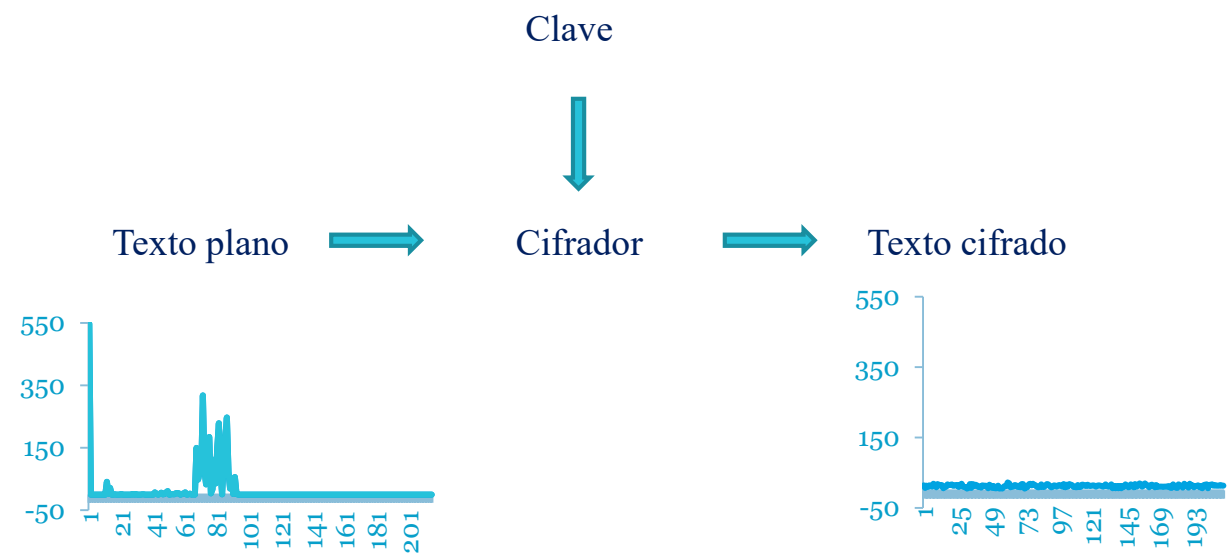


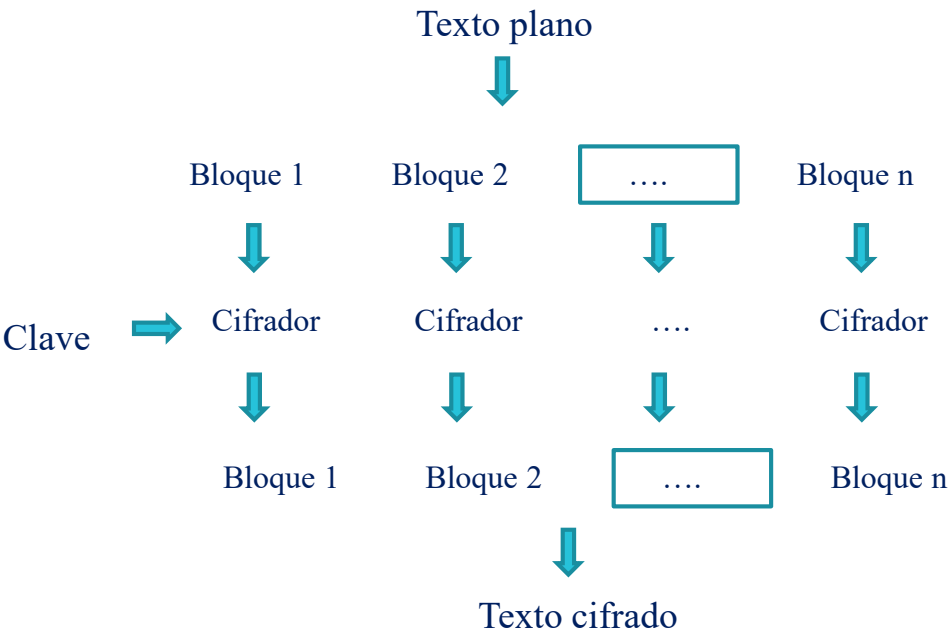
**Cifrador de Bloque de Dos Algoritmos
Cifradores Paralelos Conformados por
Secuencias Entrelazadas de Polinomios
Diferentes, en Modo de Encadenamiento de
Bloques de Cifrado en Propagación**

Andrés Francisco Farías Germán Antonio Montejano
Ana Gabriela Garis Andrés Alejandro Farías

