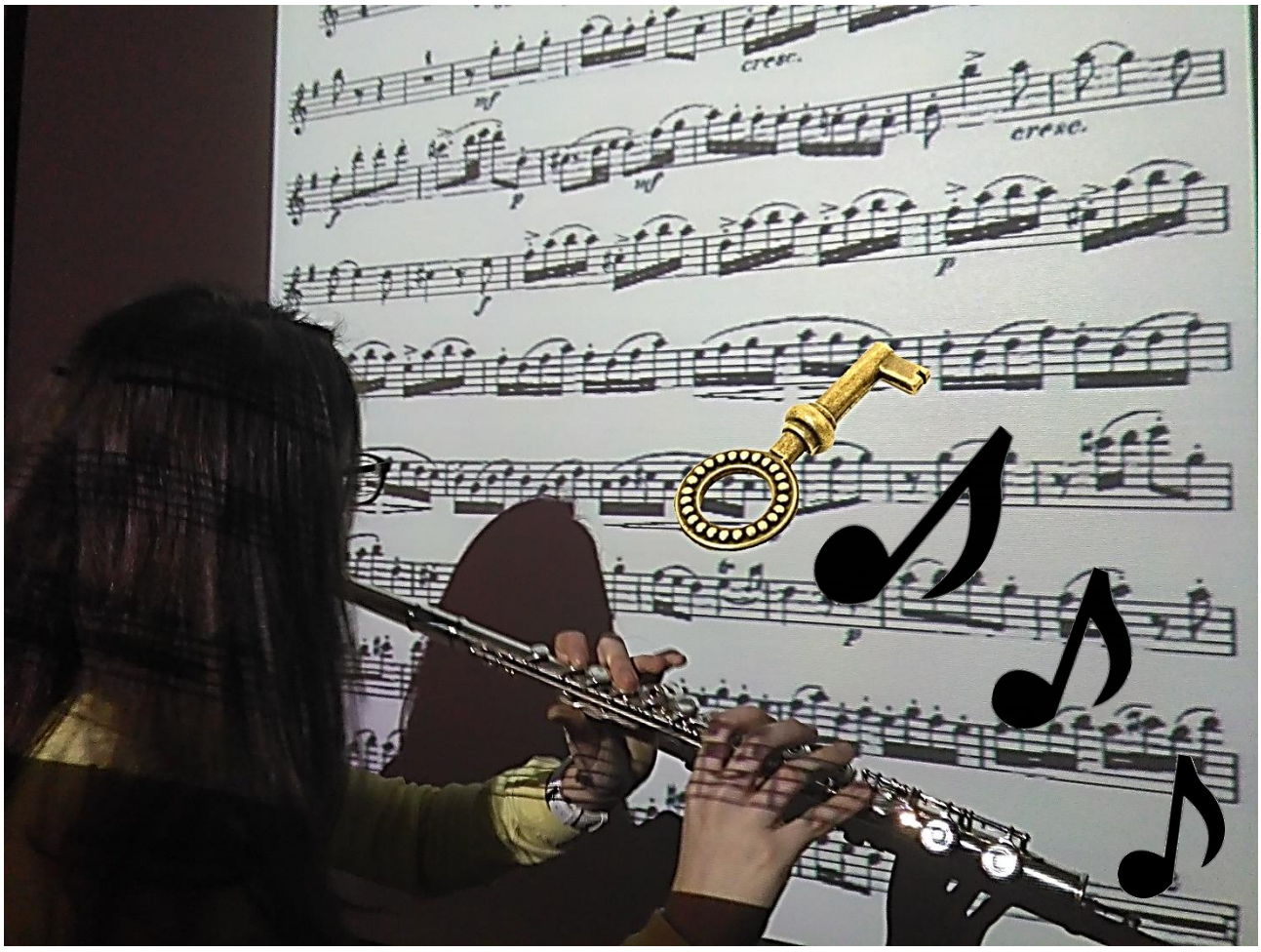
Concurso LibreTICs

APLICACIÓN DE LAS MATEMÁTICAS ORIENTADAS A LAS COMUNICACIONES: ENCRIPTACIÓN MEDIANTE ALGORITMOS EN LA TRANSMISIÓN DE MENSAJES CIFRADOS



