TALLER DE CRIPTOMATEMÁTICAS PARA JÓVENES (Y ADULTOS)

Luis Hernández Encinas

Dpto. Didáctica de las Matemáticas y de las CC.EE.

Facultad de Educación, Universidad de Salamanca

Paseo de Canalejas 169. 37008, Salamanca

Tfno: 923 294400 (ext 3356)

Email: encinas@gugu.usal.es, *URL:* http://www.usal.es/usuarios/encinas

Sociedad Castellano-Leonesa del Profesorado de Matemáticas

Resumen

Se presentan algunas nociones de la criptología moderna que pueden ser utilizadas en el aula como complemento a determinados conceptos matemáticos. Estos temas pueden ser utilizados dentro de un taller de Matemáticas y permiten divulgar algunas facetas de las Matemáticas, así como un acercamiento de los alumnos a temas de actualidad como pueden ser los relacionados con la seguridad de la información, intercambio de mensajes secretos, etc. Las actividades que se proponen pueden ser desarrolladas por alumnos de cualquiera de los dos ciclos de la E.S.O.

TALLER DE CRIPTOMATEMÁTICAS PARA JÓVENES (Y ADULTOS)

1. Introducción

El término criptología suele llevar, en ocasiones, a determinadas confusiones. Así, no es extraño encontrar libros de esta ciencia en las secciones, de bibliotecas o librerías, dedicadas al esoterismo, por ejemplo, cuando su contenido es casi totalmente matemático. Tampoco es extraño oír que se asocie esta palabra con "cosas de egipcios", "sectas", etc. Por esta razón, parece necesario aclarar desde el comienzo qué entendemos en la actualidad por criptografía y cuáles son sus objetivos.

La *criptología* (del griego cryptos = oculto y logos = ciencia) se podría definir como la ciencia de lo oculto (para una visión histórica ver Sgarro, 1990). Sin embargo, la criptología moderna, debido al tipo de sociedad en la que vivimos, tiene dos objetivos fundamentales: por un lado el de permitir que dos o más personas puedan comunicarse de forma secreta utilizando canales de comunicación inseguros, es decir, medios de comunicación que pueden ser "interceptados" por una tercera persona (teléfono, correo, fax, correo electrónico, etc.). El segundo objetivo es justamente el contrario, es decir, analizar cómo estas comunicaciones pueden ser vulneradas o rotas, para conocer su contenido.

El primer objetivo señalado es estudiado por la *criptografía*, mientras que el segundo lo es por el *criptoanálisis*. El procedimiento que se sigue para lograr comunicaciones seguras es el de disfrazar o cifrar el mensaje que se desea enviar (criptograma[1]), utilizando algún tipo de clave, de modo que sólo quien esté autorizado sea capaz de recuperar el mensaje original a partir del criptograma (ver CSID, 1993; Pastor, 1996; y Ribagorda, 1997). El proceso de cifrar el mensaje se basa en la presunta dificultad o intratabilidad computacional de resolver

[1] La Real Academia de la Lengua define el término *criptografía* como el "Arte de escribir con clave secreta o de un modo enigmático", mientras que el *criptoanálisis* es el "Arte de descifrar criptogramas", siendo un *criptograma* una "Especie de crucigrama en el que, propuesta una serie de conceptos, se han de substituir por

determinado problema matemático (Fúster et al., 1997).

La importancia de los dos términos anteriores se debe a la frecuencia con que en los medios de comunicación se habla de “hackers”, “crackers” y de aspectos relacionados con la Seguridad de la Información, que tienen que ver con Internet y redes de ordenadores, con los accesos de personas no autorizadas a los ordenadores de la OTAN, de la NASA, del Pentágono, etc. Asuntos que llaman enormemente la atención de nuestros alumnos, quienes están capacitados y muy motivados para comenzar a entenderlos, si les son presentados de una manera sencilla.

Por ello, es importante incorporar a las aulas determinados aspectos matemáticos que han ido surgiendo en esta sociedad tecnificada y de la información. Otros ejemplos matemáticos, en la línea de los que se comentan aquí, han sido propuestos por Espinel (1994), Caballero y Bruno (1994) y Espinel y Caballero (1995). Sin embargo, el problema que se presenta es determinar dónde tiene cabida este nuevo saber.

La inclusión en el aula de los aspectos matemáticos que nos rodean es una necesidad que sentimos todos y que intentamos resolver, fundamentalmente, de dos formas. Una posibilidad es la de incluir esta realidad cuando se plantean y resuelven problemas, de modo que, de alguna manera, quede incorporado al bagaje de los alumnos. La segunda forma es la de recurrir a talleres de Matemáticas.

No es el principal objetivo de este artículo discutir el lugar más idóneo donde llevar a cabo esta inclusión, sino el de presentar un ejemplo más de divulgación de las Matemáticas, utilizando temas de debate, relacionados con la criptología, que aparecen cada vez con más frecuencia y que son motivadores para nuestros alumnos.

En este caso, y debido a la diversidad de aspectos matemáticos relacionados con la criptografía que se presentarán (algoritmos, complejidad computacional, funciones

---

palabras que los signifiquen, cuyas letras, trasladadas a un casillero, componen una frase.”.

unidireccionales, protocolos para ocultar información, etc., y cuya relación con los contenidos matemáticos se comentará más adelante), se analizan diferentes actividades enmarcadas dentro de un taller de Matemáticas y criptografía. Ante esta propuesta que hacemos de un nuevo taller de Matemáticas, no podemos dejar de recomendar el lugar que consideramos puede ser más idóneo para su inclusión, en función de los objetivos que se pretenden conseguir y de los contenidos que subyacen en el taller.

Creemos que este taller debería desarrollarse como una asignatura optativa en cualquiera de los dos cursos del segundo ciclo de la E.S.O. En esta etapa, los alumnos ya tienen los conocimientos mínimos necesarios para poder desarrollar las actividades que se incluyen en el taller, así como las inquietudes y cultura que les permitirán conocer la importancia y las relaciones con el entorno que les rodea, de los contenidos de dicho taller.

El resto del artículo se distribuye como sigue. En la sección 2 se presenta una actividad relacionada con el problema de colorear mapas con determinado número de colores. En la 3 se analiza el problema de pavimentar determinadas calles de una ciudad enlodada con determinados objetivos. En §4 aparece el problema de la ciudad turística, en la que se deben colocar determinados puntos de información. Un acercamiento a las funciones unidireccionales por medio de grafos se presenta en la sección 5, y en la §6 aparece un protocolo para ocultar información. En la sección 7 se analiza cómo dos personas pueden intercambiarse mensajes secretos, mientras que en la 8 lo que se intercambian son pequeñas informaciones en presencia de un extraño, sin que la tercera persona llegue a conocer ningún trozo de dicha información. Las sección 9 presenta un método para cifrar mensajes por medio de las llamadas rejillas. En las secciones 10 y 11 se analizan cómo enmascarar un número o una imagen de modo que sea necesaria la participación de varias personas cualificadas para obtener el número o la imagen original. Finalmente, en §12 se presentan algunas reflexiones sobre las intenciones educativas y los contenidos que subyacen a este taller.