Principio del Cifrado de Mensajes



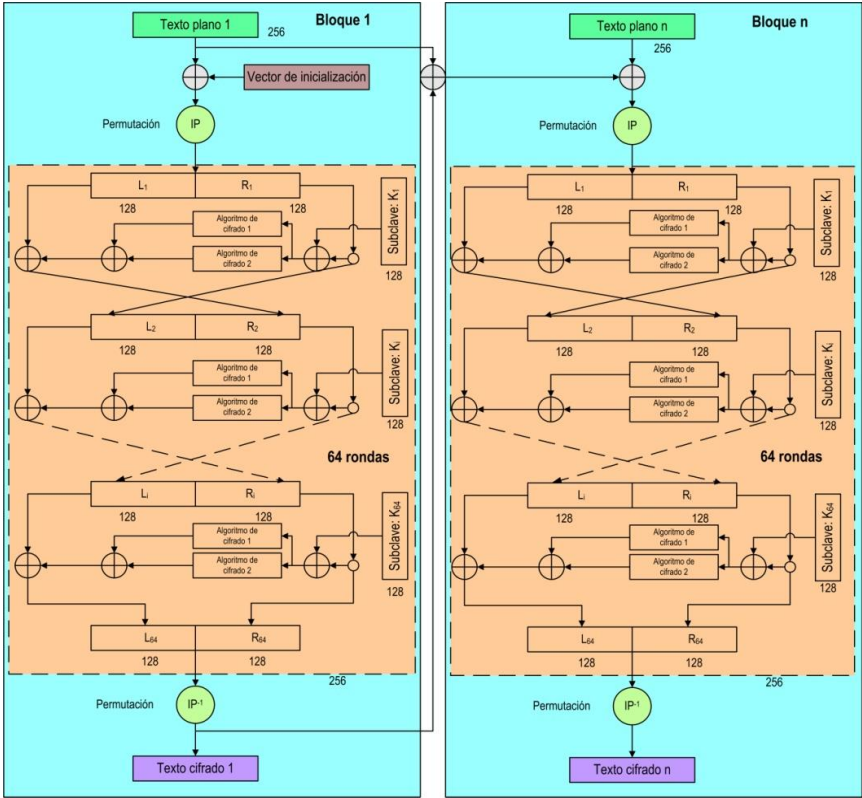
Cifrado de Bloque



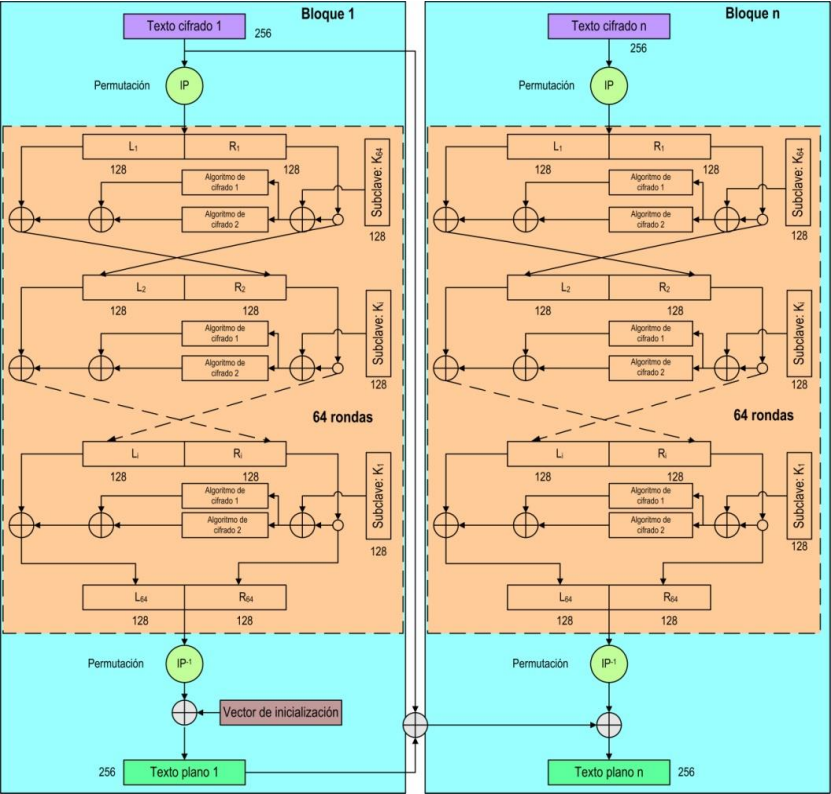
Esquema del cifrador

- Red de Feistel para cifrado
- Red de Feistel para descifrado.
- Clave y subclaves.
- Vector de inicialización.
- Algoritmos de cifrado.
- Generadores binarios pseudoaleatorios.
- Modo de operación PCBC

