La Criptografía como Contexto para Introducir el Estudio del Concepto de Función en Educación Secundaria

ALVARADO-MONROY, Angelina, OLVERA-MARTÍNEZ, María del Carmen y ALVARADO-QUIÑONES, Mario Alberto

A. Alvarado[1], M.Olvera[1] y M.Alvarado[2]

[1]Universidad Juárez del Estado de Durango
[2]Benemérita y Centenaria Escuela Normal del Estado de Durango

aalvarado@ujed.mx

C. Cristóbal, M. Olvera, V. Vargas (Dirs.) Educación para la interdisciplinariedad. Tópicos Selectos de Educación en CITeM.

Abstract

This paper reports a classroom-based study with a learning environment designed and settled in a context of cryptography and using concrete material-based tools. This design engaged students in collaborative activities of constructing models for the resolution of problems with the intention of introduce the notion of function through a set of linked representations. Two groups of students in middle school were part of this study, they were asked to perform tasks of encrypted and decrypting text messages using substitution ciphers that implicitly involve the concept of function.

This research presents a detailed analysis of students developing fluency with regard to these tasks, and of the aspects of the function concept underlying their processes of constructing models for solving problems. Students' interventions were recorded and transcribed in their entirety. Interactions while they carried out the tasks were analyzed using the theoretical-methodological tool, Abstraction in Context (Dreyfus, Hershkowitz & Schwarz, 2015). Results of this study indicated that different levels of expertise with regard to the task environment reflected and required different aspects of functions, and thus propitiated different opportunities for the emergence and management of the mathematical structure associated with the notion of function.

Models and Modeling, Cryptography, Representations of a function, Abstraction in Context

1. Introducción

La necesidad de proteger información, sobre todo en contextos de guerra, se puede observar a través de registros del siglo V a. de C. y, a partir de entonces, se pueden ver diferentes mecanismos cuyo propósito es aumentar la seguridad de la información. La criptografía (de las raíces griegas *Kryptos*-ocultar y *graphos*-escritura), ahora considerada ciencia, cada vez presenta mecanismos más sofisticados que se basan en diversas ramas de la matemática y que juegan un importante papel en la protección de información, garantizando su privacidad, integridad y autenticidad (Cortés et al., 2005). Dada la creciente demanda de expertos con conocimientos en seguridad en cómputo y criptografía, este contexto cobra relevancia para la enseñanza en la educación básica con una visión integradora de la ciencia, la ingeniería, la tecnología y la matemática.

En esta dirección, por ejemplo, White (2009) presenta los resultados de la implementación, durante cinco semanas, de una secuencia didáctica de cifrado y descifrado de información con estudiantes que finalizan la educación secundaria. En su investigación, utiliza el software *Code Breaker* para que los estudiantes puedan cifrar sus mensajes variando los parámetros de una función polinomial. Además, de utilizar la frecuencia con que aparece una letra del abecedario en un escrito, para que alguien que desconozca el proceso de cifrado de la información pueda revertir el proceso para descifrar el mensaje, es decir, realizar un criptoanálisis. White sugiere que aprender a resolver problemas en un contexto aplicado y que permita utilizar múltiples representaciones como el entorno *Code Breaker,* puede invitar a los estudiantes a ver de manera alternativa, e incluso simultánea, a las funciones como procesos y objetos.

En este trabajo, se percibe valioso el contexto de la criptografía como analogía con el concepto de función y, se presenta, una secuencia didáctica con material concreto inspirado en el cifrado clásico de Julio César y los discos de cifrado (Cortés et al., 2005) para responder a las necesidades de escuelas con acceso restringido a la tecnología.

El concepto de función se introduce en el nivel secundaria y aparece también en los programas de bachillerato y nivel superior. Dada su naturaleza transversal, al estar relacionado con diversos contenidos de disciplinas de ciencia, ingeniería, tecnología y matemáticas (CITeM), es fundamental construir un sistema conceptual robusto para la noción de función. En Artigue (1995), Evangelidou, et al. (2004) y Sierpinska (1992) se han puesto de manifiesto las dificultades de los estudiantes de diferentes niveles en relación con la noción de función y con el reconocimiento de objetos funcionales dados en diferentes representaciones. Estos investigadores identifican la necesidad de desarrollar más investigaciones sobre la comprensión y uso de funciones por los estudiantes, tratando de identificar sus dificultades y concepciones erróneas y mejores formas de aproximación a su enseñanza.

En este estudio, al igual que en gran parte de las investigaciones, se busca mejorar las formas de enseñanza y aprendizaje del concepto de función. La hipótesis es que algunas de las dificultades referidas en la literatura provienen de: la poca comprensión intuitiva, la falta de experiencias de resolución de problemas conectados con la realidad, las imágenes inadecuadas que poseen de los conceptos y de sus representaciones asociadas, la falta de articulación entre sus diferentes representaciones y la ausencia de entrenamiento para generar y usar sus propios ejemplos. En esta última parte, se deben brindar oportunidades para que los estudiantes propongan funciones que respondan con las situaciones planteadas y que tengan un significado personal. Por ejemplo, en esta investigación, los estudiantes proponen su forma de cifrar mensajes (su propia función de cifrado) y otros tratan de descifrarlos, para lo cual necesitan encontrar la función inversa.

La comprensión del concepto de función no parece fácil, dado que, por una parte, se debe apoyar el desarrollo de la habilidad para ver una función como una entidad que acepta una entrada y produce una salida y, por otro lado, apoyar el reconocimiento de las diferentes representaciones asociadas a este concepto y atender las dificultades que puedan presentar en el proceso de articulación y tránsito entre las distintas representaciones. También, el contexto donde es utilizada la noción de función puede aportar significado, Sierpinska (1992) señala que este concepto, puede definirse en notación formal simbólica, casi sin necesidad de utilizar palabras. No obstante, cuando la noción de función es utilizada en algún contexto, matemático o matematizado, el lenguaje informal surge y trae consigo significados que trascienden al mero lenguaje lógico simbólico. Finalmente, se deben ofrecer situaciones que sean relevantes para los estudiantes y permitan el surgimiento y construcción del concepto, además de visualizar su utilidad para la resolución de problemas de diferentes contextos. Esto último, tanto en los programas de estudio, como en los libros de texto, aparece en temas posteriores a la enseñanza de los conceptos reservados para aplicar lo aprendido (Lesh, English, & Fenewald, 2008), contrario a esta propuesta que sugiere propiciar el surgimiento de la noción de función a través de introducir un problema en el contexto de la criptografía.

El objetivo de este estudio es el diseño y evaluación de un ambiente de aprendizaje que utiliza un contexto para detonar el uso de distintas representaciones matemáticas y que sirve como base para posteriormente construir o refinar la noción de función. En tal ambiente se propicia el surgimiento de modelos en un contexto de cifrado y descifrado de mensajes para proteger información. Para probarlo, se implementó en dos grupos de secundaria, se analizaron sus producciones y se logró describir el proceso que siguen los alumnos cuando han de construir y refinar la noción del concepto de función a partir de conectar sus diferentes representaciones: verbal, algebraica, numérica, tabular, gráfica. En la segunda sección se presentan los elementos teóricos y metodológicos tomados en cuenta para el diseño y para el análisis de las interacciones en el aula. La tercera sección describe la metodología, los detalles del diseño y el contexto de implementación. Finalmente, a partir del análisis de los resultados se presentan las conclusiones y mejoras.

2. Marco Teórico

En esta investigación se presenta el análisis de la exploración en el aula de una secuencia diseñada desde la *Perspectiva de Modelos y Modelación* (PMM) propuesta por Lesh & Doerr (2003) como un vehículo para el aprendizaje en CITeM. Dentro de esta perspectiva, un sistema conceptual o modelo es un conjunto de elementos, relaciones, operaciones, reglas y patrones, así como de sus interacciones. Los modelos son considerados herramientas para interpretar situaciones matemáticas; y para ello se requiere de matematizar situaciones relevantes de resolución de problemas. La modelación es la acción de elaborar un modelo para interpretar, construir, predecir, describir o explicar situaciones.

En una secuencia de desarrollo de modelos los tres elementos principales son actividades: 1) que revelan el pensamiento o detonan modelos de los estudiantes; 2) en las que se exploran sus modelos; y, 3) en las que se adaptan tales modelos para aplicarse en otros contextos y para extender sus representaciones (Doerr, 2016). En este trabajo se proponen sólo actividades del tipo 1 y 2, las primeras se conocen como MEA (Model Eliciting Activities) o Actividades Detonadoras de Modelos. Lesh et al. (2000) presentan para su diseño los principios que aseguran que la situación: permita un significado personal de la realidad, provoque la construcción de modelos, brinde oportunidades para la autoevaluación de los modelos, propicie la comunicación de los mismos y conduzca a generar otros modelos al extender los previos para resolver otras situaciones.

Otro elemento teórico-metodológico relevante en este trabajo es *Abstracción en Contexto* (AiC). Aquí, la abstracción pasa por tres etapas: la necesidad de un nuevo constructo, su emergencia y su consolidación al utilizarlo en otros contextos. Las acciones epistémicas que tienen lugar durante el surgimiento del constructo son: *Recognizing, Building with, Constructing* (*R-acciones*, *B-acciones* y *C-acciones*). Tales acciones conforman el modelo *RBC-**C***, donde la segunda **C** corresponde a las acciones de consolidación.

Para el análisis de las intervenciones o interacciones en el aula se consideran *R-acciones* cuando los alumnos reconocen la información relevante para resolver la situación, conceptos implicados y sus propiedades. Es decir, seleccionan o preparan sus "bloques" en analogía con la construcción de un edificio. Se dan *B-acciones* cuando extraen significado de los enunciados, cuando realizan cálculos, cuando se establecen relaciones entre los conceptos, o cuando se utilizan las propiedades de los mismos para obtener deducciones. Este tipo de acciones ocurren cuando se entrelazan algunos de los elementos derivados de las *R-acciones* para construir con ellos una pieza mayor, es decir, unir dos o más bloques. Las *C-acciones*, o acciones de construcción, ocurren cuando *R* y *B-acciones* se entrelazan para reunir los elementos que permiten por primera vez expresar, construir y/u organizar un conocimiento nuevo.

Las acciones de consolidación, ***C**-acciones*, ocurren cuando el aprendiz es capaz de: generar otras maneras de justificar el mismo hecho, de utilizar el lenguaje de manera apropiada y, finalmente, utilizar el conocimiento construido para construir uno nuevo. Cabe mencionar que una *B* o *C acción*, puede tomar la forma de *R-acción* durante el proceso de construcción de un nuevo conocimiento.
La elección de la PMM, se ha dado, considerando que, tanto el contexto de criptografía, como la noción de función que involucra, permiten el diseño de actividades que incorporan el desarrollo de modelos matemáticos para describir una situación de la vida real y motivan el uso de medios de representación para explicar y documentar los modelos de los estudiantes (Lesh & Doerr, 2003).

Además, las actividades detonadoras y de exploración de modelos, involucran a los estudiantes en describir, revisar y refinar su conocimiento matemático y/o científico (Lesh & Doerr, 2003; Lesh et al., 2000), lo cual propicia múltiples interacciones entre estudiantes, materiales y profesor.

En este sentido, la herramienta AiC- modelo RBC (Dreyfus, Hershkowitz, & Schwarz, 2015), permite capturar la complejidad de tales interacciones y analizar el flujo de conocimiento entre los estudiantes hasta lograr un conocimiento base compartido (construyen y actualizan conocimiento de manera colaborativa en el mismo tópico). En ocasiones, también interviene el profesor haciendo preguntas adecuadas para provocar la emergencia de conocimiento nuevo.

