Cifrador de Bloque con Doble Red de Feistel y Funciones Booleanas de Alta No Linealidad

Andrés Francisco Farías – Andrés Alejandro Farías

Departamento Académico de Ciencias Físicas, Matemáticas y Naturales
Universidad Nacional de La Rioja, La Rioja. Argentina
(afarias665@yahoo.com.ar, andres_af86@hotmail.com)

Abstract. Cifrador de bloque, basado en la doble Red Feistel de 48 rondas cada una, con bloques de 256 bits de longitud y clave de 128 bits. Donde las Cajas S, de sustitución son reemplazadas por funciones booleanas que siguen los siguientes según criterios de buenas propiedades criptográficas: balance, cumplimiento del critero de avalancha estricta (SAC en inglés) y alta no linealidad.
Key Words: NLFSR, Cipher, key, boolean function, non-linearity.

1 Introducción

El presente documento expone el desarrollo de un cifrador de bloque, basado en una doble Red de Feistel que permite el cifrado y descifrado utilizando la misma estructura, donde para el caso del descifrado se utilizan las subclaves cambiando el orden de las mismas [1], [2]. La clave adoptada es de 16 caracteres, es decir 128 bits. Se utiliza como Función de Feistel, en lugar de las clásicas Cajas S (S-Box), funciones booleanas de cuatro variables, balanceadas y de alta no linealidad [3].

2 Esquema del cifrador

El cifrado de bloque se denomina así por realizar el proceso de cifrado trabajando sobre cadenas de texto de igual longitud. En este caso se utilizaron bloques de 256 bits. Luego esos bloques son ensamblados siguiendo el modo de encadenamiento de bloques de cifrado de propagación (PCBC, Propagating Cipher Block Chaining) [4]. Básicamente la estructura del cifrador está conformada por dos Redes de Feistel en que consta de: Las propia Redes de Feistel para: Cifrado y descifrado, subclaves.y función de las redes de Feistel

2.1 Redes de Feistel para el cifrado

En la figura 1, se indica la disposición del cifrador de bloque.

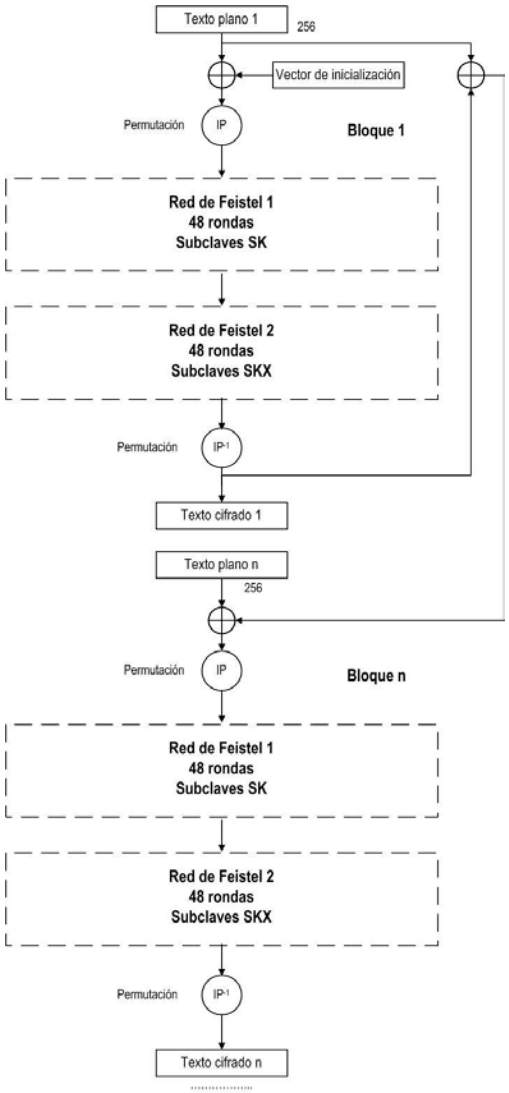

Fig. 1. Redes de Feistel para cifrado en modo PCBC

Cada bloque al ingresar a la red sufre una permutación dada por una matriz PI, luego de ello se divide al bloque en dos bloques, uno izquierdo y otro derecho, de 128 bits cada uno, a partir de ese momento esos bloques entran en las redes de Feistel. Finalmente los bloques resultantes del final de las rondas se concatenan para un formar un bloque de 256 bits, que es sometido a una nueva permutación IPI, que da como resultado el texto cifrado.

