Premios del Departamento de Matemáticas de la Universidad Autónoma de Madrid para Estudiantes de Secundaria

Quinta Edición, 2010/2011

TRABAJO: Cifrados armónicos

GANADOR EN LA CATEGORÍA DE E.S.O.

AUTORES:

- Teresa de Lera Figal
- Carlota Siljestrom Berenguer
- Juan José Villar Roldán
- Guzmán Yepes Cagigal

TUTOR:

- Manuel Béjar

CENTRO: Colegio Nuestra Señora del Recuerdo (Madrid)

CIFRADOS ARMÓNICOS

Enigma

ÍNDICE

INTRODUCCIÓN

Desde siempre ha existido la necesidad de transmitir mensajes que sólo fuesen leídos por la persona que se quisiese, es decir, que no fuesen leídos por otras personas. Esto no es fácil, ya que no podemos confiar en que los medios sean seguros, rápidos y lo suficientemente eficaces para que quien nos interese y sólo quien nos interese obtenga la información de la manera que nos convenga, ya sea un mensaje rápido o que tenga que perdurar, etc..

Ya desde la antigua Grecia y Roma se utilizaban métodos para transmitir mensajes confidenciales. El ejemplo que ha tenido más relevancia es el llamado *Cifra* de Julio César, ya que fue este emperador romano el que tuvo la idea de escribir los mensajes sustituyendo cada letra por la que estaría varios puestos más adelante en el alfabeto. Para descifrar el mensaje, el receptor simplemente debe invertir el proceso de acuerdo con la clave. No es un método muy seguro, pues sólo hay 25 maneras de cambiar el alfabeto original. Un criptoanalista podría descifrarlo rápidamente. En el siglo XIII Roger Bacon ideó unas técnicas para mejorar el cifrado y marcó las pautas de la criptografía medieval. A partir del siglo XV los criptoanalistas se percataron de que conociendo la frecuencia de las letras era posible reducir el tiempo de descifrado. Comparando la frecuencia de los caracteres en el texto cifrado con las de un texto sin cifrar en una lengua dada conocida, es posible empezar a descubrir cifras. Fue necesario introducir nuevas técnicas. Giovanni Batista escribió un manual sobre criptografía en el XVII. Se habían introducido ya caracteres nulos, que no tienen equivalente en el alfabeto original. En el XX destacamos figuras como William Friedman, que rompió la clave *púrpura* de los japoneses. Escribió una serie de manuales de criptoanálisis que marcaron un hito histórico en esta ciencia.

OBJETIVOS

En este trabajo presentamos de forma original un nuevo sistema para encriptar mensajes usando armonía musical. Exponemos dos versiones. Una primera que expresa la idea general de nuestro código y una segunda, mejorada, que hace más difícil descifrar el mensaje oculto.

ANTECENDENTES

1. CONCEPTOS BÁSICOS DE CRIPTOGRAFÍA

La ciencia que estudia la realización y utilización de códigos y cifras es la criptografía, y la que estudia los métodos para descifrar estos códigos, estos mensajes es el criptoanálisis.

1.1 Criptografía: definición, método y enseñanza

La criptografía a lo largo de la historia se basa en dos ideas o métodos: mover o intercambiar las letras del alfabeto y sustituir las letras por números. Para esto se utiliza un número llamado “clave”que se añade o se substrae del número que corresponde a la letra (en el alfabeto) que hace casi imposible la traducción de este mensaje si no se posee dicha clave. Otras formas podrían ser la traducción del mensaje a otro idioma, la utilización de taquigrafía personal. Hay que tener en cuenta que los ordenadores y las nuevas tecnologías han ayudado tanto a criptologistas como a criptoanalistas en la utilizacón de códigos.

Las tres fases que sigue un criptoanalista para descifrar un mensaje son la identificación, la “rotura” o desciframiento y el ajuste. Primero tiene que identificar el tipo de código, viendo otros posibles mensajes y buscando más información que no pertenece al mensaje en sí para intentar reconocerlo o empezar a seguir alguna pista para poder continuar. La segunda parte sería ya empezar a descifrar lo que se llamarían las “partes fijas”, partes concretas que se repiten y que se puede sacar un patrón. Finalmente se mira la estructura global integrando cada parte descifrada al conjunto y obteniendo así el mensaje completo.

Hay que tener en cuenta la diferencia entre código y cifrado, aunque a veces se confunda: mientras que los códigos son “estáticos” los cifrados son “dinámicos”, es decir, documentos encifrados utilizando un mismo código tienen los mismos parámetros, en cambio la mayoría de los sistemas de cifrados incluyen varios parámetros diferentes, aunque el mecanismo básico sea el mismo.

1.2 Evaluación del código: identificación y corrección de errores

Una vez obtenido un nuevo código (o sistema de cifras) es necesario evaluarlo mirando tres posibles situaciones: el criptoanalista tiene varios textos cifrados, tiene varios textos ya descifrados, y si tiene tanto textos cifrados como descifrados que él mismo ha elegido. Las dos primeras son las que tienen más probabilidad de ocurrir, la tercera es utilizada sobre todo como herramienta de evaluación (ya que es muy improbable que se de), ya que cuanto más difícil sea descifrar el mensaje por mucha información que el criptoanalista tenga mayor va a ser la eficacia del sistema.

Existen otro tipo de códigos llamados *códigos de detección y corrección de errores* utilizados, como su nombre indica, para identificar y corregir errores en los códigos generalmente utilizando procedimientos matemáticos. También hay códigos que sólo detectan el error, como el utilizado para detectarlos en el ISBN. El llamado “dígito de control” del ISBN se obtiene al multiplicar cada dígito por el número que ocupa en la secuencia y luego sumando los números obtenidos, cuyo resultado debe de ser 11 si el código es correcto.

Aparte de la utilización de códigos para ocultar mensajes existen métodos como el uso de tinta invisible, de micropuntos o pequeñas partes del mensaje en un lugar no sospechoso o la introducción del mensaje en otro.