2. Coloreando un mapa

La primera de las actividades de este taller consiste en plantear a los alumnos la necesidad de colorear un mapa utilizando sólo unos pocos colores. El origen del problema puede hacerse mediante una historia, que dependerá de la edad de los alumnos con los que se trabaje. La definición del problema puede hacerse de forma puramente visual, ilustrándolo con diferentes mapas, incluyendo los que haya en el propio aula. En sólo unos minutos los alumnos comprenderán cuál es el objetivo que deben conseguir: “encontrar el mínimo número de colores que se deben utilizar para colorear un mapa dado”.

La actividad puede comenzarse proporcionando a los alumnos mapas que sean coloreables con sólo dos colores. Como ejemplo de uno de estos mapas puede verse el que se presenta en la figura 1.

Figura 1. Ejemplo de mapa coloreable con sólo dos colores,
generado por solapamiento de curvas cerradas.

Una vez que los alumnos intenten colorear el mapa, descubrirán rápidamente el algoritmo que deben seguir: si un país es rojo, sus vecinos tienen que ser azules, y los vecinos de éstos volverán a ser rojos, etc.

Una vez que los alumnos han trabajado con la anterior actividad, puede resultarles divertida la propuesta de que inventen por sí mismos, o en grupos, mapas que sean coloreables con exactamente 2 colores[2].

Después de la actividad anterior, se pueden distribuir a los alumnos mapas que no sean coloreables con dos colores y que requieran de tres. El propio algoritmo utilizado por los alumnos en el caso anterior, les llevará a la conclusión de la imposibilidad de hacer el trabajo

[2] Generar mapas coloreables con sólo dos colores es fácil si se utilizan curvas cerradas que se solapan.

con sólo dos colores[3]. Como un primer ejemplo de este tipo de mapas puede verse el de la figura 2.

Figura 2. Ejemplo de mapa no coloreable con sólo dos colores.

3. La ciudad enlodada

La actividad que se presenta ahora es la que responde al problema de encontrar el árbol de mínima envergadura en un grafo[4]. Dado que este problema puede llegar a ser muy complejo para los alumnos, conviene llevar a cabo un planteamiento que les sea más cercano.

El problema puede ser planteado como sigue: "el ayuntamiento de una ciudad enlodada ha decidido que hay que pavimentar todas las calles de la ciudad que sean necesarias, de modo que cualquier vecino pueda ir desde su casa a cualquier otra casa de la ciudad por una calle que esté pavimentada, pero de modo que el coste de la pavimentación sea el mínimo posible". Así pues, se trata de pavimentar el suficiente número de calles de modo que se pueda ir de una manzana de casas a cualquiera otra sin necesidad de ir por calles enlodadas. Dado que el ayuntamiento sabe cuánto cuesta pavimentar cada una de las calles, el dinero a gastar debe ser el menor posible, debido la precariedad del presupuesto de la ciudad.

Con el planteamiento anterior, se puede representar la ciudad de forma esquemática mediante un grafo, de modo que cada uno de los vértices del grafo sea una manzana de casas y cada uno de sus lados sea una calle.

Como ejemplo de ciudad enlodada puede utilizarse el grafo de la figura 3, donde los números que hay sobre cada uno de los lados corresponden al coste, en millones de pesetas,

[3] El contraste entre el sencillo algoritmo de colorear un mapa con sólo dos colores y la aparente dificultad del algoritmo para un mapa de tres colores pone en contacto a los alumnos con uno de los problemas no resueltos más importantes de las Matemáticas: la conjetura de que la clase de problemas de complejidad **P** (conjunto de todos los problemas de decisión que son resolubles en tiempo polinómico) es distinta a la clase de problemas de complejidad **NP** (conjunto de todos los problemas de decisión para los que la respuesta SI puede verificarse en tiempo polinómico, utilizando una información extra o certificado).

[4] Determinar el *árbol de mínima envergadura en un grafo* consiste, básicamente, en seleccionar los lados del grafo cuya suma de pesos sea mínima y de modo que se pueda ir de un vértice del grafo a cualquier otro por el

que supone pavimentar dicha calle.

Figura 3. Ejemplo de grafo que representa una ciudad enlodada.

Una vez planteado el problema, los alumnos pueden trabajar en grupos, de modo que por tanteo y analizando las calles a pavimentar en cada uno de los sucesivos intentos, lograrán acercarse a la solución adecuada mediante la estrategia de ensayo y error. Es conveniente que cada uno de los grupos de trabajo comente la estrategia seguida para obtener su mejor solución. Si fuera necesario, porque ninguno de los grupos llegara a la solución óptima, se podría presentar el algoritmo de Kruskal que consiste en ir pavimentando de forma sucesiva las calles cuyo coste sea menor hasta que no sea necesario pavimentar más calles y siempre que las calles pavimentadas no formen un ciclo. Diferentes aproximaciones a la solución óptima (de valor 23) del problema anterior pueden ser las que se presentan en la figura 4.

Figura 4. Diferentes aproximaciones a la solución óptima.

4. La ciudad turística

Un problema que puede ilustrar la noción de complejidad computacional[5] (Fúster et al., 1997, Apéndice B) es el llamado problema del conjunto dominante mínimo[6].

En esta actividad el planteamiento del problema es como sigue: “en las esquinas de una ciudad turística se quieren colocar puntos de información de modo que sin importar en qué esquina esté un turista, pueda llegar a un punto de información caminando, como máximo, una manzana”. La figura 5 muestra un grafo que ilustra este planteamiento.

Figura 5. Mapa de una ciudad turística.

Después de planteado el problema, dejaremos a los alumnos que trabajen en grupos sobre el mismo. Las soluciones que obtendrán serán cada vez mejores, pero es difícil que

árbol elegido.

[5] La *teoría de la complejidad computacional* estudia el tiempo que tarda en ejecutarse un algoritmo en función del número de operaciones que realiza dicho algoritmo y en función del tamaño de la entrada del mismo.

[6] Un *conjunto dominante en un grafo* $G=(V,L)$ es un subconjunto de vértices V' de V de modo que para cualquier

lleguen a obtener la solución óptima de la localización de los 6 puntos de información.

La diferencia entre el problema de la ciudad lodosa y éste, uno fácilmente resoluble y otro aparentemente más difícil, proporciona una idea de la noción de complejidad computacional. Hay que señalar que no se conoce un buen algoritmo para resolver este problema[7], lo cual puede poner de manifiesto ante los alumnos que las Matemáticas no son algo completamente acabado, que cada día aparecen nuevos problemas para los que se debe encontrar una solución.