2.2 Redes de Feistel para el descifrado

Se indica en la figura 2:

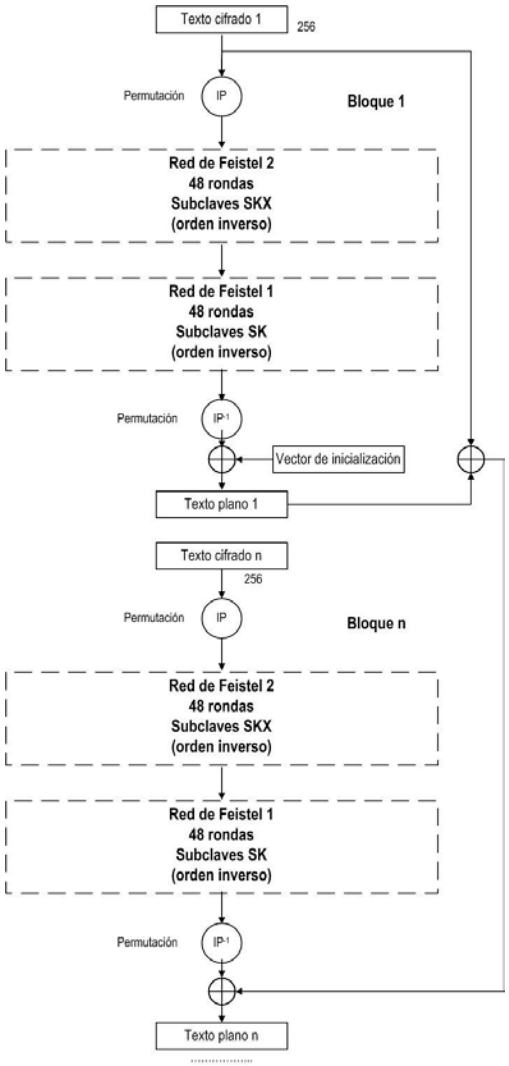

Fig. 2. Redes de Feistel para descifrado en modo PCBC

Las redes de Feistel para descrifrado son similares a la anterior, pero en este caso se toma el texto cifrado y se lo divide en bloques de 256 bits. Las permutaciones PI e IPI son las mismas que se utilizaron para el cifrado:

2.3 Clave y subclaves

Como se dijo previamente, la clave está conformada con 16 caracteres (128 bits), de las que se generan dos conjuntos de 48 subclaves de 128 bits, para cada una de las redes. Esos pares son ensamblados y luego sometidos a la permutación PC2, para obtener las subclaves finales.

2.4 Función de Feistel

La función de Feistel tiene la configuración que se indica en la figura 3:

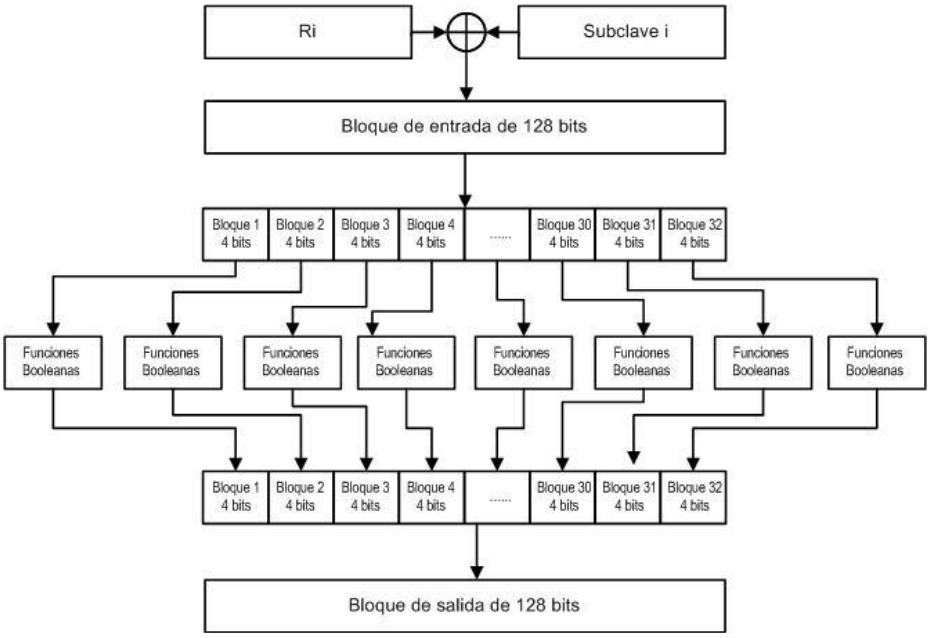

Fig. 3. Función de Feistel

La mitad del bloque de texto, la parte derecha de 128 bits, es sometida a una operación XOR con la subclave de 128 bits. Luego se divide en bloques de cuatro bits que alimentan a funciones booleanas balanceadas y de alta no linealidad, de esto resulta una salida de 128 bits.

