Criptografia a batxillerat: aplicacions de les matrius i implementació amb TAC

Víctor Ranera i Martín
Escola Joan Pelegrí
vranera@joanpelegri.cat

Resum

En aquest treball es descriu com s'ha d'aplicar l'àlgebra de matrius que forma part dels continguts curriculars de les matemàtiques de batxillerat a la criptografia. En aquest sentit, emprarem la suma i el producte de matrius i el càlcul de la matriu inversa pel mètode dels adjunts. Finalment, implementarem tot el procés de codificació, xifratge, desxifratge i descodificació amb l'entorn Octave, un llenguatge de programació pensat essencialment per a la computació numèrica.

Abstract

This article explains how to apply matrix algebra —included in the upper secondary mathematics curriculum— to cryptography. To this end, we will use the sum and the product of matrices and the calculation of the inverse matrix by the method of adjoints. Finally, we will implement the entire process of coding, encrypting, decrypting and decoding using Octave, software featuring a high-level programming language, primarily intended for numerical computations.

Objectiu

En aquesta activitat es proposa emprar l'àlgebra lineal i, en particular, les transformacions amb matrius per xifrar i desxifrar textos. En concret, es proposa emprar matrius de 3 files com a clau per xifrar i desxifrar i un alfabet de 28 símbols. No es detalla la versió general dels sistemes de xifratge, sinó que s'ha volgut anar directament a les particularitats de les adaptacions dels models proposats.

L'objectiu principal és treballar el xifratge de Hill, malgrat que s'exposaran els xifratges per permutació i de Cèsar com a introductoris. També es faran algunes observacions sobre seguretat dels sistemes emprats, però serà més a títol informatiu i amb la finalitat de pensar estratègies de millora.

Els procediments de càlcul aquí exposats es poden dur a terme amb paper i llapis amb alumnat de batxillerat, però també detallarem una proposta d'implementació amb l'entorn GNU Octave, eina essencialment compatible amb Matlab.

Introducció

La criptografia és l'estudi de les tècniques d'escriure missatges de manera secreta per tal que només un receptor autoritzat sigui capaç de llegir-los [1]. El seu origen etimològic s'ha de buscar en les paraules gregues *kriptos* («ocult») i *grafos* («escriptura»). El seu desenvolupament al llarg de la història té dues etapes: la precientífica i la moderna [2] [3]. La primera va des de la Grècia clàssica fins a la introducció dels ordinadors, cap al final de la Segona Guerra Mundial. La segona comprèn el període en què la computació té un paper cabdal, especialment per la seva capacitat de gestionar grans quantitats d'informació i fer moltíssimes operacions de càlcul. Avui dia la criptografia és una branca de les matemàtiques amb aplicacions en camps com la seguretat, la integritat o l'autenticitat de les dades, les comunicacions...

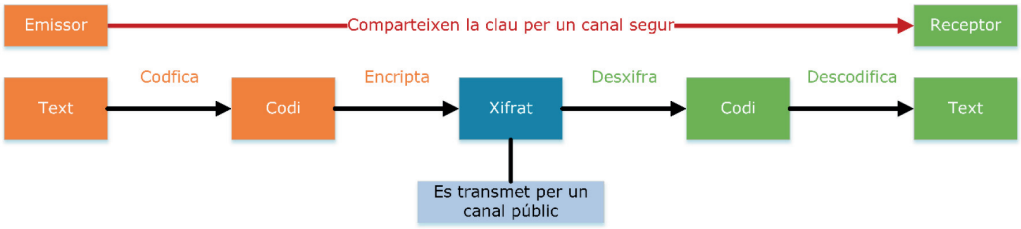
Quan un emissor vol transmetre un text o un missatge a un receptor, ho fa via un canal on aquest pot ser interceptat. Per evitar que pugui ser comprès en cas d'arribar a mans de qui no s'espera que el rebi, s'envia una versió modificada del text. El procés de modificació del text s'anomena xifratge i ha de permetre que un receptor amb la informació suficient pugui recuperar el text original. En aquest sentit, cal distingir:

- El mètode de xifratge: és el conjunt de tècniques segons les quals es modifica el text original per obtenir el text xifrat.
- El mètode de desxifratge: és el conjunt de tècniques segons les quals es recupera el text original a partir del text xifrat.
- La clau: és un o diversos valors numèrics sense els quals no es pot aplicar el mètode de xifratge [4]. Un mateix mètode de xifratge sol tenir múltiples claus. La clau de xifratge i desxifratge pot ser la mateixa o no, i fins i tot no ha de ser fàcilment deduïble l'una a partir de l'altra.

Els mètodes que aquí s'exposen pertanyen a l'època precientífica i només l'emissor i el receptor poden conèixer la clau: és el que es coneix com a clau privada. En cas que aquesta clau sigui coneguda per qui intercepta el missatge xifrat, llavors podria recuperar el text original si sap quin ha estat el mètode de xifratge. Això es deu al fet que els mètodes de xifratge i desxifratge són l'un l'invers de l'altre i la clau és la mateixa o l'una s'obté de l'altra de manera senzilla. Per tant, la clau s'ha de transmetre per un canal segur i ha d'estar ben custodiada.

Codificació

Si volem treballar amb textos des d'un punt de vista algebraic, el primer que hem de fer abans de xifrar-los és codificar-los. És a dir, hem de transformar les lletres i els símbols alfanumèrics en números. D'aquesta manera, el procés d'emissió i recepció d'un text segueix l'esquema següent:



Durant aquesta activitat emprarem un alfabet de vint-i-vuit caràcters (les lletres majúscules sense accentuar, el punt i l'espai en blanc) i farem la codificació següent:

Símbol	Codi
A	0
B	1
C	2
D	3
E	4
F	5
G	6

Símbol	Codi
H	7
I	8
J	9
K	10
L	11
M	12
N	13

Símbol	Codi
O	14
P	15
Q	16
R	17
S	18
T	19
U	20

Símbol	Codi
V	21
W	22
X	23
Y	24
Z	25
.	26
espai	27

Així, per exemple, codificarem algunes paraules o text de la manera següent:

$$PAU \rightarrow 15\,0\,20$$
$$JOAN\ PELEGRI \rightarrow 9\,14\,0\,13\,27\,15\,4\,11\,4\,6\,17\,8$$

Però aquesta tirallonga de xifres ha de disposar-se d'alguna manera per tal de poder-la gestionar. En aquesta activitat proposem que sigui en forma de matriu i així podrem recórrer a les tècniques de l'àlgebra lineal. En particular, ho farem en matrius de tres files perquè són les que més comunament manipulem al batxillerat.