3. Metodología

Esta investigación está dentro del marco del Modelo de Desarrollo Profesional Docente para Educación en CITeM (Carmona, et al., 2014). Dicho modelo está caracterizado por ser multi-nivel, interdisciplinario y diseñado para incrementar la autonomía y la agencia del profesor. Para garantizar tal incremento se sugieren cinco etapas: *diseño experto, maestros como estudiantes, práctica impromptu, implementación en el aula y formación de comunidades de práctica*. Para este trabajo el énfasis se hace en la descripción del diseño y en los resultados obtenidos al implementarlo con estudiantes de educación secundaria (detalles de estas etapas se pueden ver en Carmona, et al., 2014, pp. 17-18). Tales resultados se analizan bajo la lente de AiC, modelo RBC-**C**.

3.1 Participantes y recolección de datos

La población estaba conformada por dos grupos vespertinos de secundaria que iniciaban el tercer grado y que en lo sucesivo se distinguirán como A y B. Respecto a los conocimientos previos de los estudiantes acerca del concepto de función, se puede mencionar que en el grado anterior se abordaron "situaciones problemáticas del tipo valor faltante" sin llegar a formalizar el concepto de función ni sus expresiones, en este nivel, "$y=kx$" y "$y=mx+b$". Cabe señalar que, pese a que el programa de matemáticas de secundaria vigente, incluye algunos contenidos relacionados con el concepto de función lineal y sus representaciones, esto no significa que los estudiantes cuenten con un conocimiento consolidado respecto a este concepto y a los elementos involucrados, más aún con las ideas básicas o nociones del mismo. Es importante mencionar que antes de la implementación, no se retomó el tema de función con los estudiantes, es decir, la secuencia fue el primer acercamiento para propiciar la emergencia de modelos en los cuales la noción de función y sus diferentes representaciones cobran relevancia.

El grupo A, estaba integrado por 16 alumnos (5 mujeres y 11 varones) organizados en 8 parejas, de edad promedio 14 años; mientras que, en el grupo B participaron 12 estudiantes (6 mujeres y 6 varones) agrupados también en parejas. El nivel socioeconómico de la escuela es bajo, se encuentra en la zona periférica de la ciudad de Durango, México y un alto porcentaje de los estudiantes se insertan en esta escuela, luego de ser dados de baja de otras, a razón de su bajo desempeño y actitudes disruptivas. El nivel socioeconómico y situación geográfica de la escuela fueron elementos determinantes para la selección de los grupos y de las actividades con material concreto.

La recogida de datos se realizó por medio de: grabaciones de video, informes escritos y notas de campo. Las interacciones ocurridas en el aula fueron transcritas y para cada tarea se realizó un análisis de la interacción del grupo y el profesor y de sus respuestas escritas en las hojas de trabajo (Anexo A). Los tiempos de implementación variaron en los grupos, con el grupo B se dedicaron 4 horas, mientras que con el grupo A se extendieron hasta 6.

3.2 Diseño propuesto

La secuencia didáctica que se implementó con los estudiantes fue resultado de la etapa 1 del Modelo de Desarrollo Profesional Docente mencionado al inicio de la sección 3. Esta secuencia fue seleccionada y adaptada por el profesor titular de los grupos participantes tomando como referencia su contexto. La secuencia consta de dos hojas de trabajo (Anexo A) para guiar a los estudiantes en la organización y registro escrito de sus ideas, de tal manera, que la comunicación de sus resultados fuera lo más provechosa posible y se pudiera documentar el aprendizaje.

Para el diseño de las hojas de trabajo se tomaron en cuenta diversas representaciones del concepto de función, el objetivo didáctico y algunas otras características como: partir de una situación problemática auténtica, actual y cercana a los estudiantes; uso de material de bajo costo y fácil acceso; formular preguntas que ayudaran a reflexionar sobre el problema o contenido; explorar, manipular y discutir para resolver la situación; plantear preguntas sobre los resultados en forma de retos; y, extraer conclusiones de la tarea. Concretamente, se proponen las actividades "*Privacidad en los Datos I y II"*.

3.2.1 Actividad Privacidad en los Datos I

En esta actividad, la pregunta guía es ¿cómo "disfrazar" información para asegurar su privacidad? Se deja que los estudiantes expresen sus formas de pensamiento y posteriormente el contexto se introduce como sigue:

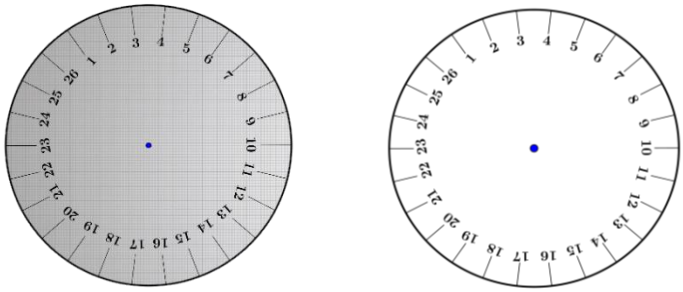
«Con el avance de la ciencia y de la tecnología, se ha vuelto cada vez más indispensable proteger archivos e información para evitar la violación de privacidad. Para dar respuesta a esa necesidad, se buscan métodos seguros para cifrar o esconder mensajes secretos. Los expertos que se ocupan de la seguridad de la información son matemáticos, ellos desarrollan formas para esconder información y formas para descifrarla, según sea el caso. Al estudio de tales formas se le conoce como Criptografía y a los métodos como sistemas criptográficos. La criptografía estudia métodos, que pudieran ser información sensible, de manera que sólo puedan ser descifrados por el receptor y por nadie más que los pudiera interceptar. El emisor y el receptor han de ponerse de acuerdo sobre la "clave" y ésta debe cambiarse con frecuencia. Un ejemplo de tales sistemas criptográficos es el que utiliza el agente Mat, para el cual necesita dos rotores como los de la figura, éstos deben recortarse y ensamblarse con un botón encuadernador de tal manera que sus centros coincidan y puedan girar uno sobre otro».

Enseguida, los participantes se involucran para comprender el funcionamiento del modelo de cifrado y descifrado de información del agente Mat que incluye primero un cifrado simple entre alfabeto y números, y un cifrado de corrimiento utilizando, como material concreto, los rotores giratorios (Figura 2.1).

Mat primero hace una correspondencia natural entre el abecedario y los números ($A \rightarrow 01, B \rightarrow 02, \ldots, Z \rightarrow 26$) *que presenta en una tabla, para minimizar el número de letras sin que se afecte la lectura de los mensajes, ha quitado algunas letras: las compuestas (ll, rr) y la ñ. Con esta asociación descifren el mensaje cifrado: 1502100520092215 1921160518010415*

Enseguida, el agente Mat prepara sus rotores ensamblados y se asegura de que coincidan el 1 con el 1, el 2 con el 2, etc. Luego elige una clave, por ejemplo 3, y gira el rotor pequeño 3 lugares. Así, el mensaje con letras que antes cifró en números (cifrado simple) queda transformado en: 1805130823122518 2224190821040718

Figura 2.1 Rotores giratorios que se ensamblan para cifrar y descifrar mensajes



Fuente: Elaboración propia

A posteriori, los participantes ponen a prueba su comprensión acerca del método del agente Mat y organizados en equipo practican el cifrado de mensajes, especificando la clave utilizada. Además, contestan las siguientes preguntas y justifican sus respuestas:

¿Qué hará el agente Mat cuando necesite cifrar la letra X (corresponde a 24) con la clave 3? Cuando el receptor del mensaje que le envío el agente Mat lo reciba, ¿qué debe hacer para descifrarlo y tener el mensaje original? Explica el método para recuperar el mensaje. ¿Qué debe hacer el receptor del mensaje que ustedes cifraron?

De la interacción con el método del agente Mat, con sus compañeros y con los rotores, surgen una gran variedad de ideas matemáticas que requieren de un espacio de socialización. Para ello, se genera un ambiente para la discusión, revisión, extensión y formalización de todas las ideas de los estudiantes. Finalmente, se presenta una actividad de autorregulación para los participantes: Piensen en una palabra que para ustedes describa la clase de hoy. Elijan una clave y cifren el mensaje. Al día siguiente, intercambien en un papel el mensaje cifrado con un compañero sin mencionar la clave utilizada. Intenten descifrar el mensaje que recibieron y, una vez recuperada la palabra original, entreguen a su maestro. En el Anexo A se puede encontrar la versión completa de la hoja de trabajo utilizada.

3.2.2 Actividad Privacidad en los Datos II

La pregunta guía para esta actividad (ver Hoja de trabajo en Anexo A) es ¿cómo mejorar el "modelo de los rotores" para cifrado de información? Para introducir el contexto se presenta el texto:

Ada y Emy, dos compañeras del agente Mat con quienes intercambia a menudo información, están preocupadas porque si alguien lograra hacerse de sus rotores podría, con algo de trabajo, descubrir la clave en turno y descifrar sus mensajes. Para evitar esta 'tragedia' piensan que es mejor tener en su cabeza el modelo con su respectiva clave y usarlos para cifrar o descifrar el mensaje con ayuda de alguna representación y, una vez alcanzado su objetivo, deshacerse de la evidencia. Ellas proponen una representación diferente para operar en el cifrado y descifrado de información.

Después de introducir el contexto, se enfoca a los participantes en las representaciones tabular y gráfica propuestas por Ada y Emy. Ellos deben utilizar tales representaciones para cifrar y descifrar mensajes y, para lograrlo, deben transitar del uso de los rotores hacia la abstracción del significado de las acciones e identificar el papel de los elementos del modelo en estas nuevas representaciones.

El modelo de Ada propone agregar dos ceros para indicar espacio en blanco para que el mensaje cifrado sea a texto seguido y no aparezcan separaciones por palabras. Propone usar la clave y con ella construir una tabla para cifrar y deshacerse de la misma una vez terminado su mensaje cifrado.Por su parte, Emy ha decidido proponer al agente Mat el modelo con una representación gráfica, respetando la idea de Ada de agregar dos ceros para indicar espacio en blanco y, una vez utilizado para cifrar, deshacerse de él.

Una vez que los participantes han interactuado con las representaciones propuestas y discutido en sus equipos, se procede a una discusión grupal para formalizar las ideas surgidas. Se deja como tarea pensar y justificar las respuestas de las preguntas siguientes:

¿Cómo quedaría el modelo de Ada con su clave si lo pasamos a su equivalente en el de Emy?
¿Cómo quedaría el modelo de Emy usando su clave si lo traducimos al de Ada?

4. Resultados

En esta sección se exponen los resultados obtenidos en la implementación las actividades detonadoras y de exploración de modelos con los dos grupos de estudiantes A y B.

Para el análisis de resultados se establecen las categorías: *(1) Modelo concreto del rotor; (2) Modelo algebraico; (3) Modelo tabular; (4) Modelo gráfico; y, (5) Transición entre representaciones y modelos*. Las interacciones se analizan a la luz de AiC Modelo *RBC-**C*** y en los fragmentos presentados se destacan en negritas las acciones de construcción.

4.1 Resultados del Grupo A

El grupo se organizó en 8 equipos de 2 estudiantes cada uno, se trabajaron cuatro sesiones consecutivas en 6 horas de instrucción. Enseguida se describe el proceso de desarrollo de modelos que propició la secuencia propuesta en la Sección 3.2 y en el Anexo A.