Autores:
Carla Martínez Nieto-Márquez
Miguel Ángel Mariano Arencón (Portavoz)
Tutor:
Miguel Ángel Ruiz Núñez.
Curso: 2º de Bachillerato

Introducción

Como se puede apreciar en este video (pulse aquí para verlo), desde el comienzo de la historia y de la conciencia de privacidad, se ha tenido la necesidad de transmitir mensajes de manera secreta y que resulten ininteligibles para receptores no autorizados, de manera que se consiga la confidencialidad de estos. Esta técnica de cifrado o codificado de los mensajes, empleada tanto en el ámbito científico como en el artístico, se denomina criptografía o encriptación. Para poder realizarla, existen una serie de métodos ya definidos; pero como todo lo relacionado con la tecnología, hoy en día se está en un continuo proceso de avances. Por eso, aparte de explicar como funcionan los métodos ya conocidos, hemos decidido plantearnos la creación de un método novedoso para poder encriptar un contenido concreto.

Para poder realizar la encriptación de cualquier contenido, es necesario disponer de unas herramientas matemáticas con las que pueda ser llevada a cabo. Para ello, empleamos los algoritmos. En matemáticas, lógica, ciencias de la computación y disciplinas relacionadas, un algoritmo es un conjunto prescrito de instrucciones o reglas bien definidas, ordenadas y finitas que permite realizar una actividad mediante pasos sucesivos que no generen dudas a quien deba realizar dicha actividad. Dados un estado inicial y una entrada, siguiendo los pasos sucesivos se llega a un estado final y se obtiene una solución. Los algoritmos se expresan de forma gráfica mediante los diagramas de flujo. Asimismo tampoco podemos pasar por alto que los algoritmos se pueden expresar a través de lenguajes de programación, pseudocódigo, el lenguaje natural.

Los algoritmos pueden ser usados en distintos ámbitos, incluso en la vida cotidiana para la toma de decisiones (figura 1). Sin embargo, el ámbito más común y el que nos interesa ahora es el de su utilización en el ámbito matemático. Por ejemplo, si tenemos dos números los cuales queremos comparar, podemos seguir una serie de pasos hasta llegar a la solución. Todo ese conjunto de pasos es lo que constituiría un algoritmo (figura 2).

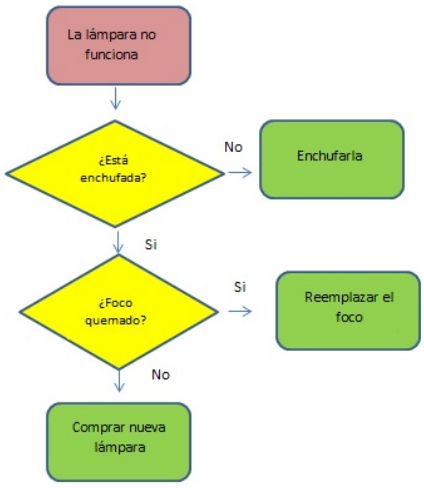


Figura 1

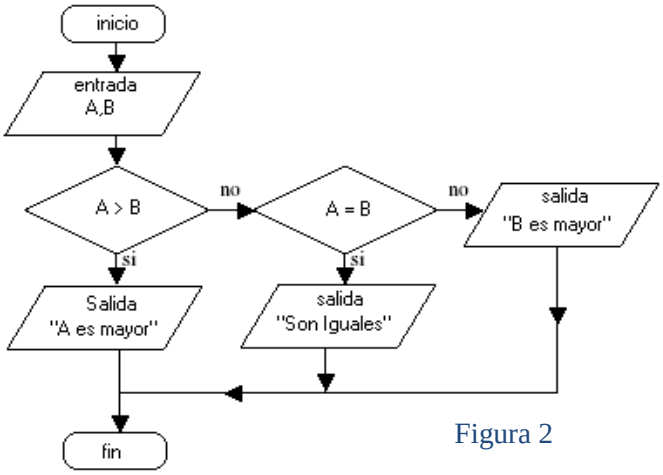


Figura 2

Estos algoritmos pueden tener distinto grado de complejidad. Así, podemos encontrar algoritmos más sencillos, como el del ejemplo anterior; a otros de un grado de complejidad mayor. Este último tipo de algoritmos es el que usaremos a continuación para desarrollar el modo de funcionamiento de los diferentes modos de encriptación.

