# David Carral -- Adán -- Nezha -- xabier

## 2º Sistemas Microinformáticos y Redes

**Unidad: 4**

**Práctica Nº: 42**

**Título: Cifrados de la antiguedad**

**Fecha: 10/12/2025**


**Seguridad Informática**

# Índice



Lista de cifrados de la antiguedad y la edad media

1. playfair
2. metodo polibios
3. cifrado cesar
4. cifrado de vingenere

# 1. Playfair

## 1.1. Que es?

Playfair, es un método de **cifrado** inventado por el físico *Charles Wheatstone*. Fué uno de los primeros métodos utilizados en los que el cifrado no se hacía letra a letra, sino con **grupos de dos** letras.

## 1.2. Como funciona?

En una tabla cuadrada (generalmente de 5x5), se escriben al azar las 25 letras del alfabeto que se van a utilizar.

Agrupamos el texto que vamos a cifrar en letras de dos en dos, y en caso de que quede en un número impar, se añade una **x** al final.

Cada pareja de letras se puede encuadrar según los siguientes cuatro casos:

1. Las dos letras están en la misma fila del cuadro.
2. Las dos letras están en la misma columna.
3. Las dos letras no están en la misma columna.

4. Las dos letras son iguales.

## 1.3. Funcionamiento

Este método codifica mal los pares de letras repetidas. Esto se puede solucionar *añadiendo un nulo*:

*Para evitar que se produzca el caso 4, cambiamos una de las letras por una x, el cual sería el nulo.

Si la pareja de letras a cifrar están en la misma fila, se substituyen por las letras situadas a su derecha.

Si las letras están en la misma columna, pillamos la letra inferior.

Si no están ni en la misma fila, ni en la misma columna, seleccionaremos la letra que coincida en el punto medio bloqueando los ejes en línea recta, priorizando el eje horizontal de la letra que toque en ese momento.

# Metodo polibios:

Se trata de un cifrado trivial donde cada carácter se corresponde a una fila y columna de la matriz.Es un caso particular de un sistema de transposición monolalfabética por lo que un análisis de frecuencias sería más que suficiente para desvelar el mensaje oculto.

Los métodos de sustitución se basan en asignar a cada letra otro ente ,que puede ser también otra letra, o un número o un símbolo especial. La cifra de Polibio es históricamente la primera que emplea métodos de sustitución .

Para explicar el funcionamiento en castellano tenemos qye recurrir a un truco,debido a que en nuestro idioma se emplean más de 25 letras, cosa que en latín y griego no ocurre.

Para codificar un mensaje primeramente fromamos la siguiente tabla:

| | A | B | C | D | E |
|---|---|---|---|---|---|
| A | a | b | c | d | e |
| B | f | g | h | i | j |
| C | k | l | m | n | o |
| D | p | r | s | t | u |
| E | v | w | x | y | z |

La letra a se cifrará como AA, la b como AB,...Hemos eliminado la letra q, lo cual no redunda en el contenido del mensaje , siempre que sustituyamos dicha letra por la k.Tampoco hemos incorporado la ñ porque se suele llevar mal con los ordenadores.

Ejemplo: Texto claro: cifradepolibio Texto cifrado: ACBDBADBAAADAEDACECBBDABBDCE

Una de las ventajas del cifrado del polibio es que emplea únicamente 5 letras para escribir cualquier mensaje,y el problema que tiene es :el mensaje cifrado tiene el doble de longitud que el texto claro.

# cifrado cesar

es un metodo simple de cifrado por sustitucion que reemplaza cada letra de un mensaje por otra que se encuentra un numero fijo de posiciones mas adelante o mas atras en el alfabeto

ejemplo :

texto plano: mensaje de ejemplo

texto cifrado:KHKVDMH GH HMHPOR

el ejemplo se hizo utilizando un desplazamiento de 3 letras mas adelante en el alfabeto

| Original | a | b | c | d | e | f | g | h | i | j | k | l | m |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| Cifrado | d | e | f | g | h | i | j | k | l | m | n | o | p |

| Original | n | o | p | q | r | s | t | u | v | w | x | y | z |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| Cifrado | q | r | s | t | u | v | w | x | y | z | a | b | c |

