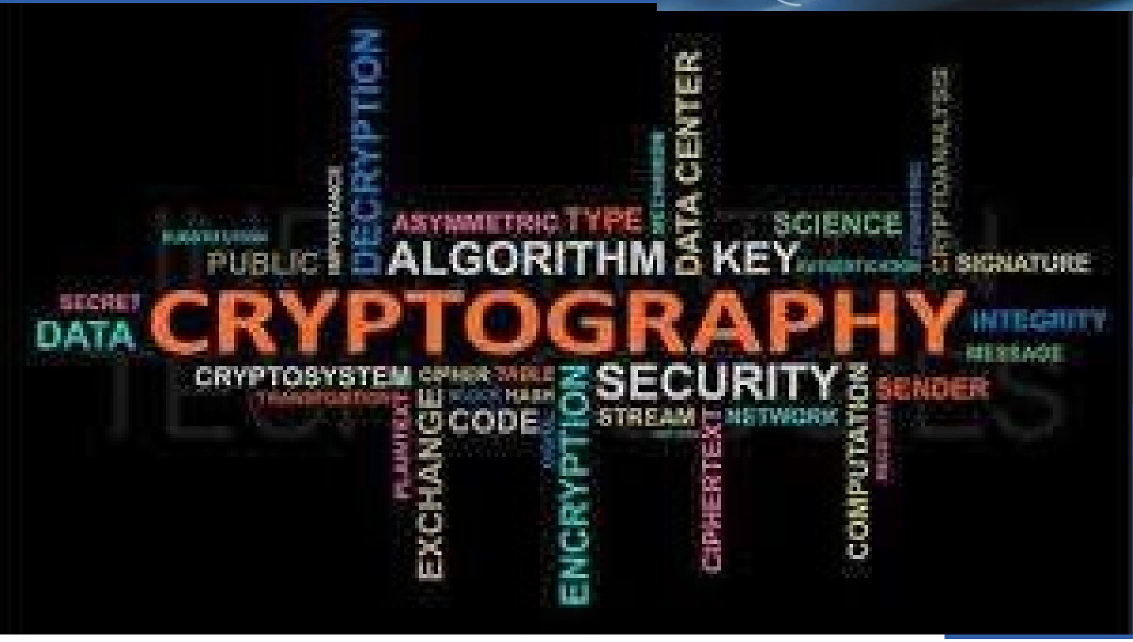
VARIOS ALGORITMOS CRIPTOGRÁFICOS ESTÁN BASADOS EN ÁLGEBRA POLINOMIAL MODULAR.

