Computación y Sistemas Vol. 7 Núm. 4 pp. 272-284


# Secuencias Cifrantes de Números Metálicos a partir de Fracciones Contínuas

***Sequences Cifrantes of Metallic Numbers to leave of Continuous Fractions***

**F.J. Romero [1] y R. Vázquez [2]**
[1] CECyT "Cuauhtémoc"
Instituto Politécnico Nacional
roifxav@hotmail.com
[2] Depto. de Ingeniería Eléctrica
Universidad Autónoma Metropolitana

*Artículo recibido en Diciembre 12, 2003; aceptado en Febrero 12, 2004*

**Resumen**

En este artículo se presenta el análisis de secuencias binarias generadas a partir de la representación en fracciones continuas de algunos números irracionales algebraicos (Razón dorada, Número de plata, Número de bronce). Este análisis se hace usando la función de auto-correlación y de la transformada de fourier. Posibles aplicaciones de estas secuencias serían en cifrados de flujo, sistemas de espectro disperso ó bien, en cajas de difusión o permutación.

$\phi$. Razón dorada
$\sigma$. Número de plata
$\delta$. Número de bronce
*FCIS*. Fracción continua infinita simple.
*FCS*. Fracción continua Simple

**Abstract**

In this article the analysis of binary sequences is presented generated starting from the representation in continuous fractions of some algebraic irrational numbers (golden Reason, silver Number, brass Number). This analysis is made using the auto-correlation function and of the one transformed of fourier. Possible applications of these sequences would be in stream cipher, systems of dispersed spectrum or well, in diffusion boxes or exchange.

$\phi$. Golden Reason
$\sigma$. Silver Number
$\delta$. Brass Number
*FCIS*. Infinita Simple Continuos Fraction.
*FCS* Simple Continuos Fraction

## 1. Introducción

Los algoritmos empleados en seguridad informática comúnmente utilizan secuencias binarias que involucran números aleatorios. Por ejemplo, los esquemas de autenticación recíproca de generación de claves de sesión o los de generación de claves para algoritmos de cifrado. Sin embargo, en este artículo se emplean secuencias binarias obtenidas a partir de la representación en fracciones continuas de algunos números irracionales metálicos. Estos números tienen un número infinito de cifras decimales, lo que llega a constituir una secuencia no periódica de números decimales. Un número irracional es un número real no racional, y algunos de ellos son algebraicos, por ser raíz de una ecuación polinomial de coeficientes enteros. Los que no cumplen con esta propiedad se llaman trascendentales (Gray R. 1994) (Romero I, 2002).

Así en este articulo, las secuencias binarias están generadas a partir de algunos números irracionales algebraicos, que se evalúan para su potencial uso en sistemas de protección de información. Algunas aplicaciones de estas secuencias serían en cifrados de flujo, sistemas de espectro disperso ó bien, en cajas de difusión o permutación. Para lograr esto se necesita un estudio probabilistico de las secuencias generadas, que demuestre que estas secuencias irracionales cumplen con los

criterios de aleatoriedad descritos por los tres postulados de Golomb (Golomb S. W., 1967), y la prueba universal de Maurer (Ueli M. Maurer, 1992 ), investigaciones publicadas en artículos que muestran los resultados obtenidos (Romero I, 2002). Cualquier número irracional puede escribirse como una FCIS. Consecuentemente, si α es una FCIS entonces α es un irracional.

Las fracciones continuas tienen algunas conexiones interesantes con el problema del Jigsaw como se describe en la literatura (Kimberling C., 1983), que a partir de una figura geométrica (rectángulo) se genera un conjunto de rectángulos girantes que producen un espiral logarítmico. Esta espiral converge una y otra vez, y en las longitudes de sus líneas que generan los rectángulos se encuentra la razón dorada siendo está el principal número metálico aquí descrito. De igual forma, tiene conexión con uno de los más viejos algoritmos de los matemáticos griegos de 300 a. C. Algoritmo de Euclid para calcular el máximo común divisor de dos números como se describe en el trabajo mencionado (Harold Davenport, 1999). En general, una fracción continua simple puede expresarse de la forma siguiente:

$$\alpha = a_o + \cfrac{1}{a_1 + \cfrac{1}{a_2 + \cfrac{1}{a_3 + \cfrac{1}{a_4 + \ldots}}}} \qquad (1)$$

Donde los números $a_0$, $a_1$, $a_2$, $a_3$, $a_4$,..., son enteros.

Usualmente este tipo de fracciones continuas pueden escribirse en lista como:

$$\alpha = [a_0, a_1, a_2, a_4, \ldots] = \frac{P_n}{q_n} \qquad (2)$$

El primer coeficiente puede ser nulo, caso en que el número real está comprendido entre 0 y 1, pero el resto de los coeficientes son enteros positivos.