5. Funciones unidireccionales

Una de las herramientas fundamentales en la criptografía moderna es el uso de las funciones unidireccionales[8] (Menezes et al., 1996). No se ha demostrado aún la existencia de funciones unidireccionales, sin embargo en la práctica criptográfica se utilizan dos funciones que parecen serlo. La primera de ellas es el producto de números primos (cuya inversa es la factorización de un número compuesto) y la segunda es la exponencial sobre un grupo finito (cuya inversa es el logaritmo discreto) (Fúster et al., 1997, p. 115).

Después de haber comentado a los alumnos que no se conoce (no que no exista) un buen algoritmo para resolver el problema anterior, es conveniente señalar que existe un algoritmo sencillo para trabajar hacia atrás, es decir, comenzar con un conjunto de vértices y obtener el mapa de la ciudad turística de una forma muy rápida.

El algoritmo tiene dos pasos. El primero de ellos consiste en dibujar tantas estrellas, hechas con puntos (vértices) y rayos (lados), como la solución que se desea; y el segundo es disfrazar el grafo añadiendo más lados. Este hecho no incrementa el número de vértices del

---

vértice *v* de *G*, se verifica que o *v* está en *V'* o tiene un vecino que está en *V'*.

[7] Por *buen algoritmo* queremos indicar un algoritmo cuya ejecución requiera de tiempo polinómico en el tamaño de la entrada.

[8] Una *función unidireccional* es una función invertible $f : A \rightarrow B$, de modo que es fácil (computacionalmente hablando) calcular la imagen de un elemento $f(a) = b$, pero es muy difícil (computacionalmente) calcular la antiimagen de un elemento: $f^{-1}(b) = a$.

conjunto dominante y a la vez dificulta la solución del problema. En la figura 6 puede verse el primer paso del algoritmo señalado para el mapa de la figura 5.

Figura 6. Primer paso para la construcción del mapa de la ciudad turística.

Para los alumnos es claro que el conocimiento de la configuración de estrellas permite obtener de forma rápida el mapa de la ciudad. Este ejemplo pone de manifiesto la ventaja de conocer funciones unidireccionales. Así, los alumnos, conociendo esta función unidireccional, podrán desafiar a otros compañeros a resolver el problema de la ciudad turística, sin más que elaborar previamente la solución al problema que vayan a plantear.

6. Ocultando información

Después de las actividades anteriores que pueden considerarse como de pre-criptografía, y que están muy relacionadas con la teoría de grafos, pasamos, a partir de esta actividad, a problemas más directamente relacionados con la criptografía.

La actividad siguiente ilustra de una forma sencilla un protocolo para ocultar información. El problema que se puede plantear en esta ocasión es el de “determinar la media de la paga semanal de los alumnos de la clase, sin que ninguno de ellos de a conocer al resto de los compañeros cuál es su paga”.

De forma más general, el procedimiento que se describe a continuación puede utilizarse para determinar la media de una colección de datos de un grupo, sin comprometer la información que posee cada uno de los miembros del grupo.

El protocolo para resolver el problema anterior es el siguiente:

- El primer alumno, por ejemplo Alicia, elige un número secreto, x, al que le añade su paga semanal, p_{Alicia}, obteniendo el valor $x + p_{\text{Alicia}}$. A continuación, Alicia susurra este valor al segundo alumno de la clase, Bernardo.
- Bernardo suma a la cantidad que le dijo Alicia su paga semanal y obtiene el valor x

$+ p_{\text{Alicia}} + p_{\text{Bernardo}}$, y susurra este valor al tercer alumno, Carmen.

- Carmen repite la operación anterior y así sucesivamente hasta que todos los alumnos hayan efectuado una operación similar.
- ...
- El último alumno, Zacarías, añade su paga semanal a la cantidad que le dijo el penúltimo alumno, Yolanda, obteniendo el valor

  $x + p_{\text{Alicia}} + p_{\text{Bernardo}} + p_{\text{Carmen}} + ... + p_{\text{Yolanda}} + p_{\text{Zacarías}}$.
- Zacarías susurra el valor que ha obtenido a Alicia, quien resta a la cantidad anterior el número secreto que sumó a su paga.
- Por último, Alicia divide la cantidad obtenida entre el número de alumnos de la clase y obtiene la paga semanal media.

La actividad a realizar por los alumnos en este caso, además de analizar el protocolo anterior, es una similar a la descrita anteriormente, como puede ser la de determinar la edad media de los alumnos, sus ahorros medios, su estatura media, etc.

7. Mensajes secretos

El objetivo de esta actividad es el de conseguir que algunos alumnos se intercambien mensajes secretos, diseñando ellos mismos métodos para cifrar los mensajes, de modo que otros intenten conocer el contenido del mensaje intercambiado. De esta forma, mientras unos juegan el papel de criptógrafos o de agentes secretos, otros harán del papel de criptoanalistas o espías. Para ello, y en lugar de presentar el método a seguir para lograr este objetivo, presentaremos a los alumnos un mensaje cifrado, que deberán tratar de descubrir.

El primer mensaje que podemos presentarles puede ser el siguiente:

BQSFTVSBUF DPÑ MFÑUJUVE

El problema que tendrán que resolver los alumnos será el de determinar su significado,

trabajando en grupos. Es de suponer que tras varios intentos llegarán a la conclusión de que cada una de las letras del mensaje cifrado debe cambiarse por la letra que le precede en el alfabeto castellano, por lo que el mensaje original era:

APRESURATE CON LENTITUD

Este mensaje se ha cifrado utilizando el procedimiento diseñado por el emperador romano Augusto, que consistía en cambiar cada una de las letras del mensaje original por su siguiente letra en el alfabeto. Por tanto, para recuperar el mensaje a partir del criptograma se debe hacer la operación contraria, esto es, cambiar cada letra del criptograma por la letra que le precede.

Complicando un poco más el cifrado anterior, se puede utilizar el cifrado de Julio Cesar, que consistía en cambiar cada una de las letras del mensaje original por la tercera letra siguiente en el alfabeto. Así, la frase

LA SUERTE AYUDA A LOS AUDACES

Se convierte en el mensaje cifrado siguiente:

ÑD VXHUWH DBXGD D ÑRV DXGDFHV

Con estos dos ejemplos serán suficientes para que los alumnos diseñen sus propios métodos de cifrado, de modo que algunos de los métodos que se les ocurrirán serán:

1. Cambiar cada letra por la *n*-ésima letra siguiente del alfabeto,
2. Cambiar la primera letra por la siguiente en el alfabeto, la segunda por la segunda siguiente, la tercera por la tercera siguiente, etc.
3. Cambiar las letras que ocupen posiciones impares por la *n*-ésima siguiente, y las que ocupen posiciones pares por la *n*-ésima anterior.
4. Etc.

