MSEL
Modelling in Science Education and Learning

Modelling in Science Education and Learning
Volume 16 (1), 2023 doi: 10.4995/msel.2023.18520.
Instituto Universitario de Matemática Pura y Aplicada
Universitat Politècnica de València

Una propuesta de práctica informática: aritmética modular y encriptación de imágenes

A proposal for computer science practice: modular arithmetic and image encryption

Fernando Giménez, Juan Antonio Monsoriu
Universitat Politècnica de València
fgimenez@mat.upv.es, jmonsori@fis.upv.es

Abstract

En este trabajo se presenta una experiencia docente diseñada a partir de una práctica de ordenador y un trabajo grupal asociado, sobre la aplicación de la aritmética modular a la encriptación/desencriptación de imágenes digitales. El procedimiento está basado en el algoritmo de cifrado de Hill. Aunque el objetivo final es que los alumnos programen en Matlab las funciones necesarias para implementar dicho procedimiento, las utilicen con ejemplos y valoren su efectividad, también pueden utilizar previamente un par de laboratorios virtuales (app designer) que se han diseñado al respecto

This paper presents a teaching experience designed on the basis of a computer practice, and an associated group work, on the application of modular arithmetic to the encryption/decryption of digital images. The procedure is based on the Hill encryption algorithm. Although the final objective is for students to program in Matlab the necessary functions to implement this procedure, use them with examples and assess their effectiveness, they can also previously use a virtual laboratory (app designer) that has been designed for this purpose

Palabras clave: Encriptación, desencriptación, aritmética modular, cifrado de Hill, imagen digital, Matlab app designer, laboratorio virtual.
Keywords: Encryption, decryption, modular arithmetic, Hill encryption, digital imaging, Matlab, app designer, virtual lab.

1. Introducción

En la era digital en que vivimos es importante el tratamiento seguro de la información. De vez en cuando van apareciendo noticias que hacen referencia a intromisiones y caídas de sistemas informáticos por ataques externos. La criptografía es un campo que a lo largo de la historia ha ido cobrando cada vez mayor importancia de cara a proteger la información (Gómez, 2010). En este trabajo abordaremos el intercambio seguro de imágenes digitales entre un emisor y un receptor a partir de un procedimiento del álgebra modular basado en el algoritmo de cifrado de Hill (Zuñiga et al., 2019). Se ha diseñado una práctica informática y un trabajo grupal que puede darse en asignaturas de Cálculo Numérico en ingenierías con el objetivo de:

- Conocer el álgebra matricial que está detrás de las imágenes digitales,
- estudiar el método de cifrado de Hill,
- aplicar dicho método a la encriptación/desencriptación de imágenes,
- experimentar con ejemplos de imágenes y valorar la efectividad del método,
- proponer formas de mejorar los resultados,
- generar las funciones de Matlab que implementen dicho método (trabajo grupal).

La experiencia docente mostrada en este trabajo ha sido llevada a cabo durante el curso 2021-2022 en la asignatura Complementos de Métodos Matemáticos para Nivelación del Máster de Ingeniería Industrial con un total de 28 alumnos. Puede darse en cualquier curso de cálculo numérico de las ingenierías.

2. Metodología

En lo que sigue presentaremos con detalle la metodología que se ha diseñado para llevar a cabo nuestra propuesta pedagógica.

2.1. Aritmética modular y cifrado de Hill

Consideremos el grupo aditivo de los enteros módulo m

$$\mathbb{Z}_m = \frac{\mathbb{Z}}{m\mathbb{Z}} = \{0, 1, 2, \ldots, m-1\}$$

con las operaciones suma y producto (módulo m). ($a \in \mathbb{Z}_m$) tiene inverso modulo m si existe un número natural en $\mathbb{Z}_m$ que multiplicado por éste de 1. Se puede demostrar que a tiene inverso m'odulo m si es coprimo con respecto a m, es decir, si a y m no tienen factores comunes.