La sucesión de coeficientes es finita si y solo si α es un número racional (es decir, un número de la forma *p/q*, con *q* diferente de cero, y con *p* y *q* números naturales sin factor común).

Si $\propto$ es un número irracional, el desarrollo es infinito y si tomamos un número finito de términos como en (2), obtenemos una sucesión de "aproximaciones racionales" al número $\propto$ que tiende a $\propto$ cuando $k \to \infty$

El matemático francés Joseph Louis Lagrange (1736-1813) probó que un número es irracional algebraico si y solo si su descomposición en fracciones continuas es periódica, (Long C. and Jordan, 1967).

## 2. Fracciones Continuas de los Números Irracionales

A continuación se describe el método que permite obtener la representación en fracciones continuas de los números irracionales algebraicos, *($\phi$, $\sigma$, $\delta$, $\sqrt{2}$ )* tomando en cuenta que tres de estos números irracionales pertenecen a la familia de los números metálicos encontrados a partir de la siguiente ecuación:

$$x^2 - nx - 1 = 0 \qquad (3)$$

### 2.1 Secuencia dorada ($\phi$)

EL número de oro ha sido ampliamente utilizado en una gran cantidad de culturas antiguas como base de proporciones, en el diseño de sus construcciones, es el primer miembro de la familia de números metálicos y es simplemente la relación que existe entre dos números de *Fibonacci* consecutivos. *Lan Stewart*, et al, han llamado a $\phi$ "el número más racional de los

irracionales" debido a esto, una forma para encontrar $\phi$ como fracción continua es primero considerar las soluciones a la ecuación (3), donde n = 1, así entonces se tiene

$$x^2 - x - 1 = 0 \qquad (4)$$

Reestructurando esta ecuación se tiene que,

$$x^2 = x + 1 \qquad (5)$$

Y dividiendo ambos lados por *x* (cuando *x* no tiende a cero) se tiene *x = 1 + 1/x* que contiene una fracción continua directamente para la raíz (positiva), Este es el valor de *x* que al que se llama $\phi$, siendo entonces,

$$\phi = 1 + \frac{1}{\phi} \qquad (6)$$

Al resolver también la ecuación (4) por la formula general se obtiene las raíces siguientes

$$\phi_1 = \frac{1+\sqrt{5}}{2} \sim 1.618... \qquad (7)$$

$$\phi_2 = \frac{1-\sqrt{5}}{2} \sim 0.618... \qquad (8)$$

Comprobando que la raíz positiva es el número de oro. Aplicando, así mismo la ecuación (6), se tiene que,

$$\phi = 1 + \frac{1}{1+\frac{1}{\phi}} \qquad (9)$$

De esta forma, si esta aplicación se hace iterativamente, se obtiene su representación en fracciones continuas.

$$\phi = 1 + \cfrac{1}{1+\cfrac{1}{1+\cfrac{1}{1+\cfrac{1}{1+.....}}}} \qquad (10)$$

En forma de lista se tiene la siguiente FCIS

$$\phi=[1,1,1,1,1,1...] = \frac{P_n}{q_n} \qquad (11)$$

$\phi$ Se puede también encontrar en muchas dimensiones de una variable geométrica, pero en lugar de representarlo como número irracional, se puede expresar de la manera siguiente. Dado un segmento de línea, se puede dividir en dos segmentos A y B de longitud cualquiera, de una manera tal que la longitud del segmento entero esté a la longitud del segmento A, mientras que la longitud del segmento A está a la longitud del segmento B. Si se calcula esta relación de transformación, se obtiene una aproximación de la razón de oro.

**2.2 Número de Plata (σ).**

Este número ha sido parte de numerosas investigaciones físicas, al tratar de sistematizar el comportamiento de sistemas dinámicos no lineales, analizando la transición de la periodicidad a la cuasi-periodicidad, también se recurre, en particular, a esté número para describir y explicar el sistema romano de proporciones como se describe en la literatura (Kappraff J. 1996).

Una forma para encontrar σ como fracción continua es primero considerar las soluciones a la ecuación (3), donde n =2, así entonces se tiene

$$x^2 - 2x - 1 = 0 \tag{12}$$

Reestructurando esta ecuación se tiene que,

$$x^2 = 2x + 1 \tag{13}$$

y dividiendo ambos lados por *x* (cuando *x* no tiende a cero) se tiene *x = 2 + 1/x* que contiene una fracción continua directamente para la raíz (positiva). Este es el valor de *x* que al que se llama Número de Plata, siendo entonces,

$$\sigma = 2 + \frac{1}{\sigma} \tag{14}$$

Al resolver también la ecuación (11) por la formula general se obtiene las raíces siguientes

$$\sigma = 1 + \sqrt{2} \quad \sim \quad 2.414213... \tag{15}$$

$$\sigma = 1 - \sqrt{2} \quad \sim \quad -0.414213... \tag{16}$$

Comprobando que la raíz positiva es el número de plata. Aplicando, así mismo la ecuación (13), se tiene que,

$$\sigma = 2 + \frac{1}{2 + \frac{1}{\sigma}} \tag{17}$$

De esta forma, si esta aplicación se hace iterativamente, se obtiene su representación en fracciones continuas.

