TALLER DE SECRETOS

Autores: CRYPTULL
Universidad de La Laguna

Resumen. El Taller de Secretos es un método de exponer como la Criptografía es un recurso útil para usar en el área de Matemáticas. Pretende dar una visión cercana, histórica e interdisciplinar de esta ciencia tanto al profesorado como al alumnado.
Se estructura en Mesas de Trabajo dedicadas, respectivamente, a:

- Códigos
- Cifrados Históricos y criptografía básica
- Criptografía científica
- Herramientas lúdicas en criptografía (técnicas y máquinas)
- Las Matemáticas en la Criptografía y el Criptoanálisis

Introducción

Se trata de describir algunas técnicas criptográficas que sean útiles para usar como herramienta didáctica en el área de matemáticas. Desde el nacimiento de la Criptografía hasta la actualidad su relación con las Matemáticas ha sido cada vez más estrecha. En la actualidad el desarrollo de la criptografía como CIENCIA está basado en las matemáticas. Para alcanzar a su actual estado la criptografía debió pasar por una larga gestación histórica como ARTE. De alguna manera podemos decir que aquel ARTE ha ido cargándose de matemáticas para convertirse en la actual CIENCIA.

En la actual Sociedad de la Información la criptografía se ha convertido en una necesidad que debería estar al alcance de cualquier ciudadano. Conocer y dar a conocer sus técnicas, sus avances y sus límites se convierten en un requerimiento social.

Metodología

El presente taller estará dividido en cinco partes. Aunque el conocimiento de todas podría ofrecer una visión más general de la criptografía y su relación con las matemáticas podríamos centrarnos en cualquiera de ellas para encontrar materiales que pueden llevarse al aula.

MESA DE TRABAJO	OBJETIVO
Códigos	Diferenciar entre criptografía y codificación.
Cifrados Históricos	Conocer los cifrados que durante siglos se han desarrollado en criptografía y las operaciones básicas de los sistemas criptográficos
Cifrados Científicos	Conocer los cifrados aparecidos a mitad del siglo XX, que incorporan a la criptografía a las ciencias por su carácter matemático.
Juguetes	Usar distintas herramientas manipulables relacionadas con la ocultación de secretos. Estenografía. Si bien no son criptográficamente consistentes, resultan lúdicos y atractivos para el aula.
Matemáticas	Plantear algunas cuestiones relacionadas con las matemáticas que encontraremos en la criptografía.

Se tratará de ofertar una exposición participativa y colaborativa. El desarrollo de los contenidos expuestos estará centrado en actividades con **MATERIALES MANIPULABLES**.

Intentaremos ofrecer una visión MANEJABLE, INTERDISCIPLINAR y CULTURAL de la CRIPTOGRAFÍA. Estimamos que estas son las características que deben valorarse para su uso DIDÁCTICO.

Manejable. Que pueda adaptarse a distintos niveles educativos y a distintos niveles de objetivos curriculares. Se centrará en los contenidos procedimentales y actitudinales, dejando los conceptuales en resúmenes y reseñas bibliográficas para el estudio de los participantes.

Interdisciplinar. Que puedan atenderse distintos campos de conocimientos y no sólo los matemáticos. Se subrayarán las fuentes literarias, los procedimientos científicos, tecnológicos y artísticos, los marcos lingüísticos, históricos y sociales.

Cultural. Que pueda dar respuesta a la creciente necesidad de la criptografía en el mundo de las Tecnologías de la Información y la Comunicación. Así como el papel que juegan los poderosos frente a los ciudadanos, así como los ámbitos de libertad y reconocimiento de derechos humanos que dicho mundo debe ofrecer.

A continuación expondremos los contenidos que incluye el "Taller de Secretos".

Comunicación

Cualquier Sistema de Comunicación estará compuesto de dos sujetos: el "Emisor" y el "Receptor" que intercambian una información: el "Mensaje" a través de un medio.

El objetivo de toda comunicación es que, finalmente, emisor y receptor compartan dicho mensaje. En ocasiones el medio tiene “ruido” que dificulta la transmisión del mensaje.