La encriptación: Algoritmos

Actualmente, existen tres algoritmos diferentes para realizar la encriptación de un contenido específico:

- Algoritmos simétricos: Estos sistemas emplean la misma clave de cifrado y descifrado, por lo que resultan relativamente sencillos.
- Algoritmos asimétricos: Estos requieren de dos claves, una privada y otra pública, ambas relacionadas con una fórmula matemática imposible de reproducir.
- Algoritmos HASH: Este algoritmo realiza un cálculo matemático sobre los datos del documento y da como resultado una combinación de números y letras que se denomina MAC.

Pasamos ahora a desarrollar el funcionamiento de cada uno de ellos, para ver luego las aplicaciones de cada uno. Además, igual que hemos explicado antes, aquí también hay diferentes grados de complejidad; siendo los simétricos los más sencillos, y los HASH los más complejos.

1. Algoritmos simétricos

Entre todos los algoritmos empleados en la encriptación, los algoritmos simétricos resultan ser los más sencillos. El sistema de cifrado simétrico es un tipo de cifrado que usa la misma clave para cifrar y para descifrar, es decir, ambas partes conocen la clave usada de antemano. Una vez de

acuerdo, el emisor cifra un mensaje usando la clave, lo envía al destinatario, y este lo descifra usando la misma clave. Existen numerosos tipos de algoritmos de los que después trataremos, pero la idea principal es que para asegurar la seguridad de un texto cifrado, nos debemos de basar en la clave; y no poner ninguna atención al algoritmo empleado, pues a un atacante no le es de ninguna ayuda conocer el algoritmo que se está usando.

Los algoritmos simétricos se apoyan en dos conceptos:

- **Confusión:** Consiste en ocultar la relación entre el texto inicial, el texto cifrado y la clave.
- **Difusión:** Consiste en repartir cada bit del mensaje original lo más separadamente posible entre el mensaje cifrado.

Podemos distinguir un variado número de algoritmos, a continuación explicaremos el funcionamiento básico de algunos de ellos y su complejidad.

Redes de Feistel

No es un algoritmo cifrado, pero es utilizado por muchos de los algoritmos que vamos a ver a continuación, consiste en dividir el texto inicial (o la información inicial) en dos mitades L y R, se toma una función y una clave K_i, se realizan una serie de operaciones con F, K y con L o R, después la cadena obtenida se cambia por la otra cadena con la que no se han realizado operaciones y se continua haciendo esta ronda de operaciones.

Su funcionamiento es el siguiente: Consideraremos que para una determinada clave entrada, las dos funciones que hemos mencionado antes (figura 3)

Entrada	F_1 Salida
00	11
01	00
10	11
11	01

Entrada	F_2 Salida
00	01
01	11
10	01
11	10

Figura 3

Después, aplicamos la función XOR, la función suma (figura 4)

XOR	0	1
0	0	1
1	1	0

Así, ahora usaremos las dos funciones iniciales y la XOR, para, mediante una serie de cálculos, convertir el mensaje de entrada en uno distinto de salida; es decir, para encriptarlo (figura 5).

