Artículo Original / Original Research

Ciencias Matemáticas, Vol. 36, No. Único, 2022-2023, Pag. 57-69
Recibido (*Received*): 25-04-2024, Revisado (*Reviewed*): 22-05-2024
Aceptado (*Accepted*): 27-06-2024, En línea (*Online*): 21-10-2024

Propuesta didáctica para la enseñanza de matrices y conceptos asociados mediante el cifrado de Hill

Didactic proposal for the teaching of matrices and associated concepts through Hill's cipher

Guillermo Enrique Ramírez Montes

Resumen El cifrado y la codificación a lo largo de la historia han sido herramientas importantes para transmitir mensajes de manera segura. En particular, el cifrado de palabras puede usarse como un recurso didáctico para la enseñanza con significado extra-matemático de conceptos matriciales fundamentales, que hacen parte de un curso usual de Álgebra Lineal. Este artículo tiene como objetivo describir el diseño de una propuesta didáctica para la enseñanza con significado extra-matemático de los conceptos de dimensión de una matriz, producto matricial, matriz inversa y determinante de una matriz, a partir del modelo del cifrado de Hill. Se presentan las conexiones que se pueden hacer entre el cifrado de Hill y cada uno de los conceptos anteriores, se propone un ejemplo de tarea matemática a abordar en la clase de Álgebra Lineal con el uso de la hoja de Excel para el trabajo de los conceptos, y se reflexiona sobre los aportes de dicha propuesta para el aprendizaje matemático del estudiantado.

Palabras Clave: cifrado de Hill, hoja de cálculo de Excel, matrices, propuesta didáctica.

Abstract *Encryption and coding throughout history have been important tools for transmitting messages securely. In particular, the encryption of words can be used as a didactic resource for the teaching with extra-mathematical meaning of fundamental matrix concepts, which are part of a usual Linear Algebra course. The objective of this article is to describe the design of a didactic proposal for the teaching with extra-mathematical meaning of the concepts of dimension of a matrix, matrix product, inverse matrix and determinant of a matrix, based on Hill's cipher model. The connections that can be made between Hill's cipher and each of the previous concepts are presented, an example of a mathematical task to be addressed in the Linear Algebra class with the use of the Excel sheet for the work of the concepts is proposed, and the contributions of this proposal for the mathematical learning of the students are reflected upon.*

Keywords: *Hill cipher, Excel spreadsheet, matrices, didactic proposal.*

Mathematics Subject Classification: 97, 97-11, 68, 68P25, 15.

Departamento de Educación Matemática, Universidad de Costa Rica, San José, Costa Rica. Email: guillermo.ramírez_m@ucr.ac.cr

Editado por (*Edited by*): Damian Valdés Santiago, Facultad de Matemática y Computación, Universidad de La Habana, Cuba.

Citar como: Ramirez Montes, G.E. (2024). Propuesta didáctica para la enseñanza de matrices y conceptos asociados mediante el cifrado de Hill. *Ciencias Matemáticas*, 36(Único), 57–69. DOI: https://doi.org/10.5281/zenodo.13961116. Recuperado a partir de https://revistas.uh.cu/rcm/article/view/9240.

Introducción

Las matrices juegan un papel muy importante en la Matemática y el Álgebra Lineal, en particular, pues son objetos matemáticos esenciales a partir de los cuales se desarrolla la teoría en un curso usual de Álgebra Lineal. Estos objetos matemáticos aparecen en diversos contextos del día a día, por ejemplo, las tablas y cuadros estadísticos, las bases de datos o el procesamiento digital de imágenes, donde la intensidad de cada pixel se puede ver como la entrada de una matriz.

No se puede dejar de lado que la enseñanza de los diferentes objetos matemáticos y conceptos asociados que se abordan en el Álgebra Lineal resultan abstractos y generan dificultades en estudiantes universitarios, en particular, estudiantes de Ingeniería y otras áreas cuya formación a fin no es la Matemática o la Enseñanza de la Matemática [5]. Tales dificultades son evidenciadas en el estudiantado desde sus primeras clases de Álgebra Lineal, al intentar comprender conceptos y procedimientos asociados, por ejemplo, a las operaciones con matrices [9].

Ante el escenario anterior surge la necesidad de buscar estrategias didácticas de enseñanza que ayuden a eliminar la abstracción asociada por los estudiantes hacia diferentes objetos matemáticos del Álgebra Lineal, lo que incluye conceptos y procedimientos matemáticos que se estudian al referirse a un determinado objeto matemático.

En este artículo se describe el diseño de una propuesta didáctica orientada a dar significado extra-matemático al objeto matemático denominado matriz y, en particular, a los conceptos de dimensión, producto matricial, matriz inversa y determinante de una matriz.

Para esto, se propone el uso de una herramienta histórica de transmisión de la información, como lo es la criptografía, donde se utiliza el modelo de cifrado de Hill para dar significado extra-matemático a los diferentes conceptos referidos. Además, se hace uso de la hoja de cálculo de Excel como recurso para que los estudiantes puedan validar sus propios modelos de cifrado de Hill, reflexionando sobre las ventajas de esta herramienta digital en el proceso de trabajo de la tarea matemática que fundamenta la propuesta. Adicionado a ello, se utiliza el trabajo en grupo y la discusión colectiva, como parte de las orientaciones recomendadas de gestión de aula en la clase de Matemática a nivel universitario.

La propuesta surge como parte de la experiencia adquirida por el autor al impartir cursos de Matemática Aplicada en la Universidad de Costa Rica, entre estos, el curso de Álgebra Lineal dirigido a carreras de Ingeniería y otras áreas. En este curso, el autor ha trabajado propuestas didácticas para la enseñanza del Álgebra Lineal, con carácter formativo, para otros conceptos no abordados en este artículo, y bajo el marco de la modelación matemática educativa, tomando como punto de referencia el conocimiento matemático previo que poseen los estudiantes sobre conceptos y procedimientos asociados al Álgebra Lineal.

La propuesta en este artículo plantea una visión diferente a lo ya trabajado pues, en lugar de hacer modelación matemática, propone que el estudiante parta de un modelo matemático que pueda replicar mediante el componente histórico como elemento de significado contextual.

Relevancia del estudio

De acuerdo con las contribuciones existentes sobre enseñanza y aprendizaje de conceptos matriciales que se recogen en la literatura [4], este estudio se distingue por: 1) el uso en conjunto del contenido matemático, el contexto extra-matemático y el recurso tecnológico para favorecer el aprendizaje significativo de las matrices y conceptos asociados; 2) el diseño de una tarea matemática abierta, es decir, que promueve en el estudiante diversidad de respuestas a partir de su creatividad y el razonamiento matemático; 3) y socializar una propuesta didáctica enfocada no solo en el diseño de la tarea matemática, sino en una gestión pertinente de la propuesta, que considera un rol activo de la persona docente como mediadora durante el monitoreo y la discusión colectiva, y un rol activo del estudiante como sujeto que reflexiona sobre su aprendizaje de manera individual y colectiva.

De esta forma, este estudio contribuye al diseño e implementación de propuestas didácticas centradas en la enseñanza de conceptos matriciales en contextos significativos, entendidos estos últimos conforme a la literatura revisada, donde el contexto extra-matemático y el recurso tecnológico son elementos a considerar para favorecer este aprendizaje significativo de los conceptos en el estudiante.

1. Estudios didácticos entorno a la enseñanza de conceptos matriciales

Si bien en las últimas dos décadas los estudios en América Latina, ligados al tratamiento didáctico de tópicos del Álgebra Lineal, se han enfocado en propuestas para trabajar conceptos asociados a las temáticas de espacios vectoriales, transformación lineal y autovalores [4], es posible encontrar algunos estudios recientes orientados al tratamiento didáctico de conceptos asociados a la temática de Matrices.

Por un lado, Bedregal-Alpaca y colaboradores [3] realizan una secuencia didáctica con estudiantes de Ingeniería, fundamentada en la Resolución de Problemas como enfoque teórico, en el contexto de artículos de oficina. La investigación procuró dar sentido al cálculo matricial mediante el estudio contextualizado del tema de operaciones con matrices. Los autores trabajan bajo la metodología de aprendizaje cooperativo apoyado con el software matemático MATLAB para la realización de cálculos. Además, estos autores proponen el uso de matrices *precio de venta-fecha por mes* y *precio de venta-artículo* para que, a partir de estas dos matrices, se le dé significado extra-matemático a la matriz producto.