Hay que hacer notar que los métodos anteriores y otros similares no son seguros en la actualidad, debido a que se puede recuperar el mensaje original utilizando métodos

estadísticos, puesto que se conoce la frecuencia de las letras y grupos de letras en castellano y otros idiomas[9].

Una extensión de esta actividad, más relacionada con la Estadística pero con una relación evidente con el caso que nos ocupa, es la de proponer a los alumnos que hagan un estudio de la frecuencia de las letras en español, eligiendo diferentes textos aleatoriamente. Una vez que los alumnos hayan hecho este estudio, se puede considerar como punto de partida la media de las frecuencias halladas por cada uno de ellos. Incluso, se podría desafiar a los alumnos a repetir esta actividad de descifrar mensajes con textos escritos en otros idiomas.

8. Cambiando la clave

Otro de los problemas básicos en criptografía es analizar cómo dos personas pueden compartir pequeñas cantidades de información en presencia de un espía, de modo que éste no consiga la información intercambiada (Fúster et al, 1997, p. 116). Esta información que las dos personas se intercambian puede servir posteriormente como la clave que usarán para comunicaciones posteriores[10]. Por ejemplo, para decidir qué método de cifrado del tipo de Cesar usarán para intercambiarse mensajes.

Para llevar a cabo esta actividad, se señalará a los alumnos que para intercambiarse palabras o frases, es más sencillo utilizar un código simple recurriendo sólo a dos símbolos, de modo similar a como se codifican las letras en el alfabeto Morse, donde sólo se usan el punto y la raya. En la actualidad es más fácil y cómodo utilizar ceros y unos, recurriendo al código ASCII de los ordenadores[11], de modo que cada letra del alfabeto está codificada por una colección de ceros y unos (cada uno de los cuales se llama bit).

[9] Un método cuasi-estadístico fue utilizado por Edgar Alan Poe para hacer que William Legrand descifrara el criptograma del pirata Kidd en el cuento del Escarabajo de Oro.
[10] Este problema se conoce como el problema del *cambio de clave de Diffie y Hellman*.
[11] El *código ASCII* (American Standard Code for Interchange Information) es el código que se utiliza para la comunicación con los ordenadores. Está formado por 256 caracteres (incluyendo las letras mayúsculas, las minúsculas, los diez dígitos, etc.), cada uno de los cuales está codificado por 8 dígitos binarios.

Por tanto, la actividad a realizar en esta ocasión es la de “permitir que dos alumnos, Alicia y Bernardo, puedan intercambiarse de forma secreta una secuencia de bits, que ninguno de los dos conoce previamente, de modo que pueda servirles como clave a partir de ese momento, y de modo que todo el proceso se realice delante de Esteban, que hará el papel de espía”.

Para esta actividad se requiere el uso de tres cartas diferentes, por ejemplo, la sota, el caballo y el rey de un palo de la baraja, de modo que para decidir cada uno de los bits, las cartas se barajan y se reparte una a cada uno de los presentes.

Antes de comenzar con el procedimiento, Alicia y Bernardo se han puesto de acuerdo en que si los dos pueden saber quien de ellos tiene la carta más alta sin que lo sepa Esteban, el bit que considerarán será: 1 si Alicia es quien tiene la carta más alta y 0 si es Bernardo el que la tiene más alta.

Alicia, después de que se hayan repartido las tres cartas, dice en voz alta una de las cartas que no tiene. Si Bernardo tiene esa carta, lo dice y barajan de nuevo las tres cartas sin decidir ningún bit. En caso contrario, es decir, si Bernardo no tiene la carta, dice “Esteban la tiene” y entonces Alicia y Bernardo saben qué carta tiene cada uno, con lo que ambos saben qué bit es el que eligen. A la vez, Esteban no ha obtenido ningún datos sobre el bit que han elegido Alicia y Bernardo. El procedimiento anterior continua hasta que se hayan completado los bits necesarios.

Una vez presentada la actividad, los alumnos analizarán las razones de porqué funciona el protocolo anterior, es decir, comprobarán que la información que consiguen Alicia y Bernardo es la misma, mientras que Esteban no es capaz de saber absolutamente ningún bit de esa información. Posteriormente, pueden dedicarse, en grupos de tres, a intercambiar colecciones de bits o pequeños mensajes (una vez que se les ha proporcionado la traducción a bits de las letras del alfabeto). Es conveniente que cada grupo repita la actividad anterior

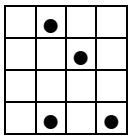
varias veces de modo que cada uno de los participantes haga el papel de espía.

9. Las rejillas

Otro de los métodos para cifrar mensajes consiste en utilizar las llamadas rejillas. Para introducir a los alumnos en esta actividad se puede recurrir a la novela “Mathias Sandorf” de Julio Verne[12], o bien inventarse una historia como la siguiente: “un agente secreto ha entrado en la habitación del hotel de un conocido espía y después de buscar por todas partes, tan sólo ha encontrado dos objetos sospechosos. El primero de ellos es un papel con las siguientes cuatro palabras:

LAAI ARSN AVUP EISM

El otro objeto sospechoso es un cuadrado de papel con algunos agujeros, como si fuera una rejilla. El agente ha copiado las cuatro palabras, la forma de la rejilla y los lugares de los agujeros:



¿Podrías ayudar al agente secreto a descubrir el mensaje oculto?”.

Dado que el mensaje está dividido en 4 palabras de 4 letras, y que esta distribución es igual al de las casillas de la rejilla, el primer paso para descifrar el mensaje consiste en distribuir el mensaje de la misma forma que la rejilla:

L A A I

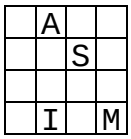
A R S N

A V U P

[12] En esta ocasión fue Julio Verne quien hizo que su personaje Mathias Sandorf utilizara este método para descifrar un mensaje y evitar una conspiración.

E I S M

A continuación se colocará la rejilla sobre el mensaje, obteniéndose lo siguiente:



Es decir, aparecen las letras ASIM. Si se gira la rejilla 90º a la derecha y se repite el procedimiento anterior, se obtienen las letras ANUE. Repitiendo el proceso anterior otras dos veces[13], se obtienen las palabras: LAVS y IRAP. Uniendo ahora todas las palabras se tiene:

ASIM ANUE LAVS IRAP

Mensaje que no tiene sentido, pero si se lee desde el final hasta el principio, el mensaje ahora ya es claro:

PARIS VALE UNA MISA

Para el procedimiento anterior hemos utilizado un mensaje en el que el número de letras es igual al de cuadrados de la rejilla, pero no es necesario que esto suceda siempre. En el caso que el mensaje tenga más letras que cuadrados la rejilla, se puede dividir éste en varias partes y realizar el procedimiento anterior con cada una de las partes. Si la última parte del mensaje tiene menos letras que cuadrados en la rejilla, se pueden añadir letras que no añadan sentido al mensaje.