$$\sigma = 2 + \cfrac{1}{2 + \cfrac{1}{2 + \cfrac{1}{2 + \cfrac{1}{\ddots}}}} \tag{18}$$

y en forma de lista se tiene lo siguiente FCIS

$$\sigma=[2,2,2,2,2,.....] = \frac{P_n}{q_n} \tag{19}$$

**2.3 Número de Bronce (δ).**

Al igual que los números metálicos anteriores sus principales aplicaciones se han dado en el diseño de construcciones y esto convierte a los números metálicos en instrumentos invalorables para la búsqueda de relaciones viables cuantitativas entre la Matemática y el Arte.

Por lo cual análogamente, resolviendo la ecuación (3), para una n = 3, se tiene el número de bronce que se denota como sigue a continuación:

$$\delta = 3 + \frac{1}{\delta} \tag{20}$$

Y

$$\delta = \frac{3+\sqrt{13}}{2} \tag{21}$$

De esta forma, si esta aplicación de la ecuación (18) se hace iterativamente, se obtiene su representación en fracciones continuas.

$$\delta = 3 + \cfrac{1}{3 + \cfrac{1}{3 + \cfrac{1}{3 + \cfrac{1}{3 + .....}}}} \tag{22}$$

Y en forma de lista se tiene la siguiente FCIS

$$\delta=[3,3,3,3,3,.....] = \frac{P_n}{q_n} \tag{23}$$

**2.4 Raíz cuadrada.**

La representación en fracciones continuas del número irracional $\sqrt{2}$ , se puede obtener como sigue:

$$\sqrt{2} = 1 + \frac{1}{x} \tag{24}$$

Usamos *1/x*, siendo *x >1*. Aquí se requiere encontrar *x*. Así que se reestructura esta ecuación para encontrar el valor de *x*, por lo que,

$$\sqrt{2} - 1 = \frac{1}{x} \tag{25}$$

$$x = \frac{1}{\sqrt{2}-1} \tag{26}$$

Ahora bien, multiplicando el término de la derecha por $\sqrt{2}+1$ tanto en el numerador como en el denominador, se tiene que:

$$x = \frac{\sqrt{2}+1}{2-1} = \sqrt{2}+1 \tag{27}$$

Sustituyendo la ecuación (3) en (6), se tiene

$$x = \sqrt{2}+1 = 1 + \frac{1}{x} + 1 = 2 + \frac{1}{x} \tag{28}$$

Ahora bien sustituyendo 2 + 1/*x* en aquellos lugares donde aparece *x*, se tiene la fracción continua para *x*.

Ahora se puede expresar $\sqrt{2}$ como una fracción continua como se muestra enseguida:

$$\sqrt{2} = 1 + \cfrac{1}{2 + \cfrac{1}{2 + \cfrac{1}{2 + \cfrac{1}{...}}}} \tag{29}$$

Por lo que se refiere a la fracción continua de $\sqrt{2}$ tenemos:

$$\sqrt{2} = [1;2,2,2,2,2,.....] \qquad (30)$$

## 3. Generación de Secuencias Binarias

A partir de la fracción continua obtenida en forma simple o en forma de lista, se empieza a generar el número irracional con 233 dígitos a partir de la siguiente ecuación.

$$a_0 + 1/(a_1 + 1/(a_2 + 1/(a_3 + 1/(a_n + 1)))) \qquad (31)$$

Existen otros métodos que se usan para calcular las fracciones continuas de un número irracional como se describe en la literatura (Lorentzen Lisa, and Waadeland Haakon, 1992).

Partiendo del método antes descrito de fracciones continuas se obtienen secuencias de los números irracionales (ϕ, σ, δ, $\sqrt{2}$ )

Para el análisis que se describe en este artículo se generó una FCS de 100 coeficientes, por ejemplo para la razón dorada ( $\phi$ ), como se muestra a continuación,

$$\phi = \{0,1, 1, 1, 1,1,1,1,.....,1,1, 1, 1\} \qquad (32)$$

$$\phi = \frac{2189229958345551690 26}{3542248481792619150 75}$$

A continuación se genera un vector decimal de la razón dorada con 233 dígitos, sin considerar la parte entera.

