UNIVERSIDAD NACIONAL AUTÓNOMA DE MÉXICO

FACULTAD DE INGENIERÍA

Estudio de un sistema cifrado de comunicación inalámbrica usando USRP

TESIS

Que para obtener el título de

Ingeniera en Telecomunicaciones

P R E S E N T A

Alma Yeni Zúñiga Bolaños

DIRECTOR DE TESIS

Javier Gómez Castellanos

Ciudad Universitaria, Cd. Mx., 2018

Agradecimientos:

A mi madre amada, Silvia Bolaños; por todo el esfuerzo, dedicación y cariño puesto en mis hermanos y en mí; así como el apoyo y paciencia que siempre me tuvo y por el que hoy he alcanzado uno de mis más grandes sueños.

A mis hermanos; Diana, Yerili y Adrian, ya que cada uno de ellos, con su ejemplo, aporto partes importantes en mi formación. Por su apoyo incondicional y la compañía que siempre me brindaron.

A Iván Pérez Montiel, por ser una de las personas que me apoyó en los momentos de crisis existencial, por inspirarme a lograr mis metas y por ser un gran ejemplo de profesionista.

A mi tutor el Dr. Javier Gómez Castellanos por su gran paciencia, apoyo y confianza. Por darme la oportunidad de desarrollar este trabajo y por los conocimientos transmitidos a lo largo del mismo.

Al M.I. Octavio Jaimes Botello por su paciencia y apoyo al explicarme algunos conceptos y dudas al iniciar este proyecto y por brindarme sus recomendaciones.

A mi hermosa Universidad Nacional Autónoma de México, mi "alma mater", a la Facultad de Ingeniería que me doto de todo y abrió las puertas del conocimiento para mí y al proyecto PAPIIT IN117017 por hacer posible este proyecto y por el apoyo económico que me brindó.

A todos los maestros de la carrera; por la gran labor de transmitir su conocimiento, por su paciencia, apoyo y consejos a lo largo de mi trayectoria académica y ser un gran ejemplo de profesionistas.

Contenido

Índice de figuras.

Índice de tablas

Índice de graficas

1. INTRODUCCIÓN

Los sistemas de comunicación cobran mayor importancia día a día debido a los servicios cada vez más amplios que ofrecen, permitiendo acceso a regiones aisladas, así como la gran cobertura que pueden brindar además del precio de producción que va disminuyendo mientras logra avances tecnológicos a pasos agigantados.

Por otra parte, debido a la evolución de las distintas técnicas de transmisión de información, es necesario centrar la atención en las diferentes tecnologías que nos facilitan esta tarea, como lo es la tecnología impresa en el NI-USRP.

El análisis del comportamiento de los parámetros de transmisión se hace con la intención de sacar el mayor beneficio de la tecnología, uno de estos parámetros es la modulación empleada, ya que cada una trae enormes ventajas, entre las que destacan menor afectación al ruido, tasas más altas de transmisión, entre otras.

Es por ello que cobra mayor importancia adentrarse en las comunicaciones digitales con la tecnología que permita mayor versatilidad, optimo del uso del espectro radioeléctrico, equipos más baratos, menor afectación al ruido y máximas tasas de transmisión.

El presente documento está enfocado al desarrollo e implementación de un algoritmo de cifrado, al monitoreo y análisis de los parámetros de eficiencia de una transmisión inalámbrica usando diferentes tipos de esquemas de modulación (BPSK, QPSK 8-PSK).

Se propone la implementación de este sistema de comunicación en la emergente tecnología de equipos de radiofrecuencia definidos por software usando los NI-Universal Software Radio Peripheral y mediante su interfase de comunicación con LabVIEW.

El sistema está compuesto básicamente por un transmisor, un canal con ruido y un receptor, que captará un texto cifrado y se analizarán los parámetros como el BER, SNR, potencia recibida y MER.

2. ASPECTOS GENERALES.

2.1. Objetivos

El objetivo principal del presente trabajo de tesis es desarrollar y analizar el diseño de un sistema de comunicación inalámbrico para la transmisión y recepción de texto cifrado, haciendo uso de una plataforma de radio definido por software (USRP), e implementando un esquema de modulación digital BPSK, QPSK y 8-PSK.

El análisis se enfocará en las características de los tipos de modulación empleados y las variaciones en los parámetros de eficiencia de las señales recibidas y manipuladas por el algoritmo situado en el trasmisor y receptor del sistema, con el fin de estudiar la sensibilidad de la comunicación inalámbrica.

Se explicarán las ventajas que presenta cada uno de los tipos de modulación empleados y se compararán los parámetros tales como el MER, BER y SNR resultantes en la demodulación y descifrado del mensaje.

2.2. Definición del problema

El constante aumento de aplicaciones en los servicios de comunicación inalámbricos y la creciente sociedad altamente dependiente de la tecnología, ha impulsado la necesidad de que los datos se transmitan de manera más rápida, segura y eficiente; por ello, hoy en día el tema de la seguridad en transferencia de información se ha hecho más relevante. Según aumente la importancia de los datos manipulados, el cifrado de datos se perfila como la herramienta de seguridad más usada.

El cifrado de datos, como es sabido, transforma la información para hacerla irreconocible e incomprensible para usuarios no autorizados, recuperar un mensaje cifrado significa contar con un método matemático de criptografía, denominados contraseñas o algoritmos.

La tecnología USRP gana cada día más atención debido a sus características, pues permite implementar una gran gama de funciones y herramientas útiles para la generación y el análisis de señales de radiofrecuencia. Se planteó desarrollar el algoritmo de cifrado asimétrico RSA basado en software, cuya peculiaridad es que utiliza dos claves diferentes para cada usuario, una para cifrar el mensaje (clave pública) y otra para descifrarlo (clave privada).

Los inconvenientes de la encriptación, teniendo en cuenta que éstos son relativos en función de los requerimientos específicos, son un mayor uso de ancho de banda en la transmisión y tiempo de procesamiento.

Como en cualquier sistema de transmisión, existe el riesgo de perder la información por problemas técnicos, cuestiones del canal de comunicación, fallas en la trama, entre otros factores. El trabajo englobará el análisis de la sensibilidad por parte del USRP, en cada una de las modulaciones ya mencionadas contra la distancia y la comparación de los parámetros de eficiencia de la transmisión.

3. METODOLOGÍA.

3.1. Gestión del proyecto

Primero. Recopilación de información previa e investigación de la tecnología que se empleará para el desarrollo del trabajo.

Segundo. Desarrollo de ejercicios para la adaptación al uso del hardware desarrollado por la National Instrument NI-USRP, bajo la plataforma programable de LabVIEW.

Tercero. Recopilación de varios tipos de fuentes de información acerca del tema principal a desarrollar en esta tesis.

Cuarto. Análisis de la información recopilada.

Quinto. Desarrollo del programa para la transmisión y recepción de texto con modulación QPSK y QAM, bajo la plataforma de LabVIEW.

Sexto. Implementación del algoritmo de cifrado de Verman en un bloque programable de LabVIEW, sobre el transmisor.

Séptimo. Implementación del algoritmo de descifrado en el receptor del sistema.

Octavo. Pruebas de funcionamiento del sistema de transmisión y recepción de texto cifrado con modulación QPSK y QAM.

Noveno. Ejecución de distintos escenarios para el sistema de comunicación con variación en la distancia entre el transmisor y receptor, para cada tipo de modulación.

Décimo. Medición y recopilación de los parámetros de cada señal recibida en los diferentes escenarios ejecutados.

Décimo primero. Análisis y comparación de los parámetros recopilados.

Décimo segundo. Realización de las conclusiones con los resultados obtenidos.

4. MARCO TEÓRICO.

En este capítulo se abordarán aspectos generales y teóricos necesarios para la definición y desarrollo del proyecto. Se describirá el dispositivo de recepción y transmisión con que se realizará este proyecto, el NI-USRP 2932, así como el entorno de programación del software LabVIEW, los tipos de modulación empleados en este trabajo. Finalmente, se describirán las características del tipo de cifrado asimétrico empleado en la transmisión.

4.1. Modulación.

La modulación se define, según la American National Standard for Telecommunications, como la alteración sistemática de una señal, denominada portadora, en función de las características de otra señal, que puede contener información, llamada moduladora, con la finalidad de obtener una nueva señal más adecuada para la transmisión *[1]*. Estas técnicas permiten un mejor aprovechamiento del canal, una reducción sustancial de las antenas de transmisión, además de mejorar la resistencia de la señal transmitida contra posibles ruidos e interferencias.

El parámetro a modificar de la portadora puede ser la amplitud, la frecuencia, la fase, la posición o la duración del pulso. Según sea la naturaleza de la señal modulada es que se denomina el tipo de modulación, por esta razón, habrá sistemas de modulación con portadoras analógicas o digitales y sistemas con moduladoras analógicas o digitales *[2]*.

Tabla 1:
Tipos de modulación según la naturaleza de la onda portadora y moduladora.

Señal Moduladora	Señal Portadora	Señal Modulada	Codificación
Analógica	Analógica	Analógica	AM, FM, PM
Digital	Analógica	Analógica	ASK, FSK, PSK
Analógica	Digital	Digital	PCM y variantes
Digital	Digital	Digital	Banda Base

Fuente: Gil, V. P. Pomares, B. J. Candelas, H. F .A. (2010). *Redes y transmisión de datos* (*p.* 58). Texto docente/Universidad de Alicante.

Gil, Pomares y Candelas (2010) sugieren una clasificación de la codificación para enviar datos.

- *"Modulación analógica: Cuando se quiere transmitir por un medio analógico, y cuya señal portadora es analógica.*
- *Modulación digital: Cuando se quiere transmitir por un medio digital, y cuya señal portadora es digital"* (p. *58).*

El tipo de modulación se elige, entre otras cosas, dependiendo del tipo de servicio que se requiere, complejidad de los equipos empleados, calidad requerida, alcance requerido y ancho de banda disponible para la transmisión.

En esencia, hay tres técnicas de modulación para transmisión digital, por desplazamiento de frecuencia (FSK), modulación por desplazamiento de fase (PSK), y modulación por variación de amplitud (ASK).

El proceso de modulación se puede hacer más complejo con la intención de aumentar la capacidad de transmitir información sin aumentar el ancho de banda de la señal modulada. De los siguientes formatos de modulación mencionados, existe la posibilidad de hacer un sistema M-Ario.

En (4.1)[1] se muestra la expresión matemática para determinar los niveles del sistema M-Ario necesarios, según las necesidades de la transmisión. La letra "M" representa la cantidad de símbolos posibles para cierta cantidad de valores binarios.

$$N = log_2 M \qquad (Ec.4.1)$$

Se puede tener un mejor entendimiento de lo que representa un sistema M-ario si de la tabla 2 se relaciona "M" con la cantidad de condiciones posibles de salida con un número de "N" bits. Esto describe los posibles sistemas M-arios disponibles según los requerimientos de transmisión *[3]*.

Tabla 2:
Niveles de sistema M-Ario

N	1	2	3	4	5	6	7	8
M	2	4	8	16	32	64	128	256

Fuente: Sánchez, R. E. J. (2016). Recuperado de: https://telecomundo.wordpress.com/2016/10/16/modulaciones-m-arias-qam-y-qpsk/

De los niveles M-arios descritos en la tabla 2, se destacan para fines de este proyecto, las modulaciones BPSQ, QPSK y 8PSK.

[1] Relación de número de bits con número de condiciones posibles del sistema M-Ario.
Fuente: Tomasi, W. (2003). Comunicaciones digitales: *Sistemas de comunicaciones electrónicas* (p. 482), 4ta edición. México

4.1.1 Binary Phase Shift Keying *(BPSK)*

Es la técnica de modulación que se caracteriza por asignar fases distintas a la onda portadora, según la señal moduladora. En la figura 1, se observa la representación de los cambios de fase a cada uno de los símbolos de la fuente, con amplitud y frecuencia constante de forma directamente proporcional a la amplitud y frecuencia de la señal moduladora *[4]*.