1.3 Aritmética modular

En criptografía y criptoanálisis es frecuente la adición y sustracción de series de números, pero para ello utilizan la llamada *aritmética modular*, que consiste en la adición y sustracción de números a partir de un número llamado *módulo*. Las dos series de números se suman o restan (sumando el módulo al resultado si es negativo) y posteriormente se opera con el módulo: se resta discontinuamente, a un par sí y a otro no y así sucesivamente. Módulos comunes son el 2, el 10 y el 26. Cuando el módulo es dos se denomina *aritmética binaria*, ya que tan sólo aparecen el 0 y el 1.

Este sistema también es utilizado para la suma y resta de letras, sustituyendo cada una por el número correspondiente a su puesto en el abecedario y operándolas siguiendo el modelo anterior.

Un código de "dos partes", más difícil de descifrar, consistiría en sustituir palabras o letras por una serie de números (que vendría indicado en un libro de códigos que pertenecería al destinatario del mensaje) y luego añadirle una *clave*, de manera que si por ejemplo a la palabra *mañana* le correspondiese el número 0009 y la *clave* fuese 2356, el código sería 2365.

Por supuesto, para incrementar la seguridad las claves se cambian regularmente, normalmente utilizando secuencias de números para definirlas. En estas frecuencias los números se suman para dar la siguiente cifra, y se le aplica un módulo para reducirlo: Ponemos por ejemplo una sucesión muy común, que empieza por 3 y 7. El 3 y el 7 se suman, dando 10, pero al aplicar (mod 10) se queda en 0. La siguiente cifra será 7+0= 7, y así sucesivamente.

Una de las secuencias más famosas es la Sucesión de Fibonacci, aunque en sí no se le aplica un módulo, solo (y no siempre) en cuestiones de encriptación. Las cifras no tienen por qué sumarse de dos en dos, ni el módulo 10, lo que hace que surjan infinidad de posibles secuencias. Además, se buscan las sucesiones en las que haya más cifras antes de repetirse la primera, por eso el primer ejemplo es de las más conocidas: se repite a las 60 cifras.

Aun así este método tiene varias propiedades numéricas que lo hacen más sencillo de descifrar: números repetidos (77, 99, 33 , 11) que aparecen cada 15 cifras, o que dos tercios de los números de la secuencia son *"raros"* y el otro tercio es *"evidente"*, siguiendo así un patrón.

2. EL CÓDIGO DE JULIO CÉSAR:

En el código de Julio César, cada letra era desplazada un número determinado de lugares en el alfabeto. (Por ejemplo 3) La A se sustituía por la D, la B por la F... Hay, por tanto, 25 versiones distintas de este código. La manera de resolverlo es ir probando todas las combinaciones posibles

ONCE Y MEDIA
RQFH B PHGLD

2.1 Debilidades y mejoras del sistema de Julio César (Cifrado Vigènere):

En el código de Julio César bastaba con probar todas las combinaciones (25). Esto se puede complicar si en lugar de desplazar la letra un número determinado de posiciones en el alfabeto, la cambiamos dependiendo de su posición. Así, podemos cambiar por ejemplo, las impares 2 posiciones y las impares 11. Si tenemos los espacios sustituidos por la letra W, y usamos tres cambios (2, 11, 17) el texto quedaría:

ONCEWYWMEDIA
QYTGHPYXVFTS

Aunque la persona supiera que se ha utilizado un encriptado de Julio César con tres cambios, tendría que probar muchísimas combinaciones y si el mensaje es corto habría demasiadas posibilidades. Si el número de cambios es igual al de letras, el mensaje es indescifrable. Si el orden de los cambios es aleatorio, tenemos un código de sustitución simple.

Cuando la secuencia de cambios no es aleatoria, se utiliza una palabra clave. Si usamos por ejemplo la palabra VASO, tendríamos una secuencia de (21,0,18,14) Se escribiría la palabra clave encima del texto repetida:

VASOVASOVASO
JNUSRYOAYDAO

2.2 Códigos de sustitución simple:

El alfabeto es sustituido por otro mezclado. Cada letra se sustituye por la que hay en esa misma posición en el alfabeto encriptado.

Ejemplo:

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
Y	M	I	H	B	A	W	C	X	V	D	N	O	J	K	U	Q	P	R	T	F	E	L	G	Z	S

ONCE Y MEDIA
KJIB Z OBHXY

Se podría intentar resolver pero habría muchas soluciones posibles. Necesitaríamos 50 caracteres para una única solución y unos 250 para una única solución fácil de averiguar, pues se pueden eliminar los espacios para hacer más difícil el poder descifrarlo y se puede utilizar alguna letra poco común para sustituir el espacio. (W: que sustituida sería la L)

Ejemplo:

KJIBLZLOBHXY

Al no eliminar los espacios del todo, se facilita el descifrarlo al receptor y al analista. Observando el alfabeto de arriba, vemos que no todas las letras han sido sustituidas (T y Q) Un alfabeto aleatorio tiene un 63% de posibilidades de tener alguna letra repetida

2.2.1 Resolución de un mensaje encriptado con código de sustitución simple

NO hay que probar todas las posibilidades. Conviene seguir los siguientes pasos:

- Contar el número de veces que aparece cada letra.
- Tratar de encontrar la que representa los espacios (La más repetida y cada pocos caracteres)
- Rescribir el mensaje separando las palabras.
- Tratar de identificar las letras más comunes
  (INGLES - ETAION; ESPAÑOL - EAOSRNI)
- Averiguar las palabras más comunes o más cortas.
- Completar el resto del texto. Si sabemos de qué trata el texto, resultará más fácil averiguar las palabras. En un texto científico: protón, electrón...

Por lo tanto, es muy peligroso juzgar la seguridad de un código por el tiempo que tardaría un ordenador en descifrarlo, ya que muchas veces bastaría con una persona para resolverlo en unos días.