2.5 Bloques con funciones booleanas

A continuación en la figura 4, se indica la estructura de cuatro bits.

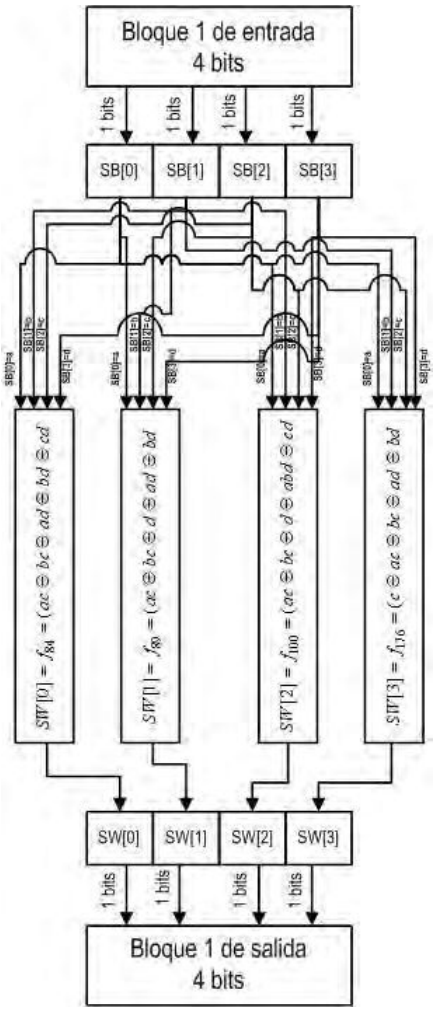

Fig. 4 Bloque de 4 bits con funciones booleanas de alta no linealidad

3 Propiedades criptográficas deseables adoptadas

A continuación se indican algunas de las propiedades criptográficamente más significativas, adoptadas para este trabajo [5], [6] y [7].

- **Función Balanceada:** Una función booleana de n-variables f es balanceada si $w(f) = 2n - 1$. Esta propiedad es deseable para evitar ataques criptodiferenciales. La función es balanceada cuando el primer coeficiente del espectro de Walsh-Hadamard, es igual a cero: $F(0) = 0$.
- **No Linealidad:** Valores altos de esta propiedad reducen el efecto de los ataques por criptoanálisis lineal. La No Linealidad de una función booleana puede ser

calculada de la transformada de Walsh-Hadamard.: $NL_f = \frac{1}{2} \cdot (2^n - |WH_{max}(f)|)$

- **Grado Algebraico:** El grado algebraico de una función, es el número de entradas más grande que aparece en cualquier producto de la Forma Normal Algebraica. Es deseable que sean valores altos.
- **SAC:** El Criterio de Avalancha Estricto requiere los efectos avalancha de todos los bits de entrada. Una función booleana se dice que satisface SAC sí y solo sí, $f(x) \oplus f(x \oplus u)$, es balanceada para toda u con w(u)=1.

4 Permutación

Se recurre a una matriz con una distribución aleatoria de las posiciones, para obtenerla se utiliza un generador de números aleatorios, en esta ocasión se adopta un generador congruencial multiplicative [8].

4.1 Generador congruencial multiplicativo:

El generador tiene la siguiente expresión:

$$x_{i+1} = (a_x \cdot x_i) mod\ m_x$$

Donde: $a_x = multiplicador, m_x = módul, x_0 = semilla$

Tabla.1. Matrices

Matriz	módulo	multiplicador	semilla
IP	1048576	1279	1153
PC1	1048576	1597	1531
PC2	1048576	1933	1759

5 Elección de las pruebas estadísticas

Algunas pruebas de la Norma NIST 800-22, del trabajo de Rukhin (et al.) [9].

Prueba de frecuencia: El propósito de esta prueba es determinar si el número de unos y ceros en una secuencia es aproximadamente el mismo que se espera de una secuencia verdaderamente aleatoria. La prueba evalúa la cercanía de la fracción de unos a ½, que es decir, el número de unos y ceros en una secuencia debe ser aproximadamente el mismo. Todas las pruebas posteriores dependen de la aprobación de esta prueba.