$\phi$ = [6, 1, 8, 0, 3, 3, 9, 8, 8, 7, 4, 9, 8, 9, 4, 8, 4, 8, 2, 0, 4, 5, 8, 6, 8, 3, 4, 3, 6, 5, 6, 3, 8, 1, 1, 7, 7, 2, 0, 3, 1, 2, 7, 4, 3, 9, 6, 3, 7, 9, 5, 6, 8, 5, 7, 5, 3, 5, 9, 1, 8, 5, 1, 0, 8, 8, 2, 9, 0, 1, 9, 8, 6, 9, 8, 8, 7, 5, 2, 2, 9, 8, 7, 6, 2, 7, 1, 5, 6, 2, 5, 2, 9, 9, 6, 3, 1, 8, 4, 2, 8, 8, 2, 9, 1, 9, 0, 2, 9, 8, 7, 0, 9, 8, 3, 0, 3, 6, 4, 5, 5, 8, 9, 1, 0, 0, 7, 1, 4, 9, 4, 4, 3, 2, 1, 8, 3, 1, 6, 8, 5, 9, 2, 7, 3, 4, 1, 9, 8, 8, 2, 9, 7, 9, 2, 0, 7, 2, 5, 9, 7, 1, 3, 6, 5, 2, 0, 1, 9, 7, 4, 3, 0, 8, 6, 5, 7, 9, 9, 0, 7, 8, 9, 1, 1, 3, 1, 8, 8, 9, 7, 0, 7, 0, 1, 0, 5, 9, 5, 8, 2, 8, 4, 3, 7, 1, 9, 6, 3, 0, 4, 4, 1, 4, 9, 3, 4, 9, 0, 6, 2, 7, 9, 8, 2, 7, 3, 5, 7, 7, 6, 0, 1]

Posteriormente se convirtió este número decimal a su representación binara, para tener una secuencia binaria de "0" y "1". Tomando esta secuencia binaria se convierte a un vector de "0"s y "1"s. Por ejemplo, el número irracional ϕ.

$\phi$ =[1, 0, 0, 1, 1, 1, 1, 0, 0, 0, 1, 1, 0, 1, 1, 1, 0, 1, 1, 1, 1, 0, 0, 1, 1, 0, 1, 1, 1, 0, 0, 1, 0, 1, 1, 1, 1, 1, 1, 1, 1, 0, 1, 0, 0, 1, 0, 1, 0, 0, 1, 1, 1, 1, 1, 0, 0, 0, 0, 0, 1, 0, 1, 0, 1, 1, 1, 1, 1, 1, 0, 0, 1, 1, 1, 0, 0, 1, 1, 1, 0, 0, 1, 1, 1, 0, 0, 1, 1, 0, 0, 0, 0, 0, 0, 1, 1, 0, 0, 0, 0, 0, 0, 1, 0, 1, 1, 1, 0, 1, 1, 1, 0, 1, 1, 1, 1, 0, 1, 1, 1, 0, 0, 1, 0, 0, 0, 0, 0, 1, 1, 0, 1, 0, 0, 0, 0, 0, 1, 0, 1, 1, 0, 0, 1, 1, 1, 0, 1, 0, 0, 1, 1, 0, 0, 1, 0, 0, 1, 0, 1, 0, 1, 0, 0, 1, 0, 1, 0, 1, 0, 1, 0, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 1, 1, 1, 0, 0, 0, 0, 0, 0, 0, 1, 1, 1, 1, 1, 0, 1, 0, 0, 1, 0, 0, 1, 0, 1, 1, 1, 0, 0, 0, 0, 0, 0, 1, 1, 1, 0, 1, 1, 0, 0, 1, 0, 1, 0, 1, 0, 0, 0, 0, 0, 1, 1, 1, 1, 1, 0, 1, 1, 1, 1, 1, 0, 0, 1, 0, 0, 0, 0, 0, 1, 0, 0, 1, 1, 1, 1, 1, 0, 0, 1, 1, 1, 1, 0, 0, 0, 1, 0, 1, 0, 0, 1, 1, 0, 0, 1, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 0, 0, 1, 1, 1, 0, 1, 0, 0, 0, 1, 1, 1, 0, 0, 1, 0, 1, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 1, 1, 0, 0, 0, 0, 1, 0, 1, 1, 0, 1, 0, 0, 0, 0, 0, 1, 1, 0, 1, 0, 1, 1, 1, 0, 1, 1, 0, 0, 0, 1, 0, 1, 1, 1, 0, 1, 0, 0, 1, 0, 0, 0, 1, 0, 1, 0, 0, 0, 1, 1, 1, 1, 0, 0, 0, 0, 0, 1, 1, 1, 1, 0, 0, 0, 0, 0, 1, 1, 1, 1, 0, 0, 1, 1, 1]

Generando un vector de 774 caracteres, el cual se analizó y se encuentra reportado en el apartado siguiente.