Este deseo, en numerosas ocasiones, se verá acompañado con otro: el de que el mensaje no sea conocido por nadie ajeno a dicha comunicación. Este concepto de ajeno suele denominarse en criptografía, por razones históricas, como el "Enemigo". Independientemente de que el Enemigo tenga la voluntad de interferir dicho mensaje o no, la comunicación, con este supuesto tendrá que usar inevitablemente conceptos y/o herramientas criptográficas.

La comunicación humana tiene como base el lenguaje y las lenguas desarrolladas por cualquier sociedad. Sin embargo, existen numerosos ejemplos de lenguajes ad hoc que son de enorme interés didáctico en el campo de las matemáticas y permiten la introducción de herramientas que serán claves para los nociones que posteriormente expondremos.

¿Qué son los códigos?

Un código es sistema de signos (que llamamos alfabeto) y de reglas (para combinar el alfabeto) que permite formular y comprender un mensaje. Se han creado numerosos códigos para distintos propósitos: el alfabeto Braille para la lectura de los ciegos, el lenguaje de los signos para la comunicación presencial para sordos, el alfabeto Morse para la telegrafía, las banderas para la comunicación marítima, el Pig Pen, etc. Cada uno de ellos tiene sus características y sus desarrollos que permiten distintos trabajos en el aula de matemáticas en campos como geometría o combinatoria.

La creación gráfica de un alfabeto, dado un conjunto de restricciones, es un ejercicio grato y permite el desarrollo de un procedimiento sistemático, e incluso algorítmico. Existen numerosos programas informáticos que permiten trasladarlos a un fichero de fuentes útiles para el ordenador. Inspirarse en los numerosos alfabetos existentes en el mundo o en las distintas caligrafías de estos, es una experiencia con cautivantes consideraciones estéticas.

Desde cualquier ejemplo que se tome es fácil alcanzar la necesidad de traducir numéricamente los alfabetos y el entorno de finito que aparece en él. Es posible desviarse hacia los códigos correctores de error o bien a la mejora que supone trabajar con un sistema binario para cualquier codificación.

Después de trabajar con códigos es necesario subrayar que la codificación no es criptografía. Que cuando un código oculta un mensaje no es por que esté diseñado para ello sino que simplemente muestra ignorancia, como padecieron Champollion o Kober cuando se enfrentaron a los signos dejados por civilizaciones desaparecidas.

¿Qué es la Criptografía?

Entendemos por criptografía al arte o la ciencia (que ambas cosas ha sido) de ocultar, mensajes escritos (independientemente si son soportados por papel, circuitos electrónicos, bandas magnéticas, etc). Los sistemas criptográficos están diseñados para que oculten lo escrito independientemente de la lengua o el código que se haya escogido.

De las manipulaciones del mensaje claro mediante estas operaciones se obtiene un criptograma. Lo importante es que existan reglas que permitan realizar estas operaciones por parte del Emisor con intención de que sean irreconocibles o difícilmente reconocibles por el Enemigo en el caso de que este alcance a leer el criptograma y que sea fácilmente restituible el criptograma a su estado inicial por parte del Receptor.

Todos los sistemas criptográficos existentes se basan en dos operaciones básicas que podemos realizar con el alfabeto del código elegido. Los signos del mensaje claro pueden ser o bien cambiados de posición dentro del mensaje, que llamaremos transposición o bien sustituidos por otros signos del alfabeto que llamaremos sustitución. Es posible también que el sistema simultanee ambas operaciones. Los sistemas que estudiaremos los agrupamos en las siguientes categorías:

- Los Sistemas de Transposición clásicos de interés didáctico son la Scitala griega y las Rejillas.

- Denominamos Sistemas de Sustitución Monoalfabéticos aquellos que usan la misma clave de sustitución para todas las letras del mensaje. Tales como, el Atbash bíblico, el mlecchiata-vikalpa del Kamasutra, el cifrado de Cesar.

- Denominamos Sistemas de Sustitución Polialfabéticos aquellos que usan la distintas claves de sustitución para distintas letras del mensaje. Tales como, el cifrado de Vigenere, el cifrado de Playfair o el cifrado de Vernam.

