# Códigos Secretos: otra forma de aplicar las matrices en Bachillerato (16-18)

**Julián Baena Ruiz**

**Tras una breve introducción para hacer referencia a distintos tipos de códigos secretos, el artículo estudia con detalle, esquemáticamente y mediante ejemplos, los códigos matriciales. Se expone, además, una forma de automatizar dichos códigos en el aula, mediante un programa escrito en dBASE III Plus. La parte final consta de unas preguntas sobre sus posibilidades didácticas.**

## Objetivo

Se quiere presentar la criptografía como un campo de aplicación del cálculo matricial y un contexto para conectar dicho estudio con la programación de ordenadores. Las ideas expuestas pretenden ser útiles a profesores que busquen enfoques distintos de esta parte del álgebra lineal y, para ello, estén dispuestos a utilizar ordenadores.

## Introducción

Criptografía significa arte de escribir con una clave secreta. Nos referiremos en adelante a esta clave con el nombre de código.

Algunos códigos secretos, a los que llamaremos elementales, se basan en la sustitución de cada carácter por un determinado símbolo. Por ejemplo si la letra A se sustituye por el signo +, la M por ?, O por % la palabra "AMO" se codifica: "+?%". Un ejemplo de ellos aparece en el cuento de Edgar Allan Poe[1] "El escarabajo de oro" [1]; aquí se explican, razonadamente, estrategias que conducen a descifrar un criptograma. Todos los códigos elementales son equivalentes y fáciles de descifrar comparando las frecuencias con que aparecen los símbolos en el texto codificado, con las frecuencias de aparición de los caracteres en el idioma usado para escribir. Algunos autores (profesores) han propuesto actividades para clase, usando códigos de este tipo [2]; en ellas se deja claro lo fácil que resulta descubrir un código elemental utilizando la Estadística.

En los últimos años, y debido al interés creciente de proteger la información en las comunicaciones, la criptografía ha logrado grandes progresos a partir de códigos secretos más avanzados, cuya descripción sería imposible sin conocimientos de álgebra [3]. Entre ellos podemos citar los que usan vectores y matrices [4] (para nosotros matriciales), basados en las ideas de Hill [5], de los que nos vamos a ocupar a continuación, y otros, que se estudian a partir de resultados de la Teoría de Números [6], iniciados con trabajos de Diffie y Hellman donde se trata la criptografía en términos matemáticos y un "sistema criptográfico" es considerado como una "familia uniparamétrica de transformaciones invertibles" [7] (pág. 646).

## Códigos matriciales

Tratando de evitar el abuso de formalismos, que puedan aburrir a los menos iniciados, la exposición de esta sección se basa en casos particulares; así el lector podrá dar, a medida que avanzamos, un tratamiento más general a todo lo que hay escrito.

Comenzamos definiendo un conjunto S formado por todos los signos disponibles para escribir los textos que después se codificarán. Este conjunto, por comodidad, lo consideramos compuesto por las letras del alfabeto castellano, (excepto la ll y la ch) el espacio (que representaremos en esta sección mediante "-"), el signo de interrogación "?" y el punto ".". Nuestro conjunto S tiene 30 elementos.

$$S = \{A,B,C,D,E,F,G,H,I,J,K,L,M,N,Ñ,O,P,Q,R,S,T,U,V,W,X,Y,Z,.,?,-\}$$

**Definición:** Llamamos S-mensaje a una secuencia de caracteres del conjunto S, que escribiremos siempre entre comillas.

Por ejemplo:
M = "HOLA-BUENAS-NOCHES"

[1] Poe fue un reconocido criptoanalista.

Establecemos, a continuación, una correspndencia 1-1, f, de S en $Z_{30}$ (conjunto de los enteros módulo 30). Por ejemplo elegimos f(x)=n, donde n es la clase del número que ocupa x en el orden dado anteriormente. De esta forma tenemos identificado S con $Z_{30}$.

**1. Pasos a seguir para la codificación**

(con un ejemplo 2x2)

Vamos a codificar el mensaje M del ejemplo anterior. Para ello seguiremos los siguientes pasos:

**1.1.** Elegimos una matriz 2x2 invertible sobre $Z_{30}$ por ejemplo:

$$A = \begin{pmatrix} 8 & 1 \\ 1 & 4 \end{pmatrix}$$

Esta matriz determina unívocamente el código y su dimensión 2x2 da nombre a los códigos de este tipo.