Modelo concreto con el rotor

Se inicia la sesión presentando un mensaje cifrado, mediante la asociación natural entre el abecedario y su número correspondiente en posición, para que sea descifrado por los estudiantes a modo de reto. Encontramos *R-acciones* cuando los estudiantes intuyen formas de cifrar mensajes [4] y buscan la naturaleza del mensaje [6] y las enlazan para la *B-acción* [8] en la que se concreta la asociación abecedario-números naturales. El profesor provoca una *R-acción* [9] para que se dé la *B-acción* [10] de poner dos cifras por letra con la finalidad de uniformar y evitar conflicto con cifrados con dos dígitos (por ejemplo, en la asignación natural, a la Z le corresponde el 26 y se podría confundir con BF, si a la B se le asignará sólo el dígito 2 y a la F el dígito 6). Esto los lleva a la *C-acción* [12] en la que hacen explícito el proceso de cifrado con la asociación natural entre alfabeto y números. En esta parte, el profesor introduce la idea de una entidad que acepta una entrada y produce una salida [13], misma que puede ser valiosa al formalizar el concepto de función.

Analizaron la pertinencia de asignar dos dígitos a cada letra del alfabeto para uniformar la asignación, la mayoría elaboró una tabla de correspondencia y descifraron el mensaje. Luego, se observan *B-acciones* [14 y 16] cuando vinculan este conocimiento con los rotores, que es el material concreto proporcionado para la actividad. Inicialmente los alumnos no identificaron el funcionamiento del rotor, fueron necesarias la construcción de la tabla y la intervención del profesor para entenderlo.

[1] P: Recibí un mensaje que no es claro para mí y pensé que ustedes podían ayudarme. No es claro porque el mensaje viene encriptado. Es decir, utilizaron una clave secreta para proteger la confidencialidad. ¿Dónde podemos encontrar situaciones en las que se requiera proteger datos?
[2] As: En una computadora con una clave … una USB puede tener contraseña.
[3] P: Podemos ir incrementando la confidencialidad de acuerdo a la importancia de los datos: en un banco, en el gobierno. Por ejemplo, en un conflicto de guerra, ¿cómo harían ustedes para enviar un mensaje?
[4] As: Por medio de números [pide explicación]. Poniendo un número para cada letra.
[5] P: A ver, este mensaje es el que necesito que me ayuden a traducir [apunta]: 020905142205140904151 9-01-20051803051815. [Trabajan] ¿Ya lo descifraron? Alguna idea de ¿cómo hacerlo? Imaginen que de esto dependen vidas, ¿cómo descifran?
[6] As: ¿Sería dinero todo esto?
[7] P: ¿Es posible?, si fuera dinero ¿tendría sentido iniciar en 0?
[8] As: No, no es cantidad … se pueden poner los números de acuerdo al orden. El 0 es la A, el 1 la B,
[9] P: Entonces, la primera palabra tiene 22 letras ¿Existirá una palabra así?
[10] As: No, … [Trabajan] … Puede ser por pares. El 01 sería la A … Tenemos una palabra de 7 letras.
[11] P: Son buenas pistas. ¿Requieren de más datos para resolver esto? [asienten], […]
[12] As: El 01 es la A, 02 la B … [muestran acuerdo con la asociación natural]. La primera palabra sería: "BIENVENIDOS".
[13] P: Muy bien, entonces este es el mensaje y la "máquina" que me permite codificarlo es esta asociación: La A con 01, B con 02, C con 03, …
[14] As: Utilizando el rotor el mensaje es "BIENVENIDOS A TERCERO".
[15] P: Sí, algo que podemos observar es que el rotor no tiene ceros, que tiene que ver esto..
[16] As: Es que se le dan dos cifras porque deben ser pares para no confundir. Si no estuvieran los ceros cómo saber en 295 si es 2 o es 29. Sí, es para una división exacta, igual de números por letra.

Posteriormente, se les propone un segundo mensaje cifrado (con clave) [17] y al querer aplicar el procedimiento previo se da una *R-acción* en la que identifican que carece de sentido [18]. Esto provoca la *B-acción* [20] que indica el uso de rotores con giro (clave). En ese momento se les facilita el rotor para su manipulación y exploración; posteriormente, construyen (*C-acción*, [22]) el modelo concreto para cifrar. A diferencia del grupo B, este rotor contenía letras y números. Las acciones que suceden [23-34] son acciones de consolidación (***C**-acciones*) para este modelo.

[17] P: […] Veamos si pueden descifrar otro mensaje [escribe]: 082019 – 10242510 – 1920 – 010619 – 06 – 2120091023. Si seguimos trabajando con el mismo sistema, ¿qué diría en la primera palabra? ¿Tiene sentido?
[18] As: "HTS", …, no tiene sentido.
[19] P: ¿Seguramente algo pasó? Para el mensaje anterior necesitaban los dos rotores [no, contestan]. Entonces, ¿por qué tendrá dos círculos el rotor? Tendremos que hacer algo, manipular los rotores tal vez. [Siguen trabajando] ¿Qué elementos necesitarían para poder descifrarlo? [exploran los rotores y tratan de descifrar el mensaje].
[20] As: Si acomodo los rotores primero con la posición de las letras y después giro uno.
[21] P: El círculo blanco tiene números y letras. El morado sólo números, a ver, entonces, dicen que el giro me permite encriptar mensajes. Si giro un lugar la A ¿dónde queda? [en 2 responden]. Entonces qué valor le corresponde al 08 [de la palabra cifrada 082019] ¿cuántos lugares se avanza para que tenga sentido el mensaje?
[22] As: La regla sería que cada número avanzara el mismo número. Por decir que todos avancen 4. Hay que encontrar esta regla [clave], lo que debemos avanzar.
[23] P: ¿Qué dice ahí? [mensaje]
[24] As: CON
[25] P: Así es, entonces que tienen que hacer para descifrar el mensaje, usen su rotor.
[26] As: [Para descifrar] Se le resta 5 [al mensaje cifrado]
[27] P: Quiere decir que la C (el 03) está en el número 8 del rotor morado … Entonces a la E que le corresponde en el [mensaje cifrado]
[28] As: El 10
[29] P: Entonces que letra es esta [24]
[30] As: La S
[31] P: ¿Están siguiendo a su compañera? [asienten]. ¿Qué sigue? … el 25, ¿qué letra es?
[32] As: La T
[33] P: ¡Completen el mensaje, descífrenlo!
[34] As: [Trabajan … Risas] Dice: "CON ESTE NO VAN A PODER"

Inician la lectura acerca del estudio de la Criptografía (Hoja de trabajo, Anexo A), y contestan las preguntas. Aquí vemos que las acciones mostradas [35-40] son ***C**-acciones* que consolidan o reafirman el funcionamiento del modelo del rotor.

[35] As: Ya profe este mensaje dice "OBJETIVO SUPERADO"
[36] P: Lo encontraron sólo con el rotor blanco [cifrado por asociación natural]. Pero, luego aparece cifrado de otra manera, con una "clave", ¿a qué se refiere esta clave?
[37] As: A avanzar 3. [
38] P: Muy bien, aquí la clave es 3, pero podemos elegir cualquier clave […] y la clave nos dice cuanto avanzar o girar (en el rotor). Por ejemplo, si la clave fuera 4, ¿qué números le corresponden a la A y a la M?
[39] As: Quedan en el 5 y en el 17.
[40] P: Una vez que sabemos cómo funciona el método con el rotor, vamos a cifrar mensajes [monitorea y pide que contesten la Hoja de Trabajo].

En la construcción de este primer modelo, para el proceso de cifrado y descifrado de mensajes, se puede observar que basan el cifrado en el uso del rotor, asociando la clave con giro que se hace en el material para identificar la "posición final" que corresponderá a cada letra; esto es, describen el proceso de cifrado en términos del uso del material concreto. Para cifrar todos hacen referencia al movimiento del rotor y 4 equipos (mitad del grupo) lograron establecer una relación aritmética para cifrar y descifrar mensajes (una producción similar se manifestó en el grupo B, tal como se muestra en la Figura 2.4).

En esta parte, con la intención de evaluar, el profesor los conduce a que retomen el proceso de cifrado y descifrado, les pide que cada equipo cifre una palabra, la intercambie con otro equipo y descifre el mensaje cifrado por ellos y viceversa. En esta actividad los equipos tardaron 8 minutos aproximadamente y sólo un equipo mostró dificultad con el cifrado, ya que se quedaron en la primera parte del proceso y el profesor los apoyó para el segundo paso (sumar la clave). En el siguiente fragmento podemos ver que los estudiantes muestran tres *R-acciones* [42, 44 y 52] y las utilizan para concretar las *B-acciones* de cifrar el mensaje y descifrar el de otros, para descifrar el de otros deben "descubrir la clave" que haga que el mensaje sea una palabra. Principalmente, realizan *B-acciones* para buscar ¿cuáles tienen oportunidad de representar una vocal? [48] y para buscar el número apropiado que usarán como clave para restar y descifrar. La acción de construcción del proceso para descifrar es explícita en [56 y 57]

.

[41] P: Recordemos el proceso de cifrado ¿qué se hace?
[42] As: A cada número le damos una letra.
[43] P: Sí, asociamos el número correspondiente a cada letra del alfabeto.
[44] A: Sumamos la clave
[45] P: Muy bien, usamos la clave y ciframos. Bueno, por equipo piensen en una palabra, usen su propia clave y cifren su mensaje. Me entregan los mensajes cifrados y yo los intercambio con otros equipos para que descifren su mensaje. [Trabajan en equipo, entregan al profesor, intercambia]
[46] P: [Supervisa] Sólo han realizado la parte de asociar el mensaje a un número, ¿ya tienen su clave? ¿cómo la usan?
[47] P: [Intercambia los mensajes] Ahora, ¿cómo descifrar un mensaje si no conozco la clave? ¿de las 26 letras alguna aparece más?
[48] As: La "a", …, la "e", bueno todas las vocales.
[49] P: ¿Qué necesitamos hacer?
[50] As: Encontrar la clave
[51] P: Bueno esa sería la primera pista y ¿cuántos números le asociamos a cada letra?
[52] As: Partimos en dos la palabra
[53] P: Muy bien y hay que buscar ¿qué clave le da sentido a "ese mensaje"? [ya descifrado]
[54] P: [Trabajan] A ver, ¿alguien reconoce este papelito?
[55] As: Sí, es nuestro
[56] As: [Un equipo] La palabra de ellos que nos tocó, es "INTERESANTE".
[57] As: La que nosotros desciframos fue "HOLA"

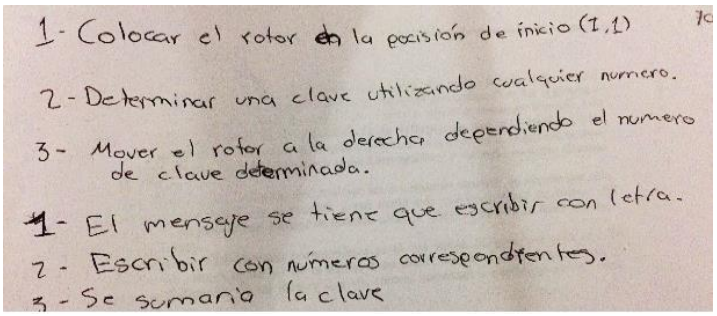
Enseguida, se muestra la construcción de elementos para un pensamiento cíclico (*C-acción* [61]). Aquí, 5 de los 8 equipos identifican el ciclo del abecedario y proponen "procedimientos" para dar continuidad con el cifrado una vez que el número inicial sumado a la clave superan los 26 dígitos que componen un ciclo.

[58] P: A ver, si ahora quiero mover la T, que corresponde al 20, con clave 12…
[59] As: Queda 32
[60] P: Pero, aquí no hay 32 [en el rotor], entonces, ¿qué pasó?
[61] As: Reinició después del 26 … queda en el 6

Modelo algebraico

Para la construcción de este modelo se dejó que los estudiantes trabajaran desde su experiencia con el modelo del rotor. Aquí 4 de 8 equipos lograron describir el proceso para cifrar y descifrar mensajes, sin embargo, escriben incluso paso a paso, el procedimiento que hay que seguir al usar el rotor, sin que esto llegue a un modelo algebraico, no establecen fórmulas ni asignan literales a las variables (Figura 2.2).