Como parte de los resultados de este estudio, los autores destacan que la mayoría de los estudiantes refieren que la propuesta contribuyó en la comprensión del concepto de multiplicación de matrices y a desarrollar su creatividad y capacidad de expresión. Bedregal-Alpaca y colaboradores [3] también destacan la importancia de trabajar los conceptos del Álgebra Lineal con contextos extra-matemáticos pues “es necesario considerar, en el proceso de enseñanza y aprendizaje, situaciones en las cuales el estudiante pueda sistemáticamente moverse entre lo concreto y lo abstracto; por lo tanto, entre los conceptos algebraicos y los procesos de dar sentido” (p. 125).

En la misma línea de operaciones con matrices, Galindo y colaboradores [9], al detectar la falta de compresión en las operaciones matriciales (suma, resta, multiplicación, producto escalar) por parte de estudiantes de licenciatura en Matemáticas, proponen trabajar la herramienta didáctica del Objeto de Aprendizaje. La propuesta se fundamenta en el modelo de Análisis, Diseño, Desarrollo, Implementación y Evaluación.

Los autores proponen actividades enfocadas en manipular imágenes digitales pixeladas, a medida que se observa la representación matricial de dicha imagen y, contrariamente, operar matrices para ver resultados sobre las imágenes asociadas. Los autores destacan la motivación de los estudiantes, quienes consiguen satisfactoriamente representar y relacionar las matrices con imágenes digitales.

Por otra parte, Kosasih y colaboradores [12] trabajan en un módulo didáctico para el tema de determinantes, para promover el pensamiento crítico a partir del aprendizaje basado en proyectos. La construcción del módulo se fundamenta en tres secciones principales. Estas secciones consideran elementos curriculares como: 1) el programa del curso de Álgebra Lineal y herramientas de aprendizaje para los conceptos trabajados, 2) la descripción del módulo, y 3) material de lectura, evaluación y de trabajo individual del estudiante. Como parte de los resultados, Kosasih y colaboradores [12] destacan que el módulo promueve el pensamiento crítico en los estudiantes, evidenciándose habilidades como la interpretación, análisis, evaluación, inferencia y explicación de resultados.

En la línea del uso del recurso digital, El-Gebeily y Yushau [6] proponen dos caminos diferentes para usar la hoja de cálculo de Excel en el estudio de los sistemas de ecuaciones lineales, matriz inversa y la programación lineal. En primer lugar, los autores proponen el uso de la herramienta *Solver* de Excel para determinar cálculos asociados al conjunto solución de un sistema lineal de ecuaciones o determinar la matriz inversa de una matriz dada; y en segundo lugar, recurren a funciones básicas de Excel directamente, sin usar la función *Solver*. Los autores enfatizan la importancia de la hoja de Excel como un recurso de fácil manejo, que permite visualizar gráficamente las soluciones de sistemas de ecuaciones; además de ayudar a que los estudiantes verifiquen sus resultados y exploren más los conceptos en estudio.

Ramírez Montes [17] utiliza la hoja de Excel para proponer una tarea de modelación matemática en el contexto de claves de acceso bancario, con estudiantes de Ingeniería y otras áreas. Aunque la propuesta del autor estuvo enfocada en la comprensión del concepto de conjunto generador y conceptos asociados, el resultado final solicitado a los estudiantes fue la confección de una matriz de clave dinámica en Excel, a la cual tuvieron que dar significado extra-matemático en términos de vectores generados por un conjunto generador. Este autor destaca el uso de la hoja de Excel para crear matrices basadas en funciones incorporadas en este software. Además, reflexiona sobre el hecho de usarlo para movilizar los conceptos y procedimientos matemáticos intencionados, dado que podría haber estudiantes que logren el producto solicitado sin movilizar dichos entes matemáticos.

En el contexto de la criptografía simétrica con software especializado para el procesamiento de imágenes, Jacques-García y colaboradores [11] proponen una propuesta didáctica usando el cifrado de Hill y el software especializado *Krynapsis*, para el estudio de la matriz inversa y con estudiantes de informática de un curso de Álgebra de Lineal. Dicho estudio procuró diagnosticar la utilidad de este software y su impacto en el proceso de enseñanza. Los autores describen el funcionamiento del software para el proceso de encriptación y desencriptación de imágenes donde:

> "Al seleccionar el menú correspondiente a la encriptación de imágenes digitales, el alumno puede seleccionar las opciones de encriptar una imagen y desencriptar una imagen. En la primera opción el alumno puede seleccionar una imagen desde su dispositivo móvil y encriptarla. La aplicación genera de forma automática una matriz o llave para llevar a cabo este proceso. En la segunda opción el alumno ingresa los elementos de la matriz inversa modular para que la aplicación desencripte la imagen de forma correcta." (p. 7)

2. Resolución de Problemas, enseñanza efectiva y aprendizaje significativo en la clase de matemática

La Resolución de Problemas es un enfoque de enseñanza que ha tomado fuerza dentro de la investigación en educación matemática, debido a que promueve en el estudiante el desarrollo de competencias para la vida [7]. Este enfoque se puede entender como una forma de aproximación sistemática donde el estudiante debe desarrollar un proceso cognitivo para conceptualizar un problema, diseñar estrategias para resolverlo y evaluar las estrategias y respuestas obtenidas [1].

Una de las ventajas de la Resolución de Problemas, según Albay [1], es que promueve el trabajo en grupo, pues enfatiza la cooperación y las interacciones entre estudiantes del mismo grupo como un medio para que surjan variedad de ideas, las cuales ayuden a sobrepasar las fases que componen al proceso de resolver el problema.

Esas fases son descritas por Polya [16] en su libro *Cómo plantear y resolver problemas*, cuyo contenido establece la existencia de cuatro fases a considerar, estas son:

1.COMPRENDER EL PROBLEMA: El estudiante, para comprender el problema, debe poder reconocer los datos, la incógnita y las condiciones del problema. Polya [16] divide esta fase en dos etapas.

La primera es la etapa de *Familiarizarse con el problema*, donde se da un primer acercamiento al problema por parte de los estudiantes, en el sentido de que se entienda de manera general. La segunda etapa es *Trabajar para una mejor comprensión*, donde los estudiantes vuelven a leer el problema e intentan comprender sus distintas partes; identifican el tipo de problema que se está trabajando, los datos que se disponen y los que faltan.

2.CONCEBIR UN PROBLEMA: En esta fase los estudiantes recurren a sus conocimientos previos para empezar a idear un plan o estrategia que permita resolver el problema. Polya [16] sugiere que la persona docente debe de ayudar a que los estudiantes logren alcanzar esas estrategias o ideas cuando no encuentran cómo empezar, pero sin referir las estrategias posibles a seguir; para lo cual es importante que la persona docente plantee al estudiante preguntas guía, previamente elaboradas.

3.EJECUTAR EL PLAN: En esta fase los estudiantes ponen a su disposición todos los recursos, conceptos y procedimientos matemáticos que haya aprendido, en su formación formal y no formal, para ejecutar su plan de resolución. La persona docente debe monitorear constantemente el trabajo de los estudiantes, verificando que estos estén avanzando. A medida que los estudiantes ejecutan su plan podrían pensar otras formas de resolver el problema, lo cual sería consecuencia de que los estudiantes movilizen competencias matemáticas que ponen en práctica su razonamiento matemático [1]. En ese sentido, la persona docente podría plantear preguntas guía durante su monitoreo que promuevan la observación de otras estrategias de resolución del problema.

4.EXAMINAR LA SOLUCIÓN: La resolución de un problema no termina al ejecutar un plan, pues se debe tener una visión retrospectiva del problema, en el sentido de que es importante revisar la solución obtenida para garantizar que responda a la situación planteada en el problema. Los posibles errores del plan, nuevas o más fáciles formas de resolver un problema o una mejor comprensión del proceso de solución, son algunas de las ventajas que se tiene al revisar lo ya realizado. Esto puede ayudar a potenciar las habilidades de resolución que tienen los estudiantes.

Hasta aquí se evidencia que la Resolución de Problemas no debe ser vista como un proceso donde solo tiene importancia el trabajo realizado por los estudiantes, sino también las decisiones que toma la persona docente para que ese trabajo de los estudiantes fluya. En ese sentido, la Resolución de Problemas invita a la persona docente a realizar una enseñanza eficiente que promueva un aprendizaje significativo en el estudiante.

Según Anthony y Walshaw [2], una enseñanza eficiente es aquella donde los estudiantes tienen oportunidades de 1) darle sentido a una situación planteada, tanto de forma individual y grupal; 2) tener espacios de diálogo enfocados en la argumentación matemática; 3) trabajar tareas matemáticas previamente diseñadas por la persona docente, donde se ofrezcan experiencias de aprendizaje que le permitan a los estudiantes razonar sobre conceptos matemáticos importantes y las relaciones entre estos; 4) realizar conexiones entre diferentes estrategias de resolución de un problema, entre diferentes conceptos matemáticos, y entre la matemática y la vida cotidiana; 5) trabajar con diferentes herramientas y con representaciones matemáticas que favorezcan el razonamiento matemático del estudiante.