## 4. Herramientas de Análisis

### 4.1 Función de auto-correlación.

Un buen criterio para seleccionar una serie de sucesiones para aplicarla a un cifrado de flujo se basa en la minimización del valor absoluto de la correlación periódica entre señales, concepto que se encuentra disponible en la literatura (Simon M. K., 1985).

$$P_{max} = \max \{ P_A , P_c \} \tag{23}$$

Donde $P_A$ y $P_c$ son la máxima salida de fase periódica de la auto-correlación y la correlación respectivamente, y $P_{max}$ es el límite mas bajo que puede expresarse para una sucesión ideal comprendido de ***u*** sucesiones distintas de longitud L por la desigualdad siguiente:

$$P_{\max} \rangle L\left[\frac{u-1}{Lu-1}\right]^{\frac{1}{2}} \tag{24}$$

Por otra parte se tiene que la secuencia de auto-correlación de una señal *x(n)*, como se describe en la literatura (Alan V., 1994), esta definida como:

$$r_{xx}(L) = \sum_{n=-\infty}^{\infty} x(n)x(n-1) \tag{25}$$

Cuando se trata de señales causales de longitud finita N, la secuencia de auto-correlación se define como:

$$r_{xx}(L) = \sum_{n=i}^{N-|k|-1} x(n)x(n-1) \tag{26}$$

Donde *i=L, k=0* para *L=>0* y *i=0, k=L* para L*<0*

En las aplicaciones prácticas presentadas, la correlación se puede usar para identificar la periodicidad de una secuencia, a partir de muestras de la señal, la cual se puede generar inmersa en ruido. Cuando una secuencia es periódica su auto-correlación exhibe la misma periodicidad y contiene picos relativamente grandes en *L= 0, n, 2n,....*

### 4.2 Probabilidad De Ocurrencia

Esta probabilidad se obtuvo aproximándola con la frecuencia relativa, en la ocurrencia de unos y ceros. Dando

Los resultados obtenidos se muestran en la tabla 1.

| Número irracional | Probabilidad de unos | Probabilidad de ceros |
|---|---|---|
| $\phi$ | 0.5013 | 0.4987 |
| $\sigma$ | 0.5220 | 0.4780 |
| $\delta$ | 0.5284 | 0.4716 |
| $\sqrt{2}$ | 0.5220 | 0.4780 |

**Tabla 1**. Probabilidad de ocurrencia

### 4.3 Trasformada de Fourier

La FFT se define como una operación sobre un vector de N puntos

$$x[n] = \{x[0],..., x[N-1]\} \tag{27}$$

Cuyo resultado es otro vector

$$X[k] = \{X[0],..., X[1],..., X[N-1]\} \tag{28}$$

También de N puntos, definida como:

$$X[k] = \sum_{n=0}^{N-1} x[n] W_N^{nk} \quad para\ K = 0,1,2,...,N-1 \tag{29}$$

Donde

$$W_N = e^{-j2\pi/N} \tag{30}$$

La operación anterior puede interpretarse como la transformación de una secuencia x[n], de N puntos, con muestras en el dominio del tiempo, en otra secuencia X[k], así mismo de N puntos, con muestras en el dominio de la frecuencia, como se muestra en las graficas de las figuras en la sección de resultados.

## 5. Resultados

Los miembros de la familia metálica, están estrechamente relacionados con el comportamiento periódico en la dinámica no-lineal, siendo por ello de gran ayuda en la búsqueda de secuencias cifrantes para sistemas de protección de información.

Las sucesiones basadas en los miembros de esta familia poseen propiedades que se muestran en las gráficas 1-8, obtenidas de las secuencias binarias de los números irracionales ($\phi$, $\sigma$, $\delta$, $\sqrt{2}$ ). En las cuales se observa su FFT (espectro de frecuencia), su auto-correlación y su probabilidad de ocurrencia.

La figura 1 Muestra la FFT de la secuencia obtenida a partir del número irracional $\phi$.se observa la distribución uniforme en el espectro con una magnitud de 25, con 774 muestras. La figura 2 muestra la gráfica de auto-correlación, con una magnitud máxima fundamental en la muestra 774, y un desvanecimiento hacia sus lóbulos laterales, se observa la similitud que existe entre los segmentos de las muestras de la misma función.