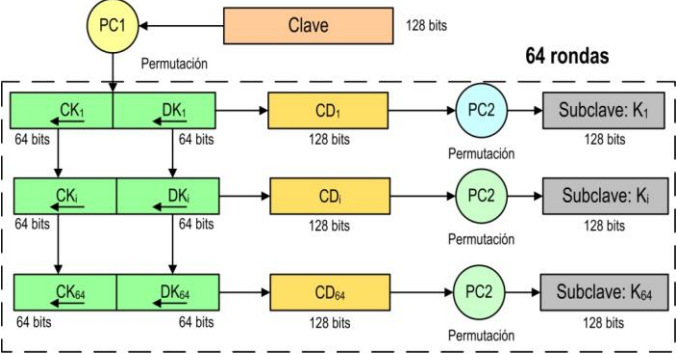
Red de Feistel para cifrado



Red de Feistel para descifrado



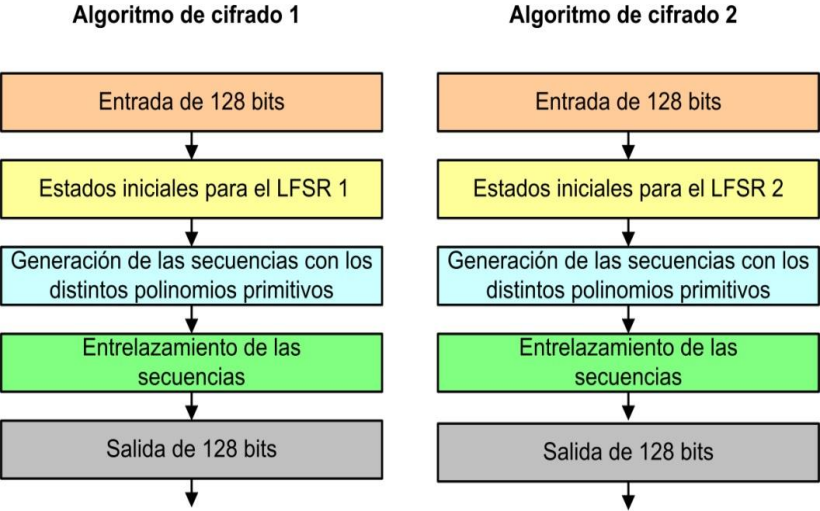
Clave y subclaves



Vector de inicialización

Es para iniciar las tareas de encadenamiento de bloques, tanto de cifrado como de descifrado. Es única para todo el proceso, debe ser secreta como la clave y su longitud es igual a la de los bloques: 256 bits.

Algoritmos de cifrado



Secuencias t-entrelazadas

Secuencia 3-entrelazada con polinomios primitivos diferentes. Los LFSR tienen una longitud de 71 bits y en tabla 1, se indican los polinomios.primitivos [5], [6], [7] y [8].

Tabla 1. LFSR, longitudes y polinomios primitivos del generador

LFSR	Longitud	Polinomios primitivos
1	71	$P(x)_1 = x^{71} + x^{59} + x^{53} + x^{48} + 1$
2	71	$P(x)_2 = x^{71} + x^6 + 1$
3	71	$P(x)_3 = x^{71} + x^{49} + x^{45} + x^{34} + x^{30} + x^{21} + 1$

Secuencia 2-entrelazada con polinomios primitivos diferentes. Los LFSR tienen una longitud de 67 bits y en tabla 2, se indican los polinomios primitivos [5], [6], [7] y [8].

Tabla 2. LFSR, longitudes y polinomios primitivos del generador

LFSR	Longitud	Polinomios primitivos
1	67	$P(x)_1 = x^{67} + x^{61} + x^{33} + x^3 + 1$
2	67	$P(x)_2 = x^{67} + x^{64} + x^{44} + x^{28} + x^{26} + x^{25} + 1$

Matrices de Permutación

Tabla 3. Matriz IP, PC1 y PC2

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

Elección de las pruebas estadísticas

Fueron seleccionadas algunas pruebas de la Norma NIST
Special Publication 800-22

Tabla 4. Pruebas estadísticas para números aleatorios y pseudoaleatorios

Pruebas estadísticas para números aleatorios y pseudoaleatorios	
1	Frecuencia (monobit)
2	Frecuencia dentro de un bloque
3	Entropía aproximada
4	Sumas acumuladas
5	Rachas
6	Prueba en serie
7	Universal
8	Coincidencia de plantillas no superpuestas
9	Complejidad lineal
10	Transformada discreta de Fourier (espectral)

Interpretación de los resultados

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

- Proporción de muestras que pasan las pruebas
- Prueba de Uniformidad de los p-valor