Així, col·locarem el codi en una matriu C amb tres files i tantes columnes com calgui i anirem situant els codis a les columnes (omplint, si cal, amb el codi corresponent a l'espai en blanc, les posicions finals que puguin quedar buides). Per exemple:

$$Text_1 = \text{«PAU»} \rightarrow C_1 = \begin{pmatrix} 15 \\ 0 \\ 20 \end{pmatrix}$$

$$Text_2 = \text{«JOAN PELEGRI»} \rightarrow C_2 = \begin{pmatrix} 9 & 13 & 4 & 6 \\ 14 & 27 & 11 & 17 \\ 0 & 15 & 4 & 8 \end{pmatrix}$$

$$Text_3 = \text{«BON DIA»} \rightarrow C_3 = \begin{pmatrix} 1 & 27 & 0 \\ 14 & 3 & 27 \\ 13 & 8 & 27 \end{pmatrix}$$

Hom podria interpretar la codificació com una mena de xifratge, ja que el text, un cop codificat, és difícilment comprensible. Tot i això, considerem que en aquesta fase no es pretén ocultar cap informació i, per tant, no podem considerar-la pròpiament un xifratge [1].

Hi ha força mètodes clàssics, coneguts com a xifratge de substitució, que tenen com a clau una taula per canviar els caràcters per alguna altra representació simbòlica [2].

Ara al text codificat li aplicarem una transformació mitjançant el que coneixem com a clau, de manera que el text resultant sigui difícilment reconeixible. Això és el que hem anomenat xifratge. Aquí estudiarem tres sistemes de xifratge en què la clau és una matriu i s'empren operacions bàsiques d'àlgebra lineal:

- Xifratge per permutacions
- Xifratge de Cèsar
- Xifratge pel mètode de Hill

Xifratge per permutacions

Aquesta tècnica és una de les més senzilles i consisteix a alterar l'ordre de les lletres d'un text: cada grup de tres lletres, les reordenem segons un cert criteri.

Per exemple, si volem que la primera passi al lloc de la segona, la segona al de la tercera i la tercera al de la primera, el xifratge serà:

$$Text_1 = \text{«PAU»} \xrightarrow{\text{codificació}} C_1 = \begin{pmatrix} 15 \\ 0 \\ 20 \end{pmatrix} \xrightarrow{\text{xifratge}} X_1 = \begin{pmatrix} 20 \\ 15 \\ 0 \end{pmatrix}$$

$$Text_2 = \text{«JOAN PELEGRI»} \xrightarrow{\text{codificació}} C_2 = \begin{pmatrix} 9 & 13 & 4 & 6 \\ 14 & 27 & 11 & 17 \\ 0 & 15 & 4 & 8 \end{pmatrix} \xrightarrow{\text{xifratge}} X_2 = \begin{pmatrix} 0 & 15 & 4 & 8 \\ 9 & 13 & 4 & 6 \\ 14 & 27 & 11 & 17 \end{pmatrix}$$

$$Text_3 = \text{«BON DIA»} \xrightarrow{\text{codificació}} C_3 = \begin{pmatrix} 1 & 27 & 0 \\ 14 & 3 & 27 \\ 13 & 8 & 27 \end{pmatrix} \xrightarrow{\text{xifratge}} X_3 = \begin{pmatrix} 13 & 8 & 27 \\ 1 & 27 & 0 \\ 14 & 3 & 27 \end{pmatrix}$$

Per tant, si algú interceptés el missatge xifrat, llegiria una col·lecció de números, que si descodifiqués donarien lloc als textos següents:

UPA

AJOPN EELIGR

NBOA D A

Aquest xifratge es pot fer amb matrius de la manera següent:

1. Partim d'una matriu identitat d'ordre 3: $I_3 = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$.
2. Reordenem les files d'acord amb el criteri que volem reordenar els grups de 3 lletres i obtenim P.
3. Codifiquem fent $X = P \cdot C$.

Així doncs, la clau de xifratge és P.

Seguint amb l'exemple anterior, on hem fet que la primera passi al lloc de la segona, la segona al de la tercera i la tercera al de la primera, la matriu A serà:

$$P = \begin{pmatrix} 0 & 0 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{pmatrix}$$

Fixem-nos que, aplicada a cadascuna de les matrius C del codi, dona:

$$C_1 = \begin{pmatrix} 15 \\ 0 \\ 20 \end{pmatrix} \xrightarrow{\text{xifratge}} X_! = P \cdot C_1 = \begin{pmatrix} 0 & 0 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{pmatrix} \begin{pmatrix} 15 \\ 0 \\ 20 \end{pmatrix} = \begin{pmatrix} 20 \\ 15 \\ 0 \end{pmatrix}$$

$$C_2 = \begin{pmatrix} 9 & 13 & 4 & 6 \\ 14 & 27 & 11 & 17 \\ 0 & 15 & 4 & 8 \end{pmatrix} \xrightarrow{\text{xifratge}} X_2 = P \cdot C_2 =$$

$$= \begin{pmatrix} 0 & 0 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{pmatrix} \cdot \begin{pmatrix} 9 & 13 & 4 & 6 \\ 14 & 27 & 11 & 17 \\ 0 & 15 & 4 & 8 \end{pmatrix} = \begin{pmatrix} 0 & 15 & 4 & 8 \\ 9 & 13 & 4 & 6 \\ 14 & 27 & 11 & 17 \end{pmatrix}$$

$$C_3 = \begin{pmatrix} 1 & 27 & 0 \\ 14 & 3 & 27 \\ 13 & 8 & 27 \end{pmatrix} \xrightarrow{\text{xifratge}} X_3 = P \cdot C_3 = \begin{pmatrix} 0 & 0 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{pmatrix} \cdot \begin{pmatrix} 1 & 27 & 0 \\ 14 & 3 & 27 \\ 13 & 8 & 27 \end{pmatrix} = \begin{pmatrix} 13 & 8 & 0 \\ 1 & 27 & 0 \\ 14 & 3 & 27 \end{pmatrix}$$