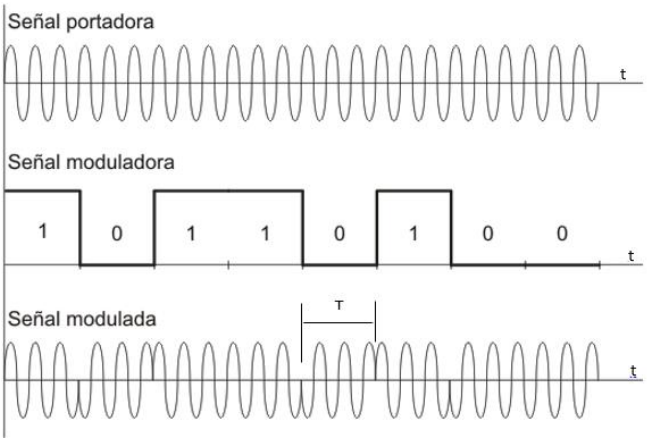


Figura 1. Modulación por desplazamiento de fase. En *Textos Científicos.* (2005). Recuperado de: https://www.textoscientificos.com/redes/modulacion/psk

Cuando M=2, suele representarse como BPSK, el sistema M-Ario más simple, tiene dos fases posibles para representar los dígitos binarios. Cuya expresión general de símbolo es representado por (4.2)[2] :

$$S_i(t) = \sqrt{\frac{2E}{T}}\cos\left(2\pi f_c t + \emptyset_i(t)\right) \qquad 0 \le t \le T_b \qquad i = 1, \dots, M \qquad (Ec.4.2)$$

Donde:

- La fase $\emptyset_i(t) = \frac{2\pi i}{M} \qquad i = 1, \dots, M$
- E es la energía del símbolo.
- T es la duración del símbolo.
- $f_c = \frac{n_0}{T}$, n_0 es un número entero que representa el número de oscilaciones producidas en la duración de un símbolo.

[2] Expresión general del símbolo para modulación BPSK. Fuente: Modulación Digital *(p. 8)*, por Murray, L, 2004, Universidad Nacional de Rosario/Área de comunicaciones Eléctricas.

Para este caso solo hay dos tipos de símbolo representados por (4.3) y (4.4)[3].

$S_1(t) = \sqrt{\frac{2E}{T}}\cos(2\pi f_c t)$ $(Ec.\,4.3)$, que representa el 1 binario.

$S_2(t) = \sqrt{\frac{2E}{T}}\cos(2\pi f_c t + \pi) = -\sqrt{\frac{2E}{T}}\cos(2\pi f_c t)$ $(Ec.\,4.4)$, que representa el 0 binario.

El diagrama de constelación que se muestra en la figura 2, representa la transmisión de las dos señales $S_1(t)\ y\ S_2(t)$. Estas están representada en un plano complejo que determina la posición de los estados de la señal en términos de amplitud y fase de acuerdo al esquema de modulación (representación de los máximos fasoriales) *[5]*. Resulta útil para visualizar el rango de error entre los símbolos que se trabajan; y el umbral de decisión que se encuentra en el receptor.

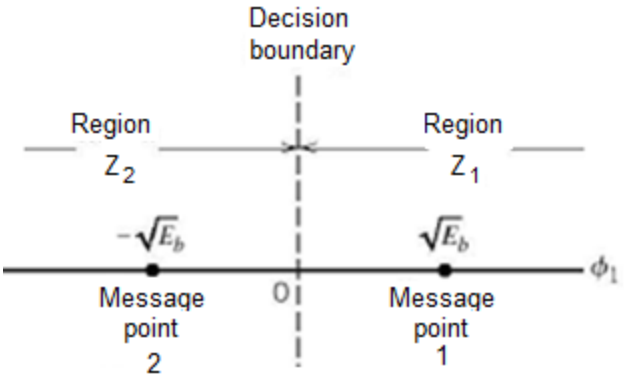


Figura 2: Diagrama de constelación para modulación BPSK. En *Modulación Digital* (*p.* 10), por Murray, L, 2004, Universidad Nacional de Rosario/Área de comunicaciones Eléctricas.

Esta modulación es considerada de las más robustas debido a la diferencia de grados entre los puntos de la constelación y se utiliza a menudo en comunicaciones inalámbricas de larga distancia, en estándares como CDMA, WiMAX (16d, 16e), WLAN 11a, 11b, 11g, 11n, satélite, DVB, sólo por mencionar algunos *[6]*.

4.1.2 Quadrature Phase-Shift Keying *(QPSK)*

La modulación por desplazamiento de fase en cuadratura es otra técnica de transmisión de información binaria. Cuando M=4, se transmiten dos bits por símbolo, es decir, un símbolo no representa 1 o 0 (como era el caso de la modulación BPSK), sino que representa 00, 01, 10, 11, con esto se sabe que habrá cuatro posibles

[3] Representación del símbolo para modulación BPSK. Fuente: Modulación Digital *(p. 9)*, por Murray, L, 2004, Universidad Nacional de Rosario/Área de comunicaciones Eléctricas.

cambios de fase en la portadora. La separación máxima entre las cuatro posibles variaciones de fase es de 90°, de modo que entre ellas sean ortogonales y para que el receptor tenga menos dificultades de distinguir entre un estado y otro *[7]*.

Para realizar la modulación en cuadratura se emplean 2 portadoras simultáneamente, esto hace que se doble la tasa de transmisión de información sin aumentar el ancho de banda, ni la probabilidad de error. La razón por la cual es posible recuperar la información efectivamente en el receptor es que las funciones portadoras son ortogonales.

La figura 3 explica de manera gráfica como la señal binaria que será modulada, se envía a un convertidor serie/paralelo para obtener de esta forma, dos señales con diferente periodo, siendo uno el doble que el inicial (frecuencia mitad) que se denomina I (in fase) y el otro Q (quadrature) *[8]*.

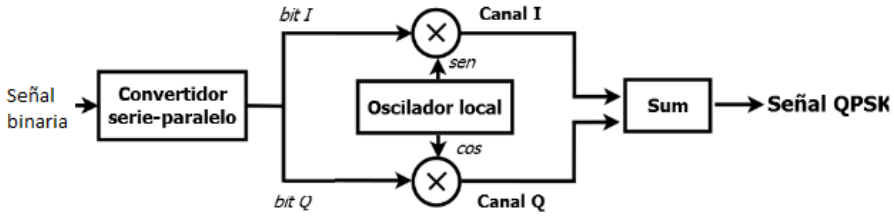


Figura 3: Modulador QPSK. En *Implementación de un modulador- demodulador digital QPSK en base a un FPGA como prototipo para un microsatélite* (*p.31*), por Castañeda A. O. D. (2015). México.

Cada una de las señales se modula por separado, con las 2 portadoras ortogonales entre sí. Finalmente las dos señales resultantes se suman y se obtiene la señal modulada en cuadratura. En la figura 4 se muestra el cambio de fase en la señal modulada según los bits de la señal moduladora (entrada).

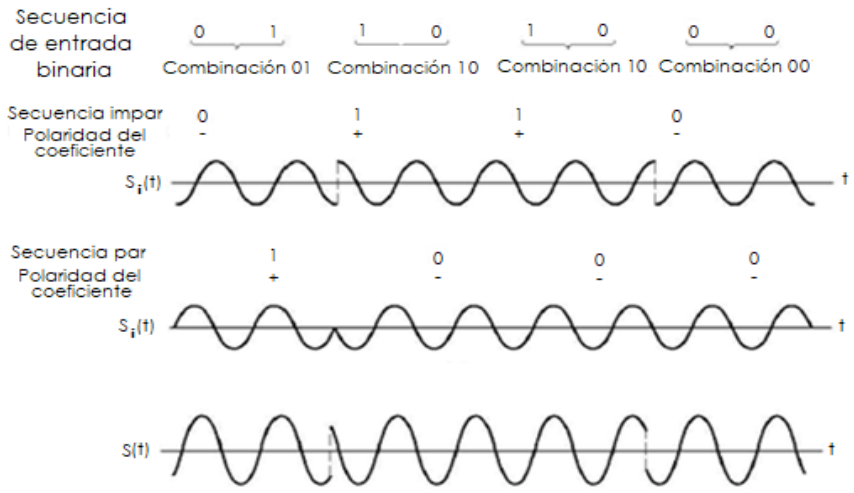


Figura 4: Modulación por desplazamiento de fase y cuadratura. En *Modulación Digital* (*p.* 22), por Murray, L, 2004, Universidad Nacional de Rosario/Área de comunicaciones Eléctricas.

La expresión matemática general de esta modulación está representada por (4.5)[4] y sus variantes según el índice i:

$$S_i(t) = \sqrt{\frac{2E}{T}}\cos(2\pi f_c t + \theta) = \sqrt{\frac{2E}{T}}\cos\left(2\pi f_c t + (2i-1)\frac{\pi}{4}\right) \quad 0 \le t \le T_b \quad i = 1,..,M \quad (Ec.4.5)$$

$$S_1(t) = \sqrt{\frac{2E}{T}}\cos\left(2\pi f_c t + \frac{\pi}{4}\right) \qquad S_2(t) = \sqrt{\frac{2E}{T}}\cos\left(2\pi f_c t + \frac{3\pi}{4}\right) \qquad (Ec.4.6)$$

$$S_3(t) = \sqrt{\frac{2E}{T}}\cos\left(2\pi f_c t + \frac{5\pi}{4}\right) \qquad S_4(t) = \sqrt{\frac{2E}{T}}\cos\left(2\pi f_c t + \frac{7\pi}{4}\right) \qquad (Ec.4.7)$$

Donde:

- E es la energía de símbolo.
- T periodo de símbolo.
- $f_c = \frac{n_0}{T}$, n_0 es un número entero que representa el número de oscilaciones producidas en la duración de un símbolo.

Tabla 3:
Representación de entradas binarias en modulación QPSK.

Código Gray	Fase de la señal	S_{i1}	S_{i2}
10	$\pi/4$	$+\sqrt{E/2}$	$-\sqrt{E/2}$
00	$3\pi/4$	$-\sqrt{E/2}$	$-\sqrt{E/2}$
01	$5\pi/4$	$-\sqrt{E/2}$	$+\sqrt{E/2}$
11	$7\pi/4$	$+\sqrt{E/2}$	$+\sqrt{E/2}$

Fuente: *Modulación Digital* (*p.* 20), por Murray, L, 2004, Universidad Nacional de Rosario/Área de comunicaciones Eléctricas.

Cada una de las cuatro posibles fases de salida en esta modulación, tiene exactamente la misma amplitud. Debido a que la región de decisión entre los estados pares es menor, comparado con la BPSK, se toma la precaución de reducir la probabilidad de error en los símbolos digitales con la codificación de la información en la fase de la señal de salida. La regla de codificación que se toma para esta modulación es con código Gray ya que se caracteriza por tener una diferencia de un solo bit entre dos símbolos que estén a una distancia mínima *[9]*.

[4] Representación del símbolo para modulación QPSK. Fuente: Modulación Digital *(p. 19)*, por Murray, L, 2004*,* Universidad Nacional de Rosario/Área de comunicaciones Eléctricas.

En la figura 5, se muestra la constelación correspondiente a la modulación QPSK, con sus cuatro diferentes símbolos y el umbral de decisión según su codificación.

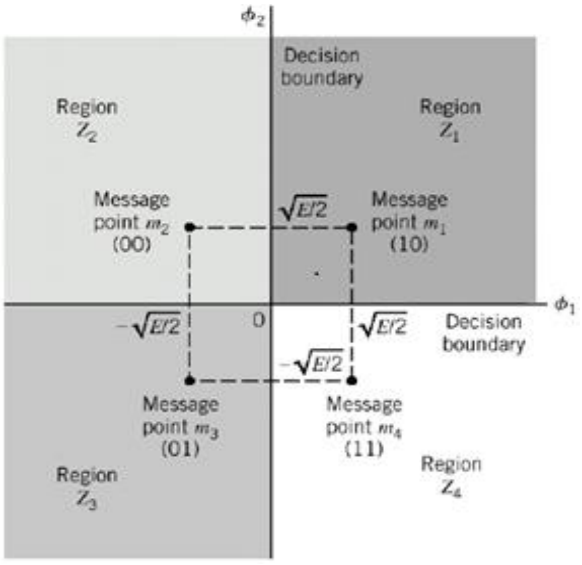


Figura 5: Diagrama de constelación para modulación QPSK. En *Modulación Digital* (*p. 2*1), por Murray, L, 2004, Universidad Nacional de Rosario/Área de comunicaciones Eléctricas.

Las aplicaciones de la modulación QPSK son similares a las de BPSK, se usan en estándares inalámbricos celulares, como GSM, CDMA, LTE, WiMAX fijo y móvil, aplicaciones de TV satelital, entre otras, También es un sistema de modulación robusto comparado con otros. Tiene la capacidad de doblar la tasa de transmisión en comparación con la modulación BPSK *[10]*.