Figura 2. 2 Descripción de los pasos para cifrar mensajes



Fuente: Producciones de los estudiantes

Mientras que 2 equipos sí logran describir el proceso, no llegan a establecer una expresión algebraica, no obstante, si logran representar simbólicamente algunas "variables" como, *"P"= posición "C"= clave "M_c"= mensaje cifrado*. El profesor pide que lo sigan reflexionando y el siguiente módulo retoma. Él se muestra inquisitivo para provocar en los estudiantes *C-acciones* [63 y 65] que conformen el proceso de cifrado y descifrado y lo plasmen en una expresión algebraica. A partir de ahí son utilizadas las fórmulas para las ***C**-acciones* que consolidan este modelo, dado que con él, ahora cifran mensajes y detectan errores [69, 70, 72]. En [72 y 73] se muestran acciones de reconocimiento del "espacio" entre palabras y cómo cifrarlo. Esto puede ayudar a refinar el modelo haciendo que sea más seguro al no revelar la separación entre palabras.

[62] P: La clase anterior ciframos y desciframos mensajes, primero con el rotor. Para deshacernos de él se establecieron otras formas de hacerlo, un par de fórmulas, ¿cuáles fueron?
[63] As: Para cifrar un mensaje se usaba la posición inicial más la clave. [Los estudiantes guían al profesor para que escriba en el pizarrón la fórmula de cifrado *MC=P1+C*]
[64] P: Recuerdan cómo descifrar.
[65] As: Lo contrario, ahora la posición final y restamos la clave. [Guían al profesor para que escriba MD=PF-C]
[66] P: De acuerdo a esto [señala las fórmulas para el proceso de cifrar y descifrar], ¿cómo sería cifrar esta frase? … [escribe la frase "CLAVE SECRETA"], usando la clave 7 ¿qué números van aquí?
[67] As: 03, ... ,12, 01, …,21,05 [el 21 lo corrigen] [68] P:"SECRETA" ¿cómo queda en números?
[69] As: 19, 05, 03, …,18, 05, 20, 01[el profesor escribe seguidos los números]
[70] As: Entonces en la de "CLAVE" no va el 21 es un 22 [el profesor corrige lo escrito]
[71] P: Ahora ya tenemos el mensaje correspondiente asociando el alfabeto con números. No hemos usado la clave.
[72] As: [Dictan al profesor el mensaje cifrado sumando la clave 7] 1019080412 espacio 26121025120108.
[73] P: [El profesor aprovecha el dictado del espacio para llevarlos a otra actividad que refina el modelo] ¿Qué pasa si alguien encuentra estos números? Aunque no tenga rotores o la clave, ¿se dará cuenta que hay un mensaje "escondido"?

Modelo tabular

Desde el inicio de la actividad hemos visto que los estudiantes construyen su propia tabla, dada la necesidad de ayudar al profesor a descifrar su mensaje (fragmento [1-34]). En cuanto a la comprensión y manejo de la tabla de asociación, se puede afirmar que reconocen la asociación letra-número como algo natural, y la tabla surge como iniciativa del grupo a partir de la necesidad de descifrar el primer mensaje. Son los estudiantes los que proponen la tabla inicial, una vez que conocen y manipulan el rotor, la tabla pasa a segundo término y basan el cifrado y descifrado en el uso y exploración del material concreto. Aunque tardan en desprenderse de los rotores, logran refinar este modelo con el modelo tabular propuesto por la Agente Ada (Hoja de trabajo en Anexo A), desde las *R-acciones* [75 y 77] de incorporación del 00 como espacio y con ello las *B-acciones* [71, 78]. Tal refinamiento se muestra en la *C-acción* [83] en la que, con éxito, lo aplican.

[74] P: [Leen el modelo de Ada y llenan la tabla] Las letras son 26, ¿es correcto trabajar con 26 elementos?
[75] As: No, son 27 ahora con el "espacio" [entre palabras]
[76] P: Exactamente, tenemos un lugar más. ¿El ciclo dónde termina?.
[77] As: En el 27, porque se agrega el espacio.
[78] P: ¿Cuál letra corresponde al 19?
[79] Q: La S (en el cifrado con clave 8)
[80] P: Entonces, ¿cómo quedaría el mensaje "SOMOS AGENTES DE CAMBIO"?
[81] As: [Dictan al profesor] 2722202227 y luego 09
[82] P: ¿Seguros?
[83] As: [Revisan] ¡Ah no! El espacio es 00 y con la clave es 08. Sigue 080915132 … No profe, tenemos errores [corrige]:
272321232708091513220113270812130811092110172 3

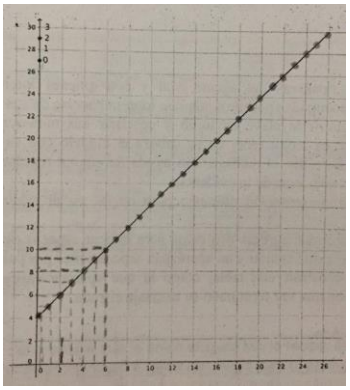
En sus producciones escritas todos los equipos completaron la tabla de manera correcta, considerando el "00" como espacio; previa intervención del docente, que hizo hincapié en revisar todos los elementos involucrados en el modelo tabular, pese a ello, un equipo al cifrar la frase "SOMOS AGENTES DE CAMBIO" utiliza comas para separar las palabras en lugar de "08" (correspondiente al espacio cifrado).

Modelo gráfico

Este modelo es interesante, dado que, en él de manera natural surgen conceptos asociados tales como: variable discreta, pensamiento cíclico, contextualización de las coordenadas, identificación de la clave de cifrado con la ordenada en el origen, cifrar, etc. Aquí los estudiantes discuten en equipo para responder las preguntas de la Hoja de trabajo (Anexo A). El profesor monitorea y al hacerlo identifica que algunos de los estudiantes ya se han dado cuenta que si unen los puntos o pares ordenados (M, M_C) se obtiene una recta, pero en el proceso de cifrado sólo algunos puntos sobre ella son los que les interesan: los puntos (M, M_C). Es decir, identifican que se trata de un ejemplo discreto al remarcar tales puntos (Figura 4.2). En la socialización vemos que hay *R-acciones* para reconocer los principales elementos de la gráfica (ejes, recta, intersección de la recta con eje de las ordenadas) que aparece en su hoja de trabajo. Luego, suceden *B-acciones* que asocian la clave utilizada con el cero (que representa el espacio entre palabras), así la clave es la ordenada al origen [85, 87], también las que identifican el mensaje original con el eje de las abscisas [89] y el mensaje cifrado con el de las ordenadas [90] y encontrar e interpretar coordenadas específicas [91, 93, 95, 97, 99] y, como *C-acciones* podemos observar que en [100] cada estudiante logra representar e interpretar una coordenada en este modelo abstracto para cifrar y además, hay la construcción y comprensión de un ejemplo discreto [102], los cuales en el contexto escolar son poco estudiados (Figura 2.3).

[84] P: Vean la gráfica y vamos a tratar de comprenderla [les pide que recuerden el modelo tabular de Ada]
[85] As: Está usando la clave 4 [modelo de Emy]
[86] P: ¿Por qué? … ¿Al cero que le corresponde?
[87] As: Donde inicia la gráfica, en la línea vertical
[88] P: A ver, aquí [señala la gráfica] ¿dónde estará el mensaje original?
[89] As: El original está en la horizontal
[90] P: Entonces el mensaje original está en el eje de las abscisas y el mensaje cifrado [contestan los alumnos que en el eje vertical] ¿qué valor le corresponde al 8?
[91] As: 12 [la clave es 4]
[92] P: Entonces, aquí está el punto correspondiente al valor cifrado [dibuja] ¿qué valor representa el cero?
[93] As: Representa al "espacio" [entre palabras]
[94] P: Sí, ¿y ya cifrado?
[95] As: Al 4
[96] P: El 1, ¿con quién se cifra?
[97] As: El 1 va con el 5, el 2 con el 6 [el profesor dibuja los puntos que le dictan]
[98] P: Marquen sobre la recta del modelo de Emy todos los puntos que representan al mensaje original y al mensaje cifrado.
[99] As: Como coordenadas todos los puntos del abecedario.
[100] P: Sí [trabajan y el profesor monitorea, luego pasa a cada estudiante a representar en el pizarrón un punto (Mo, Mc)]
[101] P: [Ya que terminan] ¿Qué pasa con el 1.5 del eje x? ¿La agregamos un 4, la clave?
[102] As: No, ese punto no existe aquí … No tenemos una letra entre la A (o sea el 1) y la B (el 2), sólo valen enteros.

Figura 2.3 Modelo gráfico con clave 4



Fuente: Producciones de los estudiantes

En el registro escrito, sólo 2 equipos ubicaron los puntos en la gráfica cuando se les pide representar el modelo de cifrado para que con él cifren o encripten la frase 'SOMOS AGENTES DE CAMBIO', el resto lo hizo con la recta completa. Por otra parte, 4 de los 8 equipos muestran evidencia de interpretar las coordenadas como (posición inicial, posición cifrada) y los otros 4 exhiben confusión en la interpretación de la pregunta, ¿Qué representa la primera coordenada de un punto sobre la recta? ya que, consideran como primera coordenada al punto (0,4) o bien el (1,5) asociado a la letra "A".

Dos equipos grafican un ciclo, es decir, el último punto representado es (22, 26). Otros 5 equipos muestran otros puntos que indican que el 23, al aplicarle la clave de cifrado (4), se corre al 27 que indica inicio de ciclo, esto es, se va a 0 y se reprenta como (23,0) y grafican hasta que "se concluye" un ciclo en el eje vertical quedándose hasta el 27, el último equipo grafica más de un ciclo. Usualmente, en las gráficas utilizadas para representar relaciones funcionales se graduan los ejes utilizando números de manera consecutiva. En este caso, se graduaron los ejes con números pares y en los equipos no se presentó problema con esta graduación. Ellos comprendieron que la letra A sin cifrar es 1 y se representa en el eje de las abscisas a la mitad de 0 y 2. Finalmente, un equipo comenzó en la coordenada (0,8) ubicándola en el origen de manera errónea.

Transición entre representaciones o modelos

En el siguiente fragmento podemos apreciar acciones de consolidación, ***C****-acciones*, de los modelos tratados anteriormente (concreto, tabular, gráfico y algebraico) al realizar correctamente la interpretación de sus elementos. Finalmente, podemos observar en [116, 118 y 120], ***C****-acciones* en las que se construye comprensión, al hacer explícita la transición y conexión entre las diferentes representaciones.

[103] P: […] Repasemos, ¿qué significa el (2, 6)?
[104] As: Una coordenada de la gráfica … que B se cifra en F … El número sin cifrar es 2 y el número cifrado es 6.
[105] P: ¿Qué hay entre ellos?, ¿qué los relaciona?
[106] As: La clave, al primero le sumamos 4, que es la clave y llegamos al segundo, cifrado.
[continúan usando gráficas para cifrar]
[107] P: [Con otros ejes] Si ahora la clave fuera 12 ¿cómo quedaría? Menos o más inclinada.
[108] As: Más inclinada
[109] P: Por ejemplo, el 2, ¿con quién iría?
[110] As: Con el 18 …No, con el 14… Sí el 14.
[111] P: ¿En cuál hay mayor ángulo de inclinación?
[112] As: En la de clave 12.
[113] P: Si representáramos la tabla del modelo de Ada, aquí en la gráfica ¿cómo quedaría?
[114] As: Así como esa, empezando el 0 con 8 que era la clave [de Ada]
[115] P: ¿Con qué otros valores?
[116] As: (0, 8), (1, 9), (2, 10), …
[1 [117] P: Si a la clave le llamamos C, piensen en una e expresión que resuma toda esta actividad
[118]As: x+c =y
[119] P: Esto propone Andrea, ¿qué significa?
[120] As: Que a los números originales se les va a sumar una clave y se tendrán los cifrados. Esto representa la manera en la que encriptamos.