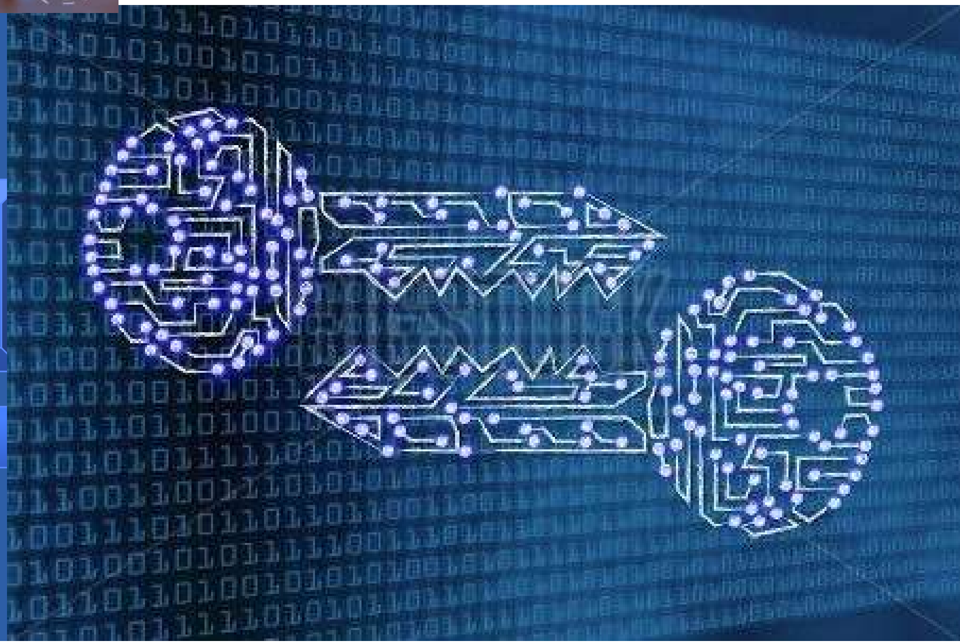
- Ejemplo: **AES**

Criptografía

Universidad Francisco de Vitoria UFV Madrid

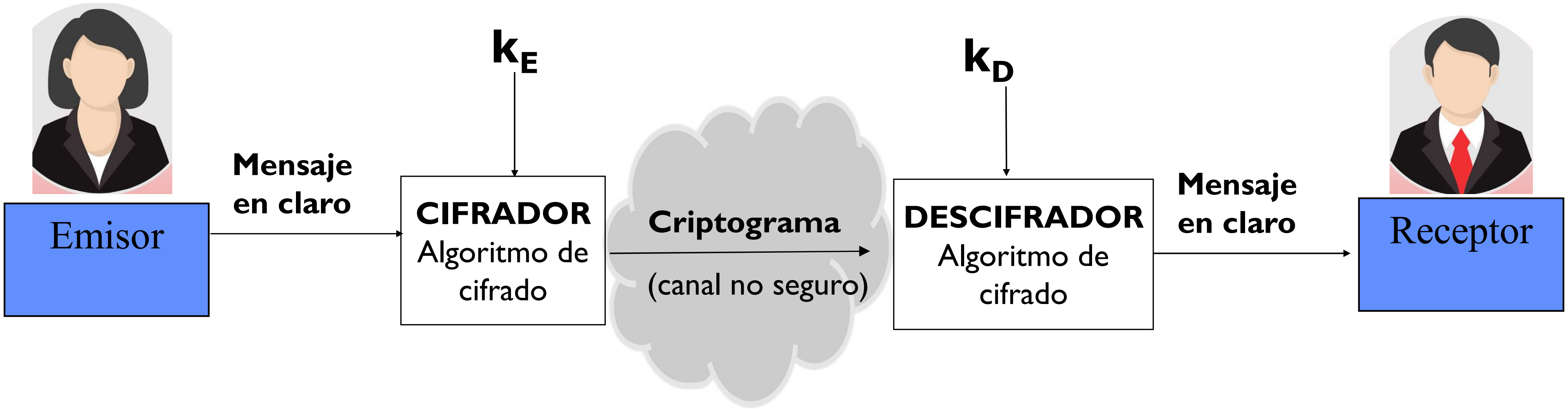
Tema 1.3 Modelo de Criptosistema





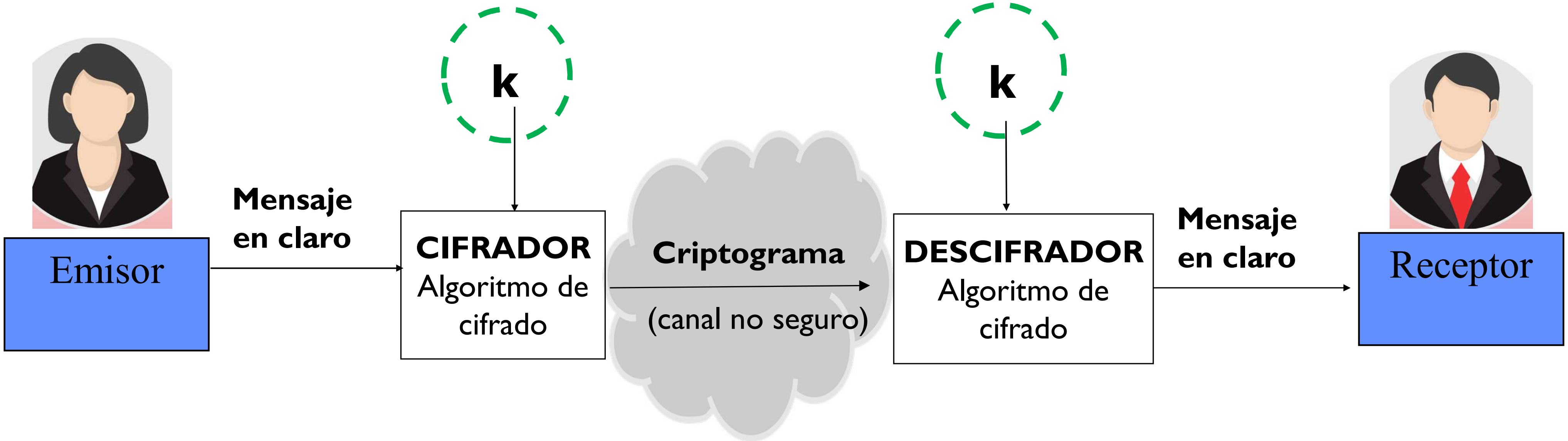
Criptosistemas

Modelo de Criptosistema



Modelo de Criptosistema

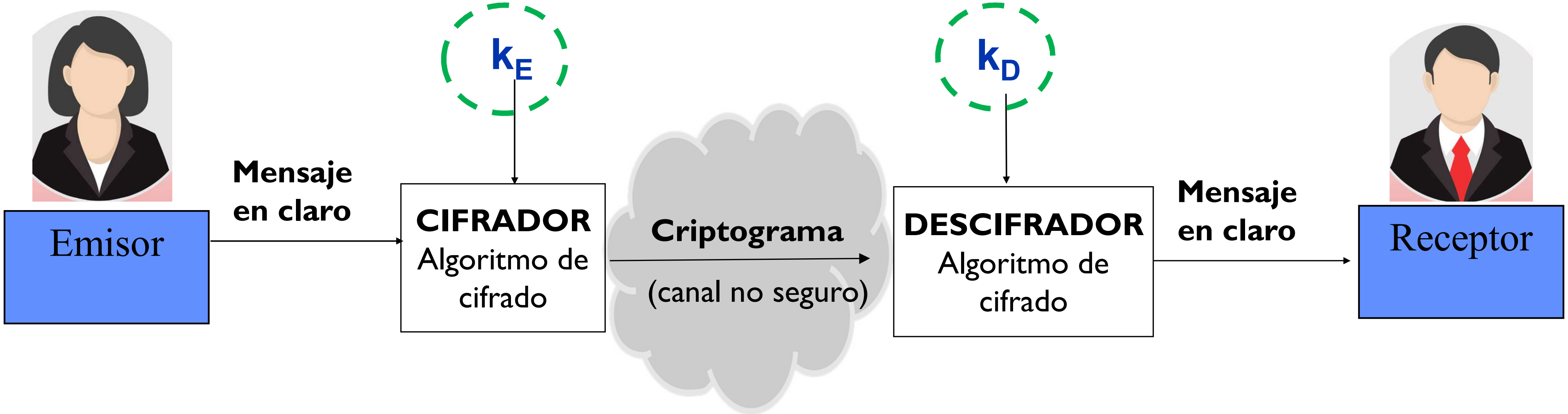
SIMÉTRICOS: Misma clave (k) para cifrar y descifrar



- La clave se acuerda y comparte entre las en modo secreto

Modelo de Criptosistema

ASIMÉTRICOS: Una clave (k_E) para cifrar y otra (k_D) para descifrar



- Base de los sistemas de clave pública

Modelo de Criptosistema

HÍBRIDOS: Combinan esquemas de clave simétrica y asimétrica

- Aprovecha la ventajas de ambos esquemas

- Múltiples topologías y combinaciones
  - Los estudiaremos en detalle en la parte de criptografía de clave pública

Criptografía

Universidad
Francisco de Vitoria
UFV Madrid

Tema 1
Introducción a la Criptografía