4.1.3 Eight Phase-Shift Keying *(8PSK)*

Una modulación de 8 fases sigue siendo un sistema M-Ario, donde M= 8, por lo que cada símbolo estará representado por 3 bits y podrán existir hasta 8 cambios de fase distintos en la portadora *[11]*.

La codificación sigue empleándose con código Gray, debido a que la probabilidad de que ocurran error de transición aumenta conforme cambian más bits simultáneamente, el hecho de que el código Gray cambie un bit entre símbolos da la ventaja de estabilizar la transición antes de cometer un error.

La figura 6 muestra la separación máxima entre cada fase de la modulación y su representación de símbolo con la codificación en código Gray.

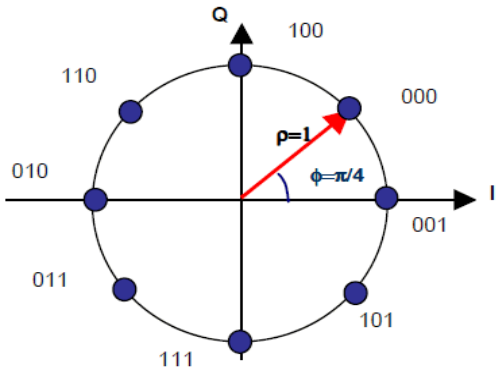


Figura 6: Diagrama de constelación para modulación 8PSK. En KEYSIGHT technologies, por Agilent Technologies, 2010.

La tasa de transmisión sigue el mismo razonamiento que para la modulación QPSK, por lo que se comprime a la tercera parte de la tasa de transmisión original.

La desventaja de los sistemas 8PSK radica en que se requiere de circuitos mucho más complejos que QPSK. Esto afecta el presupuesto de un sistema de transmisión. Además, dado que 8PSK transmite más bits por símbolo que QPSK, requiere una mayor potencia de transmisión y puede tener una tasa de error de bit más alta.

Esta técnica de modulación digital se usa en sistemas de video broadcast, aviones y sistemas satelitales *[12]*.

4.2 Parámetros de eficiencia en la transmisión

Para que un enlace de comunicaciones tenga un buen funcionamiento es necesario y de suma importancia que el sistema cumpla con ciertas especificaciones en los parámetros de trabajo.

4.2.1 Ruido

El ruido se constituye por todas aquellas señales indeseables que se introducen a lo largo del trayecto de una transmisión. Se considera como ruido a toda señal fortuita e impredecible (generado por causas internas y externas al sistema) que altera la señal deseada por el receptor *[13]*.

Las principales fuentes de ruido externo son las generadas por el hombre o por la naturaleza como el ruido atmosférico con incidencia en frecuencias por debajo de los

20 MHz, ruido espacial con incidencia en el rango de frecuencias de 8 MHz a 1.5 GHz. Mientras que el ruido interno puede ser provocado por el ruido de disparo (se debe a la llegada aleatoria de portadoras sobre un elemento a la salida de un aparato electrónico) y ruido térmico (producido por el movimiento cinético, térmico y aleatorio de los electrones, sobre cualquier conductor) cuya ecuación está descrita por (4.8)[5].

$$N(w) = KTB \qquad (Ec. 4.8)$$

Donde:
N = potencia de ruido térmico
K = constante de Boltzman $1.38x10^{-23}\,\frac{J}{K}$
T = temperatura absoluta (temperatura ambiente en °C + 273K)
B = ancho de banda (Hz)

Dado que la densidad espectral de potencia es constante y tiene todas las componentes de frecuencia en igual proporción, se suele llamar a este ruido como ruido blanco, por su analogía con la luz blanca *[14]*. El ruido es uno de los principales factores que limitan el desempeño de un sistema de comunicaciones.

4.2.2 Relación Señal a Ruido *(SNR)*

La relación señal a ruido corresponde a la relación del nivel de potencia de la señal con respecto al nivel de potencia del ruido, es un parámetro de calidad en un sistema de comunicaciones normalmente evaluado en el lado del receptor. Entre más alta sea la relación señal a ruido, mejor será la calidad del sistema *[15]*.

La relación Señal a Ruido se expresa frecuentemente en dB como se muestra en (4.9)[6]. Si el nivel de ruido aumenta, la SNR disminuye, dando a entender que la calidad del sistema se está deteriorando.

$$SNR = \frac{P_S}{P_N}\,(W) = 10\,log_{10}\left(\frac{P_S}{P_N}\right)\,(dB) \qquad (Ec. 4.9)$$

Donde:
P_S : Potencia de la señal
P_N : Potencia del ruido

[5] Expresión matemática para el ruido térmico. Fuente: Tomasi, W. (2003). Comunicaciones digitales. *Sistemas de comunicaciones electrónicas* (p. 37) (4ta edición). México.

[6] Expresión matemática para determinar la relación señal a ruido del sistema. Fuente: Juárez, O. (2016). *Estudio de Técnicas de Modulación Mediante Radios NI USRP*, (p. 14). Universidad Nacional Autónoma de México.

4.2.3 Eficiencia espectral

Una de las características fundamentales de un canal de transmisión es el denominado ancho de banda, que se detalla como el rango de frecuencias que ocupa el espectro de una señal en la que se concentra la mayor parte de su potencia. Se puede calcular a partir de una señal temporal sometida al análisis de Fourier. Las frecuencias que se encuentran entre esos límites se denominan frecuencias efectivas *[16]*.

El ancho de banda mínimo necesario para transmitir portadoras M-Arias se determina con (4.10)[7]:

$$B_{min} = \frac{R_b}{log_2 M} = \frac{R_b}{N}\ (Hz) \qquad (Ec. 4.10)$$

Donde:
B_{min} = ancho de banda mínimo. (Hz)
R_b = tasa de transmisión de bits (bits/seg)
M = cantidad de estados o variaciones en la señal modulada.
N = cantidad de bits por estado.

La eficiencia espectral o densidad de información es uno de los muchos parámetros que define la calidad de una modulación digital y nos indica cuánta información es posible transmitir sobre un ancho de banda determinado.

La eficiencia espectral de un canal de comunicación se calcula mediante el cociente entre la tasa de transmisión (Rb) y el ancho de banda mínimo necesario (B_{min}), el cual es determinado por el esquema de modulación empleado, como lo muestra (4.11)[8].

$$\eta = \frac{R_b\left(\frac{bits}{seg}\right)}{B_{min}(Hz)} = N \qquad (Ec. 4.11)$$

Cuando mayor sea este valor, mejor aprovechado estará el ancho de banda y mejor será el sistema de modulación. Aunque en general, la eficiencia espectral se normaliza a un ancho de banda de 1 Hz y en consecuencia indica la cantidad de bits por hertz que se pueden propagar a través del medio *[17]*.

---

[7] Ancho de banda mínimo. Fuente: Juárez, O. (2016). *Estudio de Técnicas de Modulación Mediante Radios NI- USRP*, (p. 12). Universidad Nacional Autónoma de México.

[8] Eficiencia del ancho de banda. Fuente: Juárez, O. (2016). *Estudio de Técnicas de Modulación Mediante Radios NI- USRP*, (p. 12). Universidad Nacional Autónoma de México.

Tabla 4:
Resumen de las características de modulación digital

Modulación	Codificación (bits)	Ancho de banda	Eficiencia de ancho de banda (bps/Hz)
BPSK	1	Rb	1
QPSK	2	Rb/2	2
8 PSK	3	Rb/3	3

Fuente: *Sistemas de comunicaciones electrónicas* (p. 505), por Tomasi, W, 2003. Pearson Education.

El análisis anterior deduce que sería factible aumentar indefinidamente la capacidad de un canal tan solo con incrementar el número de estados empleados, pero uno de los factores que realmente delimita la eficiencia espectral es el ruido.

En presencia de ruido la capacidad máxima de un canal obedece al teorema de Shannon-Hartley, que establece la capacidad de un canal (con ancho de banda finito y una señal continua que sufre un ruido gaussiano) considerando todas las posibles técnicas de codificación de niveles múltiples y polifásicas.

Para indicar la capacidad máxima del canal *C,* se emplea (4.12)[9]*:*

$$C = B\ log_2\left(1 + \frac{S}{N}\right) \qquad (Ec. 4.12)$$

Donde:
B = ancho de banda (Hz)
S = potencia media de la señal recibida.
N =potencia media del ruido.

Shannon estableció que es posible obtener una transmisión libre de errores si se considera transmitir a una tasa de transmisión menor o igual que la capacidad del canal $(R_b \leq C)$. En el caso inverso, la probabilidad del error en el receptor se incrementaría sin límite mientras se aumente la tasa. Es por esta razón que no se puede transmitir ninguna información útil por encima de la capacidad del canal *[18]*.

[9] Capacidad máxima de un canal. Fuente: Juárez, O. (2016). *Estudio de Técnicas de Modulación Mediante Radios NI- USRP*, (p. 15). Universidad Nacional Autónoma de México.

4.2.4 Tasa de error de bit *(BER)*

En los sistemas de comunicación digital, el objetivo del receptor es seleccionar correctamente los símbolos de mensaje transmitidos fuera de un conjunto finito. La presencia de ruido de canal complica la tarea y causa errores de bit.

Uno de los criterios de rendimiento más importante en un sistema de comunicación digital es la relación de error de bit.

El término de la tasa o frecuencia de errores (BER) es un registro empírico del funcionamiento real de un sistema en cuanto a errores, donde un error corresponde a la recepción de un 1 cuando un 0 fue transmitido y viceversa. El BER corresponde entonces a la proporción de bits errados respecto a los bits transmitidos en un determinado intervalo de tiempo *[19]*.

De (4.13)[10] se determina la relación entre los bits recibidos erróneamente de los bits transmitidos originalmente.

$$BER = \frac{\#\ de\ bits\ recibidos\ erroneos}{\#\ de\ bits\ transmitidos} \qquad (Ec. 4.13)$$

4.2.5 Tasa de error de modulación *(MER)*

La Tasa de Error de Modulación o por sus siglas inglesas, MER (Modulation Error Ratio) es un factor de eficiencia de suma importancia, ya que expresa la cantidad de dispersión que sufren los máximos fasoriales reales (transmitidos o recibidos), respecto a una determinada constelación ideal. Esta es una herramienta cuantitativa que permite valorar que tan buena es una señal modulada digitalmente.

El MER aporta información importante pues combina los efectos del ruido, errores de fase, error de cuadratura, y demás.

La figura 7 muestra, de forma gráfica, un indicador de calidad de la señal modulada. El término *I/Q* es una abreviatura para *en fase* y *en cuadratura,* y que representan un plano complejo que determina la posición de los estados de la señal en términos de amplitud y fase de acuerdo al esquema de modulación (representación los máximos fasoriales).

[10] Expresión matemática para determinar la tasa de error de bit. Fuente: Pallares, J. (2009). *VII Congreso Instaladores PROMAX.* (p. 5), PROMAX.

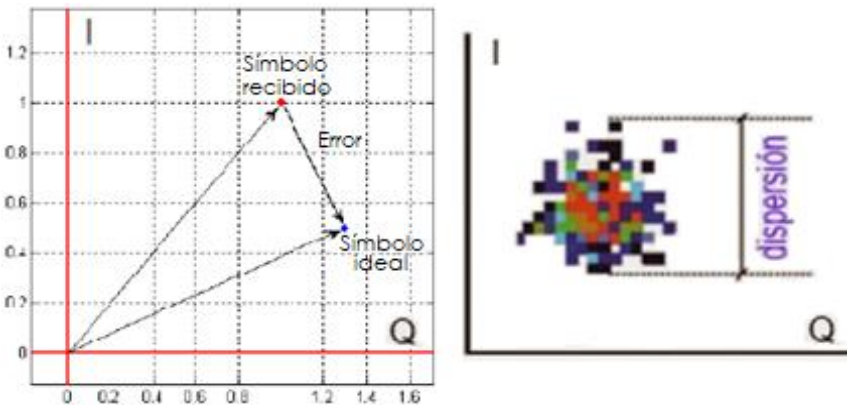


Figura 7: Representación gráfica del MER. En *Estudio de técnicas de modulación mediante radios NI USRP,* por Juárez B. O. 2016, Universidad Nacional Autónoma de México.

El *MER* representa la diferencia vectorial entre la posición ideal del símbolo en la constelación frente al valor detectado en condiciones no ideales de interferencia, cuantificado como el módulo del vector diferencia entre ambos.