Per desxifrar el missatge cal tenir en compte que si $X = P \cdot C$, llavors

$$P^{-1} \cdot X = P^{-1} \cdot P \cdot C = C$$

és a dir:

$$C = P^{-1} \cdot X.$$

La clau per desxifrar és P^{-1}.

En el cas anterior, $P^{-1} = \begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 0 & 0 \end{pmatrix}$ (fixem-nos que desfà el canvi d'ordre de files que hem fet per xifrar). Així:

$$X_1 = \begin{pmatrix} 20 \\ 15 \\ 0 \end{pmatrix} \xrightarrow{\text{desxifratge}} C_1' = P^{-1} \cdot X_1 = \begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 0 & 0 \end{pmatrix} \cdot \begin{pmatrix} 20 \\ 15 \\ 0 \end{pmatrix} = \begin{pmatrix} 15 \\ 0 \\ 20 \end{pmatrix}$$

$$X_2 = \begin{pmatrix} 0 & 15 & 4 & 8 \\ 9 & 13 & 4 & 6 \\ 14 & 27 & 11 & 17 \end{pmatrix} \xrightarrow{\text{desxifratge}} C_2' = P^{-1} \cdot X_2 =$$

$$= \begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 0 & 0 \end{pmatrix} \cdot \begin{pmatrix} 0 & 15 & 4 & 8 \\ 9 & 13 & 4 & 6 \\ 14 & 27 & 11 & 17 \end{pmatrix} = \begin{pmatrix} 9 & 13 & 4 & 6 \\ 14 & 27 & 11 & 17 \\ 0 & 15 & 4 & 8 \end{pmatrix}$$

$$X_3 = \begin{pmatrix} 13 & 8 & 0 \\ 1 & 27 & 0 \\ 14 & 3 & 27 \end{pmatrix} \xrightarrow{\text{desxifratge}} C_3' = P^{-1} \cdot X_3 =$$

$$= \begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 0 & 0 \end{pmatrix} \cdot \begin{pmatrix} 13 & 8 & 0 \\ 1 & 27 & 0 \\ 14 & 3 & 27 \end{pmatrix} = \begin{pmatrix} 1 & 27 & 0 \\ 14 & 3 & 27 \\ 13 & 8 & 27 \end{pmatrix}$$

Tornem a tenir les matrius codificades originals, és a dir:

$$C_1' = C_1$$
$$C_2' = C_2$$
$$C_3' = C_3$$

Xifratge de Cèsar

Aquest mètode de xifratge consisteix a desplaçar la codificació dels caràcters alfanumèrics *b* posicions. És a dir, per xifrar se suma *b* a cadascun dels codis en què hem convertit el text. Per tant, la clau tant per xifrar com per desxifrar és *b*, en un cas fent un desplaçament endavant i en l'altre fent-lo enrere.

Si quan desplacem un codi *b* posicions ens passem de 27, llavors tornem a començar, és a dir, li restem 28. Això és el que algebraicament es coneix com l'aritmètica mòdul i s'expressa mitjançant $\equiv$.

Atès que el nostre objectiu és treballar amb matrius, emprarem una matriu *B* amb les característiques següents:

- 3 files.
- Tantes columnes com el codi requereixi.
- Totes les entrades amb *b*.

Així, per exemple, si prenem $b = 12$ per als casos dels exemples anteriors:

$$Text_1 = \text{«PAU»} \xrightarrow{\text{codificació}} C_1 = \begin{pmatrix} 15 \\ 0 \\ 20 \end{pmatrix} \xrightarrow{\text{xifratge}} X_1 = C_1 + B_1 =$$

$$= \begin{pmatrix} 15 \\ 0 \\ 20 \end{pmatrix} + \begin{pmatrix} 12 \\ 12 \\ 12 \end{pmatrix} = \begin{pmatrix} 27 \\ 12 \\ 32 \end{pmatrix} \equiv \begin{pmatrix} 27 \\ 12 \\ 4 \end{pmatrix}$$

$$Text_2 = \text{«JOAN PELEGRI»} \xrightarrow{\text{codificació}} C_2 = \begin{pmatrix} 9 & 13 & 4 & 6 \\ 14 & 27 & 11 & 17 \\ 0 & 15 & 4 & 8 \end{pmatrix} \xrightarrow{\text{xifratge}} X_2 =$$

$$= \begin{pmatrix} 9 & 13 & 4 & 6 \\ 14 & 27 & 11 & 17 \\ 0 & 15 & 4 & 8 \end{pmatrix} + \begin{pmatrix} 12 & 12 & 12 & 12 \\ 12 & 12 & 12 & 12 \\ 12 & 12 & 12 & 12 \end{pmatrix} =$$

$$= \begin{pmatrix} 21 & 25 & 16 & 18 \\ 26 & 39 & 23 & 29 \\ 12 & 27 & 16 & 20 \end{pmatrix} \equiv \begin{pmatrix} 21 & 25 & 16 & 18 \\ 26 & 11 & 23 & 1 \\ 12 & 27 & 16 & 20 \end{pmatrix}$$

$$Text_3 = \text{«BON DIA»} \xrightarrow{\text{codificació}} C_3 = \begin{pmatrix} 1 & 27 & 0 \\ 14 & 3 & 27 \\ 13 & 8 & 27 \end{pmatrix} \xrightarrow{\text{xifratge}} X_3 =$$

$$= \begin{pmatrix} 1 & 27 & 0 \\ 14 & 3 & 27 \\ 13 & 8 & 27 \end{pmatrix} + \begin{pmatrix} 12 & 12 & 12 \\ 12 & 12 & 12 \\ 12 & 12 & 12 \end{pmatrix} = \begin{pmatrix} 13 & 39 & 12 \\ 26 & 15 & 39 \\ 25 & 20 & 39 \end{pmatrix} \equiv \begin{pmatrix} 13 & 11 & 12 \\ 26 & 15 & 11 \\ 25 & 20 & 11 \end{pmatrix}$$