**1.2.** Pasamos, mediante la aplicación f, del mensaje a un conjunto ordenado de números (imágenes de los caracteres que aparecen en M). En nuestro caso:

8 16 12 1 0 2 22 5 14 1 20 0 14 16 3 8 5 20

**1.3.** A partir de este conjunto definimos, ordenadamente, pares de números como se hace a continuación:

(8,16) (12,1) (0,2) (22,5) (14,1) (20,0) (14,16) (3,8) (5,20)[2]

**1.4.** Multiplicamos por la matriz A, cada uno de los pares anteriores y resulta:

(20,12) (7,16) (2,8) (1,12) (23,18) (10,20) (8,18) (2,5) (0,25)

**1.5.** Obtenemos una nueva secuencia numérica:

20 12 7 16 2 8 1 12 23 18 10 20 8 18 2 5 0 25

**1.6.** Aplicando la inversa de f, conseguimos el mensaje codificado:

M'= "SLGOBHALUQJSHQBE-X"

Llamaremos a M' S-mensaje codificado por A o imagen de M mediante A, y escribiremos:

$$M' = A(M)$$

**2. Pasos a seguir para decodificar un mensaje**

Es un proceso análogo al anterior. Consiste en hacer lo mismo que en 1. partiendo del mensaje M' y eligiendo, en el primer punto 1.1, como matriz, la inversa de A (que llamaremos B):

$$B = \begin{pmatrix} 4 & 29 \\ 29 & 8 \end{pmatrix}$$

No es necesario efectuar cálculos para asegurar que, el S-mensaje codificado de M', mediante B, es M.

**3. Generalización**

Es imprescindible definir con precisión el conjunto S de símbolos que se utilizarán para escribir, y su cardinal, k, nos conducirá a trabajar en el anillo $Z_k$ de los enteros módulo k.

Como se indicó antes, el código viene determinado unívocamente por la matriz invertible A (definida sobre $Z_k$). Si A es cuadrada de orden n, en el punto 1.3. formaremos n-uplas y completaremos la última con los ceros que sean necesarios (en el caso de que la longitud del S-mensaje de partida no sea múltiplo de n).

Podemos, incluso codificar usando matrices no cuadradas mxn procurando que para A (la que codifica) exista una matriz B de orden nxm tal que el producto A.B sea la matriz I (identidad) mxm; hablándose así, según la matriz, de códigos 2x2, 3x3, 4x5, etc.

Conviene destacar que un código 1x1, definido por unidad de $Z_k$, será a todos los efectos un código elemental, pues lo único que introduce es una permutación en el orden de los caracteres.

## Automatizando el proceso

Se presenta un programa (ver anexo), fruto de actividades llevadas a cabo, tanto dentro como fuera del aula, con un grupo de 18 alumnos de COU[3] que, en su mayoría (14), habían recibido (en informática de 3º) un curso completo de dBASE III, manejo interactivo y programación. El trabajo informático surgió a partir de una opinión compartida: los códigos matriciales deben automatizarse, y una razón fundamental: no es operativo ni eficaz aplicarlos manualmente.

El Programa, escrito en dBASE III PLUS, permite codificar y decodificar el contenido de una base de datos (dBASE), total -todos los campos- o parcialmente -algunos campos-.

Se ha elegido como conjunto de símbolos, el de los 255 caracteres

[2] Se colocaría un cero en el último par, si el mensaje de partida tuviese un número impar de caracteres.
[3] Del IB " Mediterráneo " de Salobreña (Granada)

ASCII, y las funciones "asc" y "chr", incorporadas al lenguaje de programación usado, han sido consideradas como f y $f^{-1}$ respectivamente. No fue necesario, para nuestros fines, hacer un estudio formal de los anillos $Z_k$, ni hubo grandes dificultades, por parte de los alumnos, con las operaciones en $Z_{255}$; a estas edades ya se ha trabajado, de manera intuitiva, la aritmética modular en diversas situaciones como, por ejemplo, en operaciones con ángulos y su reducción al primer cuadrante.

## Cuestiones posteriores

Aparte de ideas para su ampliación y mejora, la ejecución del programa puede suscitar preguntas como las siguientes: si codificamos dos veces consecutivas, ¿el resultado es una codificación matricial?, en caso afirmativo ¿qué matriz define este nuevo código? ¿Qué situaciones de codificación pueden expresarse con el producto de matrices? ¿Qué propiedades debe cumplir una matriz para que al codificar iteradamente, nos encontremos en algun paso el texto inicial?.

En las respuestas a estas y otras muchas preguntas, se espera surjan reflexiones que faciliten la elaboración de propuestas de trabajo dirigidas a las clases de los nuevos bachilleratos. En ellos sí tiene cabida el, tan olvidado, estudio de las matrices; además de su aplicación en la regla de Cramer[4], no deberíamos olvidarnos de las posibilidades educativas como modelos de representación[5] que facilitan la matematización en muchas y diferentes situaciones.