Matemáticamente y como se expresa en (4.14)[11], el *MER* se define como la relación de la cantidad de potencia que se recibe o transmite de la forma esperada o deseada (constelación ideal), entre la cantidad potencia de las señales e imperfecciones que provoquen una desviación en los símbolos de una constelación ideal (potencia de error), para un determinado número de símbolos. Este valor puede ser expresado en dB o en tanto por ciento *[20]*.

$$MER = 10 \log_{10} \left(\frac{\sum_{j=1}^{N} \left(I_j^2 + Q_j^2 \right)}{\sum_{j=1}^{N} \left(\delta I_j^2 + \delta Q_j^2 \right)} \right) dB \qquad (Ec. 4.14)$$

Donde los datos I / Q muestran los cambios en la magnitud (o amplitud) y la fase de una onda sinusoidal.

4.2.6 Antenas

En comunicaciones inalámbricas, la onda portadora de información es propagada desde el transmisor por medio de una antena. Según la definición de la IEEE una antena es un transductor que forma parte del sistema de telecomunicaciones diseñado específicamente para radiar o recibir ondas electromagnéticas *[21]*.

[11] Expresión matemática para determinar la tasa de error de modulación. Fuente: Pallares, J. (2009). *VII Congreso Instaladores PROMAX.* (p. 11), PROMAX.

Para fines de este proyecto, el USRP empleará antenas modelo VERT400, un monopolo omnidireccional tribanda cuyas bandas principales de operación se encuentran en los 144MHz (con 0dBi a 1/4 de onda), los 400MHz (con 0dBi a 1/4 de onda) y los 1200MHz (con 3.4dBi a 5/8 de onda). Tiene una longitud física de 17 centímetros, posee un conector SMA y soporta una potencia máxima de 10 watts *[22]*.

En la práctica las antenas realmente no son omnidireccionales, sino que concentran energía en unas direcciones a costa de disminuirla en otras. Para modelar este comportamiento se hace uso de un parámetro denominado ganancia directiva.

La ganancia directiva (G_D) es la relación entre la densidad de potencia radiada a una distancia fija y en una determinada dirección y la densidad de potencia que habría sido radiada a esa misma distancia por una antena omnidireccional ideal.

Teniendo en cuenta la ganancia directiva; la potencia radiada por una antena transmisora en dirección de la antena receptora será $W_T G_D$ y la densidad de potencia recibida sobre el receptor como lo muestra (4.15)[12]:

$$P = \frac{W_T}{4\pi R^2}\, G_D \qquad (Ec. 4.15)$$

Donde:
P = densidad de potencia del receptor.
W_T = potencia radiada por el transmisor.
R = radio de la superficie que abarca la radiación de la antena
G_D = ganancia directiva del transmisor.

Un análisis de la potencia de enlace tiene como objetivo determinar si la potencia recuperada en el receptor es suficiente o aceptable para que la señal deseada pueda ser percibida, en este se consideran todas las ganancias y pérdidas existentes; la Potencia Isotrópica Radiada Efectiva *(PIRE)*, está definida en la dirección máxima de directividad de la antena transmisora *[23]*.

Se calcula a través del producto de la potencia radiada y la directividad de la antena *(D)*, mediante (4.16)[13]:

$$PIRE = W_T D \qquad (Ec. 4.16)$$

[12] Densidad de potencia radiada a una distancia fija. Faúndez, M. (2001). *Sistemas de comunicaciones*. (p.65). Barcelona.
[13] Potencia isotrópica radiada efectiva. Faúndez, M. (2001). *Sistemas de comunicaciones*. (p.68). Barcelona.

4.3 Herramientas de desarrollo.

Con los grandes avances en las telecomunicaciones inalámbricas han aparecido diversas tecnologías para el intercambio de información con requisitos cada vez más exigentes. Iván Pinar y Juan Murillo (2016) señal que "*las incompatibilidades entre las diferentes tecnologías han supuesto un problema a la hora de reutilizar equipos o prestar determinados servicios*". La tecnología del Software Defined Radio (SDR) surge como opción para solucionar los inconvenientes de compatibilidad e interoperabilidad, definiendo los procedimientos y técnicas que comúnmente se implementaban por hadware (moduladores, amplificadores, codificadores, filtros, entre otros.), en problemas de software, logrando así un cambio dinámico, automático y eficiente entre tecnologías introduciendo más flexibilidad al sistema, facilitando además la capacidad de una rápida reconfiguración del enlace y sus parámetros (frecuencia, ancho de banda, modulación, potencia, y demás) *[24]*.

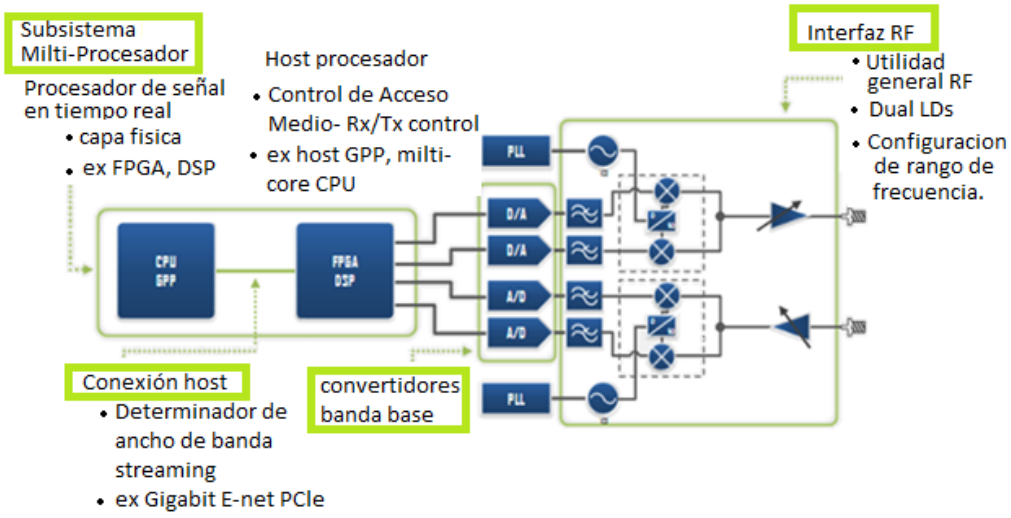


Figura 8: Arquitectura de un SDR. En *Aerospace and Defence Forum (p. 4),* por National Instruments, 2016.

En la figura 8 se muestra la arquitectura del Universal Software Radio Peripheral (USRP), que es un transceptor de radiofrecuencia sintonizable, del fabricante actual National Instruments, diseñado para la creación de prototipos de sistemas de comunicación inalámbricos combinando la tecnología de radio definido por software y mediante plataformas de desarrollo como Labview, GNURadio, Matlab, etc *[25]*.

La principal ventaja de un USRP es que mediante la conexión a una PC toma el enfoque de un dispositivo SDR. De acuerdo a las distintas mejoras que se han desarrollado sobre estos dispositivos y al tipo de comunicación que tienen con una PC; la transferencia de muestras se hace a través de una interface Gigabit Ethernet

(incrementando la transferencia de muestras y habilitando un puerto de expansión para la implementación de sistemas *MIMO*).

Los transceptores de radio NI USRP-293x definidos por software están diseñados para la enseñanza e investigación de comunicaciones inalámbricas. Para fines de este documento se describirá y utilizará el dispositivo NI USRP 2932.

4.3.1 Hardware del NI USRP 2932.

Para poder llevar a cabo el desarrollo de un sistema de comunicaciones basado en software, el USRP cuenta internamente con dos niveles de tarjeta. El primero es la tarjeta principal, que se muestra en la figura 9, también denominada tarjeta madre o motherboard.

Esta placa es la encargada, a grandes rasgos, de comunicar la señal generada vía software desde la PC hacia el módulo de RF, el cuál realizará los cambios necesarios a la señal para trasportarla a la frecuencia requerida por la aplicación.

Figura 9: Tarjera madre USRP 2932. En *Turbo envió: Una estrategia de retransmisión rápida para enviar paquetes en redes inalámbricas AD HOC,* por Jaimes, B. O. 2017.

En ella se encuentra el FPGA (*Field Programable Gate Array*) el cual realiza funciones reprogramables específicas ya sea como memoria (FLIP-FLOP tipo D), como multiplexor o con una función lógica tipo AND, OR, XOR, también se encuentran los convertidores ADCs y DACs, la alimentación y la conexión vía Ethernet.

Su función comienza a la salida de la PC y acaba cuando la señal atraviesa el convertidor digital analógico, cuando se encuentra operando como transmisor. Si está operando como receptor su trabajo empieza cuando la tarjeta hija le entrega la señal y termina cuando la señal es conducida hacia la PC y realiza la conversión digital a analógico o cualquiera que sea la descripción que el usuario requiere de la señal *[26]*.

El segundo nivel se compone de las tarjetas secundarias, hijas o daughterboards. En la figura 10 se muestra como es la tarjeta secundaria, físicamente, que existe dentro del dispositivo NI-USRP, empleada para la transmisión y recepción.

Figura 10: Tarjeta hija del USRP 2932. En *Turbo envió: Una estrategia de retransmisión rápida para enviar paquetes en redes inalámbricas AD HOC,* Jaimes, B. O. 2017.

Juan Montero (2014) considera que, la función de la tarjeta hija empieza a la salida del convertidor (DAC) y termina cuando la señal es conducida hacia el conector SMA para ser transmitida, si el dispositivo está operando como un transmisor. Si el dispositivo está operando como receptor, el trabajo de la tarjeta hija inicia cuando la señal llega al conector SMA y finaliza cuando la señal es conducida hacia el convertidos analógico digital, por ello es que se entiende que este tipo de placas están conectadas físicamente a la tarjeta madre (p. 30).

Y es así es como el USRP puede trabajar con varias tarjetas secundarias, que pueden funcionar como transmisores, receptores o transceptores.

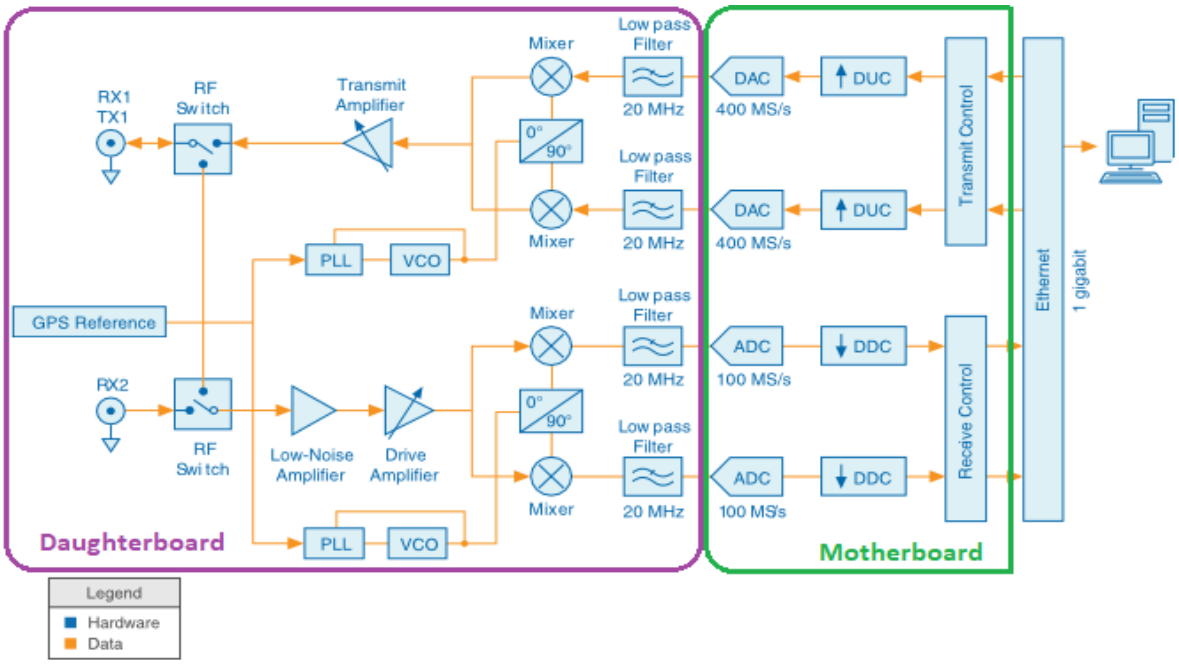


Figura 11: Diagrama de los bloques que conforman el NI-USRP 2932. En *Hands-On: Introduction to software-defined radio with LabVIEW an USRP,* por National Instruments, 2013.