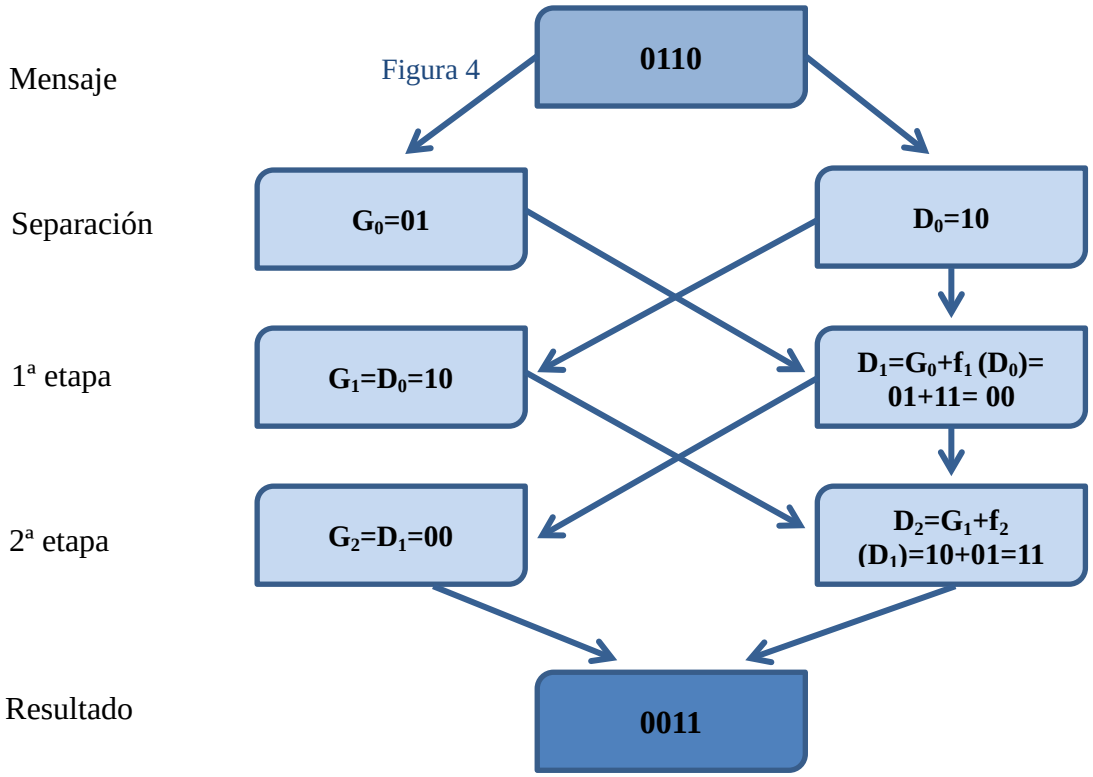


Figura 5

Ahora vamos a ver los distintos mecanismos algorítmicos para llevar a cabo esta encriptación

2. DES: Data Encryption Estándar

Es el algoritmo simétrico más extendido mundialmente. A mediados de los setenta fue adoptado como método estándar para las comunicaciones seguras.

Se trata de un algoritmo que toma un texto de una longitud finita de bits y lo transforma mediante una serie de operaciones, en otro texto cifrado de la misma longitud. DES utiliza una clave para modificar la transformación realizada por los algoritmos, esta clave mide 64 bits, aunque solo se utilizan 56 de ellos por el algoritmo. Este algoritmo es una red de Feistel de 16 rondas, con dos permutaciones que aparecen al principio y al final. Las partes principales del algoritmo son las siguientes (Figura 6):

- Fraccionamiento del texto en bloques de 64 bits (8 bytes),
- Permutación inicial de los bloques,

- Partición de los bloques en dos partes: izquierda y derecha, denominadas *I* y *D* respectivamente,
- Fases de permutación y de sustitución repetidas 16 veces (denominadas rondas)
- Reconexión de las partes izquierda y derecha, seguida de la permutación inicial inversa.

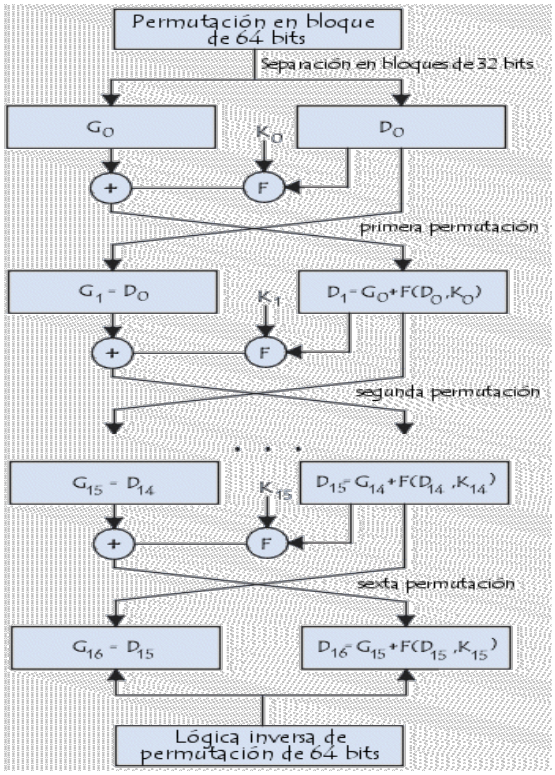


Figura 6

La flexibilidad de DES reside en que emplea el mismo algoritmo para cifrar y para descifrar.