En el conjunto de las matrices cuadradas de orden N con coeficientes en $\mathbb{Z}_m$

$$\mathcal{M}_{N\times N}(\mathbb{Z}_m) = \{(a_{ij}) : a_{ij} \in \mathbb{Z}_m\}$$

podemos considerar la suma y producto de matrices y el producto por un escalar en$\mathbb{Z}_m$. Se dice que una matriz $A \in \mathcal{M}_{N\times N}(\mathbb{Z}_m)$ tiene inversa si existe una matriz $B \in \mathcal{M}_{N\times N}(\mathbb{Z}_m)$ tal que

$$AB = BA = I \pmod{m}$$

Es conocido que una matriz tiene inversa si y solo si su determinante módulo m es no nulo y coprimo con respecto a m. El cifrado de Hill es un sistema de cifrado de sustitución poligráfica

y originalmente tiene su aplicación a texto, donde cada letra se sustituye por su ordinal en el abecedario y se genera a partir de una matriz cuadrada con coeficientes en $\mathbb{Z}_m$ donde $m$es el número total de caracteres es el alfabeto en cuestión. En la operación básica de cifrado, el texto a encriptar es un vector columna x de N términos módulo m, y la llave de encriptación es una matriz A invertible en $\mathbb{Z}_m$ y el resultado de la operación es $y = Ax(\text{mod } m)$ que da lugar al texto codificado. De esta forma, para desencriptar y se procede al camino inverso, es decir $x = A^{-1}y(\text{mod } m)$.

2.2. Aplicación a la encriptación de imágenes

Una imagen digital es una representación bidimensional de una imagen a partir de una matriz numérica. En concreto, una imagen de color RGB se representa por tres matrices bidimensionales, correspondientes a los planos en escala de rojos (R), verdes (G) y azules (B). Al respecto pueden consultarse la referencia (González et al., 2009). Para nuestro propósito trabajaremos con matrices en $\mathcal{M}_{n_1\times n_2}(\mathbb{Z}_{256})$ donde $n_1 \times n_2$ es el tamaño de la imagen (número de pixeles de la imagen dada).

Para encriptar una matriz $W = (w_{ij}) \in \mathcal{M}_{n_1\times n_2}(\mathbb{Z}_m)$ se transforma en un vector columna de longitud $k = n_1 \times n_2$

$$x = \begin{bmatrix} W_1^T \\ W_2^T \\ \vdots \\ W_{n_1}^T \end{bmatrix} \tag{1}$$

donde W_i es el i-ésimo vector fila de W y después proceder como arriba. En el proceso de decodificación una vez obtenido el vector x se reconstruye la matriz W usando

$$w_{ij} = x_{(i-1)n_2+j},\ i = 1, 2, \ldots, n_1 \ \&\ j = 1, 2, \ldots, n_2$$

Se podría aplicar la codificación básica de un bloque a partir de una única matriz de orden m, pero hay que tener en cuenta que como la gran mayoría de las fotografías se componen de matrices de tamaños muy grandes no es demasiado eficaz ni rápido trabajar con matrices llave de dicho tamaño. Tampoco es necesario que las entradas de las matrices pertenezcan a $\mathbb{Z}_{256}$: basta con que pertenezcan a $\mathbb{Z}_m$ con $m \ll 256$ para evitar problemas con el redondeo cuando se trabaja con el ordenador. La solución pasa por la descomposición del vector en vectores más pequeños de tamaños iguales a

$$x = \begin{bmatrix} \bar{x}_1 \\ \bar{x}_2 \\ \vdots \\ \bar{x}_l \end{bmatrix}$$

y luego realizar el cifrado "por bloques"

$$x = \begin{bmatrix} \bar{y}_1 \\ \bar{y}_2 \\ \vdots \\ \bar{y}_l \end{bmatrix}$$

donde

$$\bar{y}_1 = A\bar{x}_1, \quad \bar{y}_2 = A\bar{x}_2, \quad \ldots \bar{y}_l = A\bar{x}_l (\text{mod } 256).$$

Dicho esto, el procedimiento anterior presenta el inconveniente de que si alguno de los vectores $\bar{x}_j$ es el vector nulo entonces lo mismo le ocurre a $\bar{y}_j$ y en ese caso no se ha producido encriptación. Una posible forma de evitar esto es utilizar además un vector v no nulo para la codificación $\bar{y}_j = A\bar{x}_j + v (\text{mod } 256)$ y la decodificación sería entonces $\bar{x}_j = A^{-1}(\bar{y}_j - v) (\text{mod } 256)$.