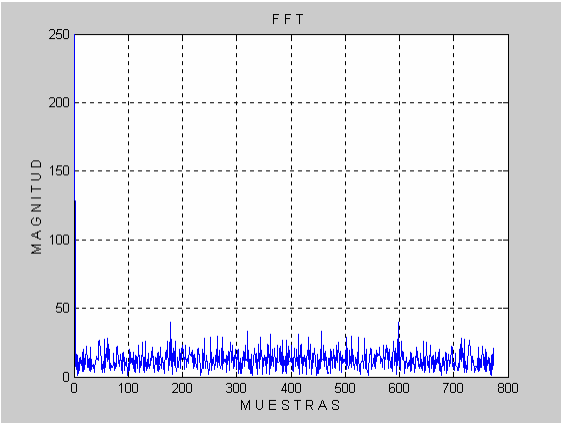


**Fig. 1** FFT de la Secuencia $\phi$

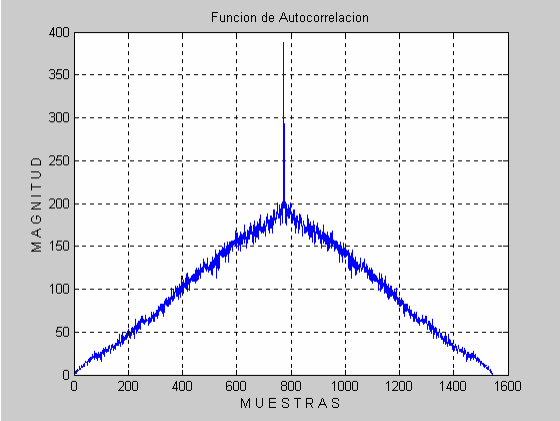


**Fig. 2** Auto-correlación de la Secuencia $\phi$

La figura 3 Muestra la FFT de la secuencia obtenida a partir del número irracional σ (número de plata). Observando la variación de máximos y mínimos de amplitud a lo largo de las 774 muestras y la distribución uniforme alrededor de la magnitud 25. La Figura 4, muestra la gráfica de auto-correlación, en la cual se presenta la muestra 774 con magnitud máxima y una similitud de la secuencia en sus lóbulos laterales debajo de la magnitud 220, observando la similitud que existe entre las muestras de la misma función.

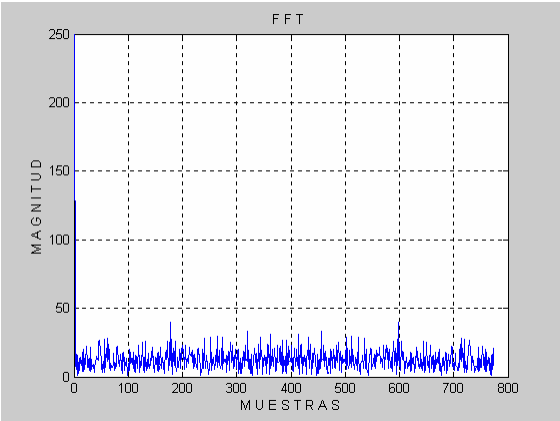


**Fig. 3** FFT de la Secuencia σ

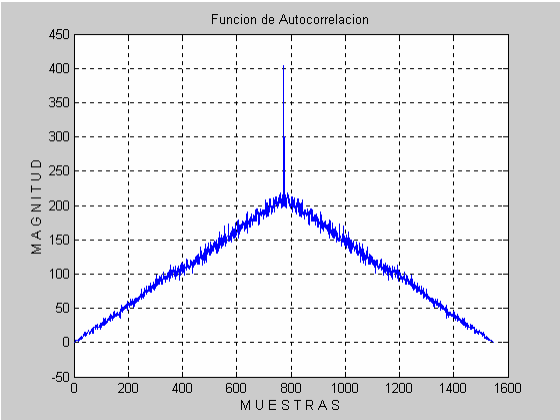


**Fig. 4** Auto-correlación de la Secuencia σ

La figura 5. Muestra la FFT de la secuencia obtenida a partir del número irracional δ, se observa que el espectro esta en un margen aproximado de magnitud 25 con una distribución uniforme, presentando valores máximos y mínimos en el espectro. La Figura 6, muestra la gráfica de auto-correlación, en la cual se presenta la muestra 774 con magnitud máxima, y la similitud de la secuencia entre los lóbulos laterales debajo de la magnitud 225.