2.3 Mejoras del código de Julio César

2.3.1 El cilindro de Jefferson

En el siglo XVIII, Thomas Jefferson inventó un aparato con discos en un eje en el que daban vueltas independientemente. Cada uno tenía un alfabeto en un orden aleatorio distinto pero teniendo el emisor y el receptor el mismo orden. El emisor colocaba el mensaje en el disco y copiaba las letras de cualquier otra línea. Así, el receptor colocaba ese código en el suyo y solo tenía que leer las líneas para encontrar el mensaje.

2.3.2 Cifrados puzzle

Hasta ahora, las letras eran sustituidas en el mensaje pero existe otro tipo de encriptación en la que las letras se mantienen pero varía su orden en el mensaje. Se usan sistemas de transposición.

2.3.3 Transposición simple

Se escribe el mensaje en un cuadro dividido en filas y columnas. Tiene un número determinado de columnas y el de filas depende de la longitud del mensaje. Las columnas se numeran con un código determinado y el mensaje se transcribe con el orden que dan los códigos de las columnas.

Ejemplo:

ESTACIÓN A LAS DOS MENOS CINCO

3 1 5 2 4

E S T A C
I O N A L
A S D O S
M E N O S
C I N C O

SOSEI AAOOC EIAMC CLSSO TNDNN

El receptor, conociendo el código solo tiene que colocar el mensaje por filas en ese orden.

¿Cómo descifrarlo? Al tener un mensaje de 25 letras, damos por hecho que están colocadas en un cuadro de 5x5. Colocando el mensaje y viendo posibles combinaciones, no resulta difícil descifrar el código de orden de las columnas. Para hacerlos más difíciles de descifrar se crearon los de doble transposición.

3 MÁQUINA ENIGMA

Esta máquina, utilizada por la Alemania Nazi fue utilizada para cifrar los mensajes enviados a lo largo de toda la 2ª Guerra Mundial. Se enviaron desde partes meteorológicos o felicitaciones de cumpleaños hasta decisiones del Alto Mando. Existía también la versión comercial (utilizada por grandes empresas para asegurar la seguridad de sus comunicaciones y que se diferenciaba por no tener un panel de conexiones) y una versión que únicamente era utilizada por la marina que incluía un cuarto (y a veces un quinto) rotor.

Panel de conexiones

La máquina pesaba alrededor de 10 Kg., por lo que su manejo y transporte no eran sencillos. Era un dispositivo electromecánico, la corriente que atravesaba los rotores era la parte eléctrica, y los rotores en si, eran la parte mecánica.

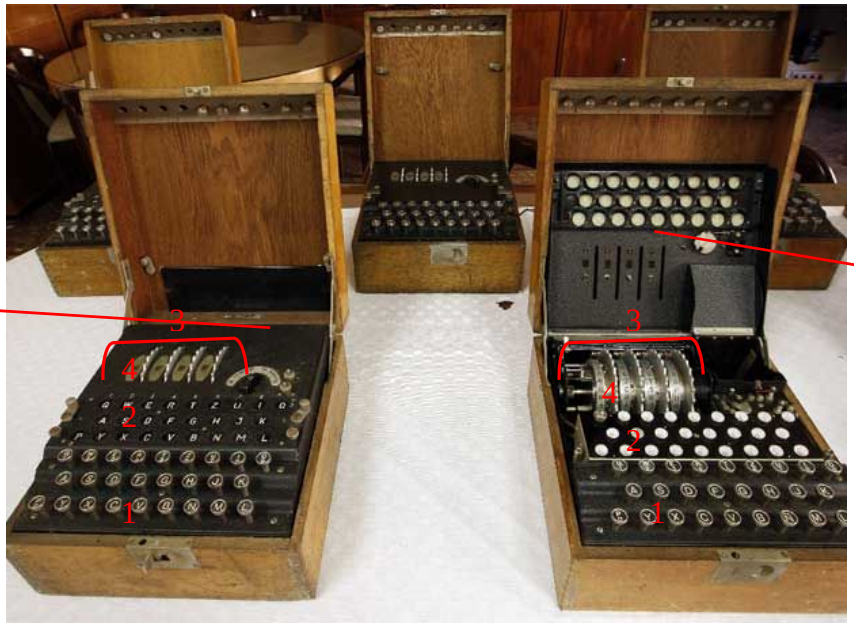
Su funcionamiento, una vez entendido no es difícil. Consta de:

- Un teclado casi igual a los actuales en el cual se pulsaba la letra a cifrar
- Un panel de bombillas que se encendían mostrando la letra cifrada
- Una serie de rotores cuyo funcionamiento explicaré posteriormente
- Un reflector para evitar que las letras no pudiesen cifrarse a si mismas
- Una pila encargada de hacer la corriente

Los rotores, que eran normalmente tres, funcionaban de manera que cada vez que el primero daba una vuelta al alfabeto, el segundo avanzaba una letra, y siguiendo ese razonamiento cada vez que el segundo daba una vuelta al alfabeto, el tercero avanzaba. Esto hacía que hubiese 17.576 alfabetos de sustitución, lo que significa que no se repetiría un alfabeto de sustitución a menos que el mensaje tuviera una longitud de más de 17.576 letras. El tercer y último rotor estaba conectado al reflector, que era otra de las muchas razones que la diferenciaba de las demás máquinas de cifrado de la época.

Los rotores tenían un cableado interior distinto. Este cableado lo que hacía era conectar los contactos de las dos ruedas de cada rotor, la exterior y la interior entre si. Las conexiones únicamente cumplían una norma, que era que los cables no podían conectar las mismas letras, es decir, que la A podía estar conectada con todas las letras del abecedario menos con la A.

Tapa cerrada



Tapa abierta

1 Teclado 2 Lámparas 3 Rotores 4 Reflector

4 PRODUCCIÓN DE SERIES DE NÚMEROS PSEUDO-ALEATORIAS

Una secuencia pseudo-aleatoria es aquella que cumple ciertos tests de aleatoriedad de un nivel determinado pero que se puede ver como una serie geométrica normal. Para criptografía estas secuencias son esenciales, pues parecen carentes de lógica pero con la clave adecuada es posible encontrar la fórmula que genera esa serie.