En esta misma línea, pero hablando de aprendizaje eficiente, Schukajlow y Blum [19] refieren que la persona docente promueve un aprendizaje eficiente cuando 1) coloca problemas matemáticos que requiera por parte de los estudiantes el construir diferentes soluciones; 2) los estudiantes discuten sus estrategias individuales de resolución con otros estudiantes; 3) los estudiantes comparan y contrastan diferentes soluciones. Estos autores también refieren la importancia de la guía que debe ofrecer la persona docente al estudiante, mediante iniciativas que consideren que el estudiante plantee y responda a sus propias preguntas, que haga relaciones entre su conocimiento previo y el conocimiento nuevo, y reflexione sobre las estrategias usadas en relación a otras.

Al promoverse los principios anteriores se promueve automáticamente el aprendizaje significativo, entendido como "un proceso por medio del cual el estudiante, para aprender, relaciona los conceptos nuevos con los conceptos que posee, así como los conceptos nuevos con la experiencia que tiene" [13], p. 142. Del cuarto principio de enseñanza eficiente, referido por Anthony y Walshaw [2], se desprende que cuando la persona docente ofrece al estudiante oportunidades de realizar conexiones entre conceptos matemáticos, así como entre conceptos matemáticos y extra-matemáticos, el estudiante se ve obligado a acudir a su experiencia y conocimientos matemáticos previos, consecuentemente, realiza aprendizaje significativo.

Monsalve-López y Zapata-Cardona [14] refieren que es importante que la persona docente promueva la práctica de tareas matemáticas que se encuadren dentro de la Matemática Realista, es decir, tareas que se caractericen por su énfasis en el trabajo de modelos matemáticos que consideren situaciones de la vida real, pues dichas tareas tienden a ser relevantes para el estudiante, lo que permite dar significado a los conceptos matemáticos. Es aquí donde el estudiante valora el aprendizaje como resultado de un proceso en el cual las matemáticas son vistas como un conocimiento práctico y útil para su día a día.

Por su parte, Galbraith y Fisher [8] destacan la importancia del trabajar tareas matemáticas destinadas al diseño o aplicación de modelos matemáticos con el apoyo de tecnología, pues el recurso tecnológico puede ayudar al estudiante a tener acceso a modelos que podrían ser no manejables o tedioso para el estudiante en el caso que tuviera que realizar el trabajo de resolución de forma manual en papel.

En lo que respecta a las orientaciones curriculares en la educación superior, da Silva Pina Neves y Carneiro [15] enfatizan las recomendaciones de la Asociación Matemática de América en relación a la enseñanza de la matemática a nivel universitario. De esta forma resaltan la importancia de que el docente cree espacios donde los estudiantes se sientan desafiados a realizar y responder preguntas, así como discutan en grupo y colectivo, para que puedan hablar sobre matemática y, al mismo tiempo, escuchen y escriban matemática a partir de las intervenciones de los demás estudiantes.

A modo de síntesis, en esta sección se ha enfatizado la importancia de la Resolución de Problemas como enfoque de enseñanza que se puede mejorar al considerar tanto principios sobre enseñanza efectiva y aprendizaje significativo; y contextos extra-matemáticos que le permitan al estudiante dar significado a los conceptos movilizados. En el caso particular del trabajo con modelos matemáticos, recomendándose el apoyo tecnológico. Por su parte, el trabajo en grupo, la discusión en grupo y la mediación pedagógica, se consideran como recomendaciones que a nivel de la educación superior deben ser consideradas por la persona docente de Matemática a la hora de proponer la gestión de clase y para favorecer la comunicación matemática en los estudiantes.

En la siguiente sección se describen los aspectos teóricos en relación al modelo matemático que fundamenta la propuesta didáctica.

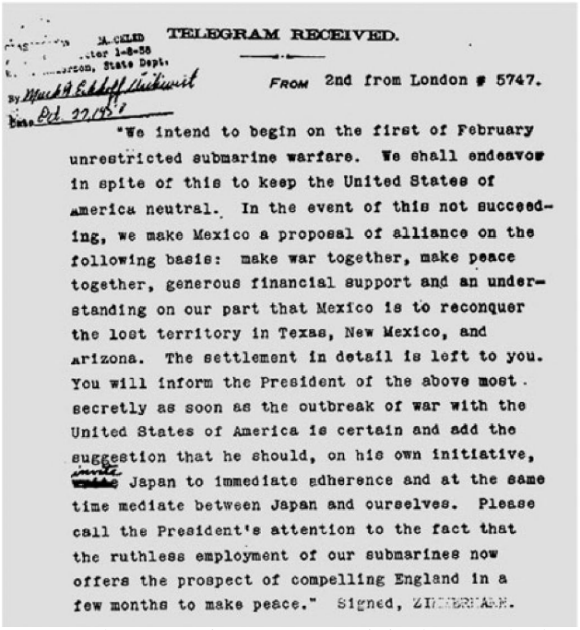
3. La codificación, el cifrado y la matemática de por medio

La criptografía ha sido usada por años en diferentes situaciones con el fin de transmitir de forma segura la información a un receptor objetivo. Su uso recae desde épocas muy antiguas, inclusive antes de Cristo. Así, por ejemplo, se tiene información sobre el uso de criptografía en tablillas babilónicas que rondan el 2500 A.C., donde "aparecen términos a los que se les ha sustraído la primera consonante, o se emplean caracteres en variantes poco habituales" [10], p. 11.

Ahora bien, al hablar de criptografía se suelen usar los términos codificación o cifrado. En el caso de la codificación, se entiende la sustitución de una o más palabras por otras; mientras que el cifrado consiste en sustituir alguna o todas las letras por otros símbolos. A modo de ejemplo, Gómez Urgellés [10] refiere los idiomas, pues al traducir una palabra de un idioma a otro se puede entender que se está realizando una codificación; mientras que realizar un cifrado de dicha palabra requeriría establecer previamente una asociación de cada letra que compone dicha palabra con un símbolo específico, el cual podría ser también una letra o un carácter no alfabético.

En las figuras 1-3 se puede apreciar un ejemplo histórico de codificación, el telegrama Zimmerman. Este telegrama fue transmitido durante la Primera Guerra mundial por el primer ministro alemán de Exteriores Arthur Zimmermann hacia el embajador alemán en Estados Unidos Johann von Bernstorff, como parte de una tentativa de Zimmermann por hacerle llegar al embajador alemán Heinrich von Eckardt, en México, un mensaje sobre un plan de ataque submarino.

En la Figura 1 se puede apreciar el mensaje original, mientras que en la Figura 2 el mensaje Zimmermann codificado. Al comparar dichos documentos se logra apreciar que se está ante un método de codificación, pues existen cantidades numéricas que se repiten, y dos o más cantidades numéricas no aparecen

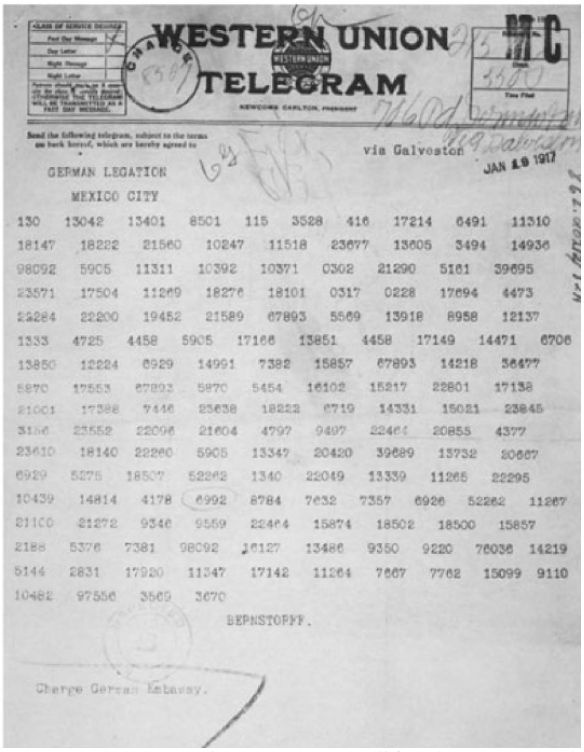


TELEGRAM RECEIVED.

FROM 2nd from London # 5747.

"We intend to begin on the first of February unrestricted submarine warfare. We shall endeavor in spite of this to keep the United States of America neutral. In the event of this not succeeding, we make Mexico a proposal of alliance on the following basis: make war together, make peace together, generous financial support and an understanding on our part that Mexico is to reconquer the lost territory in Texas, New Mexico, and Arizona. The settlement in detail is left to you. You will inform the President of the above most secretly as soon as the outbreak of war with the United States of America is certain and add the suggestion that he should, on his own initiative, invite Japan to immediate adherence and at the same time mediate between Japan and ourselves. Please call the President's attention to the fact that the ruthless employment of our submarines now offers the prospect of compelling England in a few months to make peace." Signed, ZIMMERMANN.