Prueba de frecuencia en un bloque: La meta de esta prueba es determinar si la frecuencia de unos en un bloque de M bits es aproximadamente M / 2, como se esperaría bajo un supuesto de aleatoriedad.

Prueba de rachas: Una racha de longitud k consta de exactamente k bits idénticos y está acotada antes y después con un poco del valor opuesto. El propósito de la prueba de rachas es determinar si el número de rachas unos y ceros de varias longitudes es lo esperado para una secuencia aleatoria.

Prueba de rachas de unos en un bloque: El fin de esta prueba es determinar si la longitud de la ejecución más larga de las dentro de la secuencia probada es consistente con la longitud de la serie más larga de las que cabría esperar en una secuencia aleatoria. Tenga en cuenta que una irregularidad en la longitud esperada de la serie más larga implica que también hay una irregularidad en la longitud de la serie más larga de ceros.

Prueba de sumas acumuladas: Determina si la suma acumulativa de las secuencias parciales que ocurren en la secuencia probada es demasiado grande o demasiado pequeña en relación con el comportamiento esperado de esa suma acumulada para secuencias aleatorias.

Prueba de entropía aproximada: El enfoque de esta prueba es la frecuencia de todas las posibles superposiciones patrones de m bits en toda la secuencia. El propósito de la prueba es comparar la frecuencia de bloques superpuestos de dos longitudes consecutivas / adyacentes (m, m + 1) contra el resultado esperado para un secuencia aleatoria.

6 Pruebas sobre el generador

Se analizaron cien secuencias binarias, obtenidas del cifrador a partir de cien claves distintas. El nivel de significancia adoptado para las pruebas estadísticas es de $\alpha = 0{,}01$. La hipótesis nula es: $H_0 \rightarrow p\_valor > 0{,}01$

7 Interpretación de los resultados

Teniendo los resultados se realizan dos procesos para la interpretación de los mismos:

- Proporción de muestras que pasan las pruebas.
- Prueba de Uniformidad de los p-valor
    - Tabla de frecuencia e histograma
    - Prueba de Bondad de Ajuste

El primer procedimiento se realiza considerando los resultados de todas las pruebas y el segundo se realiza en forma individual. En todos los casos se deben superar todas las pruebas para aceptar los resultados.

7.1 Proporción de muestras que pasan las pruebas

Para el análisis de los resultados, se determina la proporción de muestras que superan las pruebas, y con esos datos se construye un gráfico de puntos, luego se verifica si los mismos caen dentro de los límites superior e inferior, donde k es el número de muestras. $LS, LI = (1-\alpha) \pm 3 \cdot \sqrt{\alpha \cdot (1-\alpha)/k}$

En nuestro caso $k = 100$ y el nivel de significancia elegido es: $\alpha = 0.01$, los límites quedan:. $LS = 1{,}02$ y $LI = 0{,}96$. Los resultados se indican en la tabla

Tabla 2. Pruebas

Pruebas	Proporción	Superior	Inferior
Frecuencias	0,98	1,02	0,96
Frecuencias en un Bloque	0,97	1,02	0,96
Rachas	0,99	1,02	0,96
Rachas de Unos en un Bloque	0,99	1,02	0,96
Sumas Acumuladas Adelante	0,97	1,02	0,96
Sumas Acumuladas Atrás	0,99	1,02	0,96
Entropía Aproximada	1,00	1,02	0,96

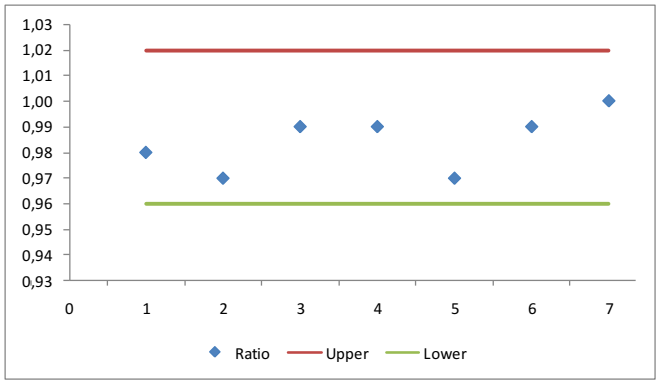

Fig. 5. Gráfico de puntos

7.2 Prueba de bondad de ajuste

Este control se ejecuta para cada prueba sobre las cien muestras, con los resultados de las frecuencias de p-valor obtenidos.