Una serie línea es aquella que que se genera cuando un término está generado por la suma de múltiplos de términos anteriores, de forma que es de orden 1 si utiliza sólo un término anterior al nuevo para crearlo; de orden 2 si utiliza dos términos; en general de orden *k* si utiliza *k* términos.

$$U_n = U_{n-1} + U_{n-2}$$

Ejemplo: serie de orden 2.

Empezamos con *k* términos al azar pues no se pueden generar, en este caso con 2 términos que pueden ser 1,1 y a partir de ahí se genera la siguiente serie:

1,1,2,3,5,8,13…

que es la sucesión de Fibonacci.

A su vez, se puede hacer sólo sumando las unidades

(1,1,2,3,5,8,3,1,4…)

y en cualquier base

(mod 2:1,1,0,1,1,0…)

que en base dos es lo mismo que poner un 1 si es impar y un dos si es par

(1,1,2,3,5,8…)

(1,1,0,1,1,0…)

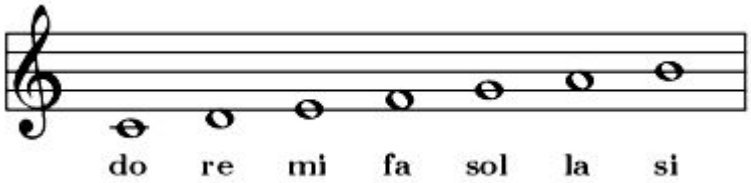
El periodo de repetición es como máximo la base elevada al orden de la serie -1 $\text{mod}(k-1)$;que en el caso de la la sucesión de Fibonacci en base 2 sumando sólo las unidades da un periodo de $2^k - 1$, que es 3 (1,1,0,1,1,0),y más aleatoria aparecerá cuanto mayor periodo de repetición tenga.

5. CIFRADO ARMÓNICO SIMPLE (CAS)

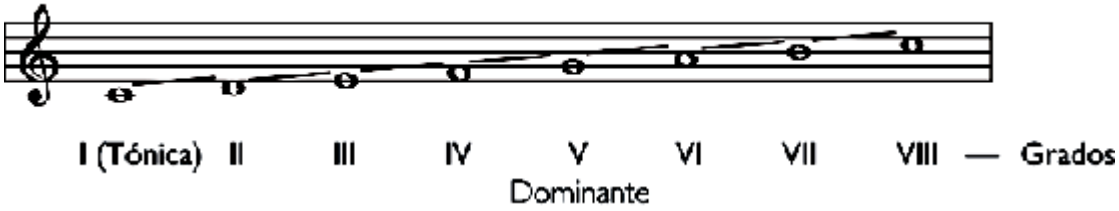
5.1 Introducción

5.5.1 Notas de la escala

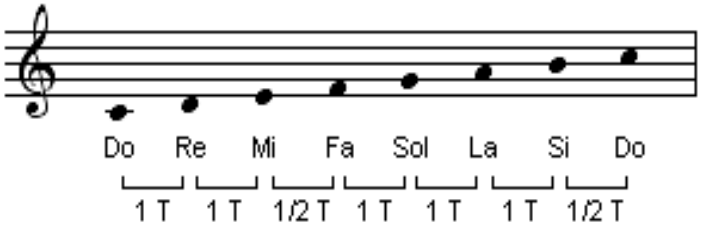
Como todos sabemos la escala musical esta formada por 7 notas, que en el caso más simple (tonalidad de Do M) es:



Algunas de estas notas tienen, dentro de cada escala un nombre especifico:



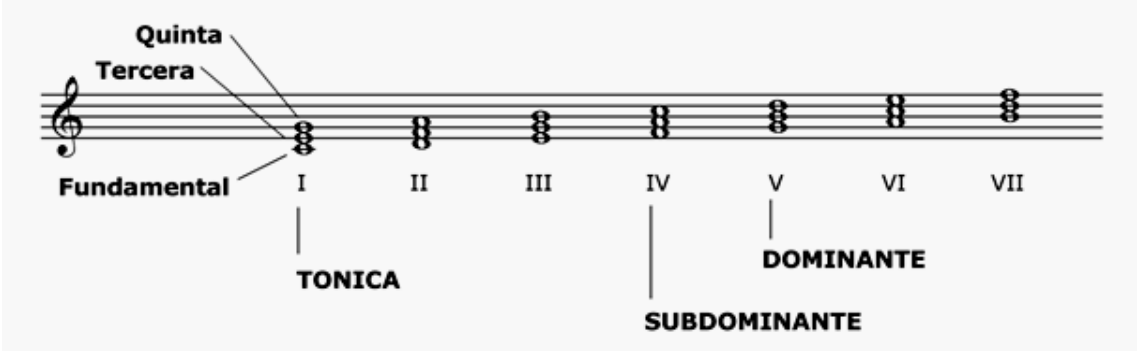
Para formar una escala mayor (M) la distancia entre las notas ha de ser la siguiente (T significa tono):



Aun así, en los ejemplos solo utilizaremos Do M para facilitar su comprensión.

5.5.2 Acordes

Los acordes se generan superponiendo una 3ª y una 5ª a cada nota de la escala. De nuevo en el caso de Do M:

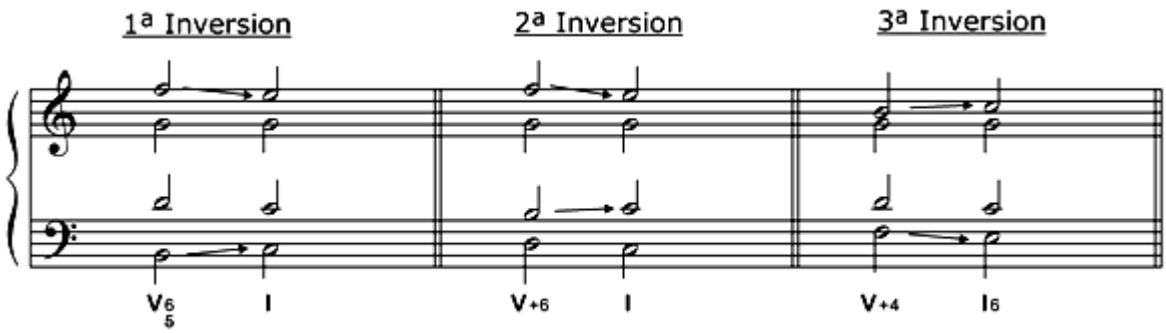


A la primera nota de cada acorde, la de la escala, se la llama **fundamental**. Como se aprecia en la imagen anterior, los acordes resultantes se numeran con un grado romano del I al VII. Los acordes de los grados I, IV y V se denominan Tónica, Subdominante y Dominante, respectivamente. En la música tonal clásica no se usa el III grado.