Figura 1. Telegrama Zimmermann original. Tomado de [10], p. 18) [*Original Zimmermann telegram. From [10], p. 18*].



WESTERN UNION TELEGRAM

via Galveston

JAN 19 1917

GERMAN LEGATION
MEXICO CITY

130 13042 13401 8501 115 3528 416 17214 6491 11310
18147 18222 21560 10247 11518 23677 13605 3494 14936
98092 5905 11311 10392 10371 0302 21290 5161 39695
23571 17504 11269 18276 18101 0317 0228 17694 4473
22284 22200 19452 21589 67893 5569 13918 8958 12137
1333 4725 4458 5905 17166 13851 4458 17149 14471 6706
13850 12224 6929 14991 7382 15857 67893 14218 56477
5870 17553 67893 5870 5454 16102 15217 22801 17138
21001 17388 7446 25638 18223 6719 14331 15021 23845
3156 23552 22098 21604 4797 9497 22464 20855 4377
23610 18140 22260 5905 13349 20420 39689 13732 20667
6929 5275 18507 52262 1340 22049 13339 11265 22295
10439 14814 4178 6992 8784 7632 7357 6926 52262 11267
21100 21272 9346 9559 22464 15874 18502 18500 15857
2188 5376 7381 98092 16127 13486 9350 9220 76036 14219
5144 2831 17920 11347 17142 11264 7667 7762 15099 9110
10482 97556 3569 3670

BERNSTORFF.

Cherye German Embassy.

Figura 2. Telegrama Zimmermann codificado. Tomado de [10], p. 18 [*Zimmermann telegram encoded. From [10], p. 18*].

juntas en lo que resta del mensaje, lo cual da para inferir que dichas cantidades no son letras, sino palabras.

Parte de la historia que envuelve al telegrama Zimmermann revela que, días más tarde al envío del telegrama, el mensaje fue interceptado y descodificado por los británicos. Parte de dicha descodificación se observa en la Figura 3.

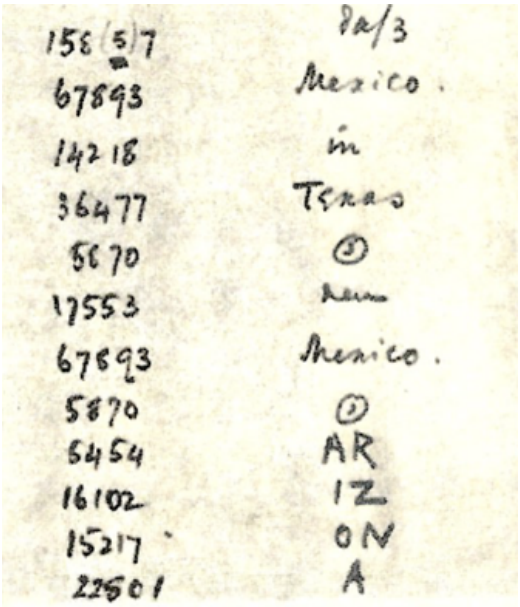


Figura 3. Descodificación parcial del Telegrama Zimmerman. Tomado de [10], p. 19) [*Partial decoding of the Zimmerman Telegram. From [10], p. 19*].

En la Figura 3 aparece el uso de la cantidad numérica 67893 como codificación de la palabra "México". Resulta interesante ver que en las cantidades numéricas utilizadas para codificar el mensaje Zimmermann, ni todas las palabras hacen referencia a una palabra completa con significado, como es el caso de las cantidades 5454, 16102, 15217 y 22501, las cuales por sí solas representan palabras sin definición en la lengua española (a excepción de la "a"), pero que al unir sus descodificaciones forman la palabra "Arizona", nombre de localidad de América del Norte, el cual sí tiene significado en el mensaje.

Por otra parte, en la Figura 4 se muestra un ejemplo de cifrado, el cifrado de la reina María de Escocia de 1587, usado para intercambiar mensajes con un aristócrata católico, en una tentativa por ocultar el plan de un asesinato fallido de la reina Isabel de Inglaterra de esa época.

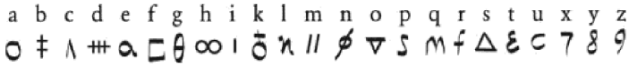


Figura 4. Cifrado del alfabeto usado por la reina escocesa María. Tomado de [10], p. 47 [*Alphabet cipher used by the Scottish Queen Mary. From [10], p. 47*].

Si bien el código usado por la reina María en sus mensajes era una combinación entre cifrado y codificación (puesto que usaba símbolos únicos para referirse a ciertas palabras), es posible encontrar una tabla solo de cifrado usado por la reina María. La tabla se presenta en la Figura 4.

De esta figura se desprende que el cifrado de la reina María no se restringía solo al uso de letras, sino al uso también de números y otros tipos de símbolos más específicos, dándole más solidez a su cifrado.

A partir de los ejemplos anteriores se puede establecer una conexión entre la encriptación y la matemática, explícitamente, la codificación y el cifrado pueden entenderse como relaciones matemáticas que establecen una biyección entre elementos de un conjunto A (formado por símbolos que conforman el mensaje original) y elementos de un conjunto B (formado por símbolos utilizados para encriptar cada símbolo o palabra del conjunto A). Aquí la condición de la biyección es colocada para poder hablar también de la descodificación o descifrado del mensaje mediante la relación inversa.

Ahora bien, como es habitual en algunas culturas asiáticas, es posible disponer de transmitir el mensaje escrito de manera vertical, o en su contraparte de manera horizontal en la cultura occidental. Esto abre las puertas para que en la encriptación también existan diversas formas para representar ordenadamente el mensaje cifrado y/o codificado. Es ahí donde entran en juego las matrices, entendidas como arreglos rectangulares formados por m filas y n columnas, en los que se puede establecer una función M entre el conjunto de los pares de enteros $(i, j), 1 \leq i \leq m, 1 \leq j \leq n$, con un cuerpo F (usualmente números reales) para detonar sus elementos $M(i, j) = M_{ij}$.

En el caso, por ejemplo, de la Figura 4, podrían definirse matrices de diferentes dimensiones para almacenar la información encriptada y, a partir de cualquiera de estas, podrá interpretarse el mensaje a desencriptar pues existe un orden que establecen los pares de enteros (i, j), lo que permite una lectura en forma horizontal o vertical del mensaje.

En lo que se refiere a los tipos de encriptación, se conoce el cifrado de Hill, que fue creado por el matemático estadounidense Lester Hill en 1929. Este cifrado se fundamenta en el uso de los conceptos del Álgebra Lineal de matriz cuadrada, matriz invertible y determinante de una matriz en combinación con la aritmética modular, es decir, la función residuo, la cual da como salida el residuo al dividir dos números enteros. La construcción del cifrado de Hill sigue el proceso matemático descrito en los siguientes párrafos.

Se establece una tabla de cifrado para los símbolos originales que componen el mensaje original mediante una biyección con otros símbolos, de tal forma que, si a_i representa un símbolo en el mensaje original, dicho símbolo tendrá asociado un símbolo de cifrado b_i, con $i \in \{1, 2, 3, \cdots, k\}, k \in \mathbb{N}$ y $(b_p = b_q) \Rightarrow (a_p = a_q)$, para que se cumpla que la correspondencia en la tabla es uno a uno. En una representación tabular se vería como se muestra en la Tabla 1.

Tabla 1. Cifrado de símbolos usados en el mensaje original [*Encryption of symbols used in the original message*].

Símbolos originales	a_1	a_2	$\cdots$	a_k
Símbolos cifrados	b_1	b_2	$\cdots$	b_k

En el caso del alfabeto usado en América Hispana, los símbolos originales serían las 27 letras del alfabeto (restringido a usar solo letras mayúsculas o solo minúsculas), por lo que en la tabla anterior se podría hacer la sustitución $a_1 = A$, $a_2 = B, \cdots, a_k = a_{27} = Z$, quedando por definir los símbolos b_i asociados a cada letra del alfabeto.