Cabe mencionar que esta sesión terminó de manera apresurada y eso puede explicar que el profesor, en [107], muestra una acción que provoca el abordar la inclinación de la recta, en la cual están incluidos los puntos de cifrado, para explorar la familia de rectas paralelas al variar la clave y ver que este parámetro mantiene invariante la pendiente o inclinación de las mismas. No obstante, en [111] cuando vuelve a preguntar y se responde en [112] de manera errónea, el profesor no corrige esta respuesta, aunque en el pizarrón se pueden apreciar las rectas paralelas.

4.2 Resultados del Grupo B

Se trabajó con 6 equipos de 2 estudiantes cada uno para implementar la secuencia en dos sesiones cubriendo 4 horas en total. Enseguida, se describen los modelos desarrollados por los estudiantes para interpretar las situaciones propuestas en la Sección 3.2.

Modelo del rotor

En esta parte el profesor realiza una introducción que provoca en los estudiantes diferentes *R-acciones* asociadas con la relevancia de una situación real, actual y cercana a ellos [122, 124, 126]: la protección de datos o información personal. Con tales acciones, logran expresar un modelo de cifrado en una *C-acción* [130] y códigos públicos [134].

121] P: Levante la mano ¿quién tenga un celular? [casi todos], ¿quién le ha puesto contraseña a su celular?, ¿quién tiene un Facebook (FB y su contraseña? [casi todos]. Bien, ¿por qué creen que es importante tener contraseña?
[122] As: Por seguridad … Para que nadie se meta en tu FB a revisar tus cosas … Por privacidad.
[123] P: ¿Dónde más creen que es importante mantener la seguridad de su información?
[124] As: En una red social ... En el correo electrónico … En un banco, cuando depositas dinero y así … En el gobierno. En cajas fuertes. En una casa. Candados de tu bici y de las maletas.
[125]P: De acuerdo a la importancia, se imaginan ¿cómo se debe incrementar el nivel de seguridad? ¿Qué protegemos en FB?
[126] As: Mensajes, conversaciones, archivos.
[127] P: En general, información que se deba proteger […] ¿Qué harían ustedes para proteger información?
[128] As: Utilizar un código
[129] P: ¿Cómo sería ese código?
[130] As: Con números … con letras … combinando los dos … con símbolos para sustituir palabras o letras …
[131] P: ¿Desde cuándo creen que existe la necesidad de proteger información?
[132] As: Desde siempre/Desde que existen los gobiernos/ Las guerras …
[133] P: Por eso, la importancia de tener sistemas cada vez más sofisticados para protegerla.
[134] As: El código Morse … El código binario
[135] P: Estos son códigos públicos, también los hay privados y otros públicos casi imposibles de descifrar [continúan y hablan de que incluso hay algunos que utilizan números primos]

Para la construcción de la correspondencia entre el alfabeto y los números naturales como un cifrado simple, en la primera actividad (Sección 3.2.1), el profesor pide a algunos estudiantes que lean la situación que describe el método que usa el agente Mat y se asegura que la comprendan. Se observan *R-acciones* [137] para identificar los principales elementos del método; *B-acciones* para enlazar la información [138], detectar posibles problemas [139], proponer formas de resolverlos [141, 143] y construir una solución funcional en la *C-acción* [145], mostrando la asociación natural de números con el mismo tamaño (dos cifras) con el alfabeto. Con la comprensión del método construido, emprenden una ***C**-acción* de consolidación [146] al descifrar un mensaje. Mostraron comprensión y manejo en la tabla y su interpretación como correspondencia natural.

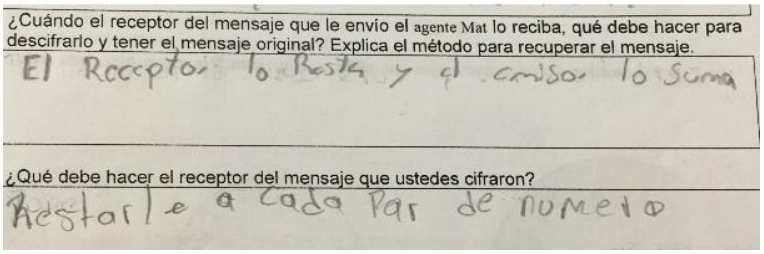
[136] P: ¿Cómo funciona el método del agente Mat? [reparte el material] ¿Ayúdenme a interpretar la tabla? [Tiempo de espera].
[137] As: Cada letra tiene un número de acuerdo a su posición. Aquí tenemos dos [tipos de] rotores, unos con letras y otros con números.
[138] P: A ver, si quiere escribir "HOLA" ¿cómo queda? [Pasa una alumna al pizarrón y escribe 815121]. Están de acuerdo [asienten]. Sin embargo, ¿qué problema podríamos enfrentar para descifrar esto?
[139] As: Que están todos los números juntos.
[140] P: Por ejemplo, este primero no sé si es 8 o es 81, o el 15, no sé si es 1 y 5 o 15. ¿Qué cambio le haríamos a esto para evitar el problema?
[141] As: Separarlos [escribe 8, 15, 21, 1]
[142] P: ¿Qué les parece está solución? A lo mejor su compañero Gustavo intercepta este mensaje ¿cuál de ellos tendría más probabilidad de descifrar?
[143] As: El segundo, el de la separación [pide explicación el profesor]. Porque están separados los números y pensaría que cada uno es una letra.
[144] P: ¿Qué hago para evitar esto? […]
[145] As: Que estén juntos, pero con un mismo tamaño [lo pasa al pizarrón y escribe 08151201].
[146] P: […] Cada número con longitud de dos cifras y ahora sí podemos identificar que el 08 es la letra H, 15 es la O, [pide que descifren un mensaje que aparece con números]. ¿Qué dice ahí? [lo descifran bien "objetivo superado"].

Para construir el conocimiento acerca del proceso para cifrar y descifrar utilizando un desplazamiento como "clave de cifrado", los estudiantes exploran el material concreto de los rotores y exhiben *R-acciones* [147, 149] para identificar su funcionamiento desde la experiencia anterior. También se observan *B-acciones* [151, 153] para enlazar la información previa, con la necesidad de tener un sistema de cifrado más seguro. En [159] muestran una *C-acción* en la cual proponen dos modelos de cifrado, uno de permutación y el otro un cifrado con clave de corrimiento 3, que justamente es el que propone el agente Mat y ellos aún no han estudiado. El profesor enseguida provoca ***C**-acciones* para extender la comprensión del método construido [160, 161, 163, 164]. Derivada de tales acciones surge una *C-acción* en la cual se construye el proceso inverso para descifrar [165]. Luego, suceden ***C**-acciones* que reafirman este proceso [166-169].

[147] As: [Una alumna expresa que si lo hiciera con los rotores le cuesta] Aquí, las letras no sabes en qué número van.
[148] P: ¿Qué harían ustedes para evitar esto?
[149] As: Aprenderse cómo acomodarlos [los rotores]… Ponerles las letras correspondientes a los números… Aprenderse la posición del abecedario, en número,
[150] P: Creen que este sistema de asociación [simple] sea muy sofisticado, o sea fácil de descifrar por alguien que lo intercepte. Por ejemplo, para ustedes, ¿cómo sería descifrar este mensaje?[020905132205130904141 9]¿Qué diría?
[151] As: [contestan] "BIENVENIDOS".
[152] P: A ver, si yo pusiera este mensaje a otro grupo ¿lo podrían descifrar?
[153] As: No, porque no saben cómo funciona [el método]…Tal vez sí se imaginen.
[154] P: Podemos decir que: al ser la asociación natural, hasta cierto punto es fácil. ¿Qué podemos hacer para mejorarlo?
[159] As: Podemos mover algunas posiciones. Intercambiar la primera con la tercera y, la segunda con la cuarta, y las demás igual [05130209220513090414 19]… También podemos sumarles algo como 3 y quedaría [anota 0512081625081612071722].
[160] P: El mensaje quedó cifrado así [señala] ¿qué hizo para transformarlo? [sumar 3, contestan]. Bueno, a esto el agente Mat le llama "clave". La clave es 3.
[leen lo que sigue] A ver si tenemos la A en el rotor grande, en el rotor pequeño, ¿qué le corresponde? [El 01, responden], ahora gírenlo cinco lugares, la "clave" sería 5. Con los rotores practiquen este sistema, cifren su propio mensaje [monitorea]. A ver usted me dice su mensaje ya cifrado.
[161] As: 11181504042123242118 [escribe].
[162] P: [espera] ¿Qué harían para descifrarlo?
[163] As: Buscar la clave … Pues primero poner las letras que son de ahí.
[164] P:¿cuáles tocan? [KRODD] ¿tiene sentido?
[165] As: Yo digo que la clave es 3, podemos restarle el 3.
[166] P: Entonces, ¿qué quedaría? [dictan 08152201 espacio 0118 …] ¿Por qué un espacio?
[167] As: Es que la primera palabra descifrada es "HOLA" y en el espacio se puede poner punto y diría "HOLA.ARTURO"
[168] P: Otro mensaje [Le dictan 082322232017] ¿Qué dice? [Le dictan HW…]
[169] As: La clave puede ser 5. No, no es 5. La clave es 4…No, porque DS no tiene sentido… Si fuera 3, ETS. No, tampoco, es 7, [Profesor:¿qué necesito?]. Conocer la clave, aquí es 2, FUTURO, síiiii.

En este grupo se observa poco uso del rotor, prefieren el uso de la tabla de asociación, además de una comprensión "rápida" del proceso de cifrado. Esto provocó que dejaran de lado al rotor y se enfocaran exclusivamente en la tabla para la correspondencia de letras-números para cifrar y descifrar, sumando la clave al valor correspondiente a cada letra. Ellos logran relacionar el descifrado con la acción de restar la clave (Figura 2.4).

Figura 2.4 Proceso de cifrado y descifrado



Fuente: Producciones de los estudiantes

En cuanto a la observación de un pensamiento cíclico, se puede decir que todos comprendieron la existencia de un ciclo, a partir de las *R* y *B-acciones* [171, 173, 175] y apoyados en ellas logran la *C-acción* [177]. Sin embargo, no todos identifican el proceso; sólo 3 equipos (mitad del grupo) encuentran el valor que corresponde a la "X".

[170] P: Si es 24 la letra y para cifrarla le sumo 3 tenemos 27, pero ¿por qué aquí [en los rotores] sólo llega hasta el 26?
[171] As: El abecedario tiene 26 letras [sin RR, LL, Ñ] Nadamás llega hasta el 26. Entonces, nos pasamos al 02.
[172] P: Entonces vuelve a iniciar un nuevo ciclo. ¿Dónde podemos ver ciclos?
[173] As: En el reloj,… [174] P: Aquí al llegar al 26 ya no pasa al 27, ¿a dónde se iría? [01, contestan]. Si tengo que cifrar la letra V [el 22, responden] si lo cifro con clave 9 ¿cómo quedaría?
[175] As: Quedaría cifrado en 05.
[176] P: [Pregunta de nuevo a un alumno] ¿Qué pasa si llegamos al 26?
[177]As: Empezar a contar de nuevo en 01.

