# INTRODUCCIÓN A LA CRIPTOGRAFÍA

*Francisco Calvo Camacho, Adrián Costales Almarza,*
*Nicole Herrero del Río, Oscar López Llorente*
*Miguel Antonio Trejo Malfaz**
*IES Alfonso VI. Plaza San Andrés s/n. 47410 Olmedo (Valladolid)*
*miguelaguassevilla@yahoo.es*

Junta de Castilla y León

XI ENCUENTRO ALUMNADO INVESTIGADOR

## INTRODUCCIÓN

En todo proceso de comunicación intervienen siempre tres elementos principales que son: **emisor, receptor y mensaje**, este último enviado a través de un canal.

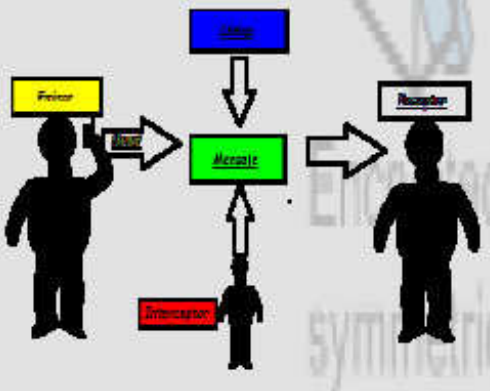
Es posible que a veces el mensaje sea interceptado por una tercera persona pudiendo conocer así el contenido del mensaje, situación poco recomendable cuando el mensaje es de carácter comprometido. Para evitar este tipo de amenazas nace la **milenaria ciencia de la criptografía**, por la cual pueden comunicarse emisor y receptor utilizando como medio un canal que en caso de ser atacado dificulte la lectura del mensaje al estar escrito en un **texto cifrado**.

La criptografía permite realizar un estudio de criptosistemas, definiendo estos matemáticamente como una **upla** ( $\mathcal{M}$ , C, K , c , d ) donde $\mathcal{M}$ denota los mensajes de tamaño n, C el conjunto de los mensajes cifrados, K el conjunto de claves o llaves, c llave de cifrado, d llave de descifrado.

El trabajo desarrollado consiste en identificar **diversos sistemas de codificación** de clave privada, denominados también como sistemas simétricos y de clave pública, denominados también como sistemas asimétricos; e intentar realizar un criptoanálisis para garantizar la seguridad del encriptado buscando los posibles ataques que se puedan hacer a este.

## IDEA BÁSICA

En toda comunicación existe un emisor que a través de un canal quiere comunicarse enviando un mensaje al receptor. Para evitar que este sea interceptado por una tercera persona debemos codificar el mensaje.




## HIPÓTESIS

**Existen sistemas de encriptamiento fiables teniendo en cuenta ciertas consideraciones**

## OBJETIVOS GENERALES

- Introducir métodos deductivos.
- Aplicar las matemáticas en otros aspectos diferentes de los académicos.
- Interrelacionar de forma motivadora diferentes ámbitos como el social, el de comunicación y el científico-tecnológico.
- Aprender a trabajar en equipo.
- Introducir las tics como herramienta para búsqueda de información.

## OBJETIVOS ESPECÍFICOS

- Aprender algún sistema de codificación.
- Identificar la seguridad y posibles métodos de ataque a textos encriptados.
- Diferenciar los sistemas simétricos de los sistemas asimétricos en criptografía.

## METODOLOGÍA

- Se han adaptado los conceptos a las aptitudes, conocimientos y capacidades para la comprensión de un público más extenso.
- Hemos buscado información contrastándola con la que ya teníamos.

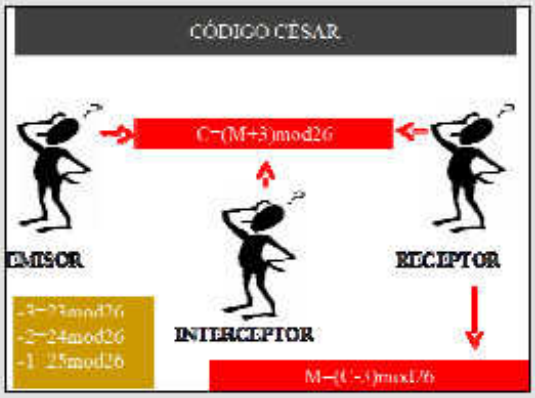
## SISTEMAS DE ENCRIPTAMIENTO

Existen dos sistemas de encriptamiento. El primero denominado de clave privada o simétrico caracterizado por usar la misma llave para el cifrado y el descifrado. Ejemplos de este sistema son el código de César y el código de Augusto. El segundo es el llamado de clave pública o asimétrico caracterizado por tener diferentes formas para cifrar y descifrar. Un ejemplo de este sistema es el R.S.A.

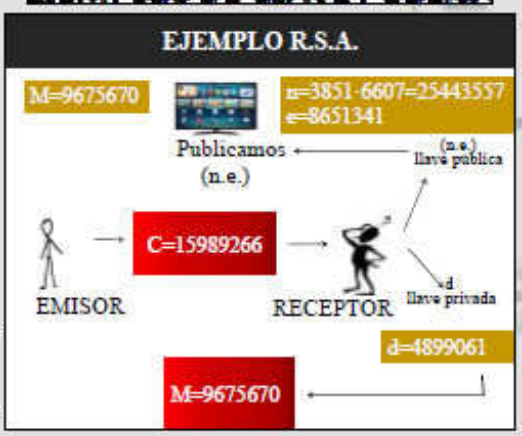
## RESULTADOS

- Distinción entre sistemas simétricos y asimétricos.
- Identificación de ataques al código de César mediante la frecuencia de letras.
- Búsqueda de otro sistema de encriptamiento para ofrecer una solución a este tipo de ataques.
- Determinación de condiciones para el sistema R.S.A.


## EJEMPLOS DE CLAVE PRIVADA




## EJEMPLOS DE CLAVE PÚBLICA




## CONCLUSIONES

- Los sistemas simétricos ofrecen menos seguridad que los asimétricos.
- El sistema más seguro que hay en la actualidad es el R.S.A. cumpliéndose ciertas condiciones.

IES Alfonso VI. Olmedo (Valladolid)

## WEBGRAFÍA

https://es.wikipedia.org/wiki/Criptografía
https://es.wikipedia.org/wiki/RSA
http://es.ccm.net/contents/criptografia-1747462277#126