Una vez definida la tabla de cifrado, se procede a hacer uso de los conceptos del Álgebra Lineal, al crear una matriz de cifrado C, con entradas enteras, la cual deberá tener como propiedades ser una matriz cuadrada y con determinante igual a uno. La condición de ser cuadrada se usa para poder calcular su determinante, mientras que la condición de que se construya de forma que su determinante sea uno es para garantizar dos aspectos: 1) que la matriz sea invertible y 2) que al multiplicar la matriz C por un vector columna $\vec{v}$ y aplicar la función residuo a cada entrada del vector originado $\vec{w} = C \cdot \vec{v}$, se garantice también la existencia del inverso en aritmética modular, es decir, que se garantice que podamos también descodificar los vectores cifrados $\vec{w}$ con la función residuo, para volver a obtener los vectores $\vec{v}$ que contienen extractos del mensaje original.

Nótese que el vector columna $\vec{v}$ debe tener tantas filas como filas tiene la matriz de cifrado C, de forma que el producto $C \cdot \vec{v}$ esté bien definido. Además, dado que las matrices se operan con cantidades numéricas, el vector $\vec{v}$ tendrá como entradas información del mensaje original en términos de los símbolos b_i, de ahí la importancia de diseñar previamente la Tabla 1. De esta forma, habrá tantos vectores $\vec{v}$ como información se deba cifrar.

En lo que sigue, se presenta la propuesta didáctica para la enseñanza con significado extra-matemático de los conceptos ya referidos, donde se muestra un ejemplo de cómo usar el cifrado de Hill para el cifrado y descifrado de un mensaje.

4. La propuesta didáctica para el abordaje de matrices

En esta sección se explica la metodología seguida para el diseño de la propuesta didáctica, que incluye la gestión que se propone para trabajar la tarea matemática que fundamenta la propuesta, el enunciado de la misma y la intención de cada una de las preguntas planteadas en esta.

4.1 Orientaciones metodológicas

Este estudio es parte de un estudio mayor, el cual tiene como objetivo identificar aprendizajes movilizados y dificultades evidenciadas por estudiantes universitarios de un curso de Álgebra Lineal, al resolver una tarea matemática que fomenta el significado extra-matemático en conceptos matriciales. El estudio asume un abordaje cualitativo dentro de un paradigma interpretativo, en el entendimiento que todo conocimiento y significado es construido por las personas participantes en la investigación, donde el investigador actúa de forma natural y deja de lado sus propias creencias para intentar comprender las experiencias vividas por los participantes [18].

Este estudio muestra el diseño de la propuesta didáctica, no resultados asociados a su implementación. Aún así, esta propuesta se ha pensado para ser desarrollada con carácter formativo y dentro de las clases de un curso de Álgebra Lineal, posterior a la enseñanza formal de los conceptos de matriz, su dimensión, determinante, matriz inversa, así como las definiciones de las operaciones matriciales usuales de producto, suma y resta de matrices.

La propuesta sigue los principios de diseño y gestión de clase que se describen más adelante, principios referidos fundamentados en el referencial teórico. Por un lado, la propuesta didáctica aboga a la Resolución de Problemas de Polya [16] como modelo metodológico de enseñanza en la clase de Matemática. Esta propuesta promueve explícitamente las siguientes cuatro etapas: 1) entender el problema, 2) configurar un plan, 3) ejecutar el plan y 4) mirar hacia atrás [7].

Por otro lado, en la sección anterior se describió, a grandes rasgos, cómo funciona el modelo del cifrado de Hill, lo que evidencia que dicho modelo recurre al uso de diferentes conceptos matriciales. En ese sentido, la propuesta didáctica propone usar dicho modelo de cifrado para que los estudiantes de un curso de Álgebra Lineal den significado extra-matemático al objeto matemático de matriz y conceptos asociados, que son conceptos trabajados previamente de manera formal por el docente al principio del curso.

Como consecuencia, el cifrado de Hill pretende que los estudiantes tengan una mejor comprensión de los conceptos asociados a esos objetos matemáticos. Al trabajar sobre los conceptos se trabaja también sobre las técnicas o procedimientos de resolución aprendidos en la clase de Matemática.

Al considerar que la propuesta didáctica está dirigida a estudiantes de diversas carreras, cuyo plan de estudio amerita aprobar un curso de Álgebra Lineal y no necesariamente estudiantes que deban abordar la temática de criptografía como parte de su formación profesional, la propuesta de este estudio tiene un carácter formativo. De esta forma, la propuesta opta por usar uno de muchos contextos en donde se le puede dar significado a objetos y conceptos matemáticos trabajados en un curso de Álgebra Lineal, pero teniendo en cuenta que sea un contexto que movilice los conceptos matemáticos deseados y que no requiera más allá de los conocimientos previos que poseen los estudiantes.

Se persigue hacer uso de un contexto extra-matemático relativamente cercano o conocido por la clase para trabajar el cifrado de Hill, dicho contexto es el de ecuaciones químicas, trabajadas en la educación secundaria del contexto costarricense en la clase de Química y retomado en varias de las carreras de ingeniería en el primer curso de química que frecuentan los estudiantes.

A partir de este contexto extra-matemático se busca promover el aspecto motivacional hacia la matemática y que las conexiones entre objeto matemático y la situación problema (o concepto matemático y la situación problema) sean más sencillas, en comparación con trabajar el cifrado de Hill en un contexto meramente matemático.

El uso de Excel persigue que el estudiante asimile las ventajas de usar un recurso de uso frecuente en diversas áreas de los negocios, pero poco usado en la Matemática en el área del Álgebra, como lo es Excel. No se busca que el estudiante aprenda a programar en el lenguaje de Excel que hay de por medio para realizar los diferentes cálculos que realiza la hoja, en su lugar se desea que el estudiante verifique sus resultados matemáticos realizados en papel, a partir de una manipulación sencilla de la hoja de Excel, donde deba ingresar las letras del mensaje que desea codificar en diferentes celdas de una columna, para a continuación ver la salida que da la hoja en celdas de otras columnas.

Finalmente, se apuesta por el trabajo individual, el trabajo en grupo y la discusión colectiva como parte de los elementos de gestión de clase recomendados en la clase de Matemática, elementos que se acoplan perfectamente a la propuesta didáctica pensada desde el enfoque de la Resolución de Problemas.

4.2 Gestión de la propuesta didáctica

Como se ha mencionado, la propuesta didáctica de este estudio está fundamentada en el marco de la Resolución de Problemas y el aprendizaje significativo de conceptos, apoyado en el uso del recurso tecnológico y el contexto extra-matemático como elementos que promueven este aprendizaje significativo. Además, se promueve el trabajo individual, el trabajo en grupo y la discusión colectiva como momentos de trabajo que enriquecen la Resolución de Problemas. En ese sentido, a continuación se describe cómo está configurada la gestión de la propuesta didáctica teniendo en cuenta este marco.

Inicialmente, se propone que el docente plantee a los estudiantes hacer lectura detenida de la tarea matemática, esto de forma individual, solicitándoles a la vez que piensen sobre conceptos matemáticos del curso de Álgebra Lineal que identifiquen en la tarea y sobre posibles ideas que se les ocurre para resolver la misma.

Posteriormente, se plantea el trabajo en grupos. La directriz inicial es que compartan lo que entendieron sobre la tarea en sus grupos, discutiendo ideas sobre lo que cada miembro interpretó que se debe hacer. Luego de dedicar unos minutos para este intercambio de ideas, el docente interviene dirigiéndose a toda la clase para ratificar que estén comprendiendo bien qué es lo que se debe hacer, lo que incluye dudas en cuanto a los términos usados para el cifrado de Hill. Es esta la fase de *entender el problema*.

Una vez que los estudiantes tienen claridad sobre lo que se debe hacer, estos trabajan en *configurar un plan* que permita resolver la tarea matemática y *proceder a ejecutar el plan*. Aquí los estudiantes trabajan sobre el cifrado y descifrado de mensajes a partir de las dos primeras preguntas de la tarea.

Luego de resolver las primeras dos preguntas, la tarea invita a los estudiantes a *mirar hacia atrás* después de haber obtenido una posible respuesta a la situación problema inicial, esto mediante una pregunta de verificación de resultados matemáticos que es planteada en la cuarta pregunta. Esta parte de verificación se trabaja a partir de la hoja de cálculo de Excel, donde se solicita verificar el cifrado final del mensaje elaborado en papel y lápiz a partir del cifrado directo del mensaje que permite el código programado en la hoja de Excel proporcionada. Se debe tomar en cuenta que la segunda pregunta de cierta forma también promueve la verificación de resultados trabajada en la pregunta uno, aunque su principal intención es replicar el modelo de descifrado del mensaje.

Durante el desarrollo de estas fases anteriores el docente deberá monitorear el trabajo realizado, de forma que pueda supervisar que el trabajo matemático vaya por buen camino. En caso de identificar posibles dificultades en algún grupo de trabajo, compete a la persona docente realizar preguntas pertinentes que permitan al grupo avanzar, pero con el cuidado de no decir cuál es el proceso a seguir correctamente a partir de tal punto de estancamiento. Una vez que todos los estudiantes concluyen su trabajo en grupo se les solicita que suban a la plataforma del curso, o vía correo, el archivo trabajado en papel y el archivo trabajado de Excel.