Cada uno de estos sistemas llevan acompañado un personaje, una época histórica, un problema político o social o una anécdota que dota de color estos sistemas.

La criptografía científica

La aparición de los ordenadores digitales, como el ENIAC en 1948, y la publicación de la Teoría de las comunicaciones secretas de Claude Shannon en 1949 marcan el comienzo de los conceptos que incorporan a la Criptografía a las disciplinas científicas.

Describiremos loa siguientes criptosistemas:

- Cifrado en flujo.
- Cifrado en bloques: DES.
- Cifrado de clave pública: RSA

La Criptografía como diversión.

Podemos lanzarnos a ocultar mensajes con una actitud lúdica sin pararnos a contemplar ni los aspectos criptológicos ni los aspectos matemáticos.

Existen un variopinto conjunto de métodos que pueden ser accesibles para los distintos niveles de enseñanza.

- Estenografía
- Tintas invisibles.
- Telégrafos visuales, mecánicos o eléctricos.
- Máquinas criptográficas: Rotadores de Alberti, Reglas de Saint Cir o Cilindros de Jefferson. Simularemos una máquina Enigma.
- Papel, lápiz y tijeras. Mensajes recortados en tiras y en puzzles, Laberintos o Rejillas de Cardano.
- Máscaras y Nomenclatores.
- Criptografía Visual.

Las matemáticas en la Criptografía

La aritmética congruencial o modular es usada en codificación y criptografía debido a que los alfabetos que se usan son conjuntos finitos, y sobre ellos generamos distintos tipos de aplicaciones matemáticas. La manipulación numérica de estos conjuntos es de los campos de mayor desarrollo en las matemáticas actuales. Requiere de conceptos que normalmente están reservados para la docencia en niveles superiores. Sin embargo, reservan conceptos y razonamientos que pueden ser abordados en la enseñanza secundaria. Como el tema de este trabajo no es la aritmética modular, ofrecemos el menor número de procedimientos que sirvan para manipular las cuestiones que la criptografía requiere.

Las operaciones en este conjunto son sencillas. Para facilitar su uso podemos usar las tablas de las operaciones suma y producto.

Estudiaremos técnicas necesarias para el cifrado y el descifrado como:

- Cálculo de inversas.
- Resolución de ecuaciones lineales.
- Resolución de sistemas de ecuaciones.

Asimismo, aportaremos algunos sistemas criptográficos puramente matemáticos, como el sistema de sustitución por transformación afín, el sistema de Hill, sistemas matriciales y cifrados en flujo.

Definiremos los sistemas de clave pública, el uso de los números primos, la factorización, y las funciones de sentido único.

Buena parte del desarrollo de este apartado será más manejable mediante instrumentos computacionales (calculadoras y ordenadores).

Estudiaremos las características del criptoanálisis.

Los procedimientos básicos del criptoanálisis son:

La búsqueda exhaustiva. Recorrer el conjunto de claves y aplicando el algoritmo inverso hasta obtener el mensaje inicial.

El análisis de frecuencias. Estudiar y conocer las frecuencias relativas tanto de las letras en el código original, como de las apariciones de las letras en criptograma. Entonces con esta información se emparejará cada letra del criptograma con una del idioma original de manera que coincidan lo más posible las frecuencias anteriores de ambas. Será necesario realizar distintos intentos con distintos emparejamientos siempre tratando que las frecuencias de las letras estén cercanas.

Tanto la búsqueda exhaustiva como el análisis de frecuencias serían herramientas extremadamente débiles si no fueran acompañadas de estudios detallados sobre las periodicidades que se generan en los criptogramas las distintas claves.

Usaremos para los procedimientos básicos los elementos de las matemáticas que pueden ser de interés para la educación. Estos son la combinatoria, la estadística descriptiva, la estadística inferencial y la búsqueda y resolución de algoritmos inversos.

Bibliografía

- BAUER, F. L. Decrypted Secrets. Springer. 1997
- CABALLERO, P. Introducción a la Criptografía. 2ª Edición. Ra-Ma. 2002.
- SINGH. S. Los códigos secretos. Debate Editorial. 2000 AGOTADO

Descarga: http://www.simonsingh.net