Como la figura 11 muestra, el NI-USRP 2932 está equipado con el Xilinx Spartan 3ADSP3400A FPGA en la motherboard, el WBX 50-2200MHz RX / TX como daughterboard y un módulo GPS opcional que incluye un reloj de referencia disciplinado. El reloj de referencia se comparte entre las rutas de transmisión y recepción, de donde se deriva el oscilador local (LO), y proporciona una precisión de frecuencia mejorada, capacidades de sincronización e información de posición de GPS.

La daughterboard WBX tiene dos puertos SMA estándar uno de los cuales se puede configurar como TX o RX desde la interface programable (LabVIEW) y el otro sólo funciona como RX. Ambos puertos pueden manejar señales con frecuencias que van desde los 400MHz a los 4.4GHz *[27]*.

4.3.2 Parámetros NI-USRP 2932.

Los parámetros configurables del dispositivo USRP 2932 para transmisión y recepción son:

- Frecuencia de la portadora
  Configurable en un rango de frecuencias entre los 400MHz a los 4.4GHz, con una resolución de 1 kHz, para el transmisor y receptor.

- Ancho de banda
  Configurable hasta un máximo ancho de banda en tiempo real instantáneo de 20MHz a 16 bits ó 40MHz a 8 bits.

- Ganancia de la antena
  Configurable para el transmisor en un rango de 0 dB – 31 dB y con una potencia máxima de salida de 50mW a 100mW (17 dBm a 20 dBm), con resolución de 1 dB. Configurable para el receptor en un rango de 0 dB – 31.5 dB, con resolución de 0.5 dB y con una potencia máxima de entrada de 0 dBm (1mW), debido a este límite, se incluye un limitador de 0 dBm en la caja frontal de RF para evitar que ingrese una potencia excesiva en el puerto de recepción.

- Muestras por símbolo
  El dispositivo es configurable hasta un máximo de 25MS/s a 16 bits ó 50MS/s a 8 bits (dependiendo de la configuración de la red y capacidades de la computadora del usuario, entre otros).

La figura 12, extraída del manual de los dispositivos NI-USRP, indica cuales son los parámetros configurables y el rango de cada uno, además de las características del hardware y sus rangos de operación.

Transmitter

Frequency range	400 MHz to 4.4 GHz
Frequency step	<1 kHz
Maximum output power (P_{out})	50 mW to 100 mW (17 dBm to 20 dBm)
Gain range	0 dB to 31 dB
Gain step	0.5 dB
Maximum instantaneous real-time bandwidth	
16-bit sample width	20 MHz
8-bit sample width	40 MHz
Maximum I/Q sampling rate	
16-bit sample width	25 MS/s
8-bit sample width	50 MS/s
DAC	2 channels, 400 MS/s, 16 bit
DAC spurious-free dynamic range (sFDR)	80 dB

Receiver

Frequency range	400 MHz to 4.4 GHz
Frequency step	<1 kHz
Gain range	0 dB to 31.5 dB
Gain step	0.5 dB
Maximum input power (P_{in})	0 dBm
Noise figure	5 dB to 7 dB
Maximum instantaneous real-time bandwidth	
16-bit sample width	20 MHz
8-bit sample width	40 MHz
Maximum I/Q sample rate	
16-bit sample width	25 MS/s
8-bit sample width	50 MS/s
Analog-to-digital converter (ADC)	2 channels, 100 MS/s, 14 bit
ADC sFDR	88 dB

Figura 12: Parámetros de Tx y Rx del NI-USRP 2932. En *Software Defined Radio Device Manual.* Por National Instruments, 2017.

Las señales entrantes al puerto pasan por el amplificador de bajo ruido y el amplificador de accionamiento. El bucle de enganche de fase (PLL) controla el oscilador (VCO) para que los relojes del dispositivo y el oscilador local (LO) puedan bloquearse en frecuencia a la señal de referencia. La señal resultante se mezclan utilizando un receptor de conversión directa (DCR) para componentes I / Q de banda base, que se muestrean mediante un convertidor analógico-digital de 2 canales, 100 MS / s, 14 bits (ADC).

Los datos I / Q digitalizados siguen trayectorias paralelas a través de un proceso de conversión descendente digital (DDC) que mezcla, filtra y diezma la señal de 100 MS / s de entrada a una tasa de transmisión especificada por el usuario. Las muestras con conversión descendente, cuando se representan como números de 32 bits (16 bits cada uno para I y Q), pasan a la computadora a través de una conexión Gigabit Ethernet estándar.

El uso de los filtros diezmadores o interpoladores se emplea para sincronizar las distintas tasas binarias con las que trabaja el enlace Gigabit Ethernet y el que el usuario requiere en la aplicación.

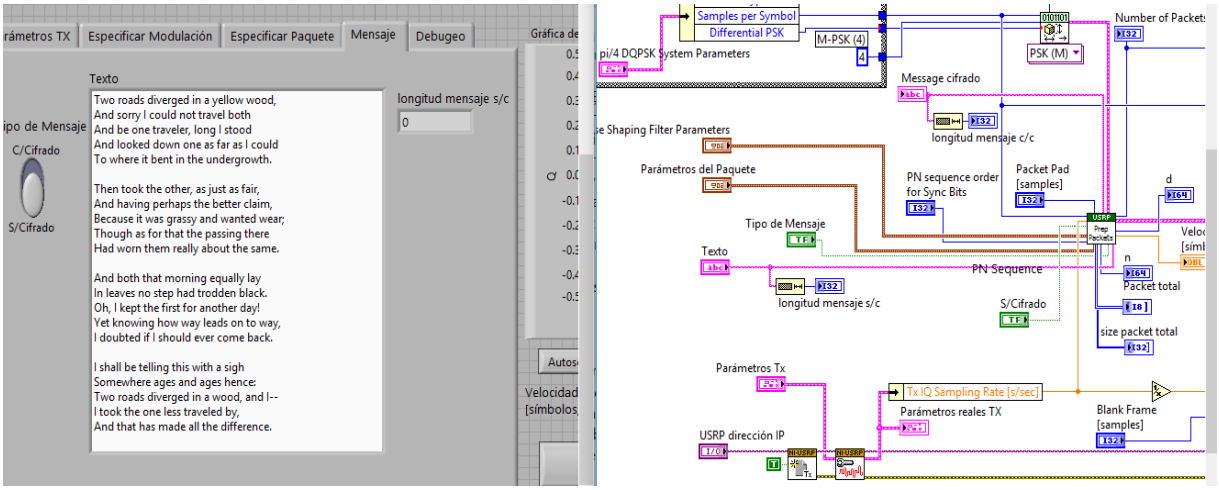
Para la transmisión, las muestras de señal I / Q de banda base son sintetizadas por la computadora y alimentadas al USRP. El hardware USRP interpola la señal entrante a 400 MS / s mediante un proceso digital de conversión ascendente (DUC) y luego convierte la señal a analógica, por medio de un convertidor digital-analógico (DAC) de doble canal y 16 bits. El filtro de paso bajo reduce el ruido y los componentes de alta frecuencia en la señal. La señal analógica resultante se mezcla a la frecuencia portadora especificada por el usuario. El PLL controla el VCO para que el dispositivo marque y LO pueda bloquearse en frecuencia a una señal de referencia. El amplificador de transmisión amplifica la señal y transmite la señal a través de la antena *[28]*.

4.3.3 Entorno de programación LabVIEW

En este capítulo se detallará el software que se ha utilizado para llevar a cabo la interacción con el hadware NI-USRP 2932 y el procesamiento de la señal en banda base, que corresponde a su vez a una parte fundamental en la implementación de algoritmos de comunicación que procesan las señales recibidas y sintetizan las señales para la transmisión.

El Laboratory Virtual Instrumentation Engineering Workbench (LabVIEW) es una plataforma de diseño de sistemas y entornos de desarrollo para un lenguaje de programación visual, desarrollado con el propósito de crear programas orientados al control, automatización, proceso y adquisición de datos (DAQ).

LabVIEW es una herramienta gráfica de POO basado en bloques, los programas hechos en LabVIEW contienen subrutinas que se conocen como "Instrumento virtual" (VI), cada VI consta de dos partes principales: el panel frontal y el diagrama de bloques, como se muestra en la figura 13.



a) *b)*

Figura 13: a) Panel frontal; b) Diagrama de bloques. En *Prácticas NI-USRP*, 2018.

El panel frontal es utilizado para interactuar con el usuario cuando el programa está corriendo, el usuario puede controlar el programa, cambiar entradas y ver datos actualizados en tiempo real. Los controles e indicadores en el panel frontal permiten al usuario introducir o extraer datos de un instrumento virtual en ejecución, cada control e indicador tiene su correspondiente en el diagrama de bloques *[29]*.

El diagrama de bloques contiene el código fuente gráfico representado en íconos que realizan determinadas funciones que incluyen estructuras incorporadas en las bibliotecas de LabVIEW VI.

La ejecución de un programa en LabVIEW está determinada por la estructura de un diagrama de bloques gráficos donde el programador conecta diferentes nodos de funciones dibujando cables entre ellos. Sin embargo, LabVIEW puede ejecutar procesos paralelos ya que múltiples nodos se pueden ejecutar simultáneamente *[30]*.

Las principales funciones que utiliza LabVIEW para interactuar con el NI-USRP se agrupan en categorías según su funcionalidad, como se muestra en la figura 14.

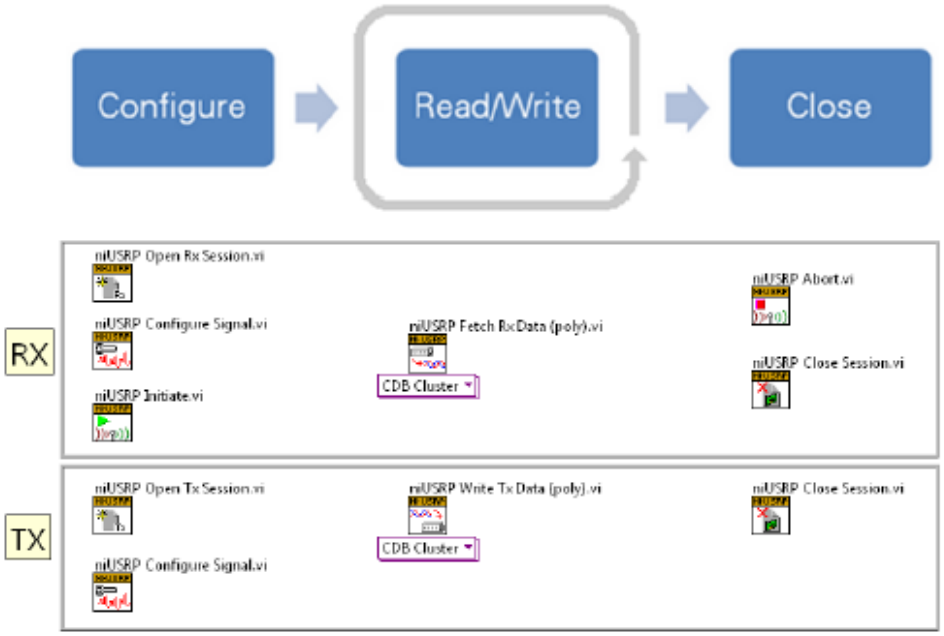


Figura 14: Principales funciones de LabVIEW para comunicación con NI-USRP. En *Hands-On: Introduction to software-defined radio with LabVIEW and USRP,* por National Instruments, 2013.

Los principales bloques VI que permiten la elaboración de cualquier tipo de esquema de comunicación a través de los dispositivos NI-USRP, están incluidos en LabVIEW Modulation Toolkit *[31]*.

A continuación se describirán brevemente la utilidad de cada VI empleado para la comunicación.

niUSRP Open Rx Session VI / niUSRP Open Tx Session VI

Es el VI empleado para crear una sesión entre el software y el dispositivo USRP útil para la recepción o transmisión de señales de radiofrecuencia. Establecen un identificador específico para cada flujo de datos que se utiliza para identificar esta sesión del instrumento en los posteriores NI-USRP VIs.

niUSRP Configure Signal VI

Este VI puede ser usado en el dispositivo de recepción o transmisión, es el encargado de establecer los parámetros definibles del USRP:

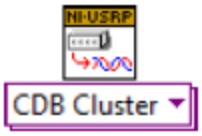
- IQ rate: especifica la velocidad de muestreo. Es el resultado de multiplicar la tasa de símbolos por las muestras por segundo.

- Carry frecuency: frecuencia portadora
- Gain: ganancia agregada en dB aplicada a la señal de RF.
- Acctive antena: especifica el puerto de la antena que se utilizará en el canal.