Para hacer este cifrado aún más seguro, se le aplica el mismo algoritmo varias veces, para fortalecer la longitud de la clave. Este procedimiento es conocido como cifrado múltiple o algoritmo DES múltiple.

3. IDEA: International Data Encription Algorithm

Trabaja con bloques de 64 bit de longitud, empleando claves de 128 bits. Al igual que en el algoritmo DES, se emplea el mismo algoritmo para cifrar como para descifrar. Se realizan 8 transformaciones idénticas llamadas rondas y una transformación de salida llamada media ronda. Emplea operaciones matemáticas distintas, la suma, la multiplicación (figura 7).

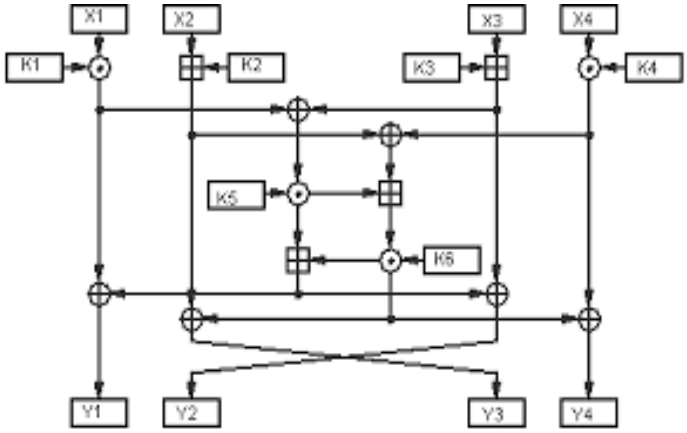


Figura 7

2. Algoritmos asimétricos

Los algoritmos asimétricos, también conocidos como llave o cable público, emplean dos llaves diferentes en cada uno de los extremos de la comunicación. Cada usuario tendrá una clave pública y otra privada. La clave privada tendrá que ser protegida y guardada por el propio usuario, será secreta y no la deberá conocer nadie. La clave pública será accesible a todos los usuarios del sistema de comunicación. Los algoritmos asimétricos están basados en funciones matemáticas

fáciles de resolver en un sentido, pero muy complicadas realizarlo en sentido inverso a menos que se conozca la llave. De esta forma, se consigue un tipo de encriptación muy fácil de ser llevada a cabo, pero difícil de desencriptar, y por tanto, de destapar (figura 8)

Figura 8

Con este sistema de criptografía, se soluciona uno de los problemas que presentaba la encriptación mediante algoritmos simétricos: la necesidad de que tanto emisor como receptor conocieran y usaran la misma clave. Con este tipo de encriptación, solo es necesario que el receptor disponga de la llave pública para poder descifrar el mensaje transmitido, ya que las dos claves están relacionadas simétricamente. Además, conociendo una clave no se puede descubrir cuál es la otra.

Aunque aparentemente este sistema sea perfecto, al solucionar los problemas del anterior; plantea otro tipo de problemas. Por tener que ser cifrado y descifrado por dos claves distintas, aunque relacionadas, el proceso tiene una duración mayor. Por ese mismo motivo, es de poca utilidad con archivos de gran tamaño; y da lugar a archivos encriptados de mayor tamaño que los originales. Todo esto, sumado a claves de mayor complejidad, da lugar a un coste mayor. Sin embargo, esto se ha visto reducido últimamente con los nuevos sistemas de clave asimétrica basados en curvas elípticas, que tienen características menos costosas. Se utiliza un híbrido formado por la criptografía asimétrica para intercambiar claves de criptografía simétrica, y la criptografía simétrica para la transmisión de la información. De esta forma, al combinar la seguridad de la criptografía asimétrica con la sencillez de la simétrica; se consigue un sistema criptográfico eficiente y seguro.

Existen varios tipos diferentes de criptografía asimétrica, como pueden ser la RSA, DH, DSA… Son mucho más complejas que las simétricas, al basarse en algoritmos con operaciones matemáticas de mayor dificultad.

3. Algoritmos HASH

Los algoritmos HASH constituyen el mecanismo de encriptación más complejo. Se basan en funciones que resumen el contenido a encriptar en un código de las mismas dimensiones alfanuméricas, independientemente de la longitud del archivo inicial. Estas funciones no tienen el mismo propósito que los otros modos de encriptación, debido a su mecanismo de funcionamiento. Así, se usa para asegurar que no se ha modificado un archivo en una transmisión, hacer ilegible una contraseña o firmar digitalmente un documento. Por eso, se podría no considerar como un algoritmo de encriptación. Por eso mismo es usado además como un mecanismo dentro de la encriptación asimétrica.