Posteriormente, se procede a realizar una discusión colectiva, donde se exponen los modelos usados para el cifrado de Hill de cada grupo. Se destacan las diferencias entre estos modelos; las conexiones que lograron realizar los estudiantes con los conceptos identificados en la fase de entender el problema, el rol que le atribuyen los estudiantes al uso de la hoja de Excel y las dificultades que tuvieron al trabajar la tarea. Esta discusión colectiva, al igual que los momentos de intervención de la persona docente en los grupos de trabajo, deberá ser grabada en audio para complementar las evidencias del trabajo escrito y digital realizado por los estudiantes, y realizar un posterior análisis de los resultados.

En relación al tiempo de trabajo, la propuesta está pensada en el contexto de una clase universitaria de al menos dos horas, donde se destinan 30 minutos para la fase de entender el problema, una hora para la fase de configuración y ejecución del plan y 30 minutos para la discusión colectiva. Se debe tener en cuenta que dentro de estos 30 minutos de discusión colectiva el docente debe exponer las ventajas y desventajas

de cada uno de los modelos de cifrado de Hill propuestos por los estudiantes, en términos de cómo se ven reflejados los conceptos y procedimientos matemáticos en estudio, así como recopilar información sobre las dificultades experimentadas por los estudiantes al resolver la tarea matemática.

4.3 Diseño de la tarea matemática

La tarea matemática que fundamenta la propuesta didáctica consta de tres partes. La primera parte tiene como objetivo familiarizar al estudiantado con el modelo del cifrado de Hill, al mismo tiempo que expone datos históricos sobre el uso de la criptografía como elemento motivador, para que el estudiante se entusiasme a comprender el modelo del cifrado de Hill. Para esta parte histórica se comparte, mediante anexos, los extractos del telegrama Zimmermann que fueron referidos anteriormente en este documento. Esta primera parte explica también el modelo del cifrado de Hill, donde se alude al uso de conceptos matriciales y términos dentro del contexto del cifrado, de forma que el estudiante realice las conexiones entre la matemática que sabe y el lenguaje nuevo en uso.

La segunda parte de la tarea tiene como objetivo que el estudiante visualice cómo se pone en práctica el cifrado de Hill, pues la experiencia docente recalca que la teoría leída requiere ser ejemplificada para que sea comprendida con mayor facilidad por los estudiantes. De esta forma, esta segunda parte es todavía de familiarización del modelo matemático, donde se busca que los estudiantes comprendan cómo trabajar el cifrado de Hill para un caso particular, el cifrado de letras del alfabeto usado en hispanoamérica.

La tercera parte ya corresponde propiamente al trabajo de producción por parte de los estudiantes. En esta los estudiantes tienen que dar respuesta a una situación problema usando el cifrado de Hill, en el contexto de ecuaciones químicas. Se comienza la redacción de la situación y se invita al estudiante a formar parte de la misma, como elemento motivador que lo desafíe. Posteriormente, se le plantea la problemática, lo que incluye las preguntas a atender.

Respecto a las cuatro preguntas colocadas, cada una tiene una intención definida a nivel de movilización de conceptos matemáticos. La primera y segunda preguntas están destinadas al trabajo de construcción en lápiz y papel del modelo, con la diferencia de que la primera pregunta desea movilizar los conceptos de matriz, dimensión, producto matricial, determinante y función resto, mientras que la segunda pregunta se centra en el concepto de matriz inversa. Por otro lado, la tercera pregunta busca que el estudiante sea capaz de usar una matriz específica que cumpla con las restricciones del modelo del cifrado de Hill, por lo que esta pregunta es de consolidación. Finalmente, la cuarta pregunta está destinada al uso del recurso tecnológico de la hoja de cálculo de Excel, como medio para que el estudiante pueda verificar sus cálculos desarrollados en papel. En la Figura 5 se muestra un extracto del archivo de Excel proporcionado.

En esta figura se muestran dos tablas. En la tabla superior, que presenta cinco columnas, se muestra el cifrador de mensaje, mientras que en la tabla inferior se muestra parte de la tabla de asignación de letras del alfabeto con números, específicamente, las 27 letras del alfabeto asignadas a los números del cero al 26, respectivamente.

Con respecto al cifrador, el estudiante debe usar la primera columna para colocar letras del mensaje dado en la tarea, colocando letras de dos en dos. Al colocar las letras a cifrar en esa primera columna, la hoja de cálculo asigna automáticamente dichas letras a números en la tercera columna (matriz de mensaje). A la vez, en la cuarta columna, se calcula la matriz de transición, mediante el producto matricial de la matriz de cifrado con la matriz de mensaje. Finalmente, en la quinta columna, se calcula automáticamente la matriz de cifrado final usando la función resto.

La segunda columna de la matriz de cifrado debe ser fijada por los estudiantes, para lo cual se ha colocado por defecto la matriz que deben usar en la tarea, a fin de que los estudiantes solo deban manipular la primera columna del cifrador. De no ser así, los estudiantes deberán usar tantas veces el cifrador como sea necesario hasta cifrar todas las letras del mensaje solicitado a traducir.

Un aspecto a considerar es que la programación elaborada en la hoja de cálculo de Excel se ha hecho de forma que solo las letras involucradas en el mensaje de la tarea son cifradas por el cifrador de la hoja de cálculo. En caso de colocarse una letra no considerada en el mensaje a verificar, el cifrador da como salida *error* en la tercera columna.

El trabajo con Excel se deja de último porque el estudiante debe primero aprender a trabajar en papel el modelo del cifrado de Hill, para que pueda reflexionar sobre las conexiones entre conceptos matemáticos y términos del cifrado antes de computar meramente números. Una vez que se ha logrado esto con las tres primeras preguntas, la cuarta pregunta no pretende que el estudiante reflexione nuevamente sobre estas conexiones de conceptos, sino sobre las ventajas del programa en comparación con el trabajo del modelo del cifrado de Hill realizado en lápiz y papel.

4.4 Enunciado de la tarea matemática

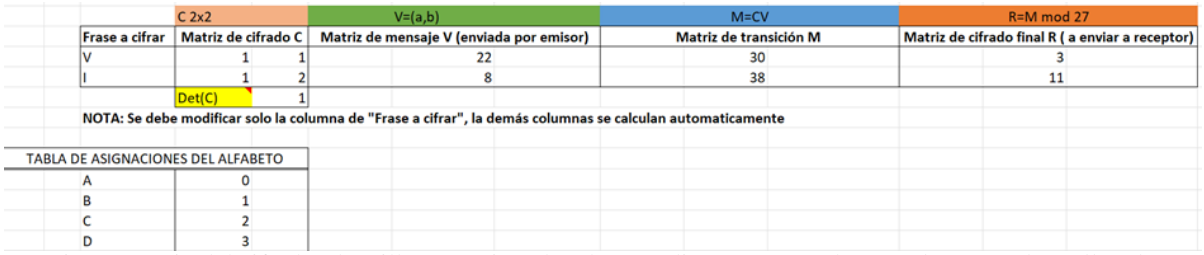
Cifrado y descifrado de mensajes

Parte A. Comprender el modelo

Sabía que durante diferentes épocas de la historia la codificación (sustitución de una palabra completa por otra) y el cifrado (sustitución de caracteres por otros) fueron recursos indispensables para transmitir información secreta.

Un dato histórico

El 17 de enero de 1917, la sección política británica conocida como Sala 40, descodificó el telegrama alemán enviado por el



	C 2x2		V=(a,b)	M=CV	R=M mod 27
Frase a cifrar	Matriz de cifrado C		Matriz de mensaje V (enviada por emisor)	Matriz de transición M	Matriz de cifrado final R (a enviar a receptor)
V	1	1	22	30	3
I	1	2	8	38	11
	Det(C)	1			

NOTA: Se debe modificar solo la columna de "Frase a cifrar", la demás columnas se calculan automaticamente

TABLA DE ASIGNACIONES DEL ALFABETO	
A	0
B	1
C	2
D	3

Figura 5. Diseño propio del cifrador de Hill proporcionado a los estudiantes en Excel [*Own design of the Hill cipher provided to students in Excel*].

ministro alemán de Exteriores Arthur Zimmermann al embajador alemán en los Estados Unidos, Johann von Bernstroff. Este telegrama tiene importancia histórica en la declaración de guerra de los Estados Unidos a Alemania. El telegrama (versión en inglés), su codificación y descodificación son presentados en las Figuras 1, 2 y 3, respectivamente.