Hay que tener en cuenta que no todos los valores en frecuencia y ganancia son válidos, estos dependen directamente de la capacidad de las tarjetas empleadas por el USRP.

niUSRP Iniciate

Este VI inicia la sesión de recepción y le informa al USRP de todas las configuraciones están completas para que el USRP comience la adquisición de IQ data.



niUSRP Fetch Rx Data (poly)/ niUSRP Fetch Tx Data (poly)

Este módulo permite recuperar datos IQ de un USRP que tiene una sesión de Rx creada con el niUSRP Open Rx Session VI. Esta información se puede graficar en el dominio del tiempo o ser procesado digitalmente para su análisis.

Este VI es polimórfico, lo que significa que hay varias versiones (instancias) del VI disponibles para elegir, dependiendo del tipo de datos con el que desea trabajar (números enteros dobles, complejos y formas de onda). En la transmisión únicamente fungirá como una "puerta de datos" hacia la antena.

niUSRP Abort VI

Este módulo le dice al USRP que detenga una adquisición en progreso. Permite cambiar la configuración sin cerrar por completo la sesión.

niUSRP Close Session VI

Este VI cierra la sesión Rx o Tx actual y libera la memoria en uso por esa sesión. Después de llamar a este VI, ya no puede transmitir ni recibir datos del USRP hasta que vuelva a abrir una nueva sesión.

4.4 Criptografía

La criptografía hace referencia al uso de códigos para ocultar, enmascarar o transformar algún tipo de información con el fin de elevar la seguridad y confidencialidad de la misma, es de este concepto que se han desarrollado a lo largo de la historia diferentes tipos de técnicas para poder lograr que la información sea recibida y descifrada únicamente por la persona a la que le fue enviado el mensaje.

Figura 15: Esquema criptográfico. En *Cifrado asimétrico,* por Michel Elkan, 2017. Recuperado de: http://seguridadwebricardomachorro5im6batiz.blogspot.com/2017/10/cifrado-asimetrico.html

La figura 15 explica de manera gráfica lo que contiene cualquier esquema básico de transmisión. Se empieza por el emisor que es el que proporciona el mensaje original, (Mcla o simplemente texto plano), para que el algoritmo de cifrado, mediante un determinado procedimiento, cifre o transforme dicho mensaje y pueda ser enviado por un canal público. El receptor, que conoce la clave que transforma ese criptograma o mensaje cifrado, puede obtener sin problemas (con ayuda de un algoritmo de descifrado) el texto original que el transmisor envió *[32]*.

Todo sistema criptográfico debe cumplir con los siguientes principios, los cuales fueron recomendados por Auguste Kerckhoffs en su trabajo "La Criptografía militar" en 1883 *[33]:*

- El criptograma debe ser indescriptable.
- El criptograma debe ser enviado por los medios de transmisión habituales.
- El sistema debe ser portátil y empleado por una sola persona.
- El proceso de descifrado debe ser fácil de usar, pero su complejidad debe ser la suficiente para mantener la seguridad del sistema

Los sistemas de cifrado modernos se pueden clasificar según el tratamiento del mensaje y según el tipo de claves empleado.

El cifrado según el tipo de claves empleado se sub-clasifican en criptosistemas simétricos y asimétricos.

4.4.1 Cifrado simétrico

También conocido como "Shared Key" o también llamado, de clave sencilla, es un tipo de sistema que tanto el emisor como el receptor comparten una única clave tanto para cifrar como para descrifrar los mensajes. Por tal motivo es que la clave de ser de carácter privado. Algunos ejemplos de algoritmos de cifrado simétricos son: DES, 3DES, AES y RC4.

Los algoritmos 3DES y AES son utilizados comúnmente por el protocolo IPSEC para establecer conexiones de VPN y el algoritmo RC4 es utilizado en tecnologías de redes inalámbricas para el cifrado de información en los protocolos de seguridad WEP y WPA versión 1.

La figura 16 representa de forma gráfica el recorrido de la transmisión de un texto con cifrado simétrico, además de los elementos involucrados en dicha transmisión.

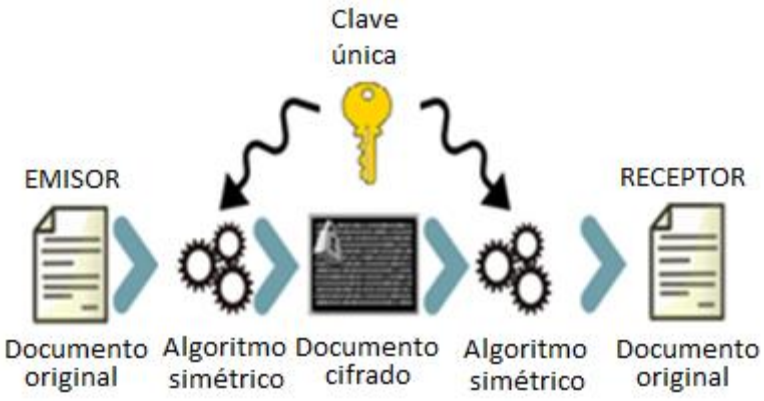


Figura 16: Diagrama de cifrado simétrico. En *Cifrado de información,* por Jorge, 2015, recuperado de: https://sites.google.com/site/ticgorge2/actividades/cifrado-de-la-informacion.

Las ventajas de un cifrado simétrico están en su rapidez de procesamiento y sencillez que permiten una fácil implementación.

Mientras que las desventajas vienen en el hecho de que la clave se debe transmitir de alguna forma para que todos, tanto emisor como receptor, tengan la misma clave y puedan leer el mensaje, pero los medios de transmisión para enviar las claves son demasiado inseguros. La otra desventaja viene en el almacenamiento de claves,

debido a que cada emisor y receptor deben tener una clave única para lograr una comunicación privada; por cada par de personas incrementa el número de claves almacenadas para cada transmisión *[34]*.

4.4.2 Cifrado Asimétrico

Un algoritmo de cifrado asimétrico o también denominado "criptografía de clave pública" se caracteriza por utilizar dos claves para lograr una comunicación privada, se dice fueron desarrollados inicialmente para dar solución a las desventajas que presentaban los algoritmos simétricos.

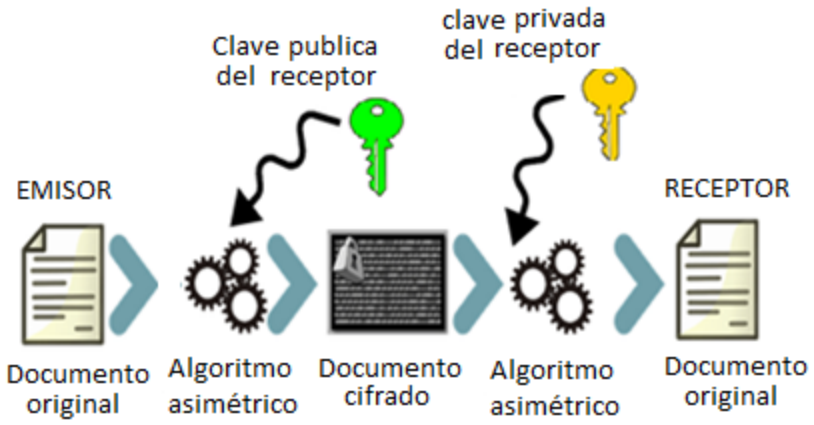


Figura 17: Diagrama de cifrado asimétrico. *Cifrado de información,* por Jorge, 2015, recuperado de: https://sites.google.com/site/ticgorge2/actividades/cifrado-de-la-informacion.

En la figura 17 se ejemplifica de forma gráfica el camino que recorre en la transmisión un texto con cifrado asimétrico.

Cada usuario que interviene en la comunicación, cuenta con dos claves o llaves, una clave pública empleada únicamente para cifrar la información que será enviada por ese usuario y una clave privada que se encarga de descifrar la información recibida. Las parejas de clave son complementarias, es decir, lo que cifra una (clave pública), sólo lo puede descifrar la otra (clave privada).

Las ventajas del cifrado asimétrico, como ya se ha comentado antes, es la seguridad que brinda sobre los cifrados simétricos (debido a que es el receptor quien descifra el mensaje con su clave privada, ya no hace un intercambio de claves) además de contener una mayor complejidad para el descifrado y la seguridad de identidad del destinatario que se proporciona gracias a la clave pública.

Las desventajas sobre este tipo de cifrado se manifiestan en que el mensaje cifrado ocupa mucho más espacio que el original, necesita de un mayor tiempo de procesamiento y las claves son de mayor longitud en comparación con las claves simétricas, debido a que necesitan proporcionar una mayor complejidad en el algoritmo de descifrado.

Los principales ejemplos de algoritmos para esta clasificación son: Diffie- Hellman, El Gmal, RSA (Rivest Shamir Adelman), Funciones Hash, Firmas digitales y Curvas Elípticas *[35]*.

4.4.2.1 Cifrado RSA

El algoritmo de clave pública RSA fue creado en 1977 por Rivest, Shamir y Adlman, pero fue publicado hasta 1978. Actualmente es el sistema criptográfico asimétrico más conocido y usado.

Para su creación se basaron en el artículo de Diffie-Hellman sobre sistemas de clave pública, crearon su algoritmo y fundaron la empresa RSA Data Security Inc., que es actualmente una de las más prestigiosas en el entorno de la protección de datos. Es el primer y más utilizado algoritmo de este tipo y es válido tanto para cifrar como para firmar digitalmente.

La seguridad de este algoritmo radica en la complejidad de la factorización de números enteros y el funcionamiento del algoritmo se basa en el producto de dos números primos grandes elegidos al azar y mantenidos en secreto *[36]*.

El algoritmo se ejecuta con los siguientes pasos para generar el par de claves (pública y privada):

1. Elegir dos números primos grandes p y q, para calcular el número n y $\emptyset(n)$ mediante la expresión (4.16)[14].

$$n = p * q \qquad y \qquad \emptyset(n) = \emptyset(p * q) = (p-1)(q-1) \qquad (Ec. 4.16)$$

[14] Calculo para n y p. Fuente: Facultad de ingeniería (2010). *Fundamentos de Criptografía de Laboratorio de redes y seguridad* [En línea]. Recuperado de: http://redyseguridad.fi-p.unam.mx/proyectos/criptografia/criptografia/index.php/5-criptografia-asimetrica-o-de-clave-publica/54-rsa-rivest-shamir-adelman

2. Seleccionar un entero positivo *e* tal que, $\frac{n}{2} \leq e \leq \emptyset(n)$, de modo que sea primo con el orden del grupo, es decir como (4.17):

$$mcd\ \left(e, \emptyset(n)\right) = 1 \qquad (Ec. 4.17)$$

3. Calcular *d* (que es el inverso de *e),* de manera que (4.18):

$$e * d = 1\left(mod\ \emptyset(n)\right) \qquad (Ec. 4.18)$$

4. Para concluir, la pareja *(n,e)* pasa a ser la clave pública, y (n,d) la clave privada, que al igual que los valores de p, q y $\emptyset(n)$ deben permanecer en secreto.

Para enviar un mensaje con este tipo de cifrado, primero se debe determinar la longitud del número *j,* que determina el número de bytes para formaran cada elemento a cifrar, de modo que según el sistema de numeración en el que se esté codificado cumpla con (4.19):

$$b^j < n \qquad (Ec. 4.19)$$

Donde *b* es la base del sistema de numeración.

El proceso de cifrado consiste en transformar el mensaje *M* a un mensaje cifrado *C*, de acuerdo con (4.20):

$$C = M^e (mod\ n) \qquad (Ec. 4.20)$$

Para ello se utiliza la clave pública del receptor conformada por los números *e y n*.

Para descifrar el criptograma *C* se utiliza la clave privada, conocida sólo por el receptor, conformada por los números *d y n, y* mediante (4.21)[15]:

$$M = C^d (mod\ n) \qquad (Ec. 4.21)$$

Se logra recuperar con éxito el texto original.

[15] (4.17) – (4.21) Fuente: Facultad de ingeniería (2010). *Fundamentos de Criptografía de Laboratorio de redes y seguridad* [En línea]. Recuperado de: http://redyseguridad.fi-p.unam.mx/proyectos/criptografia/criptografia/index.php/5-criptografia-asimetrica-o-de-clave-publica/54-rsa-rivest-shamir-adelman

5. DESARROLLO

En este apartado se describirá el funcionamiento de los VIs (programas) ocupados, las diferentes estrategias de programación y los diversos problemas que han surgido a lo largo del desarrollo del presente proyecto.