5.5.3 Inversión de los acordes

Una inversión de un acorde es colocar el orden normal de sus notas de forma distinta, es decir, cuando normalmente la fundamental es la nota más grave del acorde, una inversión hace que la más grave sea la Tercera o la Quinta. Estos nombres se dan según el intervalo que separe a esa nota de la fundamental.

Los acordes, al estar formados por tres notas solo tienen dos inversiones, más el estado Fundamental (cuando la fundamental está en el Bajo), pero en la música Clásica el acorde de Dominante se le puede añadir una cuarta nota, llamada Séptima, que hace que tenga 3 inversiones más el estado Fundamental.



Como se ve en el ejemplo, el acorde es de dominante en la tonalidad de Do Mayor, por lo que la nota más grave debería ser un Sol(fundamental), pero al estar en 1ª, 2ª y 3ª inversión la nota más grave es un Si (tercera), Re(quinta), y Fa(séptima), respectivamente.

5.2 Cifrado

5.2.1 Asociación de letras y números a las notas

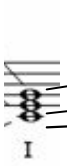
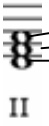
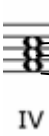
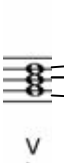
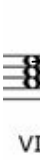
El cifrado armónico simple se basa en asociar a cada nota de un acorde un número de forma general, de manera que a todos los acordes se les asocia el número de la siguiente forma:

Fundamental=0, Tercera=1, Quinta=2

El I grado de Do M se le asociarían así

Do=0, Mi=1, Sol=2

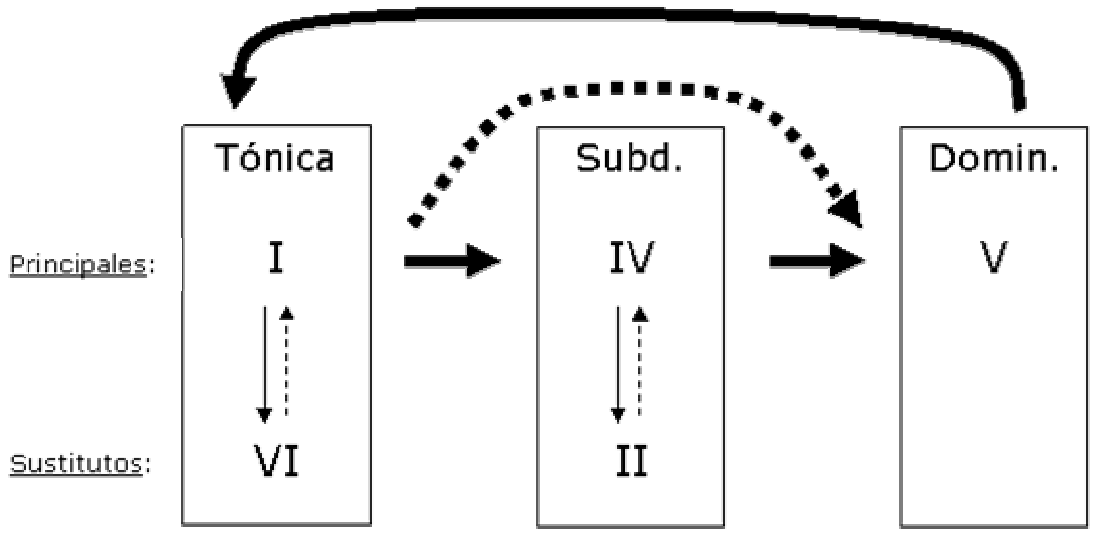
Y luego a cada nota de cada acorde específico se le asocia una letra del abecedario, de manera que cada acorde tiene tres letras diferentes entre sí y entre las otras letras de otros acordes:

 I	A2 B1 C0	 V 1ª Inversión	P2 Q1 R0
 II	D2 E1 F0	 V 2ª Inversión	S2 T1 U0
 IV	G2 H1 I0	 V 3ª Inversión	V2 Y1 Z0
 V	J2 K1 L0	W=VV X=CS N=Ñ	
 VI	M2 N1 O0		

Como se puede ver en la segunda columna, hacemos como que las inversiones del quinto grado son acordes distintos entre ellos y entre el acorde de quinto grado en estado Fundamental, para tener más letras que se puedan poner en el mensaje.

5.2.2 Desarrollo de los acordes

Entonces, tras saber qué mensaje se quiere enviar, se escriben en la partitura los acordes que correspondan con las letras a transmitir, pero teniendo en cuenta las leyes de la Armonía (es preciso que esta operación la realice un músico) y teniendo en cuenta también el orden en el que deben realizarse algunos de estos acordes para que suene clásico, que es el siguiente:



Cuando se necesita escribir un acorde y no es posible hacerlo si se quiere seguir este orden, se pueden escribir acordes de más que no deben ser contados como parte del mensaje. Para señalizar cuáles no deben ser contados, se puede usar:

- *Las ligaduras*, es decir, los acordes que queden dentro de la ligadura a excepción del 1º y el último no han de ser contados.

- *Los elementos expresivos*, como puntos o rayas sobre el acorde indicarán que ese acorde no ha de ser contado.