Se basa en una función unidireccional, de forma que usa algoritmos que aseguran que el mensaje que se transmite no podrá ser nunca descifrado ni por el emisor, ni interceptándolo en mitad de la transmisión (figura 9). Además, como se generan resúmenes de una longitud concreta, hay más combinaciones posibles de contenidos a encriptar, que de códigos encriptados. Por ese motivo, es posible que para distintos mensajes a encriptar obtengamos un mismo resultado, pero esto no supone un problema, ya que si se consiguieran (con un buen algoritmo) dos hash iguales los contenidos serían totalmente distintos.

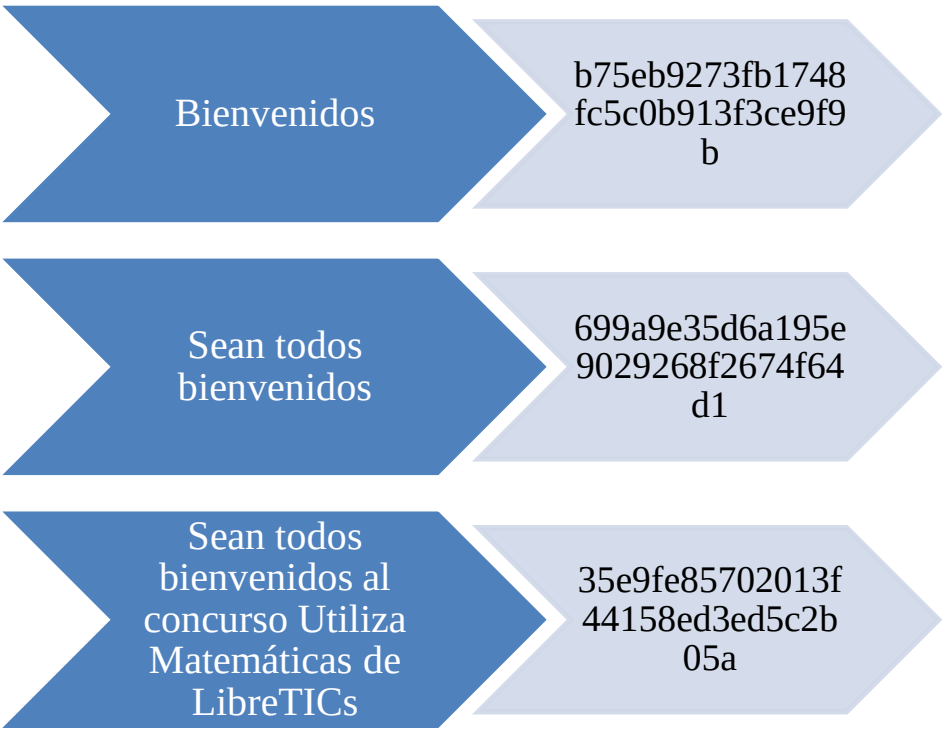


Figura 9

Aplicaciones

Esta investigación sobre los algoritmos relacionados con la encriptación nos ha llamado la atención y ha despertado nuestra creatividad. Por eso, hemos pensado que una buena forma de poner en práctica aquello que hemos aprendido es creando nuestro propio código de encriptación, y como nosotros fijamos las normas, hemos decidido que una buena forma es asociando este contenido matemático a la música. Así, además, podemos crear sistemas de encriptación novedosos y más complejos de destapar

Como mostramos en el video inicial, cualquier melodía puede esconder un mensaje secreto, y puede hacer que, por ejemplo, un bando salga victorioso de la guerra. Para que contenga un mensaje secreto, lo 1º que hay que hacer es pasar ese mensaje a código binario. Como ejemplo, hemos usado el enunciado: *El enemigo se acerca*. Utilizando un código creado por nosotros (figura 10), que establece una relación entre números y letras, hemos convertido la frase en una combinación de números: 40 47 40 49 40 48 44 42 51 55 40 36 38 40 54 38 36

Después, hemos convertido cada uno de esos números a binario, según el proceso habitual. Así, hemos obtenido la frase ya en binario.