5.1 Diagrama de bloques

Para la implementación del sistema de transmisión y recepción inalámbrica usando modulaciones BPSK, QPSK y 8PSK se usaron como base las prácticas y ejemplos de aprendizaje distribuidas por el soporte de National Instrument,

5.1.1 Transmisor

En la parte de la transmisión la figura 18 representa la parte frontal del programa encargado de manipular la información y adecuarla para ser enviada.

Los parámetros de la transmisión impactados por el usuario se toman como datos de configuración para la interface de comunicación entre labVIEW y el USRP.

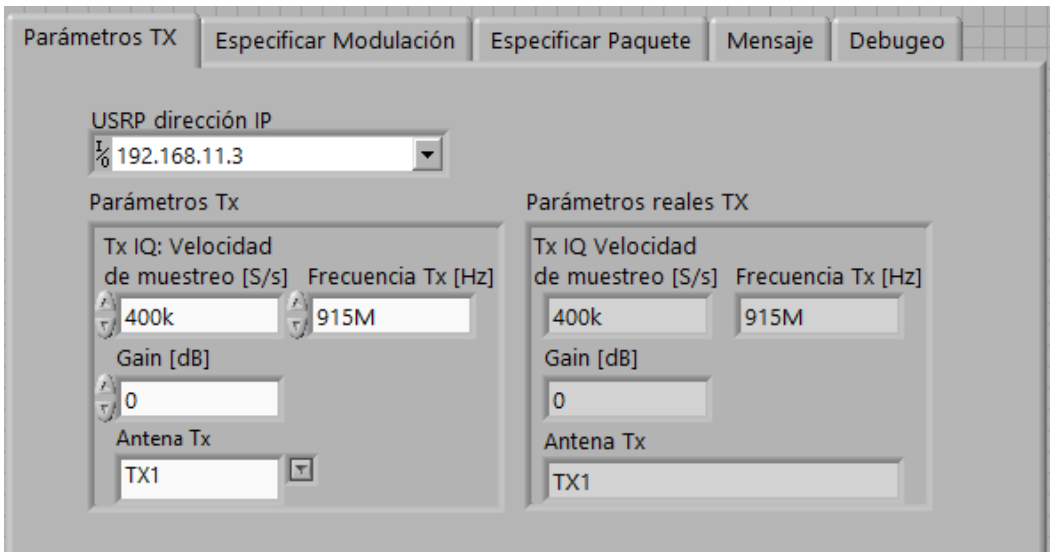


Figura 18: Parámetros de configuración de LabVIEW para el USRP. En *prácticas del NI-USRP*, por la autora, 2018.

Dentro del diagrama de bloques del VI que corresponde al transmisor se pueden ubicar las partes encargadas de la configuración del USRP y la zona encargada del procesamiento de la señal. Uno de los principales bloques encargados del procesado de la señal es el *MT Generate PSK System Parameters (M)*, este se encarga de la configuración para la modulación que será realizada.

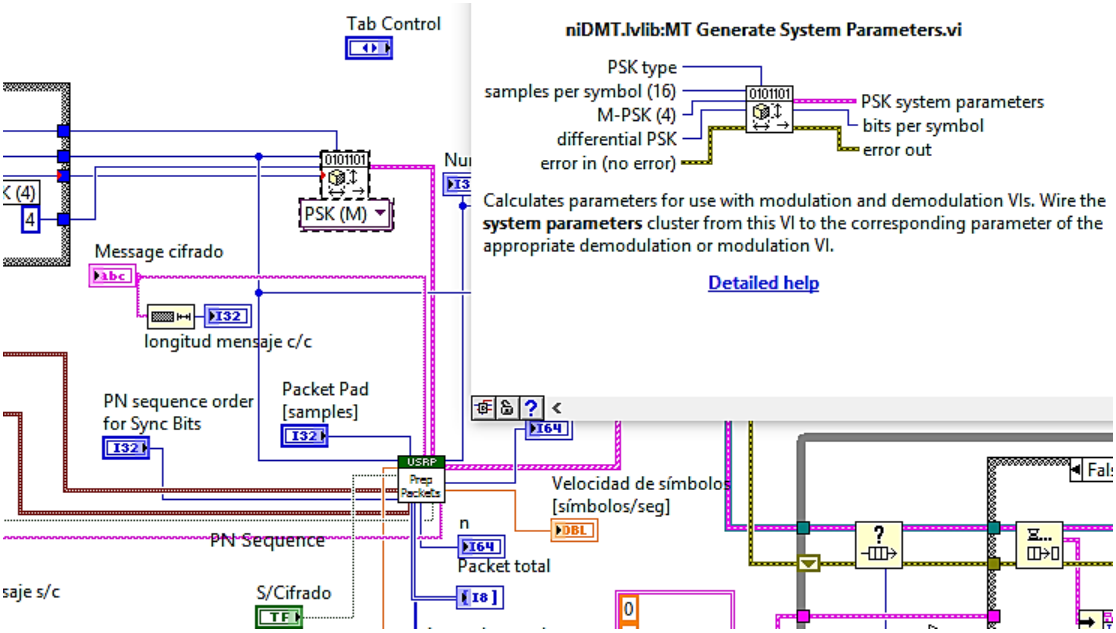


Figura 19: Diagrama de bloques de Transmisor. En *prácticas del NI.USRP*, por la autora, 2018.

Como se muestra en la figura 19, la principal función de este bloque (*Generate System Parameters*) es crear el mapeo de la información en la modulación empleada (constelación) a partir de los parámetros seleccionados por el usuario en el panel frontal del programa, justo en el apartado de las especificaciones de la modulación donde se identifica el orden M-ario, el tipo de PSK y muestras por símbolo entre otros [37]. Para ejemplificar lo anterior, se muestra la figura 20.

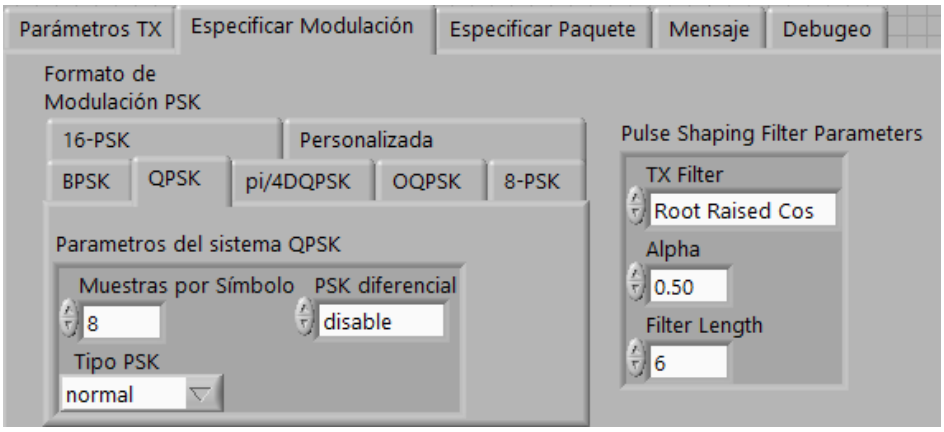


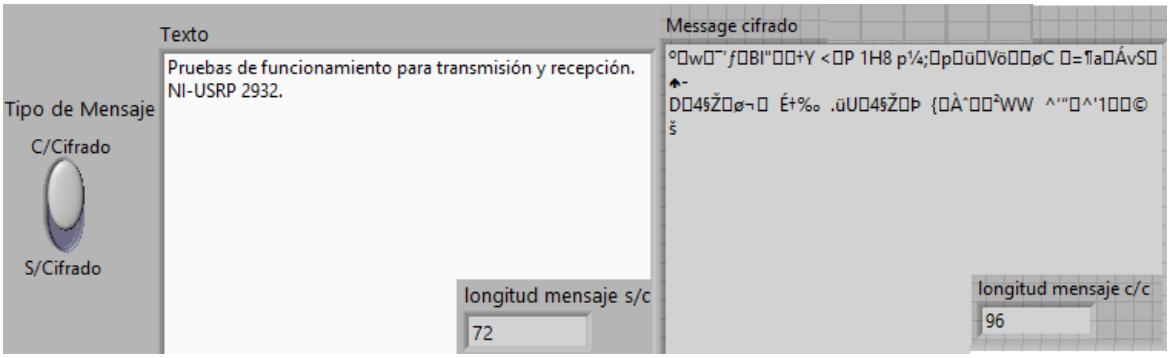
Figura 20: Parámetros de modulación de Transmisor. En *prácticas del NI-USRP*, por la autora, 2018.

Para que el algoritmo de cifrado se ejecute de manera correcta es necesario tener como datos de entrada el texto plano que se requiere cifrar y el número de bits exclusivos de información, por paquete que se desea enviar.

El diagrama de bloques creado específicamente para el cifrado RSA generará los números primos necesarios para obtener los parámetros que conformaran las claves privadas y públicas necesarias para el cifrado como para el descifrado del texto.

En el apartado de anexos se muestra un diagrama completo del programa hecho para el cifrado RSA que pasa un texto plano a una cadena de bits que corresponden al texto cifrado.

Mientras que el panel frontal del proyecto muestra lo que la figura 21, se identifica la longitud de los caracteres del mensaje de texto plano y cifrado, y se agrega la opción de elegir entre cifrar o no el texto.



a) *b)*

Figura 21: a) Texto plano b) texto cifrado. En *prácticas del NI-USRP*, por la autora, 2018.

El mensaje cifrado es preparado y concatenado con una serie de bytes, dictaminados por el programador en el panel frontal, que complementan el paquete antes de ser modulado.

La descripción del paquete para este ejemplo con tamaño de 434 bits está formado por:

Tabla 5:
Estructura del paquete.

Bits Guarda	30
Bits Sincronía	20
Bits Cabecera	128
Bits Mensaje	128
Bits Redundantes	128

Fuente: Archivo de la autora, 2018.

La cadena de bits correspondientes al texto cifrado en conjunto con los bits de encabezado, bits de guarda, bits de sincronía y bits redundantes forman el paquete final de información que posteriormente pasará al proceso de modulación para, finalmente, ser enviado.

El VI encargado de modular la señal, recibe el nombre de *Modulate PSK.vi*. Este módulo recibe los datos validados del *PSK System Parameters.vi* y la tasa de símbolos por segundo. La figura 22 es la representación gráfica de los elementos que componen al bloque modulador PSK.

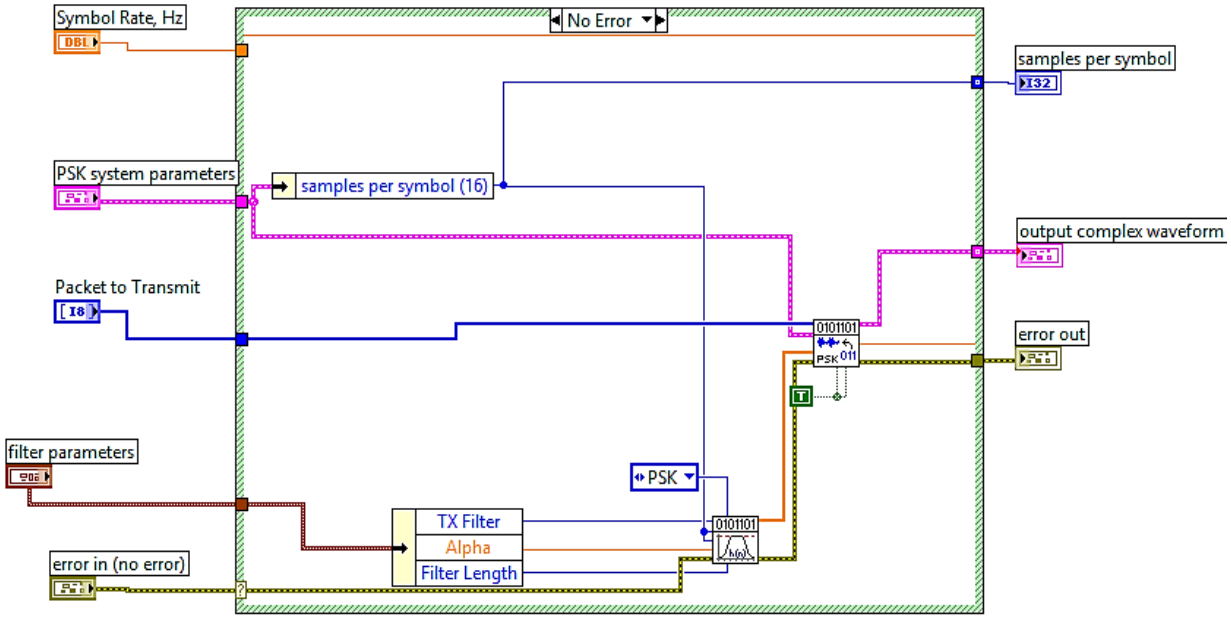


Figura 22: Composición del Modulador PSK. En *prácticas del NI-USRP*, por la autora, 2018.