La actividad anterior pueden repetirla los alumnos tal y como se ha presentado, de modo que un alumno cifre un mensaje mientras que otro trata de descifrarlo. Después de esta primera actividad, sería recomendable que cada alumno diseñara una rejilla de tamaño 4×4, diferente de la usada anteriormente. De esta manera, se podría poner de acuerdo con algún compañero en la rejilla a utilizar y pedir a cualquier otro que intente descifrar el mensaje, sin conocer la rejilla.

[13] De esta forma, la rejilla ha sido girada un total de 270º. Este proceso puede poner a los alumnos en la pista para una de las actividades que se proponen posteriormente: diseñar nuevas rejillas.

Complicando un poco más la actividad anterior, se podría pedir a los alumnos que intentaran diseñar rejillas de tamaño 5×5 o 6×6, por ejemplo[14].

10. La caja fuerte del banco

El problema que se presenta en esta actividad requiere más tiempo que las presentadas hasta ahora. Entra dentro de lo que, en criptografía, se conoce como división de secretos[15] (Salomaa, 1990 y Schenier, 1993). En este caso se trata de presentar a los alumnos un protocolo que permita a una persona enmascarar un número, dividiéndolo en varios trozos y entregando cada trozo a una persona diferente, de modo que el número secreto sólo pueda ser recuperado cuando se unan los trozos de un determinado número de esas personas.

Una situación real en la que se presenta un protocolo parecido al que se desarrollará más tarde, y que puede aclarar a los alumnos lo que se pretende, es el siguiente: "una sucursal bancaria tiene 3 empleados, pero ninguno de ellos quiere tener toda la responsabilidad de conocer la combinación de la caja fuerte de la sucursal. El problema que se presenta es cómo lograr que cada mañana se abra la caja fuerte del banco para hacer los pagos necesarios, sin que la responsabilidad recaiga en un único empleado".

Una forma de solventar este problema, de modo que la caja fuerte pueda ser abierta cada mañana, consiste en dividir la combinación de la caja en tres partes, una para cada empleado, de modo que ésta sólo pueda ser abierta cuando se unan las combinaciones parciales de, al menos, 2 de los empleados. De este modo, ninguno de ellos puede, de forma individual, abrir la caja y así, la responsabilidad de llevar a cabo su apertura queda distribuida entre los empleados.

[14] El diseño de rejillas de tamaño 6×6 es similar al de las de tamaño 4×4. Sin embargo, no se pueden construir rejillas de orden impar dado que existe una casilla central y al girar la rejilla, esta casilla permanece fija.

[15] La *división de secretos* se lleva a cabo cuando una instancia superior no desea que determinado secreto sea conocido en su integridad por una única persona. Entonces, la instancia divide el secreto en varias partes de tal forma que para recuperar el secreto en su totalidad sea necesario el concurso de terminado número de partes, siendo imposible recuperarlo con menos de las establecidas.

Los problemas similares al planteado anteriormente se conocen como esquemas umbrales (Blackley, 1979 y Shamir, 1979) y tienen dos valores que los definen: el número de personas cualificadas para obtener el secreto y el número de participantes[16]. En general, un esquema umbral para dividir el secreto *S*, en *m* partes (llamadas sombras) y en el que hay *n* participantes debe cumplir las siguientes condiciones:

1. Cada participante recibe de forma secreta una sombra de las *n* en que se ha dividido el secreto.
2. Cualesquiera *m* participantes cualificados pueden determinar el valor del secreto sin más que compartir las sombras que cada uno de ellos posee.
3. Ningún grupo de *m*-1 participantes, o menos, puede conocer ninguna información sobre el valor secreto.

En estos esquemas hace falta un observador, que es quien lleva a cabo el proceso de dividir el secreto en las *n* sombras y que entrega, secretamente, cada una de las sombras a cada uno de los participantes.

Para conocer cómo trabajan los esquemas umbrales, vamos a presentar un ejemplo de cómo construir un esquema umbral 2 de 2, donde el secreto es una cadena de bits. En este caso, el secreto debe romperse en 2 sombras, de modo que cada una de ellas estará formada por una colección de bits, y será necesaria la colaboración de las dos partes para recuperar el secreto original.

Supongamos que el secreto elegido por el observador es la siguiente cadena de bits: S=(0100101). El observador elabora la primera de las sombras de forma aleatoria: s_1=(1100110). Para construir la segunda sombra el observador utiliza la siguiente tabla de sumar: $0 \oplus 0 = 0$, $0 \oplus 1 = 1$, $1 \oplus 0 = 1$ y $1 \oplus 1 = 0$[17]. Como se cumple que: $0 \oplus 1 = 1$, $1 \oplus 1$

[16] El procedimiento anterior de los empleados del banco se conoce como *esquema umbral* 2 *de* 3, dado que la combinación de la caja se divide en 3 partes y es necesario reunir, al menos, 2 de ellas para poder abrirla.

[17] Nótese que esta tabla de sumar corresponde a la suma en el grupo de las clases residuales módulo 2.

= 0, 0 ⊕ 0 = 0, 0 ⊕ 0 = 0, 1 ⊕ 1 = 0, 0 ⊕ 1 = 1 y 1 ⊕ 0 = 1, la segunda sombra es: s_2=(1000011).

Para recuperar el secreto, basta con que los dos participantes pongan en común sus dos sombras y las sumen, bit a bit: 1 ⊕ 1 = 0, 1 ⊕ 0 = 1, 0 ⊕ 0 = 0, 0 ⊕ 0 = 0, 1 ⊕ 0 = 1, 1 ⊕ 1 = 0 y 0 ⊕ 1 = 1; lo que proporciona el valor secreto original: *S*=(0100101).

Si uno de los participantes quisiera recuperar el secreto original utilizando sólo su sombra, debería suponer cuál es la sombra del otro participante. Para ello necesitaría probar, en el ejemplo anterior, un total de 2^7 = 128 posibilidades (dos valores, 0 y 1, a colocar en 7 posiciones).

Después de la presentación hecha, la actividad de los alumnos consiste en dividirse en grupos de 3, de modo que uno de ellos haga el papel de observador y construya un esquema parecido al presentado anteriormente. En este caso, el secreto del observador puede plantearse como la combinación de una caja fuerte donde se encuentran determinadas instrucciones que deberán seguir los otros dos participantes. Estos dos participantes deberán intentar por sí mismos recuperar el secreto pensado por el observador. Dado que no conseguirán recuperarlo de forma individual, deberán ponerse de acuerdo para compartir la información que posee cada uno de ellos y recuperar, de esta forma, el secreto del observador.

