7 CONCLUSIONES

En esta tesis se formuló un criptosistema caótico de señales de información y en base a éste se diseñó un criptocircuito caótico. El criptosistema se basó en un sistema caótico de tirón el cual presenta las siguientes ventajas sobre otros a la hora de ser diseñado en circuito:

- Las variables de estado son todos voltajes y se eliminó el uso de inductores.
- Las no linealidades del sistema son lineales por partes, lo que hace más sencillo (en componentes) al sistema. Además se procuró que las funciones lineales por partes fueran continuas, para evitar que los efectos de histéresis fueran muy significativos en la dinámica del sistema.
- La matriz de coeficientes del sistema caótico es de tipo companion, por lo tanto las sumas de las variables del sistema sólo se hacen a la entrada de un integrador.
- El sistema es fácilmente escalable en frecuencia, tan sólo hay que cambiar el valor de la variable $\tau = (RC)^{-1}$, en los bloques integradores.
- El circuito diseñado usa valores reales de los capacitores y resistencias, con el fin de que pueda ser fácilmente armado en un futuro; además debido a la simplicidad de diseño que se logró en el circuito éste bien podría miniaturizarse en un chip.

En esta tesis se utilizó un método para lograr sincronía entre encriptor y desencriptor el cual consiste en convertir al sistema caótico del desencriptor en un observador no lineal del encriptor para así llevar el error de sincronización a 0. Se observó que en este método, y en general en la literatura, no se toman mucho en cuenta las características de la función de encripción; por lo tanto se formuló una expresión general para la función de encripción y la de desencripción basada en funciones biyectivas no lineales, para proteger la información tanto en amplitud como en frecuencia sin hacer que el sistema saliera de su régimen

caótico. Se encontró que la transformación no lineal del encriptor provoca que la energía de la señal de información se riegue en un rango más amplio de frecuencias, lo que ayuda a garantizar la seguridad del sistema.

Se probó que la función de encripción en promedio no afectaba al sistema, y al simular el sistema se llegó a otro resultado importante en referencia la relación que debe guardar el nivel de potencia de la señal de información a comparación del nivel de potencia de la llave que lo encripta; el cual se recomendó que la señal de información fuera menor en 10dBW a la señal llave de encripción.

A partir de simulaciones se comprobó que el circuito encriptor transforma la señal de información a una señal encriptada la cual transmite al desencriptor sumada a una potente señal de sincronía; y que el desencriptor transforma la señal encriptada en la señal de información si está bien sincronizado con el encriptor; cosa que sucede cuando se transmite en un canal sin ruido. A partir de simulaciones se encontró una curva que relaciona el radio entre la señal transmitida y el ruido y entre la señal recuperada y el ruido, y en base a esa curva se puede seleccionar la potencia de la señal de transmisión para obtener la deseada relación entre la señal de información y el ruido en el desencriptor.

Es importante comentar en este punto que si lo que se requiere es trabajar a altas frecuencias y comunicaciones basadas en caos es más conveniente trabajar con dispositivos optoelectrónicos los cuales pueden operar a frecuencias muy altas. Hasta el momento el desarrollo de los sistemas de encripción optoelectrónicos han sido basados en esquemas de la segunda generación. Queda abierta la posibilidad de crear un sistema de tercera generación y de lograrse, se tendrían las grandes ventajas de seguridad de los criptosistemas caóticos, y las grandes velocidades de los sistemas optoelectrónicos. El circuito que se diseñó funciona bien en rangos de kHz, por lo tanto aplicaciones específicas

para dicho circuito sería la encripción de audio, o señales digitales de baja tasa de bit por segundo.

En conclusión, en esta tesis se estudió, formuló y diseñó un criptosistema caótico para la transmisión segura de señales. Además, se aportaron algunos conceptos y requerimientos en relación a la función de encripción, y las potencias de las señales involucradas en el sistema. Las comunicaciones basadas caos son un área que sigue en desarrollo y es probable llegar a implantar dichos sistemas en un futuro no muy lejano, queda por delante estudiar métodos que no sean tan sensibles al ruido, así como un análisis criptográfico más completo sobre los sistemas.