# cifrado vegenere

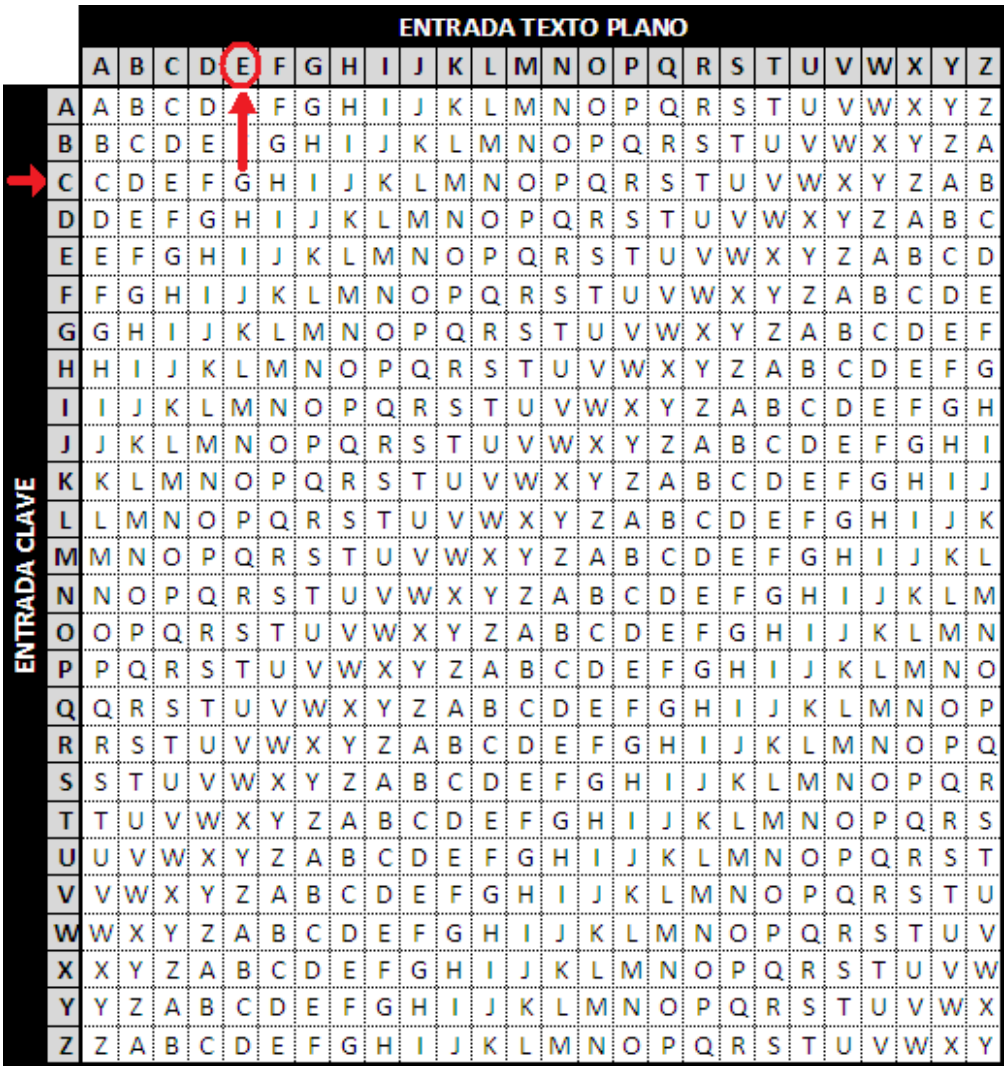
es un metodo de cifrado polialfabetico que utiliza una palabra clave para cifrar un mensaje funciona repitiendo la palabra clave asta que tenga la misma longitud del mensaje cada letra se cifra con una tabla de vegenere que es una tabla de 26 filas y 26 columnas donde cada fila se desplaza un lugar respecto a la fila anterior

ejemplo :