11. Enmascarando una imagen

Si en lugar de ocultar un número o un mensaje, lo que se desea enmascarar es una imagen, en blanco y negro, estamos ante la criptografía visual, que hace uso de los esquemas visuales umbrales (Nahor y Shamir, 1995; y Stinson, c.p.). Estos esquemas visuales siguen el mismo procedimiento que los esquemas de la actividad anterior, pero con las siguientes características:

1. El secreto *S* es una imagen formada por pixeles cuadrados blancos y negros[18].
2. Las *n* partes o sombras en que se divide la imagen secreta son otras tantas transparencias cada una con una imagen que tiene el mismo tamaño y el mismo número de pixeles que la imagen original.
3. La recuperación de la imagen secreta se lleva a cabo mediante la superposición de *m* transparencias cualesquiera, de modo que no es posible obtener la imagen original con sólo *m*-1, o menos, de ellas.

La actividad a desarrollar ahora será la de construir las sombras en que se dividirá una imagen, para después fotocopiar cada una de las sombras a transparencias y proporcionar una transparencia a cada participante. Con la superposición de determinado número de transparencias se obtendrá la imagen oculta, pero esto no se logrará superponiendo menos transparencias.

Vamos a detallar cómo construir un esquema visual umbral 2 de 2[19], de modo que podamos enmascarar una imagen para luego recuperarla. Dado que el esquema es 2 de 2, la imagen se dividirá en 2 sombras o transparencias, una para cada uno de los participantes, de modo que ninguno de ellos pueda conocer ninguna información de dicha imagen original a partir de la imagen que recibe, y de tal manera que sólo se pueda recuperar la imagen original superponiendo las 2 transparencias en que se ha dividido la imagen.

Para elaborar las sombras supondremos que la imagen a ocultar está contenida en un rectángulo, dividido en pixeles. Los pixeles que definen la imagen secreta serán blancos y negros. Vamos, entonces, a enmascarar la figura siguiente, que representa al número π:

Figura 7. Imagen secreta a ocultar.

[18] Un *pixel* es el elemento de dibujo que permite presentar en los monitores de los ordenadores las imágenes que en él aparecen. Para evitar recurrir al uso de ordenadores en esta actividad, se recomienda hacer la analogía de que cada pixel es como cada una de las bombillas que forman parte y definen algunos anuncios luminosos, con la salvedad que aquí los pixeles tendrán forma cuadrada.

[19] El esquema visual umbral 2 de 2 anterior puede extenderse a esquemas 2 de *n* y, de forma más general, a *esquemas visuales umbrales m de n*. Sin embargo, las técnicas matemáticas empleadas en estos últimos son más

Conviene señalar que esta figura contiene muy pocos pixeles, por lo que el proceso será puramente ilustrativo, sin buscar una buena definición de la imagen resultante. Más adelante se presentarán otras imágenes enmascaradas con el mismo protocolo pero definidas con más pixeles, lo que hará que su definición sea mucho mejor.

El esquema visual 2 de 2 para dividir la imagen secreta consiste en enmascarar cada uno de los pixeles de la imagen original en dos pixeles, cada uno de los cuales ocupará en lugar del pixel original pero en cada una de las sombras. Para llevar a cabo este enmascaramiento del pixel original, cada uno de los pixeles de cada una de las sombras está dividido en dos semipixeles, la mitad blanco y la mitad negro. El algoritmo para enmascarar cada uno de los pixeles originales se ilustra en la figura 8 y es el siguiente:

Figura 8. Enmascaramiento de un pixel original en un esquema 2 de 2.

Si el pixel original es blanco, el observador lanza una moneda al aire, de modo que si el resultado es cara, elige como pixeles para cada una de las sombras los dos pixeles de la primera línea de la figura 8.a; si el resultado es cruz elige como pixeles para cada sombra los dos pixeles de la segunda línea. De forma análoga se procede para enmascarar un pixel negro, utilizando la figura 8.b. El algoritmo que se acaba de describir se ejecuta con cada uno de los pixeles de la imagen secreta.

Antes de conocer las 2 sombras obtenidas mediante el algoritmo anterior, vamos a analizar las características de dicho algoritmo. Cada pixel enmascarado de la imagen original da lugar a dos pixeles, uno para cada sombra. Cada uno de estos nuevos pixeles está dividido en dos semipixeles uno blanco y el otro negro. La obtención de un semipixel blanco-negro o negro-blanco tiene la misma probabilidad (p = 0'5), y no depende del color del pixel original[20]. Además, como el proceso de enmascaramiento de los pixeles es aleatorio, pues depende del resultado de lanzar una moneda al aire, y los resultados obtenidos en cada prueba

complejas y no serán comentadas aquí.

[20] Por este motivo, los pixeles de las sombras obtenidos no proporcionan ninguna información a los participantes

son independientes, no se obtiene información adicional si se observa un grupo de pixeles en cualquiera de las sombras.

Por otra parte, cuando se superponen las dos sombras (ver las columnas s_1+s_2 de las figuras 8.a y 8.b) se obtiene, si el pixel original era blanco, un pixel negro-blanco o blanco-negro, y un pixel negro si el pixel original era negro. Por tanto, cuando se superponen los pixeles de las sombras de un pixel original negro, se obtiene un pixel negro en la imagen que se recupera. Mientras que los pixeles blancos pierden contraste por el hecho de que el pixel que se obtiene al superponer las sombras es negro-blanco o blanco-negro y no completamente blanco[21].

Después de las consideraciones anteriores sobre el algoritmo definido, si la sucesión de caras (c) y cruces (x) obtenida por el observador para enmascarar cada uno de los 64 pixeles fue:

c	c	x	x	x	c	x	c
x	x	c	c	x	x	x	x
c	c	x	x	c	c	x	c
c	c	x	c	x	c	c	x
x	x	c	c	x	c	x	c
x	x	c	c	x	c	x	c
c	x	x	c	x	x	x	c
c	c	c	x	x	c	c	x

las sombras obtenidas son las que se muestran en las figuras 9 y 10:

Figura 9. Sombra obtenida para el primer participante.

Figura 10. Sombra obtenida para el segundo participante.

Las dos sombras serán impresas o fotocopiadas por el observador a dos transparencias y entregadas de forma secreta a cada uno de los dos participantes. Superponiendo las dos

sobre el color del pixel original.

[21] Esta pérdida de contraste en la imagen obtenida al superponer las sombras hace que se recomiende el uso de imágenes claramente definidas.

transparencias de las dos sombras anteriores, la imagen original recuperada es la que se muestra en la figura 11[22].

Figura 11. Imagen secreta recuperada.

Después de la presentación anterior, la actividad de los alumnos consiste en dibujar una imagen con contrastes definidos, utilizando pixeles cuadrados, y luego enmascarar la imagen que han elaborado.

La actividad anterior se puede extender de forma sencilla a esquemas visuales 2 de 3 mediante un algoritmo similar al descrito anteriormente y utilizando las sombras que se presentan en la figura 12:

Figura 12.- Sombras de un pixel en un esquema 2 de 3.