A	**36**
B	37
C	38
D	39
E	40
F	41
G	42
H	43
I	44
J	45
K	46
L	47
M	48
N	49
Ñ	50

O	51
P	52
Q	53
R	54
S	55
T	56
U	57
V	58
W	59
X	61
Y	62
Z	63

Figura 10

E	L	E	N	E	M	I	G	O	S	E
101000	101111	101000	110001	101000	110000	101100	101010	110011	110111	101000

A	C	E	R	C	A
100100	100110	101000	110110	100110	100100

Para establecer los espacios entre palabras pondremos un 0 que en la partitura se representará por una coma (,)

101000 101111 0 101000 110001 101000 110000 101100 101010 110011 0 110111 101000 0 100100 100110 101000 110110 100110 100100

Para complicar aún más nuestra encriptación daremos la vuelta al mensaje, lo permutaremos, como si empleáramos un espejo; de manera que quede de la siguiente forma:

001001 011001 011011 000101 011001 100100 0 000101 111011 0 110011 010101 001101 000011 000101 100011 000101 0 111101 000101

A continuación, tenemos que definir nuestro código que relacione números con notas (figura 11).

Altura (nota)	Binario	Duración
Do	000	Cuadrada (8)
Re	001	Redonda (4)
Mi	010	Blanca (2)
Fa	011	Negra (1)
Sol	111	Corchea ($^1/_2$)
La	100	Semicorchea ($^1/_4$)
Si	101	Fusa ($^1/_8$)
Do”	110	Semifusa ($^1/_{16}$)

Figura 11

Los tres primeros bits indicarán el sonido, y los tres últimos indican la duración (Nombre de la nota, Duración):

001001 011001 011011 000101 011001 100100 0 000101 111011 0 110011 010101 001101 000011 000101 100011 000101 0 111101 000101

001001 RE REDONDA
011001 FA REDONDA
011011 FA NEGRA
000101 DO SEMICORCHEA
011001 FA REDONDA

100100 SOL CORCHEA

0

000101 DO SEMICORCHEA

111011 DO” NEGRA

0

110011 SI NEGRA

010101 MI SEMICORCHEA

001101 RE SEMICORCHEA

000011 DO NEGRA

000101 DO SEMICORCHEA

100011 SOL NEGRA

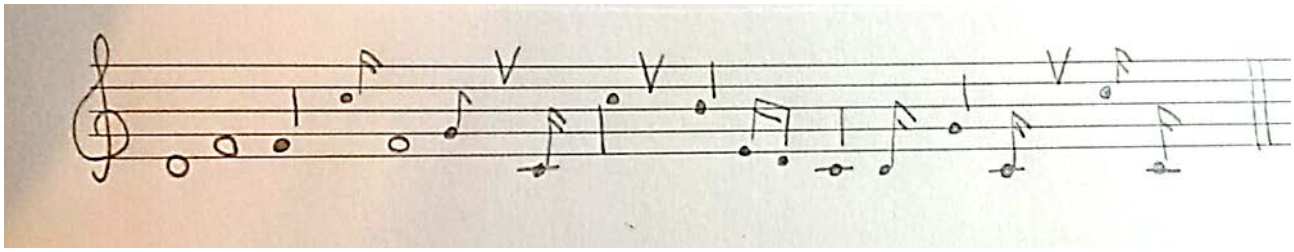
000101 DO SEMICORCHEA

0

111101 DO” SEMICORCHEA

000101 DO SEMICORCHEA

La partitura quedará de la siguiente forma:



Así, ya tendríamos nuestro mensaje para transmitir totalmente encriptado con un código que solo nosotros conocemos. En caso de que queramos hacer el proceso contrario, es decir, desencriptarlo; solo tendremos que seguir los pasos que hemos realizado, pero a la inversa. Para empezar, conociendo el código con el que asociamos números y sonidos, deduciríamos los números del código binario permutado. Una vez obtenidos, debemos volver a invertirlos, para obtenerlos en el orden inicial. Después, teniendo en cuenta los ceros que se referían a espacios entre palabras que deberíamos haber destacado de una forma distinta al pasar de la partitura a números, ya que repreentaban comas; pasaremos esos números binarios a números del sistema decimal con el cálculo binario inverso. Una vez hecho eso, asociamos las cifras a las letras según nuestro código, y ya tendremos el mensaje que deseábamos transmitir de nuevo.