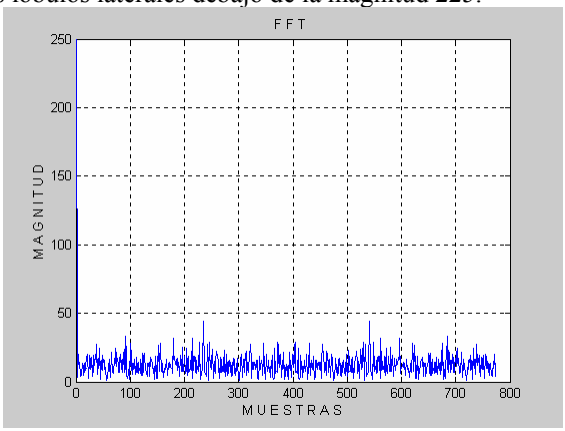


**Fig. 5** FFT de la Secuencia δ

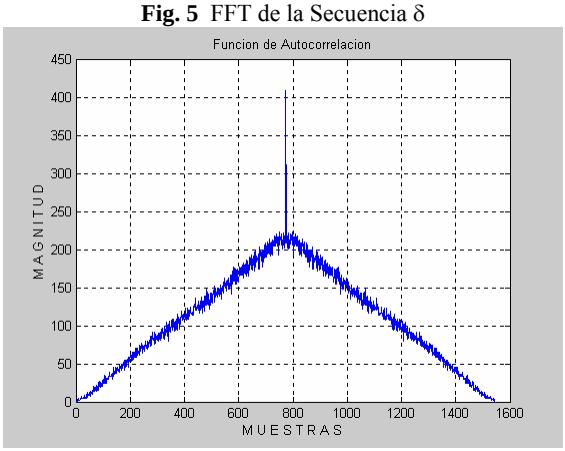


**Fig. 6** Auto-correlación de la Secuencia δ

La figura 7 Muestra la FFT de la secuencia obtenida a partir del número irracional $\sqrt{2}$ , se observa que el espectro esta en un margen aproximado de magnitud 25 con una distribución uniforme presentando una variación de máximos y mínimos de amplitud a lo largo de las 774 muestras. La Figura 8, muestra la gráfica de auto-correlación, en la cual se presenta una muestra fundamental máxima cercana a la magnitud 400 y una similitud entre los lóbulos laterales debajo de la magnitud 220.

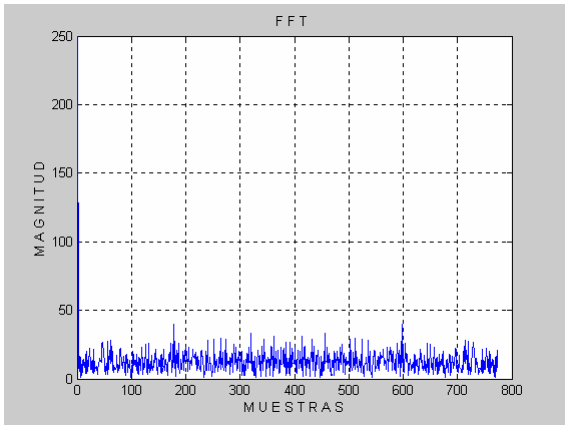


**Fig. 7.** FFT de la Secuencia $\sqrt{2}$

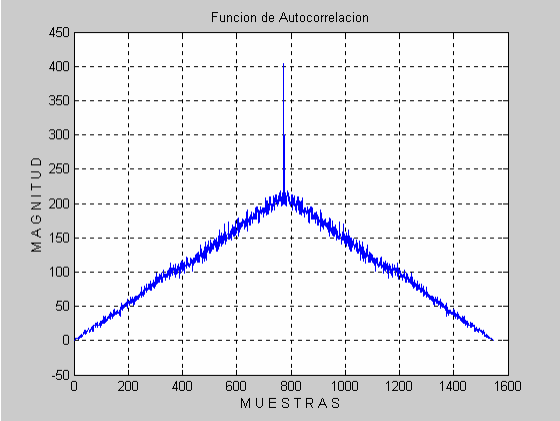


**Fig. 8** Auto-correlación de la Secuencia $\sqrt{2}$

**Gráficas de la probabilidad de ocurrencia**

En la figura 9 se observa la probabilidad de ocurrencia de las secuencias binarias, observando como la secuencia de la razón dorada (1) es muy similar al número de bronce(3), así como la secuencia del número de plata (2) es muy similar al número irracional Sqrt[2] (4). Esto se debe la relación que existe entre las secuencias binarias, notando como a partir de la muestra 1 y hasta la muestra 10 se nota la variación de probabilidad de ocurrencia, por tal motivo se toma este rango para graficar ya que después de la muestra 15 las secuencias binarias son similares y no presentan cambios.

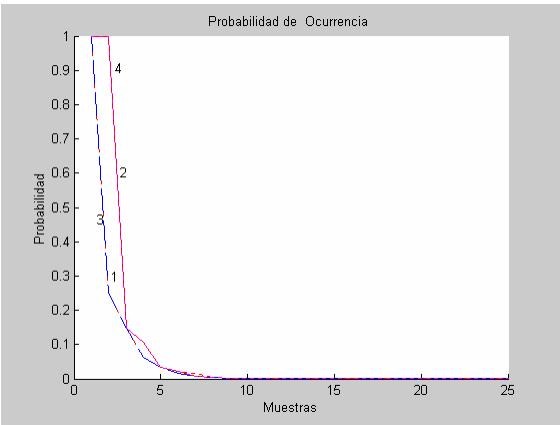


**Fig.9** Probabilidad de Ocurrencia

## 6. Conclusiones

Al obtener las secuencias binarias por medio de fracciones continuas, se piensa en su aplicación de estas, a sistemas de protección de información, como por ejemplo, en esquemas de flujo o comunicación para espectro disperso. Se observa dos requerimientos que toda secuencia cifrante que debe satisfacer para su correcta aplicación al cifrado en flujo, su periodo y su facilidad de implantación.