El que farà el mètode de desxifratge és restar b a tots els codis. Com hem dit, la clau és la mateixa b: generarem una matriu B, com abans, i per desxifrar restarem b a tots els elements. Tornarem a aplicar l'aritmètica mòdul 28, en aquest cas sumant 28 als possibles negatius.

Seguint amb l'exemple:

$$X_1 = \begin{pmatrix} 27 \\ 12 \\ 4 \end{pmatrix} \xrightarrow{\text{desxifratge}} C'_1 = X_1 - B = \begin{pmatrix} 27 \\ 12 \\ 4 \end{pmatrix} - \begin{pmatrix} 12 \\ 12 \\ 12 \end{pmatrix} = \begin{pmatrix} 15 \\ 0 \\ -8 \end{pmatrix} \equiv \begin{pmatrix} 15 \\ 0 \\ 20 \end{pmatrix}$$

$$X_2 = \begin{pmatrix} 21 & 25 & 16 & 18 \\ 26 & 11 & 23 & 1 \\ 12 & 27 & 16 & 20 \end{pmatrix} \xrightarrow{\text{desxifratge}} C'_2 = X_2 - B =$$

$$= \begin{pmatrix} 21 & 25 & 16 & 18 \\ 26 & 11 & 23 & 1 \\ 12 & 27 & 16 & 20 \end{pmatrix} - \begin{pmatrix} 12 & 12 & 12 & 12 \\ 12 & 12 & 12 & 12 \\ 12 & 12 & 12 & 12 \end{pmatrix} = \begin{pmatrix} 9 & 13 & 4 & 6 \\ 14 & -1 & 11 & -11 \\ 0 & 15 & 4 & 8 \end{pmatrix} \equiv \begin{pmatrix} 9 & 13 & 4 & 6 \\ 14 & 27 & 11 & 17 \\ 0 & 15 & 4 & 8 \end{pmatrix}$$

$$X_3 = \begin{pmatrix} 13 & 11 & 12 \\ 26 & 15 & 11 \\ 25 & 20 & 11 \end{pmatrix} \xrightarrow{\text{desxifratge}} C'_3 = X_3 - B =$$

$$= \begin{pmatrix} 13 & 11 & 12 \\ 26 & 15 & 11 \\ 25 & 20 & 11 \end{pmatrix} - \begin{pmatrix} 12 & 12 & 12 \\ 12 & 12 & 12 \\ 12 & 12 & 12 \end{pmatrix} = \begin{pmatrix} 1 & -1 & 0 \\ 14 & 3 & -1 \\ 13 & 8 & -1 \end{pmatrix} \equiv \begin{pmatrix} 1 & 27 & 0 \\ 14 & 3 & 27 \\ 13 & 8 & 27 \end{pmatrix}$$

Tornem a tenir les matrius codificades originals, és a dir:

$$C'_i = C_i \; \forall i \in \{1, 2, 3\}$$

Xifratge de Hill

El xifratge de Hill va ser ideat per Lester S. Hill [5]. Aquí es presenta una versió amb algunes variacions per tal que els càlculs es puguin fer amb paper i llapis en una aula de batxillerat com a aplicacions de les matrius.

Bàsicament, aquest xifratge consisteix a obtenir una matriu A amb les característiques següents:

- Que sigui invertible, és a dir, que existeixi A^{-1}.
- Que les seves entrades siguin enters.
- Que el seu determinant no sigui múltiple de 2 ni de 7 (que són els divisors primers de 28).

Xifrarem fent $X = A \cdot C$ tenint en compte que pot ser que algun dels termes de X tingui coeficients majors que 27 o menors que . En aquests casos, sumaríem o restaríem tantes vegades 28 com calgués (buscaríem un valor congruent mòdul 28, que denotem amb l'operador $\equiv$) a cadascuna de les entrades perquè el resultat estigués entre i 27. Malgrat que l'aritmètica mòdul 28 no formi part del currículum de l'ensenyament preuniversitari, és fàcilment explicable a l'alumnat perquè l'alfabet que tenim té aquesta mida i cal fer reduccions a codis entre i 27.

Per exemple, si prenem $A = \begin{pmatrix} 1 & 1 & 0 \\ 2 & -1 & 1 \\ 0 & 2 & -1 \end{pmatrix}$ llavors $A^{-1} = \begin{pmatrix} -1 & 1 & 1 \\ 2 & -1 & -1 \\ 4 & -2 & -3 \end{pmatrix}$ i el procés de xifratge serà:

$$C_! = \begin{pmatrix} 15 \\ 0 \\ 20 \end{pmatrix} \xrightarrow{\text{xifratge}} X_1 = A \cdot C_1 = \begin{pmatrix} 1 & 1 & 0 \\ 2 & -1 & 1 \\ 0 & 2 & -1 \end{pmatrix} \cdot \begin{pmatrix} 15 \\ 0 \\ 20 \end{pmatrix} = \begin{pmatrix} 15 \\ 50 \\ -20 \end{pmatrix} \equiv \begin{pmatrix} 15 \\ 22 \\ 8 \end{pmatrix}$$