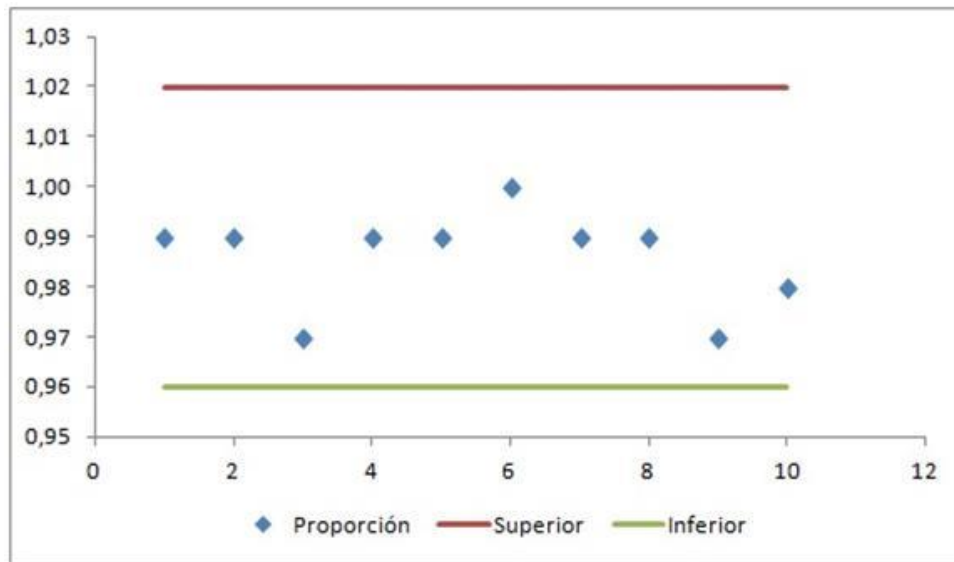
Pruebas Estadísticas de Aleatoriedad

Cien muestras correspondientes a cien claves

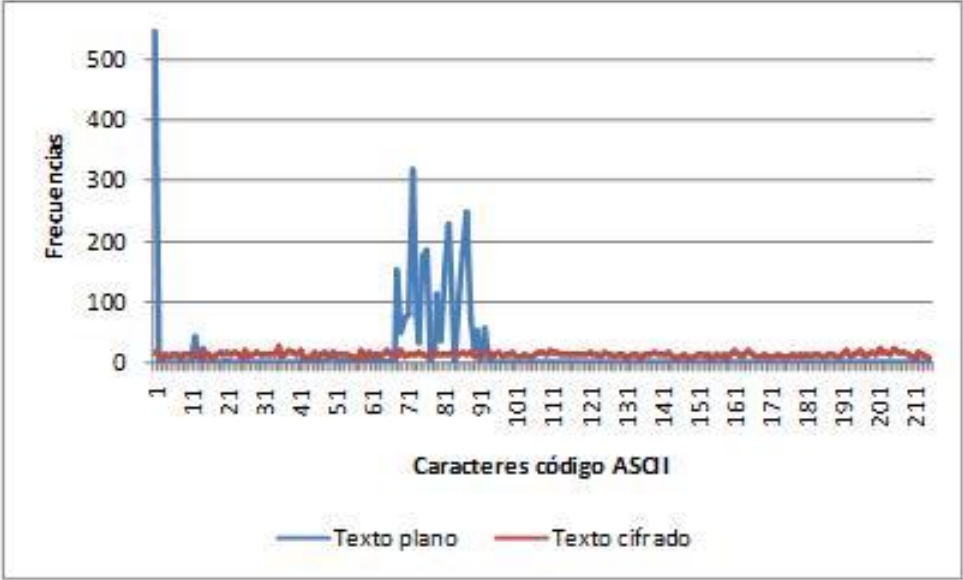
. Pruebas estadísticas para números aleatorios y pseudoaleatorios

	Pruebas estadísticas para números aleatorios y pseudoaleatorios	Total	Pasan	Propor.	Superior	Inferior
1	Frecuencia (monobit)	100	99	0,99	1,02	0,96
2	Frecuencia dentro de un bloque	100	99	0,99	1,02	0,96
3	Entropía aproximada	100	97	0,97	1,02	0,96
4	Sumas acumuladas	100	99	0,99	1,02	0,96
5	Rachas	100	99	0,99	1,02	0,96
6	Prueba en serie	100	100	1,00	1,02	0,96
7	Universal	100	99	0,99	1,02	0,96
8	Coincidencia de plantillas no superpuestas	100	99	0,99	1,02	0,96
9	Complejidad lineal	100	97	0,97	1,02	0,96
10	Transformada discreta de Fourier (espectral)	100	98	0,98	1,02	0,96

Cantidad de muestras que superan las pruebas



Comparación de frecuencia de caracteres de texto plano y texto cifrado



¡Gracias, por su atención!