A modo de ejemplo se presentan las sombras de otras imágenes, así como las imágenes recuperadas en cada caso.

Figura 13. Símbolo π.

Figura 14. Bandera canadiense.

Figura 15. Símbolo de victoria.

12. Intenciones educativas

Como ya hemos comentado en la Introducción, la principal intención educativa que subyace al taller que se propone es la divulgar determinados aspectos de las Matemáticas, que quedan fuera de los contenidos de los curricula actuales, pero que no dejan de aparecer en los medios de comunicación y que son de absoluta actualidad. En este caso, son aspectos matemáticos relacionados con la seguridad de la información y de la criptología, pero que están basados en conceptos matemáticos conocidos (o al alcance) de nuestros alumnos.

[22] En la figura 11 se presenta la imagen recuperada con dos tonos para que se aprecie la imagen original y la pérdida de contraste. Ya se comentó que la imagen elegida estaba definida por muy pocos pixeles, con el objetivo de prestar la mayor atención al procedimiento y éste no quedara ensombrecido por la cantidad de

Además, de esta forma se trataría de “sistematizar” de alguna forma, algunos de los juegos que han practicado nuestros alumnos (sin saber que estaban haciendo Matemáticas), como el de enviarse mensajes secretos, utilizando para ello los más “sofisticados” métodos de cifrado.

Por otra parte, hay que tener en cuenta que una forma de presentar la criptografía a los alumnos podría ser algo así como la “ciencia de las matemáticas y los ordenadores con la presencia de un adversario, enemigo o espía”, lo que lleva presente aspectos relacionados con el drama y el suspense. Además, no hay que olvidar que una de las cosas que motivan más a los alumnos de cualquier edad es todo aquello que tenga que ver con el hecho de derrotar a los “malos” e incluso de jugar a “ser uno de los malos”.

En cuanto al nivel educativo en el que se podría desarrollar este taller, creemos que un lugar adecuado sería en cualquiera de los dos cursos del segundo ciclo de la E.S.O., como una asignatura optativa. Es cierto que algunas de las actividades que se proponen podrían ser llevadas a cabo en cursos anteriores, pero creemos que para sacarles mayor partido convendría que los alumnos tuvieran un determinado bagaje cultural, que les permitiera comprender la transcendencia de los problemas reales y cotidianos que se esconden detrás de las actividades que vayan a realizar: cuestiones de economía local (pavimentación de calles y temas turísticos), la responsabilidad de abrir la caja fuerte de un banco, enviar mensajes de forma secreta, etc.

Con relación a los cuestiones puramente matemáticas, conviene destacar que aparecen dos asuntos básicos: el relacionado con los conceptos matemáticos y el relativo a los aspectos metodológicos. Los primeros aparecen de forma clara en las actividades propias de la criptología (a partir de la §6); mientras que los segundos aparecen a lo largo de todas la actividades. Hemos pretendido que en las primeras actividades (de la §2 a la §5) no aparezcan conceptos matemáticos claramente definidos, de modo que a la hora de desarrollar la

---

pixeles a enmascarar.

actividad en cuestión, se haga especial hincapié en la metodología y en los aspectos didácticos que lleva la propia actividad, de modo que los alumnos aprecien especialmente los problemas que surgen y su planteamiento, y aborden su solución sin ideas preconcebidas.

Con relación a los conceptos matemáticos, y por no hacer una lista exhaustiva de los mismos, se puede mencionar que aparecen los siguientes:

- estadísticos (determinación de medias en §6, elaboración de tablas de frecuencias en §7);
- de numeración (trabajar en base binaria con bits y sumar números en esta base en §8 y §10).
- geométricos (giro y diseño de rejillas en §9, con el análisis de lo que podría llamarse semejanza de rejillas);
- de combinatoria (determinar el número de pruebas a realizar para descubrir un secreto en §10);
- probabilísticos (lanzamiento de una moneda y discusión de cuestiones de aleatoriedad, independencia y equiprobabilidad de sucesos en §11);

Para terminar, cabe destacar la presencia en las actividades de los siguientes aspectos metodológicos:

- el trabajo en grupo (en la mayor parte de las actividades);
- la elaboración de algoritmos y el análisis del su correcto funcionamiento, apreciando que las soluciones que se obtienen se acercan cada vez más a la óptima (§2, §7 y §8);
- la propuesta de nuevos problemas, diseñados por los propios alumnos (§2, §5 y §7);
- apreciar la complejidad de algunos problemas matemáticos y su falta de solución; notando que las Matemáticas no son algo acabado y que se pueden presentar nuevos problemas, completamente actuales, de fácil comprensión pero de difícil solución (§2 y §4);
- la utilización de diferentes estrategias para la resolución de problemas: de ensayo y error (§2 y §3), aproximarse a la solución de forma sucesiva (§4), suponer el problema resuelto

(§5), etc.

- interdisciplinariedad: Lengua (lectura de novelas de Alan Poe y Julio Verne, con cuestiones criptológicas, recomendadas en §7 y 9), Idiomas (análisis de las frecuencias de las letras en otros idiomas y descifrado de mensajes escritos en tales idiomas §7), Dibujo y Diseño (elaboración de imágenes definidas por píxeles en §11), Informática (trabajo con el código ASCII, bits y píxeles en §11 e implementación de los algoritmos diseñados en las distintas actividades).

Referencias bibliográficas

BLACKLEY, G. R. (1979): Safeguarding cryptographic keys. Proceedings of the National Computer Conference, American Federation of Information Processing Societies Proceedings 48, 313-317.

CABALLERO, P. y BRUNO C. (1994): "Uso didáctico de la criptografía: la administración de secretos". *Suma*, n.º 19, 59-64.

CSID (1993): Glosario de términos de Criptología. Publicación interna. Madrid.

ESPINEL, M. C. (1994): "El lenguaje de los grafos". *Suma*, n.º 16, 19-28.

ESPINEL, M. C. y CABALLERO, P. (1995): "La matemática que protege de errores a los números de identificación". *Suma*, n.º 20, 77-84.

FELLOWS, M. R. and KOBLITZ, N. (1993): Combinatorially based cryptography for children and adults. Comunicación personal.

FÚSTER, A.; GUÍA, D.; HERNÁNDEZ, L.; MONTOYA, F. y MUÑOZ, J. (1997): Técnicas criptográficas de protección de datos. RA-MA. Madrid.

MENEZES, A. J.; OORSCHOT, P. C. VAN and VANSTONE S. A. (1996): Handbook of applied cryptography. CRC Press, Boca Ratón, U.S.A.

NAOR, M. and SHAMIR, A. (1995): Visual cryptography. Advanced in Cryptology,

Eurocrypt’94, *Lecture Notes in Computer Science* 950, 1-12.