Ha de tenerse en cuenta que, excepto en el acorde del quinto grado, da igual en qué inversión se escriban los acordes.

5.3 Desarrollo de las cifras

Tras escribir los acordes en la partitura, se ve qué números corresponden a cada letra, de forma que el mensaje entero forma un gran número de ceros, unos y doses. Este número indica qué nota de cada acorde se debe descifrar.

Por ejemplo, si se quiere decir HOLA, QUÉ TAL se debe anotar el número 1002101120, según la tabla del punto ***5.2.1***, y estos números significan que del acorde 1º en la partitura, se debe descifrar la Tercera, del 2º se debe descifrar la Fundamental, del 3º se debe descifrar la Fundamental, etc. de forma que el orden de la cifra empezando por la izquierda del número significa el acorde de la partitura que se debe descifrar, y el valor de esa cifra simboliza la nota del acorde que se debe descifrar.

El problema reside en que ese gran número es imposible indicarlo en una partitura, pues el único número que aparece normalmente en las mismas es el de ***Negra=X***, que en la música normal indica el número de *Negras* que suenan durante un minuto.

Pero para que este número sea realista, es necesario que sea un número natural dentro del intervalo (30, 210), por lo que es necesario convertir el gran número en un número dentro de ese intervalo, proceso que se hace de la siguiente manera:

El gran número, que está en base 3, se pasa a base 10, pero todos los nueves que aparezcan se transforman en ceros, y se presupone que el número nuevo (con todos los nueves ya transformados en ceros) está en la base más alta posible, y ese número se pasa a base 10, al cual también se la transforman los nueves en ceros, etc. y así sucesivamente hasta que el número esté dentro del intervalo ideal para el número ***Negra=X*.**

Para el receptor, el número de las bases que se presuponen se da a entender con signos de Dinámica, (que en partituras normales indican la intensidad, y se colocan debajo de los acordes) para lo que utilizaremos este cuadro:

FF (fortísimo): Base 9
F (forte): Base 8
mF (mezzoforte): Base 7
mP (mezzopiano): Base 6
P (piano): Base 5
PP (pianísimo): Base 4

La forma de indicar las Bases que se presuponen es la siguiente: la primera Base que se presupone se indica colocando su signo correspondiente al principio de la partitura, da igual con qué acorde se sitúe. La siguiente base que se presupone se indica colocando su signo correspondiente después del primero, y así sucesivamente.

Para indicar al receptor qué ceros se transformarán en nueves y cuáles no, se usará el siguiente método, (para el cual es necesario ver este cuadro)

sfz (sfortzando): el 0 es realmente un 0.
FP (forte piano): el 0 es un 9

Dentro del intervalo de acordes que estén bajo la dinámica del signo que corresponda a la presupuesta base del número con el que hay problemas con los ceros, se escriben los anteriores signos de dinámica (***sfz, FP*****)** de forma que si sólo hay un cero, se escribe un solo signo, si hay un dos ceros, se escriben dos de esos signos, en el orden en el que aparecen(si va primero el real 0, se escribe primero un ***sfz***, y luego un ***FP***, y viceversa) y así constantemente.

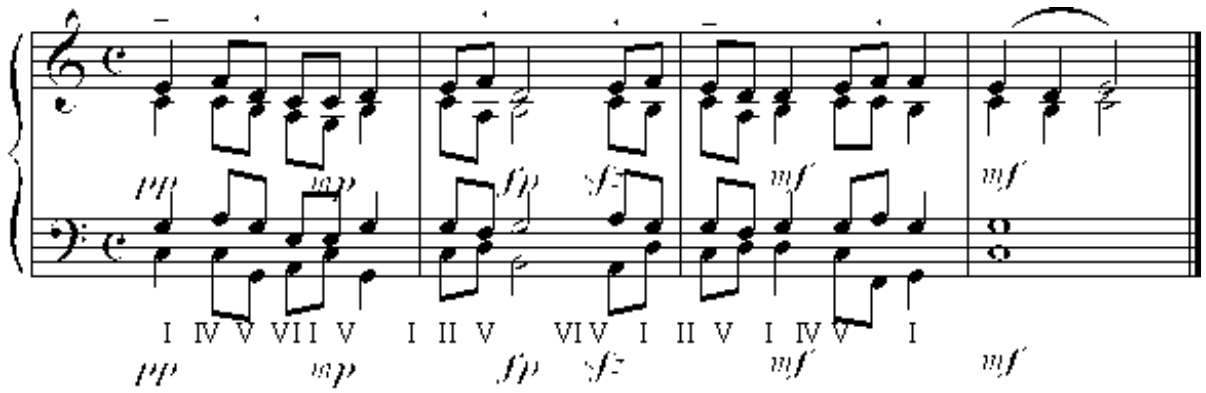
Hay que tener en cuenta que lo importante es el orden entre los signos de Dinámica, y no la relación entre estos y los acordes a los que acompañan, este es un aspecto puramente musical.

A continuación exponemos un ejemplo.

Vamos a utilizar el número que significa *HOLA QUÉ TAL*, que recordamos que era 1002101120: este se pasa a base 10, que es 21426, que a su vez se presupone que está en la base más alta posible, que es Base 7, y se pasa a base 10, que es 5361, que a su vez se presupone que está en base 7 y se pasa a base 10, que es 1905, y aquí el nueve se transforma en cero, por lo que tenemos 1005, que se presupone que está en base 6 y se pasa a base 10, que es 221, que se presupone que está en base 4 y se pasa a base 10, que es 41, que está dentro del intervalo ideal para el número ***Negra=X*****.**

El orden empezando por el principio de los signos de dinámica es: ***mF, mF, mP***, ***FP***, ***PP***.