Matemática detrás del cifrado y codificación de mensajes

En el caso del cifrado, una forma de transmitir esta información es utilizando matrices C cuadradas de dimensión $n \times n$ y matrices columnas V de dimensión $n \times 1$, para poder obtener las matrices:

$$M = C \cdot V \text{ y } R = M \mod 27.$$

La matriz C, llamada *matriz de cifrado del mensaje* es una matriz invertible, con la restricción de que su determinante sea 1.

En el caso de la matriz R , esta toma cada entrada de M y las reemplaza por el residuo proveniente de hacer la división de la entrada respectiva entre 27. Así, por ejemplo:

$$M = \begin{pmatrix} 30 \\ -18 \end{pmatrix}, \quad R = M \mod 27 = \begin{pmatrix} 3 \\ 9 \end{pmatrix}.$$

Pues al dividir 30 entre 27 el residuo es 3, es decir, $30 \mod (27) = 3$. Para el caso de -18, siendo negativo, primeramente, sumamos 27 tantas veces como sea necesario hasta obtener un número entre cero y 26. En este caso basta hacer $-18+27=9$, de donde se obtiene que $-18 \mod (27) = 9$, pues, por propiedades de la función residuo, se tiene que:

1) $p+n \mod (n) = p \mod (n)$, para $p \in \mathbb{Z}$.

2) $k \mod (n) = k$, para $0 \leq k < n$.

Se toma el módulo 27 considerando que el alfabeto tiene 27 letras, las cuales se pueden asociar a los números del 0 al 26, vistos como los posibles residuos de dividir un número entero entre 27.

Para cifrar una parte de un mensaje, se coloca la información a cifrar en forma de una matriz columna V, para lo cual previamente se tiene que haber reemplazado las letras por números del 0 al 26, según su posición en el alfabeto u otra forma definida de orden. Posteriormente, se calcula $M = C \cdot V$, una vez escogida la matriz C cuadrada y con determinante igual a 1. Al tener M, la matriz de transición, se aplica la función residuo o función módulo a cada entrada de M, a fin de obtener R, *la matriz de cifrado final* con componentes numéricas entre 0 y 26. A partir de aquí se interpretan dichas componentes como letras del alfabeto nuevamente. De esa forma, dada una matriz V, matriz de mensaje original, la matriz R da el cifrado de cada entrada de la matriz V.

Para descifrar el mensaje, se considera el proceso inverso:

$$\text{si } M = C \cdot V \text{ y } R = M \mod 27,$$
$$\Rightarrow V = C^{-1} \cdot M \text{ y } V = (C^{-1} \cdot R) \mod 27.$$

En particular, la igualdad $V = (C^{-1} \cdot R) \mod 27$ será la que permitirá determinar en forma directa la matriz V de mensaje original a partir de la matriz R de cifrado final y la matriz inversa de la matriz de cifrado C.

PARTE B. Un ejemplo a considerar

Las letras del alfabeto de la A a la Z se pueden enumerar con los números del 0 al 26. Si consideramos una matriz columna $\begin{pmatrix} A \\ E \end{pmatrix}$, se podría escribir numéricamente como $V = \begin{pmatrix} 0 \\ 4 \end{pmatrix}$, cuyo cifrado seguro es posible obtener al definir, por ejemplo, una matriz $C = \begin{pmatrix} 1 & 1 \\ 1 & 2 \end{pmatrix}$, obteniendo la matriz transitoria de cifrado $M = \begin{pmatrix} 4 \\ 8 \end{pmatrix}$, cuyas componentes ya son números entre 0 y 26; por lo cual, se obtiene:

$$R = \begin{pmatrix} 4 \\ 8 \end{pmatrix} \mod 27 = \begin{pmatrix} 4 \\ 8 \end{pmatrix}.$$

De esta forma, la matriz $V = \begin{pmatrix} 0 \\ 4 \end{pmatrix}$ tendría por cifrado final la matriz $R = \begin{pmatrix} 4 \\ 8 \end{pmatrix}$, en la cual el cero se sustituye por el cuatro y el cuatro por ocho; por lo tanto, en el mensaje original se sustituye la A por la E y la E por la I, siendo este el cifrado realizado.

En caso de tener la matriz R, y querer buscar la matriz V, se puede obtener esta última a partir del proceso inverso, usando $V = (C^{-1} \cdot R) \mod 27$.

Veamos:

$$R = \begin{pmatrix} 4 \\ 8 \end{pmatrix} \text{ y } C = \begin{pmatrix} 1 & 1 \\ 1 & 2 \end{pmatrix},$$
$$\Rightarrow C^{-1} = \begin{pmatrix} 2 & -1 \\ -1 & 1 \end{pmatrix},$$
$$\Rightarrow C^{-1} \cdot R = \begin{pmatrix} 2 & -1 \\ -1 & 1 \end{pmatrix} \cdot \begin{pmatrix} 4 \\ 8 \end{pmatrix} = \begin{pmatrix} 0 \\ 4 \end{pmatrix}.$$

De aquí se obtiene que:

$$V = \begin{pmatrix} 0 \\ 4 \end{pmatrix} \mod 27 = \begin{pmatrix} 0 \\ 4 \end{pmatrix}.$$

PARTE C. Poner en práctica el cifrado de Hill con ecuaciones químicas

Suponga que, como estudiante de un curso de química, está interesado(a) en transmitirle a un(a) compañero(a) de clase que faltó cierto día a la clase de química la ecuación que describe la conversión del monóxido de carbono en metano, explícitamente:

$$CO + 3H_2 \rightarrow CH_4 + H_2O.$$

Aprovechando que usted y su compañero(a) conocen el cifrado de Hill, usted decide pasarle a él/ella en la clase de Álgebra Lineal la ecuación química haciendo uso de dicho cifrado, a modo de practicar el uso de operaciones matriciales a partir del cifrado de Hill.

A partir de lo anterior,

1. Proponga un cifrado de Hill para la ecuación química, explicando cómo procedió en la construcción matemática del mismo; es decir, refiriendo cómo procedió en la construcción de la matriz de mensaje original, la matriz de cifrado del mensaje y la matriz de cifrado final.
2. Verifique el correcto cifrado de la molécula H_2O usando el proceso de descifrado.
3. Use la matriz de cifrado de la parte B y la correspondiente tabla de asignación de letras del alfabeto, para cifrar la frase “la vida es bella".
4. Verifique el cifrado correcto de la frase del punto 3 usando para tal efecto la plantilla de cálculo de Excel proporcionada en el siguiente enlace: Cifrado de Hill Excel.

Descargue el archivo *online* en su computadora y trabaje sobre este archivo descargado, no trabaje sobre el archivo en línea. Use tantas matrices de mensaje como sea necesario para visualizar su verificación de cifrado en la hoja de Excel. Suba a la plataforma del curso una imagen de la resolución por escrito de la actividad del punto 1), 2) y 3), así como el archivo de Excel trabajado en el punto 4), donde realiza su verificación de cifrado de la frase referida.

Conclusiones

A partir de la propuesta didáctica presentada se pueden referir diferentes conexiones entre el cifrado de Hill y conceptos matriciales fundamentales en el Álgebra Lineal.

En primer lugar, el modelo del cifrado de Hill propone el uso de matrices cuadradas, pero no restringe la dimensión de las matrices, por lo que el modelo permite que los estudiantes acudan al concepto de dimensión de una matriz para reflexionar sobre cuál será la manera más adecuada para cifrar letras de un mensaje. Se infiere que una matriz de dimensión $n \times n$ debe conducir a los estudiantes a evidenciar que ello les permitirá cifrar n letras por turno, por lo que entre mayor sea el valor de n menos veces tendrán que repetir el proceso de cifrado de letras.

Ahora bien, el estudiante intuirá que trabajar con una matriz muy grande sin apoyo de recurso tecnológico digital tendrá sus desventajas, pues la matriz de cifrado tendrá más entradas, siendo más difícil encontrar una matriz invertible con determinante igual a uno con solo lápiz y papel. Además, el cálculo de este determinante será de mayor complejidad entre mayor sea la dimensión de esta matriz de cifrado. De esta forma, el planteo de la matriz de cifrado obliga al estudiante a hacer conexiones entre el concepto de dimensión de una matriz, el propio concepto de matriz y el concepto de determinante de una matriz.

En segundo lugar, el concepto de producto matricial lo deben movilizar los estudiantes, independientemente de la matriz de cifrado definida, pues la multiplicación de matriz de cifrado por matriz de mensaje, o la multiplicación de la matriz inversa de la matriz de cifrado por matriz de cifrado total es requerida obligatoriamente, independiente de si se está en el proceso de cifrado o descifrado. En ambos casos el estudiante verá que se requiere de una multiplicación para encontrar una matriz de transición, a la cual después deberá aplicarle la función resto. En el caso especial de descifrado, el concepto de matriz inversa surge de forma espontánea, y el estudiante debe percibirlo así, haciendo la relación de que lo opuesto de cifrado de un mensaje es el descifrar dicho mensaje, por tanto, recurrir a realizar operaciones inversas.