$$C_2 = \begin{pmatrix} 9 & 13 & 4 & 6 \\ 14 & 27 & 11 & 17 \\ 0 & 15 & 4 & 8 \end{pmatrix} \xrightarrow{\text{xifratge}} X_2 = A \cdot C_2 =$$

$$= \begin{pmatrix} 1 & 1 & 0 \\ 2 & -1 & 1 \\ 0 & 2 & -1 \end{pmatrix} \cdot \begin{pmatrix} 9 & 13 & 4 & 6 \\ 14 & 27 & 11 & 17 \\ 0 & 15 & 4 & 8 \end{pmatrix} =$$

$$= \begin{pmatrix} 23 & 40 & 15 & 23 \\ 4 & 14 & 1 & 3 \\ 28 & 39 & 18 & 26 \end{pmatrix} \equiv \begin{pmatrix} 23 & 12 & 15 & 23 \\ 4 & 14 & 1 & 3 \\ 0 & 11 & 18 & 26 \end{pmatrix}$$

$$C_3 = \begin{pmatrix} 1 & 27 & 0 \\ 14 & 3 & 27 \\ 13 & 8 & 27 \end{pmatrix} \xrightarrow{\text{xifratge}} X_3 = A \cdot C_3 = \begin{pmatrix} 0 & 0 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{pmatrix} \cdot \begin{pmatrix} 1 & 27 & 0 \\ 14 & 3 & 27 \\ 13 & 8 & 27 \end{pmatrix} =$$

$$= \begin{pmatrix} 15 & 30 & 27 \\ 1 & 59 & 0 \\ 15 & -2 & 27 \end{pmatrix} \equiv \begin{pmatrix} 15 & 2 & 27 \\ 1 & 3 & 0 \\ 15 & 26 & 27 \end{pmatrix}$$

El desxifratge es fa mitjançant A^{-1}, és a dir, la clau per desxifrar és la matriu inversa de la clau de xifrar:

$$C_1' = A^{-1} \cdot X_1 = \begin{pmatrix} -1 & 1 & 1 \\ 2 & -1 & -1 \\ 4 & -2 & -3 \end{pmatrix} \cdot \begin{pmatrix} 7 \\ 22 \\ 8 \end{pmatrix} = \begin{pmatrix} 15 \\ 0 \\ -8 \end{pmatrix} \equiv \begin{pmatrix} 15 \\ 0 \\ 20 \end{pmatrix}$$

$$C_2' = A^{-1} \cdot X_2 = \begin{pmatrix} -1 & 1 & 1 \\ 2 & -1 & -1 \\ 4 & -2 & -3 \end{pmatrix} \cdot \begin{pmatrix} 23 & 12 & 15 & 23 \\ 4 & 14 & 1 & 3 \\ 0 & 11 & 18 & 26 \end{pmatrix} =$$

$$= \begin{pmatrix} -19 & 13 & 4 & 6 \\ 42 & -1 & 11 & 17 \\ 84 & -13 & 4 & 8 \end{pmatrix} \equiv \begin{pmatrix} 9 & 13 & 4 & 6 \\ 14 & 27 & 11 & 17 \\ 0 & 15 & 4 & 8 \end{pmatrix}$$

$$C_3' = A^{-1} \cdot X_3 = \begin{pmatrix} -1 & 1 & 1 \\ 2 & -1 & -1 \\ 4 & -2 & -3 \end{pmatrix} \cdot \begin{pmatrix} 15 & 2 & 27 \\ 1 & 3 & 0 \\ 15 & 26 & 27 \end{pmatrix} =$$

$$= \begin{pmatrix} 1 & 27 & 0 \\ 14 & -25 & 27 \\ 13 & -76 & 27 \end{pmatrix} = \begin{pmatrix} 1 & 27 & 0 \\ 14 & 3 & 27 \\ 13 & 8 & 27 \end{pmatrix}$$

En l'exemple que acabem de veure s'ha produït la circumstància que $det\ (A) = 1$, la qual cosa ens ha facilitat el càlcul de la matriu inversa. Però si $det\ (A) \neq \pm 1$, llavors haurem de recórrer al càlcul de la matriu inversa via

$$A^{-1} = \frac{1}{det\ (A)}\, adj\ (A)^T$$

Tenint en compte que $\frac{1}{det\ (A)}$ ha de ser l'invers mòdul 28 de $det(A)$. O, el que és el mateix, cal buscar un valor u enter tal que

$$det(A) \cdot u = 1 + k \cdot 28 \text{ per algun } k \in \mathbb{Z}.$$

Dit d'una altra manera, cal cercar u que verifiqui

$$det(A) \cdot u \equiv 1.$$

L'existència de u és coneguda a partir de la identitat de Bézout:

$$det(A) \cdot u + 28 \cdot v = 1.$$

El mètode per obtenir u s'escapa de l'objectiu que aquí ens plantegem, però es pot recórrer a eines informàtiques o, només per a alguns casos, a la taula següent per obtenir-lo:

$\det(A)$	-11	-9	-5	-3	3	5	9	11
u	5	3	11	9	-9	-11	-3	-5

Per tant, la clau per desxifrar serà

$$u \cdot\ adj\ (A)^T \equiv \frac{1}{det\ (A)}\, adj\,(A)^T.$$

Per exemple, si $A = \begin{pmatrix} 2 & 1 & -1 \\ 3 & -2 & 0 \\ 1 & 1 & -2 \end{pmatrix}$, llavors $det\ (A) = 9$ i $u = -3$. Xifraríem fent:

$$X_1 = A \cdot C_! = \begin{pmatrix} 2 & 1 & -1 \\ 3 & -2 & 0 \\ 1 & 1 & -2 \end{pmatrix} \cdot \begin{pmatrix} 15 \\ 0 \\ 20 \end{pmatrix} = \begin{pmatrix} 10 \\ 45 \\ -25 \end{pmatrix} \equiv \begin{pmatrix} 10 \\ 17 \\ 3 \end{pmatrix}$$

i desxifraríem via:

$$C_1' = u \cdot adj\,(A)^T \cdot X_1 = -3 \cdot \begin{pmatrix} 4 & 6 & 5 \\ 1 & -3 & -1 \\ -2 & -3 & -7 \end{pmatrix}^T \cdot \begin{pmatrix} 10 \\ 17 \\ 3 \end{pmatrix} =$$

$$= \begin{pmatrix} -12 & -3 & 6 \\ -18 & 9 & 9 \\ -15 & 3 & 21 \end{pmatrix} \cdot \begin{pmatrix} 10 \\ 17 \\ 3 \end{pmatrix} = \begin{pmatrix} -153 \\ 0 \\ -36 \end{pmatrix} \equiv \begin{pmatrix} 15 \\ 0 \\ 20 \end{pmatrix}$$