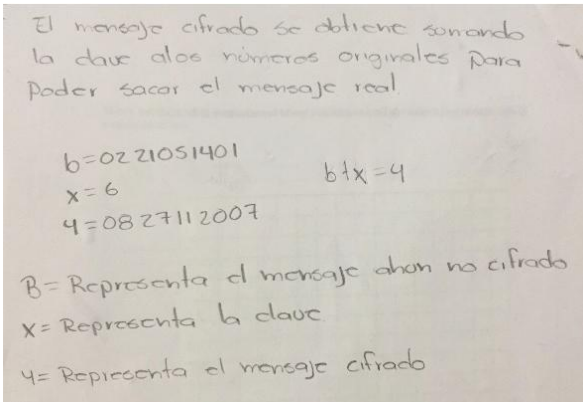
Modelo algebraico

Los alumnos describen el proceso de cifrado en una *B-acción* a través de los pasos a seguir [179]. Con ello, en una *C-acción* [181] asignan una letra al mensaje original, una a la clave y una más al mensaje cifrado, representándolas en una relación funcional $y=x+b$, que puede verse en la mayoría de las producciones escritas que pide el profesor en [182]. No obstante, no se hace una socialización del rango y dominio asociado al ciclo.

[178] P: Vamos a escribir un proceso, a tratar de explicarlo. Díganme con sus palabras ¿cómo sería el proceso para cifrar el mensaje? A ver, "BUENA CLASE" ¿qué debo hacer para cifrarlo?
[179] As: Primero cifrarlo con sus números originales [le dictan] 0221051401 …] … Luego se le suma el número que queramos … La clave … Con una clave 6 … [le dictan] 0827112007.
[180] P: ¿Cómo puedo explicar esto con una fórmula? ¿Cómo quieren llamarle a la clave?
[181] As: "x" la contraseña y al mensaje "b", … al mensaje oculto "y".
[182] P: Bueno, escriban en su hoja de trabajo con sus propias palabras el proceso y con fórmula también. Cada quien con las letras y las palabras que quiera usar y que entiendan mejor.

En la Figura 2.5 se aprecia una explicación de la fórmula explícita, esto da cuenta de una conexión del contexto de la situación a la representación simbólica. Para Lannin, et al. (2008), aunque los estudiantes "batallen" con el uso de variables, y primero sean capaces de describir con sus propias palabras la fórmula, esto constituye un cimiento importante para transitar al uso de los símbolos y a una representación algebraica.

Figura 2.5 Representación simbólica del proceso de cifrado del mensaje



Fuente: Producciones de los estudiantes

Modelo tabular

Si recordamos la interacción para construir el modelo concreto del rotor, podemos ver, que en este grupo, la construcción de una tabla de asociación y su comprensión ha propiciado que de manera temprana el modelo del rotor se haya sustituido por el uso de la tabla. Así, los estudiantes aprehenden el modelo que propone Ada (Sección 3.2.2 y Anexo A), aunque completan la tabla de asociación sin considerar el cambio generado al agregar el "00", que es el espacio entre palabras. Los estudiantes pueden interpretar fácilmente la información para determinar la clave utilizada por Ada y cifrar el mensaje "SOMOS AGENTES DE CAMBIO".

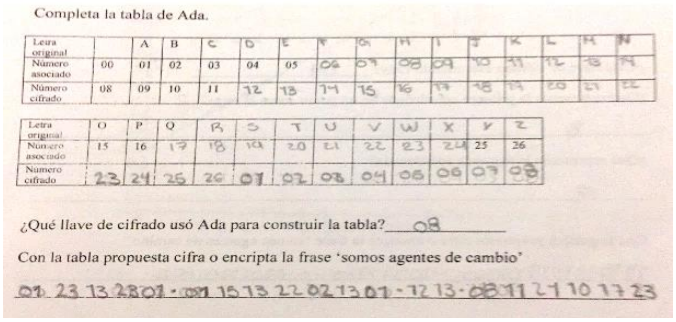
Para salvar la omisión del "00" discuten y analizan este cambio de manera grupal y reconocen la necesidad de agregar el "27" para poder completar el ciclo, cifrar el "espacio" y que no fuera evidente que el "00" lo representaba.

En el siguiente fragmento se puede observar una *R-acción* [186] que atribuye importancia al cifrado del "espacio entre palabras" para refinar y hacer más seguro el proceso de descifrado. Con esto, se provocan *B-acciones* para asignar un número al "espacio" y modificar el número de elementos en juego [188, 191 y 193]. Dada la observación y su buen manejo con las tablas, rápidamente muestran una *B-acción* donde determinan la clave de cifrado de Ada [194] y seguidamente, vienen nuevas *B-acciones* para cifrar el mensaje solicitado con dicha clave y mostrar comprensión del nuevo elemento y la importancia de también cifrarlo [201, 202, 204, 206]. Finalmente, se da la *C-acción* [208] que indica la comprensión de este modelo como un refinamiento del de los rotores.

[183] P: [El profesor aprovecha que al cifrar un mensaje le dictan el espacio entre palabras para llevarlos a un modelo tabular que refina el modelo concreto] ¿Qué pasa si alguien encuentra estos números? Aunque no tenga rotores o la clave se dará cuenta que hay un mensaje "escondido".
[184] As: Sí
[185] P: ¿Por qué?
[186] As: Por el espacio, hay dos palabras.
[187] P: Se puede hacer que [otros] no sepan el número de palabras y hacerlo más seguro.
[188] As: Sí, con un número.
[189] P: Precisamente Ada pensó en esta situación … [Lee e introduce]
[190] P: ¿Con qué número vamos a representar el espacio entre palabras?
[191] As: Con el 00
[192] P: Teníamos 26 letras y agregamos el espacio, ¿cuántos lugares debemos tener ?
[193] As: 27 [llenan la tabla]
[194] P: Cifren el mensaje "somos agentes de cambio" con la clave que usó Ada.
[195] As: ¿El 8?... al 00 le vamos a dar el 09, … ¡nooo!, el 08. ¿Verdad que es el 08?
[196] P: Sí el 08 representa el espacio en blanco y el 8 es la clave. [Monitorea]
[197] As: [En un equipo] Vamos entonces a poner un 08 aquí [señalan el espacio]
[198] P: [Nota confusión] Sí, recuerden que ya no dejaremos espacios entre palabras. 00 es la posición inicial del "espacio" entonces, ¿cómo queda ya cifrado?
[199] As: 08 …Ya profe, listo, … Ya …
[200] P: [Revisa a los equipos] Completen los números que pasan del 26 y escriban el número cifrado correspondiente … Revisen y recuerden que no dejamos espacios entre palabras.
[201] P: Bueno ya utilizando la tabla cifraron "SOMOS AGENTES DE CAMBIO". Cada equipo me va a dictar una letra del mensaje como queda ya cifrada con el método de Ada. A ver, iniciamos con ustedes.
[202] As: 28, no 27, 23, … [entre los alumnos se corrigen y el profesor les pregunta cuando identifica un error]
[203] P: Seguros que la "T" se cifra con 28
[204] As: No, sólo llega hasta 27, ..., empezamos de nuevo con el 01[al final consiguen en grupo dictar al profesor el mensaje cifrado correctamente: 27232123270809151322011327081213081109211017 23]
[205] P: Así debe quedar, sino, revisen su error. Algunos equipos, cuando pasé [al monitorear el trabajo], seguían dejando el "espacio" sin utilizar el 00 y otros más ponían el 00 para el "espacio" ya en el mensaje cifrado. ¿A ver cuál es el error si ponemos 00?
[206] As: Que no estaría cifrado y debemos también cifrar el "espacio" con la clave 8 y queda 00 más 8, queda cifrado como 08.
[207] P: Muy bien, si dejamos ese 00 en el mensaje cifrado, daríamos información de que representa un espacio y entonces el modelo no mejoró [en seguridad]. Entonces, este modelo es el que propone Ada, ¿cuál les parece más fácil, el de los rotores o este [tabular]?
[208] As: Igual, pero este es más seguro …, sólo se agrega el cero para el "espacio" y en lugar de los rotores usamos la tabla.

Podemos observar que este proceso de incluir y cifrar el "espacio" le costó más trabajo al grupo B y el profesor constantemente trata de dirigir la atención y comprensión de los alumnos. Sin embargo, en su registro escrito únicamente sólo 4 equipos reajustan su mensaje cifrado y 2 de estos mantienen el error en la tabla (Figura 2.6). Es decir, la letra S al cifrar con la clave 8 quedaría 00 y ellos ponen 01 y, en el mensaje cifrado en lugar de poner un 08 en el "espacio" ponen un ".[punto]".

Figura 2.6 Modelo tabular, inclusión del 00 como "espacio"



Fuente: Producciones de los estudiantes

Modelo gráfico

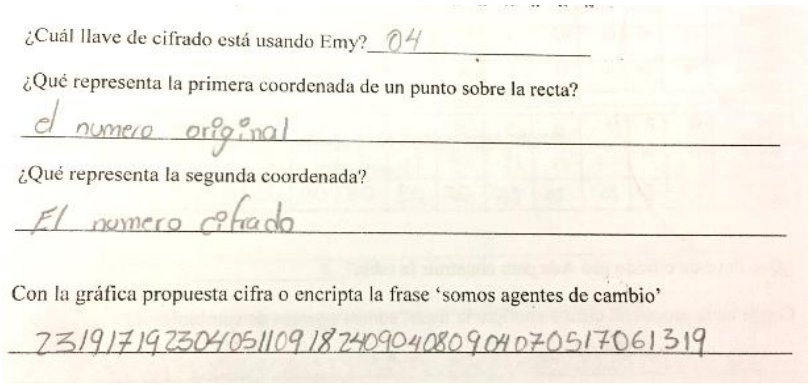
Para la construcción y comprensión de este modelo, primero identifican en las *R-acciones* [210 y 211], ¿qué representa cada eje? Posteriormente, se dan cuenta que la graduación de los ejes va de dos en dos, y exhiben una *B-acción* que muestra que pueden y deben representar también las letras de lugar impar [214]. También, se observa que muestran otras *B-acciones* [218 y 224] que indican cómo relacionar los puntos del eje "*x"* con los del eje "*y"* a través de la clave [218 y 224] y que operan con la información precedente para encontrar la clave como la ordenada al origen. Esto hace que desde las *R* y *B-acciones* anteriores, logren construir el modelo gráfico para cifrar y descifrar al mostrar comprensión e interpretación de los pares ordenados (*C-acción*, [233]).

[209] P: La agente Emy propone otro modelo, pero usando una gráfica. Vamos a analizarlo y me van a decir ¿cómo funciona este modelo para cifrar? Y si hace lo mismo que el del "rotor" y el de la tabla. Si tienen alguna idea me lo hacen saber [monitorea]. Ya dos equipos saben cómo funciona la gráfica
Entonces, en la tabla teníamos una fila para letras, otra para su posición y otra para el mensaje cifrado. ¿Aquí en la gráfica cómo funciona? [reproduce la gráfica que aparece en la hoja de trabajo]... ¿qué podemos decir de la gráfica? … ¿cómo encriptar un mensaje utilizando esto? … Con ella puedo cifrar la frase "CÓMO ANDAS" [210] As: Los números que representan el alfabeto están en la línea horizontal … El cifrado está en la otra [línea/eje].
[211] P: ¿Cómo se llaman los ejes? [espera respuesta] Eje de las abscisas o de las "x" este [señala el horizontal] y éste [señala el] es el eje de las ordenadas o eje "y". ¿Qué representa cada eje? ... Este 2 qué significa [señala las abscisas].
[212] As: ¿La clave?
[213] P: ¿Cómo?, por ejemplo, en este mensaje ["CÓMO ANDAS"] ¿cómo cifro la letra "C"?
[214] As: [Silencio] La "C" la represento en medio del 2 y del 4 … En las abscisas.
[215] P: Muy bien, aquí iría la "C" [la ubica] y ya encriptada ¿cómo iría? ¿dónde?
[216] As: En el otro eje [acá y le señala al profesor sobre el eje de las ordenadas].
[217] P: Depende de cómo cifrar. [218] As: Ah sí, depende de la clave [toman tiempo pensando en cuál es la clave].
[219] P: A ver, ¿qué letra va aquí en el origen?
[220] As: El 00
[221] P: ¿Qué representa?
[222] As: El "espacio" [entre palabras]
[223] P: Muy bien, al cifrarlo ¿a dónde se va?
[224] As: Al 4, …, ¿esa es la clave? [algunos muestran duda y sorpresa]
[225] P: Entonces 00 va al 04. ¿Recuerdan los pares ordenados?
[226] As: Sí, … 00 y 04 [El profesor escribe en el pizarrón (00,04), (01,05)]
[228] P: A ver, la "B" ¿cómo queda representada con el cifrado?