PASTOR, D. (1996): Diccionario enciclopédico del espionaje. Complutense. Madrid.

RIBAGORDA, A. (1997): Glosario de términos de seguridad de las T.I. Coda. Madrid.

SALOMAA, A. (1990): Public-key cryptography. Springer-Verlag. Berlín.

SCHNEIER, A. (1979): Applied cryptography. John Wiley & Sons. New York.

SGARRO, A. (1990): Códigos secretos. Pirámide. Madrid.

SHAMIR, A. (1979): How to share a secret. *Communications of the ACM* 22, 612-613.

STINSON, D. R. An introduction to visual cryptography. Comunicación personal.

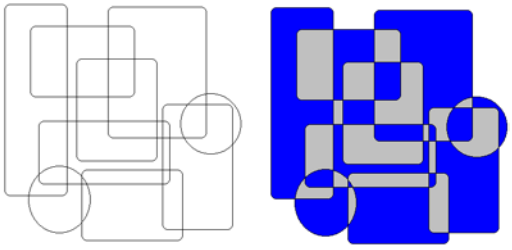


Figura 1

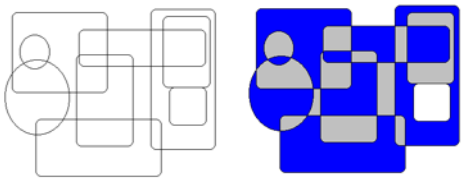


Figura 2

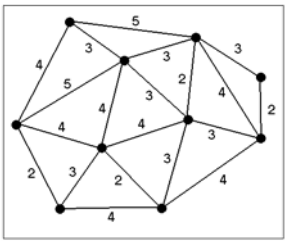


Figura 3

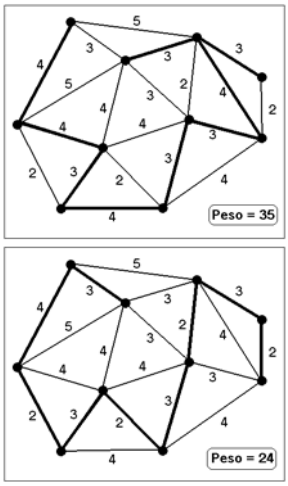


Figura 4

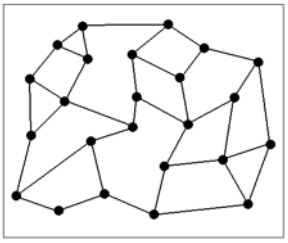


Figura 5

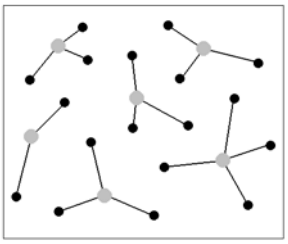


Figura 6

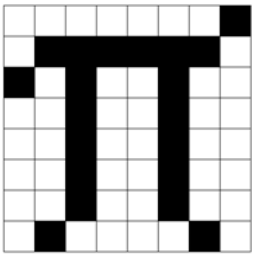


Figura 7

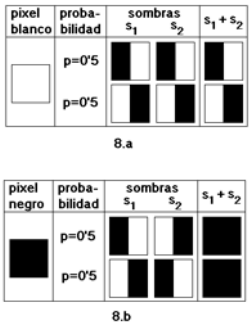


Figura 8

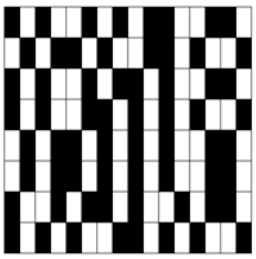


Figura 9

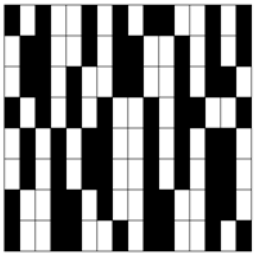


Figura 10

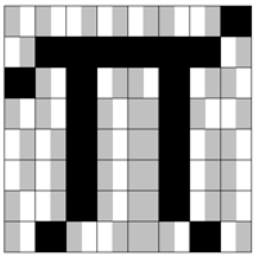


Figura 11

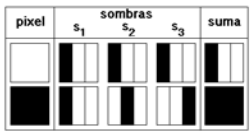


Figura 12

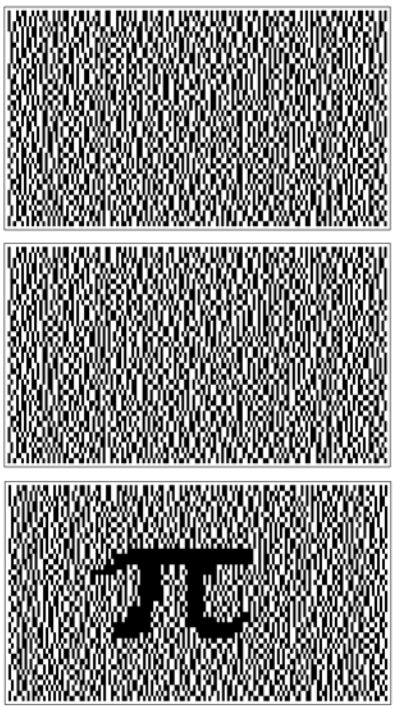


Figura 13

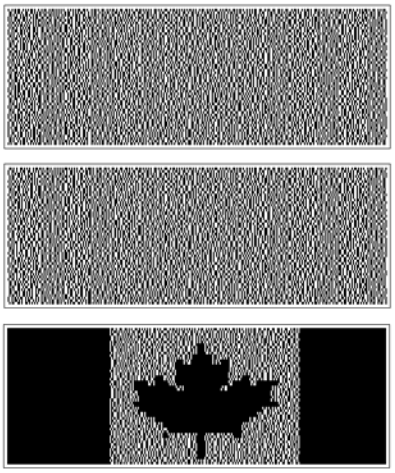


Figura 14

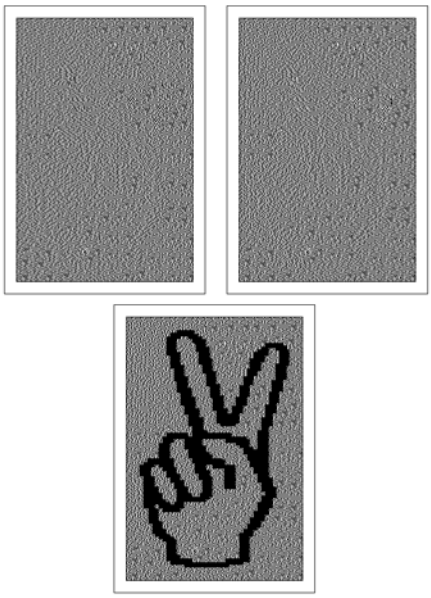


Figura 15