De esta manera, el receptor coge el número 41, que está escrito arriba de la partitura, y lo pasa a Base 4(por el **PP**) dando 221, que a su vez presupone que está en Base 10 y lo pasa a Base 6(por el **mP**) dando 1005 al que se le transforma el primer 0 en un 9(por el **FP**) y el segundo 0 en un 0(por el **sfz**)dando 1905 que a su vez presupone que está en Base 10 y lo pasa a Base 7(por el **mF**) dando 5361, que se presupone que está en Base 10 y se pasa a Base 7 otra vez(por el repetido **mF**) dando 21426, que se presupone que está en Base 10 y se pasa por último a Base 3,(por no haber más signos de Dinámica en la partitura) dando el número 1002101120, que es el código para descifrar los acordes.



6. CIFRADO ARMÓNICO MÚLTIPLE (CAM)

CAC tiene sus bases en CAS, por eso, todo lo dicho anteriormente, es igualmente valido para CAC.

6.1 Introducción

La única y principal diferencia entre CAS y CAM es que en CAS, solo utilizamos una tonalidad. En CAM utilizaremos un gran número de tonalidades, a saber, todas las mayores. Esto nos permitirá darle mayor riqueza a la pieza escrita, y por lo tanto mayor naturalidad, y nos abrirá un abanico de nuevas posibilidades que explicaremos posteriormente.

6.2 Dominantes secundarias

Para pasar de una tonalidad a otra de forma natural y fácil se usa en armonía las dominantes secundarias, es decir, crear un acorde inestable que el acorde siguiente a ese sólo pueda ser el I grado de la tonalidad a la que queremos llegar, y no hay nada más inestable y que resuelva en un I grado que la dominante(el V grado). Por eso se le llama Dominante, y lo de secundaria es por que la Dominante principal es el V grado de la tonalidad en la que estamos y las Dominantes Secundarias son los V grados de otras tonalidades.

Se ve claramente a continuación..

6.2.1 Construcción de una dominante secundaria

- Las dominantes secundarias normalmente llevan 7ª. Nosotros las construiremos, de momento, como acordes de 7ª de dominante.

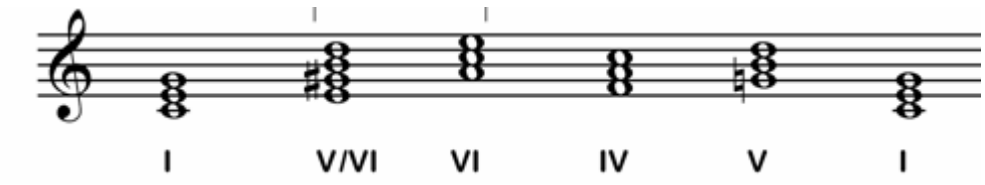
- Para construirla, tenemos que pensar en la dominante de la tonalidad (mayor) del grado al que preceden.

- Veamos esto con un ejemplo. Queremos conocer cuál es el V del VI en Do M:

1º - El VI grado en esta tonalidad es un acorde de La menor.

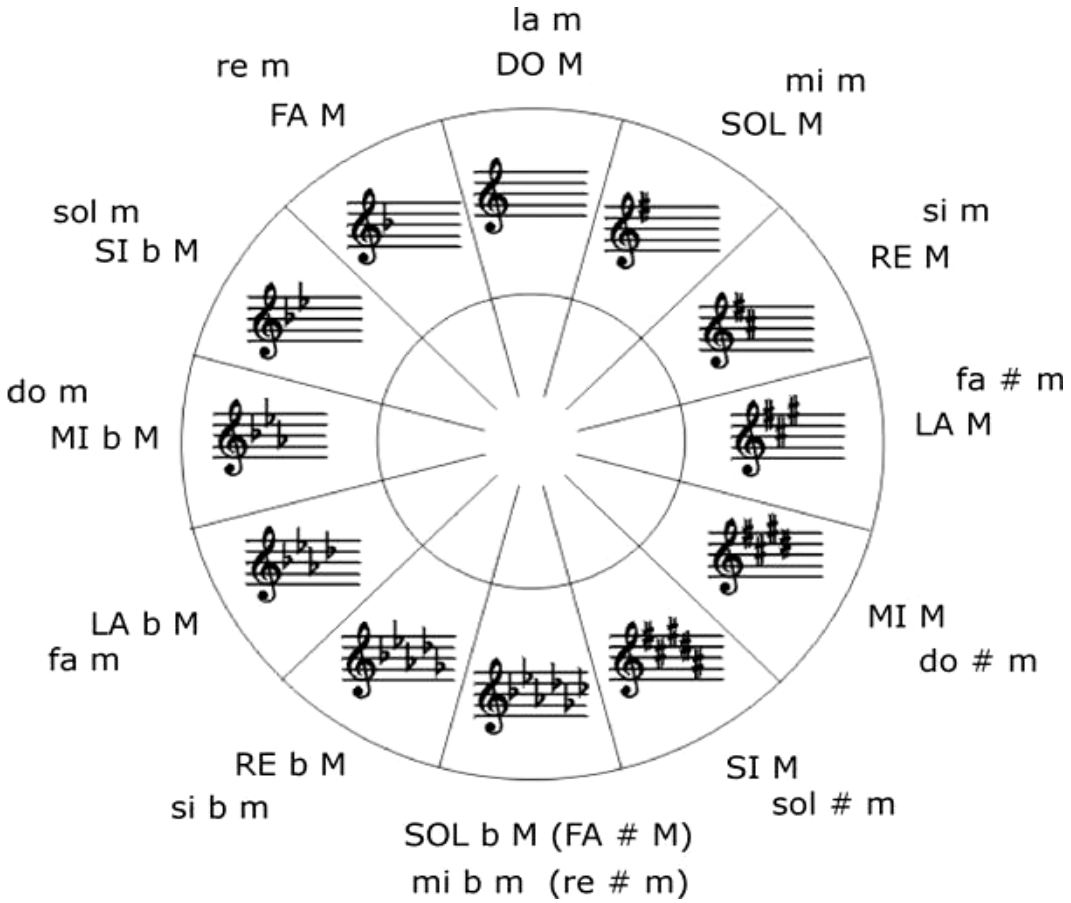
2º - Tenemos que pensar cuál es la dominante con 7ª de La (Mayor)

3º - La respuesta es un acorde formado por las notas Mi-Sol#-Si-Re



6.3 Círculo de quintas

El círculo de quintas es una manera fácil y visual de ver todas las tonalidades.