[229] As: (02, 06)
[230] P: Este eje [abscisas] ¿qué representa?
[231] As: El número sin cifrar, …, el mensaje descifrado
[232] P: Muy bien, la posición original o el mensaje "descifrado" como lo dijeron ustedes. ¿Y este [señala el eje de las ordenadas]?
[233] As: Mensaje cifrado, …, posición final
[234] P: ¿Por qué creen que aquí no usan letras [como en el modelo del rotor y el de la tabla]?
[235] As: Para que no sea tan fácil de descubrir … por seguridad … para no poder leer el mensaje.
[236] P: Exactamente, se omiten las letras para que sea más dificil darse cuenta que se usa para cifrar mensajes […] Pero ahora, nosotros sí sabemos que [en las abscisas] el 2 representa la "B" y cifrado en las ordenadas el 6 lo representa. Por lo tanto, ya saben su funcionamiento y pueden contestar las preguntas [de la hoja de trabajo].

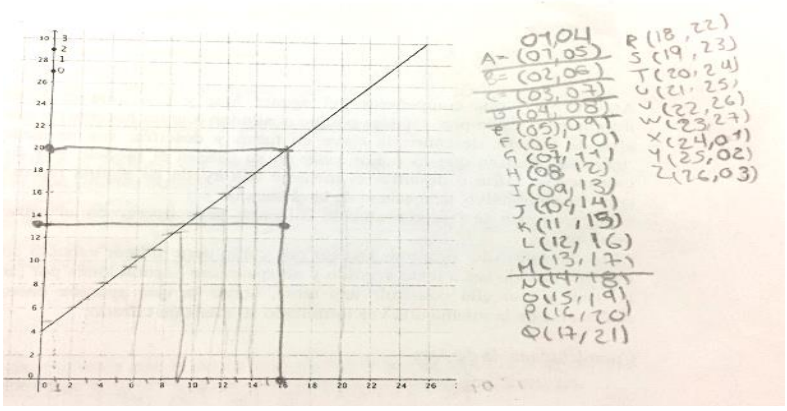
En los registros escritos se puede ver que todo el grupo identifica la "clave de cifrado" a partir de la observación de la gráfica y que 2 equipos logran identificar que la primera coordenada de un punto sobre la recta representa "el número original" y que la segunda coordenada representa "el número cifrado". Al cifrar la frase "SOMOS AGENTES DE CAMBIO" con base en la gráfica, 2 equipos lo hicieron correctamente (figuras 2.7, 2.8) y otros 2, pese a que hicieron el procedimiento de cifrado, tomaron como mensaje original el mensaje cifrado con la tabla (clave 8) y no con la clave 4 que correspondía al modelo gráfico (Figura 2.9).

Figura 2.7 Identificación de la representación de las coordenadas dentro del contexto



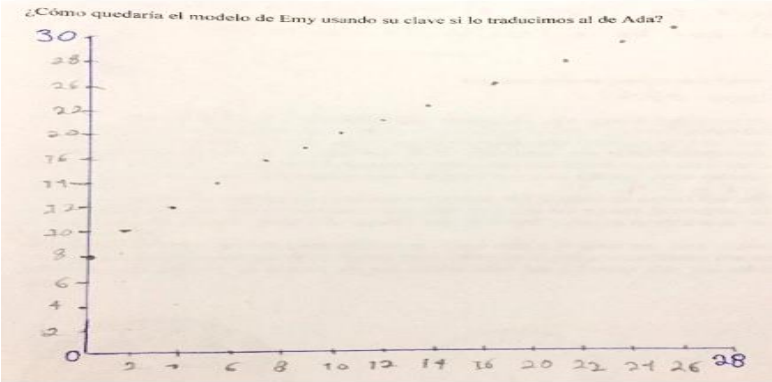
Fuente: Producciones de los estudiantes

Figura 2.8 Representación gráfica y tabular



Fuente: Producciones de los estudiantes

Figura 2.9 Representación gráfica con clave 08



Fuente: Producciones de los estudiantes

Transición entre representaciones o modelos

Del modelo tabular a la gráfica, todos los equipos ubicaron los puntos con escala de 2 en ambos ejes. Sin embargo, 3 equipos graficaron sólo un ciclo y los otros 3 contemplaron valores mayores a "26" en el dominio y el rango, sin que eso signifique que es claro para ello el comienzo de otro ciclo. Aquí se considera que el uso del rotor favorece la comprensión del ciclo y este grupo rápidamente transitó de la tabla al rotor y dejó de lado este modelo al no observar de manera rápida la asociación de letras y números en el rotor pequeño (a diferencia del grupo A).

Finalmente, en los dos grupos se observó que el profesor siempre se mostró inquisitivo y esperando el tiempo suficiente para que los estudiantes contestaran y, de no ser así, reformulaba la pregunta para garantizar la respuesta de los estudiantes. Este comportamiento, en ambos grupos provocaba el surgimiento de las *RBC-**C** acciones* durante las interacciones entre ellos, permitiendo que expresaran su pensamiento. También, como puede observarse en las secciones 4.1 y 4.2, constantemente el profesor propicia la conexión entre las diferentes representaciones para el cifrado y descifrado.

Agradecimiento

Al *Consejo de Ciencia y Tecnología del Estado de Durango* por su financiamiento a través del proyecto *Reunión Nacional de Educación en Ciencia, Ingeniería, Tecnología y Matemáticas* 2017. A la *Universidad Juárez del Estado de Durango* y a la *Facultad de Ciencias Exactas* por su apoyo a través del *Programa de Fortalecimiento a la Calidad Educativa* P/PFCE-2016-10MSU0010C-06. A la Secretaría de Educación del Estado de Durango a través del proyecto *Estrategias para la implementación de las habilidades matemáticas en Educación Básica* y del *Programa de Fortalecimiento a la Calidad Educativa* 2017. A campusviviente.org, proyecto *Campus Viviente en Educación en CITeM* y a Karla Campos Martínez como estudiante colaboradora.

Conclusiones

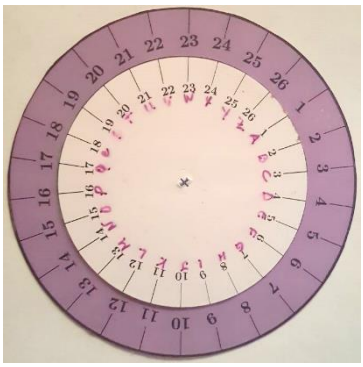
Se diseñaron actividades detonadoras y de exploración de modelos en un contexto de cifrado y descifrado de información para su protección. La interpretación de las situaciones presentadas y el manejo del material concreto permitieron que los estudiantes exploraran y analizaran diferentes representaciones de los modelos propuestos para resolver la situación (gráfica, aritmética, tabular, algebraica y verbal), así como sus relaciones; y más aún, lograran transitar entre dichas representaciones. La socialización fue un espacio que favoreció el análisis, la confrontación y la reflexión de las ideas, incluso aquellas que conducían a un conocimiento erróneo, lo que permitió que los estudiantes refinaran sus modelos.

Los alumnos tuvieron oportunidad de manipular el material y poner en práctica lo sugerido en las actividades y con ello, surgieron formas de pensamiento matemático que conducen a refinar el modelo para hacerlo "más seguro" prescindiendo del material concreto. Como resultado de la implementación de estas actividades detonadoras y de exploración de modelos es posible sugerir que pueden ser una plataforma para extender el conocimiento de los estudiantes y llevarlos a la formalización del sistema conceptual desde un sustento en una estructura matemática que involucra principalmente los conceptos, procesos y representaciones asociadas a las relaciones funcionales.

A diferencia de las prácticas comunes, en las cuales primero se aprende acerca del concepto y, posteriormente, se aplican los aprendizajes en la resolución de problemas. El proponer situaciones que provoquen la construcción de conocimiento desde la necesidad de comprenderlas o resolverlas compromete el pensamiento del estudiante y, con ello, se deriva un aprendizaje a largo plazo. Como lo sugiere Sierpinska (1992), en esta investigación se ha observado que el contexto en el cual la noción de función es utilizada, en analogía con el cifrado y descifrado de información, propicia el surgimiento del lenguaje informal y trae consigo significados que trascienden al mero lenguaje simbólico.

En ambos grupos se obtuvieron resultados diferentes. Al grupo A se le dio mayor tiempo para que a partir de un reto ellos construyeran sus propios modelos (*principio de construcción de modelos*, Lesh et al., 2000) para cifrar (fragmentos [1-16] y [17-34]), posteriormente trataron de vincularlos para comprender los modelos del rotor, gráfico y algebraico. El modelo del rotor fue muy utilizado por los estudiantes, dado que el profesor, para facilitar su comprensión, incluyó en el rotor de números su letra asociada, esto dificultó que se desprendieran del rotor y, en consecuencia, que les llevara dos horas más de tiempo la secuencia que al grupo B (Figura 2.10). Mientras que en el grupo B (fragmento [121-135]), se puso mayor énfasis en hacer que la situación presentada fuera relevante para los estudiantes, siguiendo el *principio del significado personal de la realidad* que plantean las actividades reveladoras del pensamiento (Lesh et al., 2000) y esto propició que tuvieran claridad en la importancia de lograr incrementar la seguridad en el modelo de cifrado (*principio de generación de nuevos modelos*), pusieran a prueba sus modelos (*principio de autoevaluación*) con ello se observó que en este grupo tomaron tiempo para manipular, comprender y conectar todos los modelos (rotor, tabular, gráfico, algebraico), pero desprendiéndose rápidamente del uso del rotor y considerando central el uso de la tabla de asociación. También, con la relevancia de la situación se logró que sus explicaciones verbales de una representación algebraica o fórmula estuvieran conectadas con el contexto de la situación (ver fragmento [178-182] y Figura 2.5), atendiendo el *principio de comunicación o documentación de modelos* (Lesh et al., 2000).

Figura 2.10 Rotor modificado por el profesor



Fuente: Producciones del profesor

Derivado de los resultados obtenidos en la implementación se sugieren algunas mejoras. En cuanto a las hojas de trabajo, se sugiere una actividad previa en la que se presente a los estudiantes una situación en la que ellos tengan un mensaje que requiera protegerse, para explorar en sus formas de pensamiento. Para el uso del material concreto, se recomienda no modificar los rotores agregando elementos para facilitar su comprensión y manejo, dejarlos entender su funcionamiento les permite identificar sus debilidades y buscar mejores modelos.

Mientras que, si se les facilita su uso, tardarán en desprenderse de este modelo concreto al no tener necesidad de encontrar mejores formas de cifrado y descifrado. Otra recomendación es incluir las dos formas de introducir la situación que utilizó en los dos grupos. El presentar retos para cifrar y descifrar provoca el surgimiento de sus propios modelos y el explorar el contexto de la situación y la importancia de proteger su información propicia que ésta sea relevante para ellos y los motive a involucrarse con las otras actividades propuestas para mejorar, explorar y extender sus modelos, logrando que sean más seguros como lo demanda el contexto. Con lo anterior, se puede afirmar que se cubrirían parte de las actividades recomendadas para una Secuencia de Desarrollo de Modelos (Doerr, 2016), es decir, las que detonan modelos y aquellas en las cuales se exploran los mismos.