El procedimiento puede mejorarse utilizando las matrices $A, A^2, A^3, \ldots, A^l \text{ mod } m)$ para cada uno de los bloques.

2.3. La práctica informática y el trabajo

La práctica está diseñada de la siguiente forma: los estudiantes disponen de un documento en pdf que recoge los pasos que hay que seguir, junto con dos laboratorios virtuales (app designer de Matlab) que se ha diseñado para que puedan experimentar en la propia aula informática y la propuesta de trabajo grupal (Attaway, 2019 y Matlab App Designer). Se trata de:

1. Antes de la realización de la práctica los alumnos deben de leer y estudiar la parte de la práctica que presenta el método del cifrado de Hill y como trabaja Matlab con las imágenes digitales y formar los grupos de trabajo.
2. Al comienzo de la práctica el profesor repasa de forma breve lo anterior y les indica como trabajar con el laboratorio virtual.
3. Se estudian varios ejemplos de encriptación de fotografías para ver y analizar los resultados de la encriptación para cada uno de los métodos propuestos en el apartado 1.1.
4. El profesor presenta el trabajo a realizar consistente en la programación de varias funciones de Matlab que implementen los métodos estudiados
5. Los alumnos comienzan a elaborar el trabajo que acabaran más tarde y lo enviaran entonces al profesor para su corrección.

2.4. Los laboratorios virtuales de encriptación y desencriptación

La Figura 1 recoge un ejemplo de aplicación de la app designer code.mlapp.

Figura 1: Ejemplo de la aplicación code.mlapp con método 1.

Las entradas son:

- Tipo de encriptación: método 1 (sin vector auxiliar no nulo y una única matriz), método 2 (con vector auxiliar no nulo y una única matriz) y método 3 (con vector auxiliar no nulo y matrices A,A^2,A^3,...).
- Matriz: Matriz llave.
- m: Valor máximo de las entradas de la matriz llave
- Off/On: si se selecciona las imágenes se muestran con la aplicación por defecto del ordenador
- Ayuda: Abre un pequeño manual de uso.
- Nombre de la imagen codificada
- Seleccionar foto y CODIFICAR: cuando se pulsa se ejecuta la app. Al acabar se puede elegir donde guardar la foto codificada.

La app *designer decode.mlapp* tiene el diseño y las entradas similares a las de *code.mlapp*.

Si se aplica el método 1 con una matriz invertible de orden 6 a la clásica fotografía lenna.jpg se observa que se obtienen buenos resultados (ver Figura 1). Sin embargo, si se aplican los métodos 1 y 2 a la imagen de un código de barras los resultados finales dejan bastante que desear (ver 2 (a), (b) y (c)). El método 3 si proporciona muy buenos resultados (Figura 2 (d)). Incluso con una imagen completamente negra (Figura 3 (a) y (b)) el procedimiento es muy eficiente. Cuando se modifica, aunque sea ligeramente, alguna de las entradas de la matriz llave, al decodificar no es posible recuperar la imagen original. La Figura 3 (c) muestra la imagen decodificada usando la matriz llave con la entrada (1,1) con valor 14 en vez de 16 que es el original.

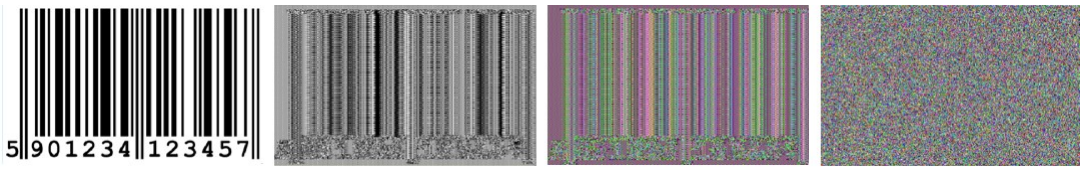

Figura 2: (a) Imagen original, (b) imagen codificada método 1, (c) imagen codificada método 2, (d) imagen codificada método 3.