texto plano : ejemplo

clave : vegenere

texto cifrado : ZNKZTCS




| ENTRADA CLAVE | A | B | C | D | E | F | G | H | I | J | K | L | M | N | O | P | Q | R | S | T | U | V | W | X | Y | Z |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| A | A | B | C | D | E | F | G | H | I | J | K | L | M | N | O | P | Q | R | S | T | U | V | W | X | Y | Z |
| B | B | C | D | E | F | G | H | I | J | K | L | M | N | O | P | Q | R | S | T | U | V | W | X | Y | Z | A |
| C | C | D | E | F | G | H | I | J | K | L | M | N | O | P | Q | R | S | T | U | V | W | X | Y | Z | A | B |
| D | D | E | F | G | H | I | J | K | L | M | N | O | P | Q | R | S | T | U | V | W | X | Y | Z | A | B | C |
| E | E | F | G | H | I | J | K | L | M | N | O | P | Q | R | S | T | U | V | W | X | Y | Z | A | B | C | D |
| F | F | G | H | I | J | K | L | M | N | O | P | Q | R | S | T | U | V | W | X | Y | Z | A | B | C | D | E |
| G | G | H | I | J | K | L | M | N | O | P | Q | R | S | T | U | V | W | X | Y | Z | A | B | C | D | E | F |
| H | H | I | J | K | L | M | N | O | P | Q | R | S | T | U | V | W | X | Y | Z | A | B | C | D | E | F | G |
| I | I | J | K | L | M | N | O | P | Q | R | S | T | U | V | W | X | Y | Z | A | B | C | D | E | F | G | H |
| J | J | K | L | M | N | O | P | Q | R | S | T | U | V | W | X | Y | Z | A | B | C | D | E | F | G | H | I |
| K | K | L | M | N | O | P | Q | R | S | T | U | V | W | X | Y | Z | A | B | C | D | E | F | G | H | I | J |
| L | L | M | N | O | P | Q | R | S | T | U | V | W | X | Y | Z | A | B | C | D | E | F | G | H | I | J | K |
| M | M | N | O | P | Q | R | S | T | U | V | W | X | Y | Z | A | B | C | D | E | F | G | H | I | J | K | L |
| N | N | O | P | Q | R | S | T | U | V | W | X | Y | Z | A | B | C | D | E | F | G | H | I | J | K | L | M |
| O | O | P | Q | R | S | T | U | V | W | X | Y | Z | A | B | C | D | E | F | G | H | I | J | K | L | M | N |
| P | P | Q | R | S | T | U | V | W | X | Y | Z | A | B | C | D | E | F | G | H | I | J | K | L | M | N | O |
| Q | Q | R | S | T | U | V | W | X | Y | Z | A | B | C | D | E | F | G | H | I | J | K | L | M | N | O | P |
| R | R | S | T | U | V | W | X | Y | Z | A | B | C | D | E | F | G | H | I | J | K | L | M | N | O | P | Q |
| S | S | T | U | V | W | X | Y | Z | A | B | C | D | E | F | G | H | I | J | K | L | M | N | O | P | Q | R |
| T | T | U | V | W | X | Y | Z | A | B | C | D | E | F | G | H | I | J | K | L | M | N | O | P | Q | R | S |
| U | U | V | W | X | Y | Z | A | B | C | D | E | F | G | H | I | J | K | L | M | N | O | P | Q | R | S | T |
| V | V | W | X | Y | Z | A | B | C | D | E | F | G | H | I | J | K | L | M | N | O | P | Q | R | S | T | U |
| W | W | X | Y | Z | A | B | C | D | E | F | G | H | I | J | K | L | M | N | O | P | Q | R | S | T | U | V |
| X | X | Y | Z | A | B | C | D | E | F | G | H | I | J | K | L | M | N | O | P | Q | R | S | T | U | V | W |
| Y | Y | Z | A | B | C | D | E | F | G | H | I | J | K | L | M | N | O | P | Q | R | S | T | U | V | W | X |
| Z | Z | A | B | C | D | E | F | G | H | I | J | K | L | M | N | O | P | Q | R | S | T | U | V | W | X | Y |