A partir de lo anterior, se observa que la propuesta didáctica de este artículo promueve que el estudiantado pueda dar significado extra-matemático a los conceptos objetivo de la propuesta; una vez que los estudiantes se ven obligados a establecer conexiones entre las matrices construidas y la situación problema, y, por ende, se les exhorta a reflexionar sobre cómo la elección de una u otra matriz afecta la dificultad matemática de resolución de la tarea y si esa elección se ajusta a lo solicitado en la situación problema. Algunas conexiones surgirán de forma natural y otras deberán ser promovidas por la persona docente mediante los momentos de monitoreo y durante la discusión colectiva principalmente.

A diferencia de propuestas de estudios enfocados en la encriptación, como el de [11], la propuesta aquí presentada no limita al estudiante al trabajo de matrices con una sola dimensión o al trabajo con tecnología, sino que promueve el trabajo sin apoyo de recurso tecnológico digital y con recurso tecnológico. Esta característica de un trabajo apoyado y no restringido al uso del recurso tecnológico es fundamental para fomentar las conexiones anteriormente mencionadas. Además, tal como fue referido por [3], el contexto extra-matemático es fundamental para que el estudiante pueda transitar entre lo concreto y lo asbtracto, de donde se desprende la importancia del uso del contexto histórico de la encriptación en esta propuesta, usada a lo largo de la historia.

Dado que este trabajo es una propuesta didáctica para la enseñanza de conceptos, pero que no se ha implementado aún, se pueden desprender varias preguntas de investigación que favorezcan la mejora de la misma, entre ellas: ¿cuáles conexiones son conseguidas de forma natural por los estudiantes y cuáles son promovidas por la persona docente durante la ejecución de la propuesta?, ¿cuáles son las principales dificultades que presentan los estudiantes después del trabajo de la propuesta?, ¿son capaces los estudiantes de darle significado a las matrices en contextos similares a los del cifrado de mensajes?, ¿qué adaptaciones debe sufrir la propuesta ante un escenario donde no se disponga del recurso tecnológico? Estas y otras preguntas más pueden ponerse sobre la mesa, pero siempre teniendo en cuenta que el fin es su implementación para la mejora del aprendizaje de los estudiantes y que, como cualquier propuesta de clase, siempre es posible hacerle mejoras.

Suplementos

Este artículo no contiene información suplementaria.

Conflictos de interés

Se declara que no existen conflictos de interés. El autor declara que no hubo subvenciones involucradas en este trabajo.

Referencias

[1] Albay, E.M.: *Analyzing the effects of the problem solving approach to the performance and attitude of first year university students*. Social Sciences & Humanities Open, 1(1):100006, 2019. https://doi.org/10.1016/j.ssaho.2019.100006.

[2] Anthony, G. and M. Walshaw: *Characteristics of effective teaching of mathematics: A view from the West*. Journal of Mathematics Education, 2(2):147–164, 2009. https://www.researchgate.net/publication/228743535_Characteristics_of_Effective_Teaching_of_Mathematics_A_View_from_the_West.

[3] Bedregal-Alpaca, N., O. Sharhorodska, D. Tupacyupanqui-Jaen, and V. Corneko-Aparicio: *Problem based Learning with Information and Communications Technology Support: An Experience in the Teaching-Learning of Matrix Algebra*. International Journal of Advanced Computer Science and Applications, 11(3):125–130, 2020. http://dx.doi.org/10.14569/IJACSA.2020.0110315.

[4] Bianchini, B.L., G.L. de Lima, and E. Gomes: *Linear algebra in engineering: an analysis of Latin American studies*. ZDM, 51(7):1097–1110, 2019. https://doi.org/10.1007/s11858-019-01081-5.

[5] Chérrez Ibarra, R. y M. Escalona Reyes: *El proceso de enseñanza-aprendizaje de las matrices en la carrera de Ingeniería Civil de la Universidad Laica Eloy Alfaro de Manabí*. Mikarimin. Revista Científica Multidisciplinaria, 5(2):51–60, 2019. https://dialnet.unirioja.es/servlet/articulo?codigo=8605616.

[6] El-Gebeily, M. and B. Yushau: *Linear system of equations, matrix inversion, and linear programming using MS Excel*. International Journal of Mathematical Education in Science and Technology, 39(1):83–94, 2008. https://doi.org/10.1080/00207390600741710.

[7] Espinal Meneses, M.L., Doris Peñaloza y Y. Gelvez: *Método de Pólya como estrategia pedagógica para fortalecer la competencia resolución de problemas matemáticos con operaciones básicas*. Zona Próxima, (31):8–25, 2019. https://doi.org/10.14482/zp.31.372.7.

[8] Galbraith, P. y D. Fisher: *Tecnologia e modelacão matemática: enfrentando desafios, abrindo portas*. Quadrante, 30(1):198–218, 2021. https://doi.org/10.48489/quadrante.23710.

[9] Galindo, D., E. Osorio y S. Serrano: *Objeto de aprendizaje para las operacione con matrices para el procesamiento digital de imágenes*. En Prieto, M., S. Pech y J. Angulo (editores): *Tecnología, innovación y práctica educativa*, páginas 18–28. CIATA, 2020. https://www.researchgate.net/publication/343046240_Objeto_de_Aprendizaje_para_las_Operaciones_con_Matrices_en_el_Procesamiento_Digital_de_Imagenes.

[10] Gómez Urgellés, J.: *Matemáticas y códigos secretos*. RBA Libros, 2018. https://books.google.com.cu/books/about/Matem~A\T1\textexclamdownticas_y_c~A{^3}digos_secretos.html?id=rVTODwAAQBAJ&redir_esc=y.

[11] Jacques-García, F.A., S.L. Magdaleno-Canchola, R.A. Hernández-Rico, U. Chávez Morales y J.I. Olvera-Suárez: *Krynapsis: Un software para la enseñanza de las matrices inversas modulares*. Revista Electrónica de Divulgación de la Investigación, 13:1–15, 2017. https://www.researchgate.net/publication/327895628_Krynapsis_Un_software_para_la_ensenanza_de_las_matrices_inversas_modulares.

[12] Kosasih, U., A.H. Sumartana, Y.L. Sulastri, D. Ahmatika, and A.T. Ramandhita: *Critical Thinking on the Determinants Matrix: The Development of A Teaching Module*. Tadris: Jurnal Keguruan dan Ilmu Tarbiyah, 8(2):303–314, 2023. http://dx.doi.org/10.24042/tadris.v8i2.17059.

[13] Miranda-Nuñez, Y.R.: *Praxis educativa constructivista como generadora de Aprendizaje Significativo en el área de Matemática*. Cienciamatria: Revista Arbitrada Interdisciplinaria Koinonía, 7(13):79–91, 2022. https://doi.org/10.35381/cm.v6i1.299.

[14] Monsalve-López, D.L. y L. Zapata-Cardona: *Procesos de matematización de estudiantes en la resolución de tareas matemáticas realistas*. Revista Virtual Universidad Católica del Norte, (70):228–259, 2023. https://doi.org/10.35575/rvucn.n70a9.

[15] Pina Neves, R.d.S. y R. Carneiro: *Cenários de pesquisa em educacão matemática*. Paco e Littera, 2020. https://www.pacolivros.com.br/cenarios-de-pesquisa-em-educacao-matematica.

[16] Polya, G.: *Cómo plantear y resolver problemas*. Trillas, 1965. https://etrillas.mx/libro/como-plantear-y-resolver-problemas_1760.

[17] Ramírez-Montes, G.: *Ambientes de modelación matemática con Excel en el aprendizaje del concepto de conjunto generador*. En Scott, P., Y. Morales y Á. Ruiz (editores): *Memorias XVI Conferencia Interamericana de Educación Matemática: Resolución de problemas y modelización*, páginas 8–15. CIAEM, 2023. https://ciaem-iacme.org/memorias-xvi-ciaem.

[18] Scheiner, T.: *If we want to get ahead, we should transcend dualisms and foster paradigm pluralism*. Compendium for early career researchers in mathematics education, pages 511–532, 2019. https://doi.org/10.1007/978-3-030-15636-7_27.

[19] Schukajlow, S. and W. Blum: *Methods for teaching modelling problems*. In Greefrath, G., S. Carreira, and G. Stillman (editors): *Advancing and Consolidating Mathematical Modelling*, pages 327–339. Springer, 2023. https://doi.org/10.1007/978-3-031-27115-1_20.