Figura 3: (a) Imagen original, (b) imagen codificada método 3, (c) Imagen decodificada con matriz llave incorrecta.

3. Resultados

Durante la sesión práctica se pudo constatar una buena acogida por parte de los alumnos que, según nos dijeron, se divirtieron mucho probando mediante el laboratorio virtual como afectaba el método de encriptación a los diversos ejemplos que fueron ensayando. Tras la elaboración y posterior evaluación de los trabajos, en la siguiente práctica informática se procedió a llevar a cabo una pequeña encuesta para valorar los resultados. La Tabla 1 muestra la breve encuesta que se les paso y la Figura 4 los resultados obtenidos.

Valora de 1 (mínimo) a 5 (máximo) los siguientes apartados:					
Me ha servido la información recogida en el documento de la práctica	1	2	3	4	5
El laboratorio virtual ha satisfecho mis expectativas	1	2	3	4	5
El trabajo propuesto ha sido adecuado	1	2	3	4	5
En general me ha gustado la experiencia y la considero útil	1	2	3	4	5

Tabla 1: Encuesta de satisfacción de la práctica de encriptación de imágenes

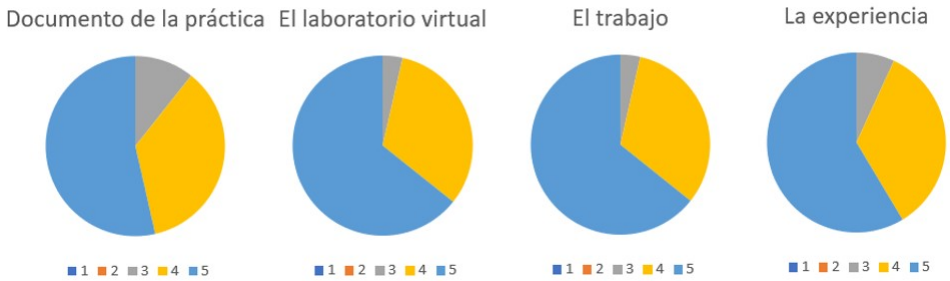

Figura 4: Resultados de la encuesta.

4. Conclusiones

Los alumnos han valorado muy positivamente la práctica y el correspondiente trabajo posterior tal y como muestran no solo las encuestas sino las impresiones recibidas por los profesores durante su realización. En su mayoría lo ven como una aproximación útil y muy interesante al tema de la seguridad informática de la información y su vinculación con la matemática discreta.

Agradecimientos

Los autores agradecen al Instituto de Ciencias de la Educación de la Universitat Politècnica de València por su ayuda al Equipo de Innovación y Calidad Educativa MSEL.

Referencias

- Attaway, S. (2019).
  MATLAB: A Practical Introduction to Programming and Problem Solving.
  Ed. Butterworth Heinemann.
- De la Fuente, E. (2015).
  Método grupal para el aprendizaje de la matemática.
  Praxis Investigativa ReDIE. Vol. 7, num. 13, 117–126.
- Gómez, J. (2010).
  Matemáticos, espías y piratas informáticos (Codificación y Criptografía).
  España, RBA Coleccionables S.A.
- González, R. C., Woods, R. E., Eddins, S. E. (2009).
  Digital image processing using Matlab.
  González, Woods, & Eddins.
- Matlab App Designer, (2022).
  https://www.mathworks.com/help/matlab/app-designer.html
- Vidal, A., Boigues, F. J., Estruch, V. D. (2017).
  La importancia de la sesión grupal en la clase inversa: Trabajos colaborativos en una asignatura de Matemáticas de Grado durante el curso 2016-2017.
  eXIDO 17.
- Zuñiga, G., López, F. E., Quenta, R. F. (2019).
  Criptografía con matrices, el cifrado de Hill. Criptografía en Algebra Lineal.