Conclusiones

Hoy en día, la tecnología está en auge. Cada vez son más las áreas de trabajo e investigación que requieren de una serie de conocimientos de informática mínimos, que cada vez están también más extendidos. Por ese motivo, la encriptación nos ha parecido un tema muy interesante, ya que cualquier plus en conocimientos de este tipo puede suponer una gran ventaja en el mundo laboral. Y más aún si está relacionado con el mundo de la privacidad, algo que ha alcanzado a todo el mundo, y que cualquier persona desea.

Sin embargo, como no es fácil conseguirla, se requiere de una serie de herramientas muy avanzadas, las cuales nos han permitido también adentrarnos más a fondo en las matemáticas, en el campo de los algoritmos. Además, al ser un área en desarrollo, se pueden inventar constantemente nuevos métodos de encriptación, como hemos hecho nosotros mismos en este trabajo. Y, aunque para ellos son importantes tener unas bases matemáticas bien definidas; lo más importante es darle ese toque de originalidad y creatividad, que, aparte de permitirnos crear algo novedoso, haga que sea algo muy difícil de imaginar por cualquier otra persona; y que, por tanto, dificulta la desencriptación, mejorando la seguridad de cualquier contenido encriptado mediante nuestro código secreto. Si a todo esto le sumamos el relacionar áreas como la informática y las matemáticas, con otras tan dispares como la música, conseguimos que este trabajo no suponga solo ampliar nuestros conocimientos sobre un campo de las ciencias o presentarnos a un determinado certamen, si no también mejorar nuestra capacidad de emprendimiento e innovación, algo que se hace fundamental en nuestra sociedad para alcanzar el éxito, tanto personal como laboral.

Forma de Exposición

Vamos a emplear una presentación para explicar en qué consisten los algoritmos, y los distintos tipos de éstos que se emplean en la encriptación. Además mostraremos una pequeña melodía, que será una pequeña frase encriptada; explicando el modo en que hemos llegado a esa frase, y los distintos pasos de la encriptación del mensaje. Uno de nosotros tocará dicha melodía con la flauta travesera. Esta melodía corresponderá a la frase: “Abre la puerta”, que previamente habremos encriptado según nuestro propio código. Así, un pequeño robot, también conocedor del código que hemos usado, al percibir la melodía y desencriptarla; procederá a realizar la acción ordenada, abriendo una pequeña puerta que fabricaremos de forma muy sencilla.

Bibliografía

- https://es.wikipedia.org/wiki/Algoritmo
- http://enriquebarrueto0.tripod.com/algoritmos/sesion03algoritmos.htm
- http://www.redeszone.net/2010/11/16/criptografia-algoritmos-de-cifrado-de-clave-asimetrica/
- https://es.wikipedia.org/wiki/Criptograf%C3%ADa_asim%C3%A9trica#Seguridad
- http://www.ecured.cu/Algoritmo_asim%C3%A9trico
- http://www.iit.upcomillas.es/palacios/seguridad/cap05.pdf
- http://www.karapanza.net/cripto-que/
- https://www.gnupg.org/gph/es/manual/c190.html
- http://www.segu-info.com.ar/criptologia/simetricos.htm
- http://www.genbetadev.com/seguridad-informatica/tipos-de-criptografia-simetrica-asimetrica-e-hibrida
- https://es.wikipedia.org/wiki/Data_Encryption_Standard
- https://es.wikipedia.org/wiki/Cifrado_de_Feistel
- http://serdis.dis.ulpgc.es/~iicript/FICHEROS%20WEB/criptografia%20moderna/redes%20Feistel_files/voila_data_002/voila_data_002/voila_002.htm
- http://es.ccm.net/contents/130-introduccion-al-cifrado-mediante-des
- https://prezi.com/n0uq2ltct_gf/algoritmo-idea/
- http://www.genbetadev.com/seguridad-informatica/que-son-y-para-que-sirven-los-hash-funciones-de-resumen-y-firmas-digitales
- http://gaussianos.com/algoritmos-hash-i-introduccion/
- http://www.redeszone.net/2010/11/09/criptografia-algoritmos-de-autenticacion-hash/
- https://es.wikipedia.org/wiki/Funci%C3%B3n_hash