## Bibliografía


[1] POE, E. A. (1970). **Narraciones Completas**. Ed. Aguilar, Madrid. pp. 383-432.

[2] AZARQUIEL (Grupo) (1982). **Curso Inicial de Estadística en el Bachillerato**. Ed. ICE, Madrid.

[3] GARDNER, M. (1977). **Claves de nuevo tipo cuyo desciframiento ocuparía unos cuantos millones de años**. Investigación y Ciencia 13. pp. 96-101.

[4] CHILDS, L. (1979). **A concrete introduction to higher algebra**. Ed. Springer, New York.

[5] HILL, L. S. (1931). **Concerning Certain lineal transformations apparatus of cryptography**. American Mathematical Monthly 38. pp. 135-154

[6] NICOLAS, J. L. (1984). **Test de primalité**. Expositions Mathematicae 2. pp. 223-234.

[7] DIFIE, W.; HELLMAN, M. E. (1976). **New directions in cryptography**. IEEE Transactions on Informations Theory (vol. IT-22) 6. pp. 644-654.

[8] MEC. (1991). **Bachillerato. Estructura y contenidos**. Ed. MEC, Madrid.

[9] CARRETERO, R. ET. AL. (1989). **Diseño curricular de Matemáticas 16-18**. Ed. Consejería de Educación y Ciencia, Sevilla.


## ANEXO

**A.- FICHERO PROGRAM.PRG**

```
set echo off
set talk off
set procedure to proced
clear
text
        ESTE PROGRAMA CODIFICA O DECODIFICA
        CUALQUIERA DE LOS CAMPOS DE UNA BASE
        DE DATOS
        (Es importante que tenga delante el nombre de
        los campos de la base que desea codificar)
endtext
do while .t.
   text
      ¿QUÉ DESEA?
            (A) CODIFICAR
            (B) DECODIFICAR
            (C) SALIR
   endtext
   wait "PULSE UNA OPCION..." to op
   if upper(op)="A"
     do codifica
   endif
   if upper(op)="B"
     do decodif
   endif
   if upper(op)="C"
     clear
     clear all
```

[4] Vuelve a incluirse en los documentos del MEC [8].

[5] En este sentido se hacen recomendaciones desde los diseños de Andalucía [9].

```
      close procedure
      ?"ADIOS...."
      exit
    endif
enddo
```

**B.- FICHERO PROCED.PRG**

```
PROCEDURE CODIFICA
clear
accept "NOMBRE DE LA BASE DE DATOS..." to base
use &base
clear
a11=2
a12=9
a21=1
a22=5
do while .t.
  accept "Nombre del campo a codificar..." to field
  do while .not. eof ( )
    store &field to campo
    result=""
    if mod(len(campo),2)=1
      campo=campo+" "
    endif
    j=1
    do while j<=len(campo)/2
      k=len(campo)
      x1=asc(campo)
      x2=asc(substr(campo,2,k-1))
      campo=substr(campo,3,k-2)
      y1=x1*a11+x2*a21
      y2=x1*a12+x2*a22
      result=result+chr(mod(y1,255))+chr(mod(y2,255))
    enddo
    ?result
    replace &field with result
    skip 1
  enddo
  clear
  do while .t.
   wait " CAMPO &field CODIFICADO.  ¿CODIFICAR OTRO
CAMPO? (S/N)  " to r
    if  r$"SsnN"
      go top
      exit
    endif
  enddo
  if r$"Nn"
    exit
  endif
enddo
return

PROCEDURE DECODIF
clear
accept "NOMBRE DE LA BASE DE DATOS..." to base
use &base
clear
a11=5
a12=246
a21=254
a22=2
do while .t.
  accept "Nombre del campo a decodificar..." to field
  do while .not. eof ( )
    store &field to campo
    result=""
    if mod(len(campo),2)=1
      campo=campo+" "
    endif
    j=1
    do while j<=len(campo)/2
      k=len(campo)
      x1=asc(campo)
      x2=asc(substr(campo,2,k-1))
      campo=substr(campo,3,k-2)
      y1=x1*a11+x2*a21
      y2=x1*a12+x2*a22
      result=result+chr(mod(y1,255))+chr(mod(y2,255))
    enddo
    ?result
    replace &field with result
    skip 1
  enddo
  clear
  do while .t.
    wait "CAMPO &field
DECODIFICADO.¿DECODIFICAR OTRO CAMPO?(S/N) "
to r
    if  r$"SsnN"
      go top
      exit
    endif
  enddo
  if r$"Nn"
    exit
  endif
enddo
return
```

**Julián Baena Ruiz**
*I.B. "Mediterráneo".*
*Salobreña (Granada).*