Operacions amb matrius a Octave

Octave és un programari lliure que ens permet una gestió àgil dels procediments de càlcul que aquí necessitem. Tot i això, hem definit algunes funcions que faciliten la comprensió dels càlculs.

Vegeu algunes funcions i la sintaxi bàsica d'Octave que necessitem:

- Introduir una matriu `A` 3×3 per files:
  `A=[[a11 a12 a13];[a21 a22 a23];[a31 a32 a33]].`
- Introduir una matriu `A` 3×3 per columnes:
  `A=[[a11;a12;a13] [a12;a22;a32] [a13;a23;a33]].`
- Calcular la matriu transposada de la matriu `A`: `trasposta A=A'`.
- Calcular el determinant de la matriu `A`: `a=det(A).`
- Calcular la matriu inversa de la matriu `A`: `invA=inv(A).`
- Determinar el nombre de files i columnes d'una matriu `A`: `m=rows(A)`
  `n=columns(A).`
- Generar la matriu identitat d'ordre 3, I_3: `I=eye(3).`
- Generar una matriu de `m` files i `n` columnes amb `1` a totes les entrades: `A=ones(m,n).`
- Generar una matriu de `m` files i `n` columnes amb nombres a l'atzar entre `0` i `1` segons una distribució uniforme a totes les entrades:
  `A=rand(m,n).`
- Calcular el màxim comú divisor `d` de `p` i `q` i obtenir els coeficients de la identitat de Bézout `(p*u+q*v=d)`:
  `[d,u,v]=gcd(p,q).`
- Obtenir el residu de la divisió de `p` per `m`:
  `r=mod(p,m).`
- Convertir una dada en un enter de 8 o 16 bits:
  `n=int8(x)`
  `n=int16(x).`
- Per recuperar el darrer càlcul dut a terme tenim ans.

A més, hem definit tres funcions:

- Codificar en una matriu un text d'acord amb l'alfabet i la metodologia definits en aquest article:
  `C=codifica(text).`
- Descodificar de manera inversa a com ho fa la funció *codifica*:
  `text=descodifica(C)`
- Calcular la matriu adjunta de la matriu `A`:
  `adjuntaA=adj(A).`

Aquestes funcions són al *bucket* https://octave-online.net/bucket~NQzX4rncyNJxKFDYdWc2m, es mostren a la part final d'aquest article i es poden descarregar de: https://drive.google.com/file/d/1oc4rTk99DS78ZNnsVTky7Be6rBO_RrB6/view?usp=sharing.

Aplicació amb Octave

Podem proposar al nostre alumnat que dugui a terme manualment els exercicis següents, i altres que se'ns puguin acudir, i després seguir el procediment amb Octave. Aquí s'opta per la versió en línia d'Octave, però també es pot emprar la versió que s'instal·la a l'ordinador, la qual està disponible per a diversos sistemes operatius.

Xifratge per permutacions

Procediment matemàtic	**Implementació amb Octave**
———	Accedim al *bucket* de la versió en línia d'Octave: https://octave-online.net/bucket~NQzX4rncyNJxKFDYdWc2m
Xifrarem mitjançant el xifratge per permutacions tot canviant la 1a fila per la 3a i deixant la 2a com està: $P = \begin{pmatrix} 0 & 0 & 1 \\ 0 & 1 & 0 \\ 1 & 0 & 0 \end{pmatrix}$	`I=eye(3)` `P([1 3],:) = I([3 1],:)`
Volem transmetre el text «*PLOU I FA SOL*». Cal codificar-lo a la matriu *C*.	`C=codifica("PLOU I FA SOL")`
Encriptem el text codificat: $X = P \cdot C$.	`X=P*C`
Aquest seria el missatge que hauríem de transmetre. Si algú l'interceptés sembla difícil que en pogués fer res. Provem de descodificar-lo.	`descodifica(X)`
Trobem la clau per desxifrar: P^{-1}.	`inv(P)`
Desxifrem *X*.	`ans*X`
Descodifiquem i obtenim el missatge original.	`descodifica(ans)`

Xifratge de Cèsar

Procediment matemàtic	**Implementació amb Octave**
———	Accedim al *bucket* de la versió en línia d'Octave: https://octave-online.net/bucket~NQzX4rncyNJxKFDYdWc2m
Xifrarem mitjançant el mètode de Cèsar i la clau és $b = 17$.	`b=17`
Volem transmetre el text *PLOU I FA SOL*. Cal codificar-lo a la matriu *C*.	`C=codifica("PLOU I FA SOL")`
Creem una matriu *B* amb les mateixes mides que la matriu *C* del codi. La matriu *B* tindrà totes les entrades iguals a *b*.	`ones(rows(C),columns(C))` `B=b*ans`
Encriptem el text codificat: $X = C + B$.	`X=C+B`
Reduïm les entrades a valors entre i 27.	`X=mod(X,28)`
Aquest seria el missatge que hauríem de transmetre. Si algú l'interceptés sembla difícil que en pogués fer res. Provem de descodificar-lo.	`descodifica(X)`
Desxifrem *X*.	`X-B`
Reduïm les entrades a valors entre i 27.	`mod(ans,28)`
Descodifiquem i obtenim el missatge original.	`descodifica(ans)`