Tabla 3. Pruebas χ^2

Pruebas	χ^2	$\chi^2 ref$	Pasa
Frecuencias	0,130	0,0001	Sí
Frecuencias en un Bloque	0,946	0,0001	Sí
Rachas	0,883	0,0001	Sí
Rachas de Unos en un Bloque	0,154	0,0001	Sí

Sumas Acumuladas Adelante	0,019	0,0001	Sí
Sumas Acumuladas Atrás	0,067	0,0001	Sí
Entropía Aproximada	0,699	0,0001	Sí

7.3 Análisis final

En base a los resultados de la pruebas se realiza una tabla resumen.

Tabla 4. Análisis final

Análisis	Pruebas	Resultados
Proporción de secuencias que pasan las pruebas	Todas	Supera
Distribución uniforme de p-valor	Frecuencias	Supera
	Frecuencias dentro de un bloque	Supera
	Rachas	Supera
	La más larga racha de unos en un bloque	Supera
	Sumas acumuladas adelante	Supera
	Sumas acumuladas atrás	Supera
	Entropía estimada	Supera

En definitiva las secuencias que entrega el generador son pseudoaleatorias.

8 Comparación de frecuencias

Diferencias entre texto plano y texto cifrado.

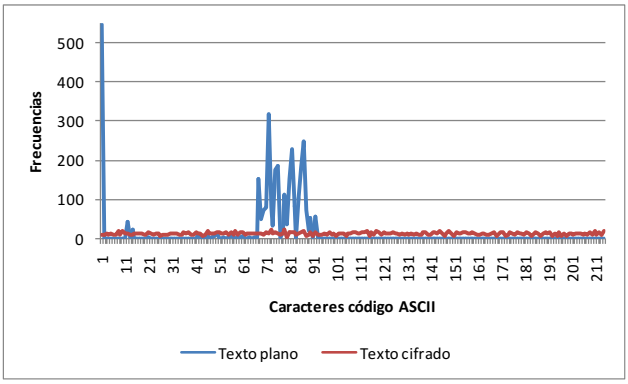

Fig. 6. Frecuencias de caracteres del texto plano y cifrado

9 Conclusiones

Se ha presentado un cifrador de bloque con algunas características interesantes tales como clave de mayor longitud y la incorporación de funciones booleanas de alta no linealidad.

Sobre este diseño se pueden implementar otras variantes para lograr futuras versiones que contemplen entre otras cosas: claves más largas y mayor cantidad de funciones booleanas y otros métodos de concatenación de bloques.

La respuesta de esta versión fue buena y entregó un texto cifrado con una frecuencia de caracteres con cierta uniformidad, lo que hace difícil un criptoanálisis basado en la estadística de aparición de caracteres.

Los cifrados son herramientas útiles cuando se necesita dar seguridad a información de tipo confidencial.

10 Referencias

[1] Massodi, F., Alam, S. and Bokhari, M., "An Analysis of Linear Feedback Shift Registers in Stream Ciphers", International Journal of Computer Application, 16 (17), pp. 0975 – 887, 2012.

[2] Canteaut, A. and Filio, E., "Ciphertext only reconstruction of stream ciphers based on combination generators. Fast Software Encryption 2000", Lecture Notes in Computer Science, 1978, pp. 165–180, 2001.

[3] Menezes, A.,Van Oorschot, P. and Vanstone, S., "Handbook of Applied Cryptography", Massachusetts Institute of Technology, 1996.

[4] Parr, C. and Pelzl, L., Understanding Cryptography, Springer, 2010.

[5] Constantinescu, N., "Combining Linear Feedback Shift Registers", in Annals of University of Craiova, Math. Comp. Sci. Ser, 2009, 36 (2), pp. 42–46.

[6] Braeken, A.: Cryptographic Properties of Boolean Functions and S-Boxes. Faculteit Ingenieurswetenschappen. Katholieke Universiteit Leuven (2003)

[7] Elhosary, A., Hamdy, N., Farag, I., Rohiem, I.: State of the Art in Boolean Functions Cryptographic Assessment. International Journal of Computer Networks and Communications Security.1. (3), 88--94 (2013)

[8] Fishman, G.: Multiplicative Congruential Random Number Generators with Modulus 2ß : An Exhaustive Analysis for ß = 32 and a Partial Analysis for ß = 48. Mathematics of Computation. 54. (189), 33--344 (1990)

[9] Rukhin, A., Soto, J., Nechvatal, J., Smid, M., Barker, E., Leigh, S., Levenson, M., Vangel, M., Banks, D., Heckert, A., Dray, J., and Vo, S., "A Statistical Prueba Suite for Random and Pseudorandom Number Generators for Cryptographic Applications", National Institute of Standards and Technology, (2000).