En la investigación realizada, el modelo RBC-**C** se considera apropiado para analizar la complejidad de las interacciones que conducen a los estudiantes a construir conocimiento compartido derivado de la necesidad de resolver la situación. Por ejemplo, en los grupos A y B respectivamente, fue posible identificar las acciones de construcción de los alumnos: un mecanismo de cifrado simple por asociación [12; 130 y 145]; el cifrado de sustitución con desplazamiento en un número que funciona como clave [22; 159, 165 y 177]; sus propios ejemplos de cifrado y de su proceso inverso asociado para descifrar [56 y 57]; la representación verbal del proceso de cifrado (Figura 2.2); la representación algebraica del cifrado [63 y 181], (Figura 2.5) y descifrado [65]; la representación tabular [83 y 208] que refina el modelo representado en [12]; la representación gráfica a través de las coordenadas (Mensaje original, Mensaje cifrado) en [100 y 233]; la articulación de la representación gráfica y la algebraica [118], (Figura 2.8) y la de éstas con la verbal [120].

Aunque, las acciones de construcción reportadas corresponden a los estudiantes, el profesor juega un papel importante como mediador. En este sentido, para Voigt (1995) a través de las discusiones, los estudiantes y el profesor constituyen una explicación que quizás no es posible que sea construida de manera individual. Se llega al conocimiento intercambiando ideas. Por ejemplo, en [13] se puede observar que el profesor utiliza lo aportado por los estudiantes para darle forma e introducir la noción de función como una entidad que acepta una entrada y produce una salida, misma que puede ser valiosa al formalizar dicho concepto. Por lo anterior, se considera importante reportar las interacciones completas de estudiantes y profesor, dado que, contribuyen a que este estudio sea replicable al aportar información detallada acerca de lo valioso de la práctica inquisitiva del profesor para el logro de los estudiantes.

Para dar continuidad a este trabajo, se sugieren investigaciones que vinculen las ideas generadas en este estudio con la finalidad de formalizar el concepto de función; posteriormente, actividades en las que se adapten y extiendan estos modelos de cifrado y descifrado al uso de funciones del tipo "$y=mx+b$" y otras polinomiales.

Anexo A

Privacidad en los datos II

¿Cómo mejorar el "modelo de los rotores" para cifrado de información?

ADA Y EMY, dos compañeras del agente Mat y con quienes intercambia a menudo información, están preocupadas porque si alguien lograra hacerse de sus rotores podría, con algo de trabajo, descubrir la clave en turno y descifrar sus mensajes. Para evitar esta 'tragedia' piensan que es mejor tener en su cabeza el modelo con su respectiva clave y usarlos para cifrar o descifrar el mensaje con ayuda de alguna representación y, una vez cubierto su objetivo, deshacerse de la evidencia.
Ellas proponen una representación diferente para operar en el cifrado y descifrado de información.
El modelo de Ada propone agregar dos ceros para indicar espacio en blanco para que el mensaje cifrado sea a texto seguido y no aparezcan separaciones por palabras. Propone usar la clave y con ella construir una tabla, como la que aparece enseguida, para cifrar y deshacerse de la misma una vez terminado su mensaje cifrado.

8.- Completa la tabla de Ada.

Letra original		A	B												
Número asociado	00	01	02	03	04	05									
Número cifrado	08	09	10	11											

Letra Original	O	P	Q								
Número asociado	15	16								25	26
Número cifrado											

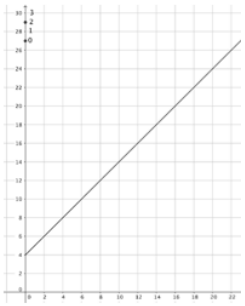
¿Qué clave de cifrado usó Ada para construir la tabla? _____

Con la tabla propuesta cifra o encripta la frase 'somos agentes de cambio'

_____

Por su parte Emy ha decidido proponer al agente Mat el modelo con una representación gráfica y una vez utilizado para cifrar deshacerse de él.

9.- Marca sobre la recta propuesta por Emy **TODOS** los puntos que corresponden con el modelo de cifrado



¿Cuál clave de cifrado está usando Emy?_____

¿Qué representa la primera coordenada de un punto sob

_____

¿Qué representa la segunda coordenada?

_____

Con la gráfica propuesta cifra o encripta la frase 'somos

_____

Un alto para la discusión, revisión y ext
ideas en grupo.

Tarea

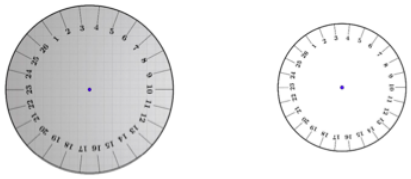
¿Cómo quedaría el modelo de Ada con su lave si lo pasa
el modelo de Emy?
¿Cómo quedaría el modelo de Emy usando su clave si l

Privacidad en los datos

¿Cómo "disfrazar" información para asegurar su privacidad?

Necesitas: Rotores como los de la Figura

CON EL AVANCE de la ciencia y de la tecnología, se ha vuelto cada vez más indispensable proteger archivos e información para evitar la violación de privacidad. Para dar respuesta a esa necesidad, se buscan métodos seguros para cifrar o esconder mensajes secretos. Los expertos que se ocupan de la seguridad de la información son matemáticos, ellos desarrollan formas para esconder información y formas para descifrarla, según sea el caso. Al estudio de tales formas se le conoce como Criptografía y a los métodos como sistemas criptográficos.
La criptografía estudia métodos, que pudieran ser información sensible, de manera que sólo puedan ser descifrados por el receptor y por nadie más que los pudiera interceptar. El emisor y el receptor han de ponerse de acuerdo sobre la "clave" y ésta ha de cambiarse con cierta frecuencia.
Un ejemplo de tales sistemas criptográficos es el que utiliza el agente Mat, para el cual necesita dos rotores como los de la figura, éstos deben recortarse y ensamblarse con un botón encuadernador de tal manera que sus centros coincidan y puedan girar uno sobre otro.



¿Cómo funciona el método del agente Mat?
Mat primero hace una correspondencia entre el abecedario y los números, para minimizar el número de letras sin que se afecte la lectura de los mensajes ha quitado algunas letras: las compuestas (*ll, rr*) y la *ñ*.

A	B	C	D	E	F	G	H	I	J	K	L	_ .	S	T	U	V	W	X	Y	Z
01	02	03	04	05	06	07	08	09	10	11	12	_	19	20	21	22	23	24	25	26

1.- Con esta asociación, encripta el mensaje: 'objetivo superado':

_____

Enseguida el agente Mat prepara sus rotores ensamblados y s
el 1 con el 1, el 2 con el 2, etc. Luego elige una clave, por ejem
en 3 lugares.

2.- Transforma el mensaje 'Objetivo superado 'con la clave que

_____

3.- Ensayen en equipo a cifrar el mensaje que prefieran utiliz
Mat.
Pueden utilizar la clave que ustedes decidan.
Mensaje a cifrar: _____
Mensaje correspondiente en números: _____
Mensaje cifrado utilizando la clave_____: _____

4.- ¿Qué hará el agente Mat cuando necesite cifrar la letra X
clave 3? Expliquen:

5.- Cuando el receptor del mensaje que le envío el agente Mat
para descifrarlo y tener el mensaje original? Explica el método

6.- ¿Qué debe hacer el receptor del mensaje que ustedes cifra

7.- Expliquen de una manera "breve" y sin usar los rotores el m
agente Mat.

Actividad individual de autorregulación

Un alto para la discusión, revisión y
las ideas en grupo.

Piensen en una palabra que para ustedes describa la clase de hoy
mensaje. Al día siguiente, intercambien en un papel el mensaje c
mencionar la clave utilizada. El mensaje que recibieron inte
recuperada la palabra original, entreguen a su maestro.

Referencias

Artigue, M. (1995). La enseñanza de los principios del cálculo: problemas epistemológicos, cognitivos y didácticos. En M. Artigue, R. Duoady, L. Moreno & P. Gómez (Eds.) *Ingeniería didáctica en educación matemática.* pp. 97-140. México: "Una empresa docente" & Grupo Editorial Iberoamericano.

Carmona, G., Reyes, J., Vargas, V., Cristóbal, C., Alvarado, A., López, A., & Mata, A. (2014) Comunidad de Comunidades Campus Viviente en Educación en Ciencia, Ingeniería, Tecnología y Matemáticas (CITeM): Una Experiencia de Colaboración Internacional hacia la Formación de una Red Temática. En M. Ramos & V. Aguilera (Eds). *Ciencias Multidisciplinarias,* 1(1), (pp. 109-125). Valle de Santiago, Guanajuato: ECORFAN.

Cortés, A., Díaz, S., Torres, J., Tapia, H., & Basurto, R. (2005). *Elementos de Criptografía Clásica. Serie Matemática Aplicada y su Enseñanza*. Sociedad Matemática Mexicana-CIMAT. México DF.

Evangelidou, A., Spyrou, P., Elia, I., & Gagatsis, A. (2004). University students' conceptions of function. En M. Johnsen & A. Berit (Eds). *Proceedings of the 28th Conference of the International Group for the Psychology of Mathematics Education* (PME28), 2 (pp. 351-358). Bergen, Noruega: PME.

Doerr, H. (2016). Designing Sequences of Model Development Tasks. En C. Hirsch & A. Roth, (Eds.), *Annual perspectives in Mathematics Education 2016: Mathematical Modeling and Modeling Mathematics* (pp. 197-206). Reston, VA: NCTM.

English, L. D., Lesh, R., & Fenewald, T. (2008) Future directions and perspectives for problem solving research and curriculum development. En Santos-Trigo, Manuel & Shimizu, Yoshi (Eds.) *Proceedings of the 11th International Congress on Mathematical Education*, Monterrey, Mexico.

Dreyfus, T., Hershkowitz, R., & Schwarz, B. (2015). The nested epistemic actions model for abstraction in context: theory as methodological tool and methodological tool as theory. En A. Bikner-Ahsbahs, C. Knipping y N. Presmeg (Eds.), *Approaches to Qualitative Research in Mathematics Education* (pp. 185-217). NY:Springer.

Lannin, J. K., Townsend, B. N., Armer, N., Green, S., & Schneider, J. (2008). Developing meaning for algebraic symbols: Possibilities and pitfalls. *Mathematics Teaching in the Middle School*, 13(8), 478-483.

Lesh, R. A. & Doerr, H. (2003). *Beyond constructivism: A models and modelling perspective on teaching, learning, and problem solving in mathematics education.* Mahwah, NJ: Lawrence Erlbaum Associates.

Lesh, R., Hoover, M., Hole, B., Kelly, A., & Post, T. (2000). Principles for developing thought-revealing activities for students and teachers. En A. Kelly & R. Lesh (Eds.), *Handbook of Research Design in Mathematics and Science Education* (pp. 591–646). Mahwah, NJ: Lawrence Erlbaum Associates.

Sierpinska, A. (1992). Theoretical perspectives for development of the function concept. En G. Harel & E. Dubinsky (Eds.) *The concept of function: Aspects of Epistemology and Pedagogy* MAA, 25 (pp. 23-58). Washington: The Mathematical Association of America.

Voigt, J. (1995). Thematic patterns of interaction and sociomathematical norms. In P. Cobb & H. Bauersfeld (Eds.), *Studies in mathematical thinking and learning series. The emergence of mathematical meaning: Interaction in classroom cultures* (pp. 163-201). Hillsdale, NJ, US: Lawrence Erlbaum Associates, Inc.

White, T. (2009). Encrypted objects and decryption processes: Problem-solving with functions in a learning environment based on cryptography. *Educational Studies in Mathematics.* 72, 17-37.