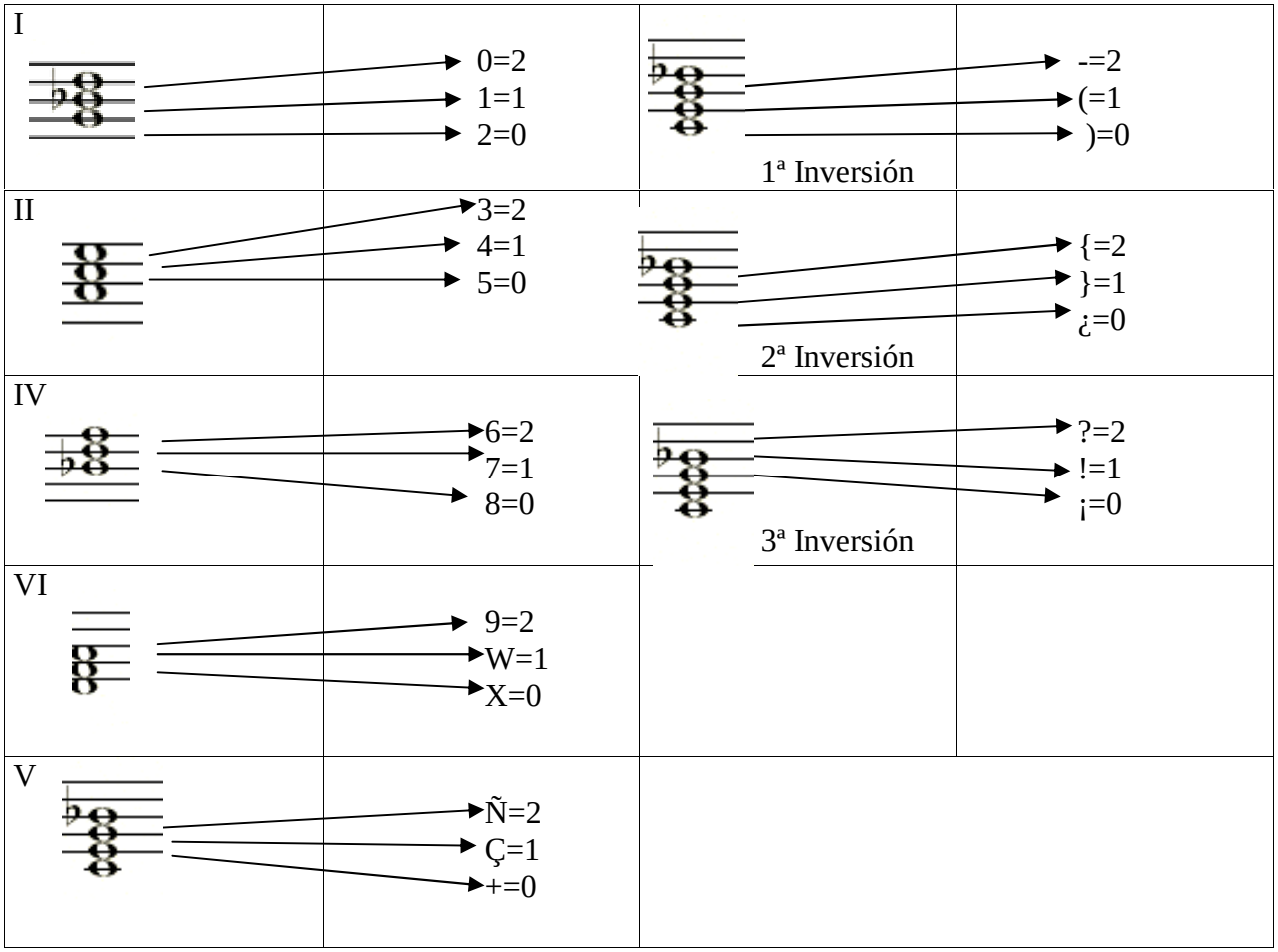
Aunque para CAC, obviaremos las tonalidades menores.

6.4 Aplicación a la criptografía

Debido a la introducción de las dominantes secundarias ampliamos la gama de letras que puede haber por nota. Es decir, ahora un Sol, no solo puede ser la 5ª de I de Do M, sino la fundamental de I de Sol M, o la tercera de V de La b M.

Para ello simplemente rotaremos la tabla creada anteriormente. Es decir, cada vez que demos un paso hacia la derecha de Do M, la A, y con ella todas las demás letras se moverán un puesto hacia abajo. Al dar un paso hacia la izquierda de la tabla la A, y todas las demás, se moverán un puesto hacia arriba.

Debido a que en CAS no se pueden introducir números, utilizaremos una tonalidad que utilizaremos para introducir números en nuestros mensajes. Esta tonalidad será Fa M. Esta tonalidad ha de ser saltada cuando contemos pasos para mover la tabla.



CONCLUSIÓN

Hemos elaboramos una partitura que encripta mensajes siguiendo los siguientes pasos: 1) Asociación de un número a cada nota del acorde. 2) Asociación de una letra a cada nota del acorde. 3) Transcripción a la partitura, escribiendo los acordes de las letras del mensaje. 4) El número que corresponde a cada letra (pasado a una cifra entre 30 y 210) se escribe en el lugar que en una partitura indica el número de negras por minuto. La única diferencia entre CAS y CAM, es que CAM utiliza saltos de tonalidades.

BIBLIOGRAFÍA

Aunque la segunda parte del trabajo es totalmente original, incluimos una brevísima bibliografía que hemos usado para la primera parte.

Churchhouse, R. (2002) *Codes and ciphers. Julius Caesar, the Enigma and the internet.* University Press. Cambridge.

Kennedy, G. (2004) *El manuscrito Voynich. Un enigma sin resolver*. Melusina. Barcelona.