Xifratge de Hill

Procediment matemàtic	**Implementació amb Octave**
———	Accedim al *bucket* de la versió en línia d'Octave: https://octave-online.net/bucket~NQzX4rncyNJxKFDYdWc2m
Xifrarem mitjançant el mètode de Hill i la clau és $A = \begin{pmatrix} 1 & -1 & 0 \\ 0 & 2 & 1 \\ 1 & -2 & 1 \end{pmatrix}$	`A=[[1 -1 0];[0 2 1];[1 -2 1]]`
Volem transmetre el text *PLOU I FA SOL*. Cal codificar-lo a la matriu *C*.	`C=codifica("PLOU I FA SOL")`
Encriptem el text codificat: $X = A \cdot C$.	`X=A*C`
Fem que les entrades de la matriu amb el text xifrat estiguin entre i 27.	`X=mod(X,28)`
Aquest seria el missatge que hauríem de transmetre. Si algú l'interceptés, sembla difícil que en pogués fer res. Provem de descodificar-lo.	`descodifica(X)`
Observem que el determinant de la matriu de la clau de xifratge és 3.	`det(A)`
Cerquem *u* tal que $det(A) \cdot u \equiv 1$.	`[g,u,v]=gcd(det(A),28)`
Trobem la clau per desxifrar $u \cdot adj\ (A)^T$ i li reduïm les entrades a valors entre i 27.	`u*adj(A)'` `mod(ans)`
Desxifrem *X*.	`ans*X`
Reduïm les entrades a valors entre i 27.	`mod(ans,28)`
Descodifiquem i obtenim el missatge original.	`descodifica(ans)`

Observacions finals sobre seguretat

Segons el principi de Kerckhoffs, la seguretat dels sistemes criptogràfics no es basa a ocultar el sistema de xifratge, sinó en la dificultat d'aconseguir la clau [6]. En conseqüència, disposar d'un ampli ventall de claus farà que sigui menys probable que l'enemic l'encerti o que, a còpia d'anar provant, la trobi.

La llengua en la qual pot estar escrit el text que volem transmetre, li confereix unes característiques com ara la freqüència de cadascuna de les lletres o de certes paraules en els textos que no tots els sistemes de xifratge oculten. D'aquí neix la criptoanàlisi, és a dir, el conjunt de tècniques per analitzar el text xifrat i intentar deduir-ne la clau [3].

Xifratge per permutacions

Aquest mètode, tal com l'hem plantejat, reordena les tres files de la matriu. Per tant, el total de claus possibles és el nombre de permutacions de tres elements, és a dir $3! = 6$. Això el fa molt insegur davant d'algú que vagi provant claus.

Xifratge de Cèsar

Tal com s'ha plantejat aquí, hi ha tantes possibles claus com desplaçaments es puguin fer, és a dir, 28. Tampoc no sembla un bon sistema, però seria fàcilment millorable. Per exemple, podríem fer el conegut com a mètode de xifratge afí, que aplica a cadascun dels codis c una transformació del tipus $x = a \cdot c + b$. Matricialment, ho podem escriure com:

$$X = A \cdot C + B$$

on A és una matriu diagonal. La matriu B podríem definir-la de diverses maneres, però proposaríem fer-ho com:

$$B = \begin{pmatrix} b_1 & b_1 & \dots \\ b_2 & b_2 & \dots \\ b_3 & b_3 & \dots \end{pmatrix}$$

D'aquesta manera, la clau seria $\left(\begin{array}{ccc|ccc} a_{11} & a_{22} & a_{33} & b_1 & b_2 & b_3 \end{array} \right)$.

Com que el sistema ha de ser invertible, les entrades d'A han de ser coprimeres amb la mida de l'alfabet, és a dir, 28. Així, $\{a_{ii}\}_{i=1}^{3}$ podrà ser qualsevol dels elements de $3, 5, 9, 11, 13, 15, 17, 19, 23, 35, 27\}$. Per a B no hi ha cap mena de restricció [4]. Per tant, el nombre possible de claus serà $11^3 \cdot 28^3 = 29218112$.

Xifratge de Hill

El xifratge de Hill presenta un problema de seguretat per altres motius. El fet que la matriu A de xifratge té 28 possibles entrades en cadascuna de les seves posicions i, per tant, per força bruta es podria provar amb les $28^9 = 10.578.455.953.408$ claus possibles i esperar que, després de desxifrar el missatge, alguna d'elles produís un text comprensible. Hem de

reduir aquest nombre tenint en compte que, d'aquestes possibles claus, força tindrien el determinant amb valor múltiple de 2 o 7. Algunes alternatives podrien ser augmentar la mida de l'alfabet o que aquesta sigui un nombre primer prou gran [7] [8].

Però el risc més important és que algú conegui el text pla C i el xifratge d'aquest, X. Com que $X = A \cdot C$, llavors podria saber la clau fent $A = X \cdot C^{-1}$. Per tal que la matriu C sigui invertible, es pot prendre un menor qualsevol 3×3 de C que tingui aquesta propietat.

Una manera de fer front a aquest problema de seguretat és afegir una transformació de Cèsar afí, és a dir, triar una matriu $B_{3\times n}$ de manera que el xifratge sigui:

$$X_{3\times n} = A_{3\times 3} \cdot C_{3\times n} + B_{3\times n},$$

i la clau estaria formada per les matrius A i B [9].

Conclusions

El conjunt de propostes presentades aquí ens ha servit per il•lustrar a l'alumnat de segon de batxillerat les possibles aplicacions de les matrius. Cada vegada són més freqüents la contextualització dels continguts d'aprenentatge i l'aprenentatge basat en problemes. L'alumnat no sol conèixer gaires aplicacions de les matemàtiques més enllà d'emprar-les en altres matèries, fet que redueix la concepció que alguns dels estudiants poden tenir d'elles a quelcom purament acadèmic.