Todas las soluciones positivas de la ecuación (3) son miembros de la familia de números metálicos recientemente introducida por la aurora, como se puede aprecias en la literatura (*Vera. W. de Spinadel, 1998*), siendo el número de oro el que posee una descomposición en fracciones continuas más lentamente convergente, pues los denominadores que van a pareciendo a medida que se calcula una nueva aproximación son los más pequeños posibles.

Es difícil evaluar si una secuencia binaria es suficientemente segura para su utilización en criptografía, ya que no existe un criterio general y unificado que lo certifique. La complejidad computacional de un algoritmo se mide por dos variables

comúnmente, el tiempo y el espacio o requerimientos de memoria, ambos expresados en función del tamaño de la entrada (Luce*na López, 2001*). Esto es un análisis que se ha realizado utilizando algoritmos probabilísticos como: los Postulados de Golomb (*Romero Ibarra, 2002*), o la Prueba Universal de Maurer (Romero Ibarra 2002), utilizando los números irracionales descritos.

## Referencias


1. **Alan V.** and **Alan S. Willsky**, "*Señales y Sistemas*", Primera Edición, Prentice Hall Inc., 1994 pp 62, 155.
2. **Gray R.** "Georg *Cantor and Transcendental Number*": Amer Math Monthly, p. 101, 819-832, 1994.
3. **Harold Davenport** "*The Higher Arithmetic by Harold Davenport*", Cambridge University Press, (7th edition) 1999,
4. **Kappraff J.** "*Architecture and Mathematics*" Ed. Kim Williams, 1996.
5. **Kimberling C**, "*A visual Euclidean algorithm in Mathematics Teacher"*, vol 76 (1983) pages 108-109.
6. **Long C. T**. and **Jordan J. H.**, "*A Limited Arithmetic on Simple Continued Fractions*", Fibonacci Quarterly, Vol 5, 1967, pp 113-128;
7. **Lorentzen Lisa**, and **Waadeland Haakon,** "*Continued Fractions With Applications*", North-Holland (1992), pp 10-25.
8. **Lucena López M.** "*Criptografía y Seguridad en Computadoras*", 3er edición, versión 1. junio del 2001.
9. **Romero Ibarra** y **Vázquez Medina**, "*Evaluación y análisis de secuencias cifrantes irracionales usando la prueba universal de Maurer*", IPN, SEPI ESIME CULHUACAN. Artículo presentado en el congreso CITEL 2002, 25-29 de noviembre, La Habana Cuba.
10. **Romero Ibarra** y **Vázquez Medina**, "*Análisis de secuencias cifrantes generadas a partir de números irracionales, utilizando los Postulados de Golomb*", IPN, SEPI ESIME CULHUACAN. Artículo presentado en el congreso IEEE ROC&C´ 2002. 1-6 de octubre, Acapulco.
11. **Romero Ibarra** y **Vázquez Medina**, "*Secuencias cifrantes generadas a partir de números irracionales trascendentales*", IPN, SEPI ESIME CULHUACAN. Artículo presentado en el congreso ELECTRO 2002, 21-25 de octubre, Chihuahua .
12. **Simon M. K.** et al., "*Spread Spectrum Communications*", vol. 1 Rockville, MD: Computer Science Press, 1985.
13. **Ueli M. Maurer**. *"A Universal Statiscal Test for Random Generators*", Journal of Cryptology. Vol. 5, No. 2, p. 89-105, 1992
14. **Vera W. de Spinadel**, "*From the Golden Mean to Chaos*", Nueva Libreria, 1998.

***Francisco Javier Romero Ibarra.*** *Nacido en México D.F. Estudios de bachillerato en CECyT "Cuauhtémoc" y educación superior en ESIME unidad Culhuacán, obteniendo el titulo de Ing. en Comunicaciones y Electrónica, Estudio de Posgrado en ESIME Culhuacán, obteniendo el titulo de M. en C. de Ingeniería en Microelectrónica, con investigación en "Cifrado de Flujo". Catedrático de la CECyT Cuauhtémoc del Instituto Politécnico Nacional y de la Universidad Tecnológica de México (UNITEC).*

***Rubén Vázquez Medina.*** *He received the Electronic Engineering degree from the Universidad Autónoma Metropolitana (UAM) in 1988. He is Master in Science by the Investigation Center of Advanced Studies of the National Polytechnic Institute of Mexico (CINVESTAV-IPN). He is currently working toward the Ph. D. degree at UAM. From 1990 to 1993 he was with the Electrical Engineering Department UAM-Iztapalapa and since 1997, he is with the graduate department of the Electrical Engineering School of the IPN. From 1993 to 1997 he was in Merkatel, S.A. de C.V.*