En aquest sentit, no se solen exposar aplicacions de les matrius més enllà de l'estudi de sistemes d'equacions lineals i la criptografia ens dona un exemple d'aplicació de les matemàtiques. El problema principal que ens podem trobar amb el nostre alumnat és la manca d'experiència prèvia en criptografia i seguretat i, per tant, l'esforç addicional que cal fer per situar l'objecte d'estudi i la seva terminologia.

El principal repte que s'albira és plantejar el tema de l'estudi de les matrius com un aprenentatge basat en problemes (ABP). És a dir, podem crear la unitat didàctica de les matrius tot plantejant el repte de xifrar i desxifrar textos i anar fent exercicis d'operacions de matrius, càlcul de determinant i rang, deducció de la inversa, resolució de sistemes d'equacions..., tot utilitzant els diferents mètodes de xifratge exposats aquí.

Finalment, malgrat que els tres mètodes de xifratge presentats aquí poden no ser prou segurs ni eficients des del punt de vista de les operacions de càlcul que impliquen, hem gaudit d'una experiència d'aplicació de l'àlgebra lineal.

Annex. El codi font que ens ajuda a treballar

Per fer més àgil i clar el desenvolupament d'aquesta activitat s'han definit algunes funcions en un fitxer de scripts d'Octave. Tot seguit hi ha els codis QR per accedir-hi o descarregar-los i es dona la transcripció de les funcions desenvolupades.

Octave *online bucket*	**Descàrrega dels scripts**

```
## Funcions per dur a terme la pràctica de
## Criptografia de Batxillerat

1;

## La funció codifica rep com a argument una variable de tipus text
## i retorna una matriu amb 3 files on va col·locant el text d'acord
## amb la codificació de l'alfabet establerta

function matriuDeCodis=codifica(pEntrada)
    alfabet=["ABCDEFGHIJKLMNOPQRSTUVWXYZ. "];
    n=length(pEntrada);
    codis=[0,1,2,3,4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20,21,22,23,24,25,26,27];
    for i=1:n
    matriuDeCodis(1+mod(i-1, 3), 1+idivide(i-1, 3))= codis(findstr(alfabet, pEntrada(i)));
    endfor
    if(mod(n, 3)==1)
                    matriuDeCodis(2, 1+idivide(n-1, 3))= codis(findstr(alfabet, " "));
                    matriuDeCodis(3, 1+idivide(n-1, 3))= codis(findstr(alfabet, " "));
    endif
    if(mod(n, 3)==2)
                    matriuDeCodis(3, 1+idivide(i-1, 3))= codis(findstr(alfabet, " "));
    endif
endfunction

## La funció descodifica rep com a argument una matriu de 3files amb
## els codis i retorna un text net, és a dir, canviant el codi de cada
## símbol alfanumèric per ## el símbol mateix
function textNet=descodifica(pEntrada)
    alfabet=["ABCDEFGHIJKLMNOPQRSTUVWXYZ. "];
    dim=rows(pEntrada)*columns(pEntrada);
    codis=[0,1,2,3,4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20,21,22,23,24,25,26,27];
    for i=1:dim
                    textNet(i)=alfabet(1+pEntrada(i));
    endfor
endfunction

## La funció cofactor rep com a arguments una matriu quadrada pMatriu
## i dos índexs (pI i pJ). Retorna la matriu de cofactors
function C=cofactor(pMatriu, pI, pJ)
          m=rows(pMatriu);
          n=columns(pMatriu);
          for i=1:m
                    if(i!=pI)
                              if(i<pI) p=i;
                              elseif(i>pI) p=i-1;
                              endif
                              for j=1:n
                                        if(j<pJ) q=j;
                                        elseif(j>pJ) q=j-1;
                                        endif
                                        if(j!=pJ) M(p,q)=pMatriu(i,j);
                                        endif
                              endfor
                    endif
          endfor
          C=(-1)^(pI+pJ)*det(M);
endfunction

## La funció adjunta rep per argument una matriu i retorna la seva adjunta
function adjunta=adj(pMatriu)
          m=rows(pMatriu);
          n=columns(pMatriu);
          for i=1:m
                    for j=1:n
                              adjunta(i,j)=cofactor(pMatriu, i, j);
                    endfor
          endfor
endfunction
```

Bibliografia

[1] Juher, D. (2004). *L'art de la comunicació secreta. El llenguatge de la criptografia*. Barcelona: Llibres de l'Índex.
[2] Taranilla, C. (2017). *Los lenguajes secretos a lo largo de la historia*. Còrdova: Guadalmazán.
[3] Domingo Ferrer, J., Herrera Joancomartí, J. (1999). *Criptografia per als serveis telemàtics i el comerç electrònic*. Barcelona: Edicions de la Universitat Oberta de Catalunya.
[4] Koblitz, N. (1987). *A Course in Number Theory and Cryptography*. Nova York: Springer.
[5] Hill, L.S. (1929). Cryptography in an Algebraic Alphabet. *The American Mathematical Monthly*, 36, 6, juny-juliol, 306-312.
[6] Kerckhoffs, A. (1883). La cryptographie militaire. *Journal des Sciences Militaires*, ix, 5-38.
[7] Toorani, M., Falahati, A. (2009). A secure cryptosystem based on affine [en línia], 14 setembre 2009. A: https://onlinelibrary.wiley.com/doi/pdf/10.1002/sec.137.
[8] Saxena, A., Iohiya, H., Patidar, K. (2017). A Novel Technique of Hill Cipher for Evaluation of Non-invertible key matrix. *International Journal of Advance Research in Science and Engineering*, 6, 1, p. 856-862.
[9] Sharma, N., Chirgaiya, S. (2013). «A Review of Modern Hill Cipher Techniques». *International Journal for Scientific Research & Development*, 1, 10, ISSN (online): 2321-0613.