Como datos de salida, ofrece una secuencia compleja de símbolos que generarán una forma de onda. Posee tres instrumentos virtuales fundamentales; uno de validación (recibe la validación hecha en el *PSK System Parameters.vi* y procede o detiene el flujo de datos), un módulo encargado de realizar el mapeo de símbolos (*PSK MAP Symbols.vi*) y otro que se encarga de realizar el filtrado virtual de los símbolos mapeados *[38]*.

Oswaldo Juárez (2016) señala que *"su principal función es la de concatenar constantemente los símbolos mapeados a un determinado número de bits. Lo anterior permite que exista un flujo constante de información en la transmisión" (p.43).*

La implementación de un filtro antes de la modulación, en la parte de la transmisión, se usa debido a que en una modulación simple resulta muy complicado para el

demodulador recuperar los datos. El filtro de coseno elevado se emplea para minimizar la interferencia entre símbolos (ISI) y combatir los inconvenientes que pueda provocar está en la recepción y demodulación de la señal.

El bloque *Generate Filter Parameters.vi* valida los parámetros definidos por el usuario y genera un vector que contiene los coeficientes del filtro *[39]*.

La última sección en el transmisor es la zona del código, enfocada a la transmisión del flujo de la información. Hace uso de un *clúster* que almacena y transmite los datos que comunicará al *SDR*. Dado que el clúster se encuentra dentro de un *loop*, la transmisión se detendrá únicamente cuando el usuario detenga intencionalmente el programa o cuando dicho buffer de memoria llegue a su límite.

5.1.2 Receptor

Debido a que el dispositivo de recepción debe conocer la estructura de la constelación que recibirá, es requerimiento primordial que contenga a la entrada de los parámetros de configuración del USRP, el mismo formato de modulación que fue indicado en el transmisor así como la tasa de muestreo, y la frecuencia de la portadora, ya que debe de existir una sincronización entre el dispositivo transmisor y el receptor con sus correspondientes interfaces, de lo contrario el receptor tendrá problemas al demodular la señal recibida.

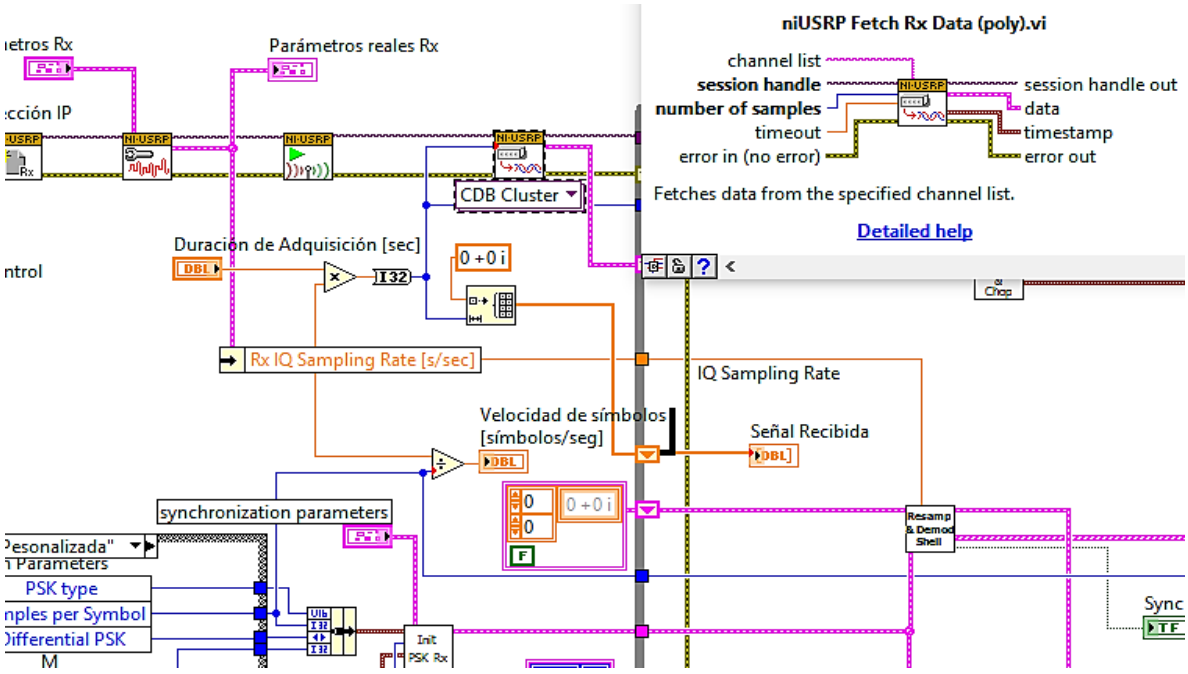


Figura 23: Diagrama de bloques Receptor. En *prácticas del NI-USRP*, por la autora, 2018.

Mediante la figura 23 se puede observar el diagrama de bloques que compone de forma general el dispositivo receptor, pero es, específicamente, mediante el módulo *niUSRP Fetch Rx Data (poly).vi* es que se obtienen los datos adquiridos por la antena, hay que tener en cuenta que para que la función trabaje correctamente hay que introducirle, por dato, el número de muestras que se obtiene en la adquisición del canal *[40]*. De esta manera, la adquisición no se realiza de manera continua, si no cada "x" número de muestras.

La figura 24 muestra el panel frontal donde se encuentran los parámetros configurables del receptor y los cuales deben ser idénticos a los capturados por el dispositivo transmisor, como se mencionó anteriormente.

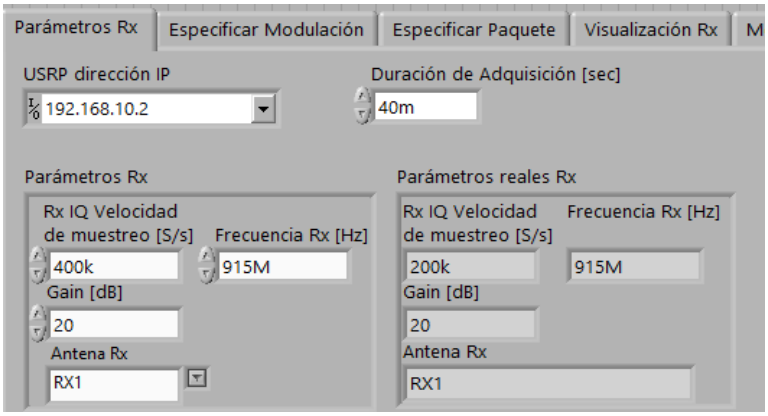


Figura 24: Panel frontal Receptor. Prácticas de NI-USRP, por la autora, 2018.

La figura 25 muestra una parte de los componentes del diagrama de bloques, donde, una vez obtenidos los datos complejos de la entrada, la señal se introduce en el módulo llamado *MT Resample (Complex Cluster).vi*.

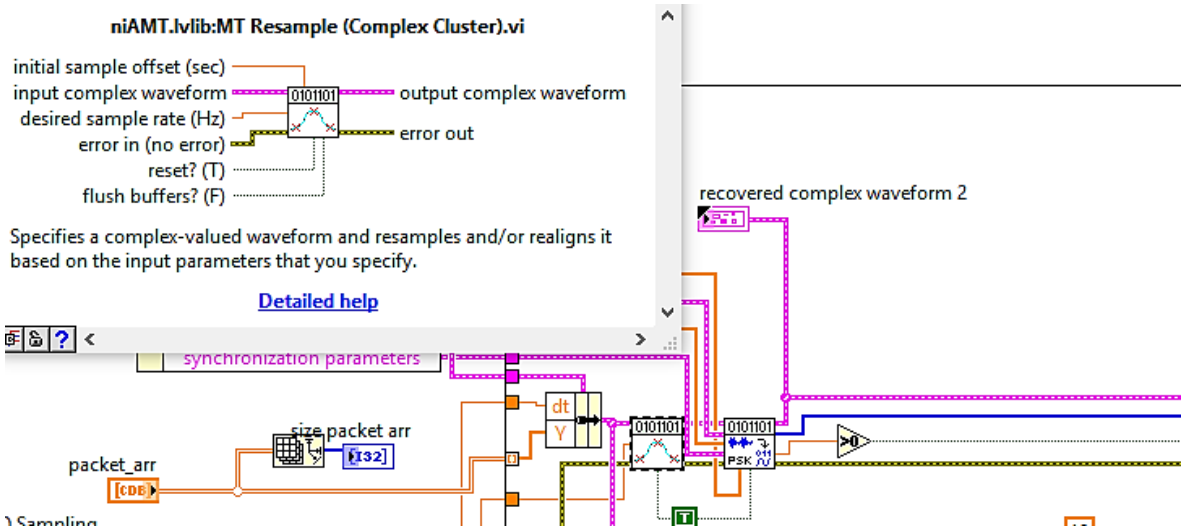


Figura 25: Diagrama de bloques para el procesamiento de la señal. Prácticas de NI-USRP, por la autora, 2018.

Según Oswaldo Juarez (2016) "*En éste módulo se realiza una reducción lógica en el número de muestras tomadas de acuerdo a la entrada, que debe ser igual al IQ Sampling Rate indicado por el usuario en el transmisor" (p.45),* por esta razón es que debe existir una sincronización con los datos que el usuario impacta en el transmisor y el receptor.

Dicho de una forma simplificada, éste módulo se encarga de realizar una decimación virtual cuya salida sea una forma de onda compleja con una tasa de muestreo similar a la obtenida por el *Modulate PSK.vi*, en el transmisor.

Una vez hecho esto, la señal se introduce en *MT Demodulate PSK.vi* para realizar la demodulación de la señal. Considerando que los datos especificados por el usuario hayan sido correctos en la sincronización con el transmisor y que el procesamiento de los mismos haya sido realizado de forma adecuada en los módulos y secciones antes mencionadas, el demodulador *PSK* debería conocer el valor complejo de cada símbolo de las constelaciones recibidas, los parámetros del filtro empleado, la velocidad de transmisión de los símbolos y el valor del elemento (en código Gray) asociado a cada símbolo de la constelación *[41]*.

A la salida del demodulador se obtiene el flujo de datos de información y la forma de onda de la misma. El bloque de validación de paquetes analiza los bits de sincronía y agrupa los paquetes correctos, para después separar la información útil de cada paquete, de los bits concatenados para la transmisión del mensaje.

Dejando sólo los bits del mensaje cifrado, el bloque del algoritmo de descifrado es empleado y sabiendo los números *n y d* que conforman la clave privada del receptor se obtiene con éxito el texto descifrado.

La figura 26 ejemplifica el resultado final de la ejecución, correcta, del bloque descifrador empleado en el dispositivo receptor.

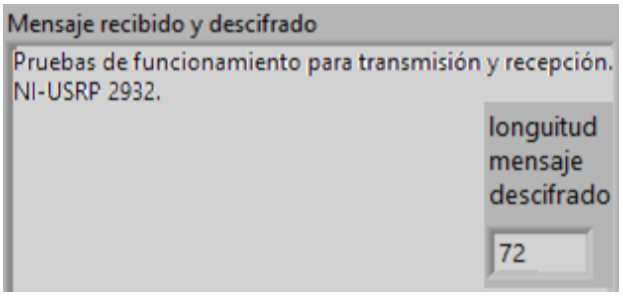


Figura 26: Panel frontal con texto descifrado. Prácticas de NI-USRP, por la autora, 2018.

5.2 Pruebas de funcionamiento

Los experimentos fueron realizados en un espacio cerrado donde los dispositivos tuvieran una línea de vista con aproximadamente 5 metros de distancia máxima ente ellos.

Se sabe que la ganancia del transmisor puede ajustarse de 0 a 30dB y la atenuación puede manipularse a través del atenuador incrustado en la antena del sistema NI-USRP, es de esta forma que la recepción del SNR puede controlarse.

Uno de los principales objetivos de este proyecto radicaba en el análisis de la relación entre la potencia de transmisión y recepción, así como los efectos que tiene la atenuación sobre ésta, con los diferentes sistemas de modulación.

Como se mencionó anteriormente el ruido del canal influye de manera directa en los parámetros de eficiencia de un enlace de comunicación. Para obtener la potencia promedio del ruido en los dispositivos de transmisión y recepción se procesó el espectro libre mostrado en la figura 27.

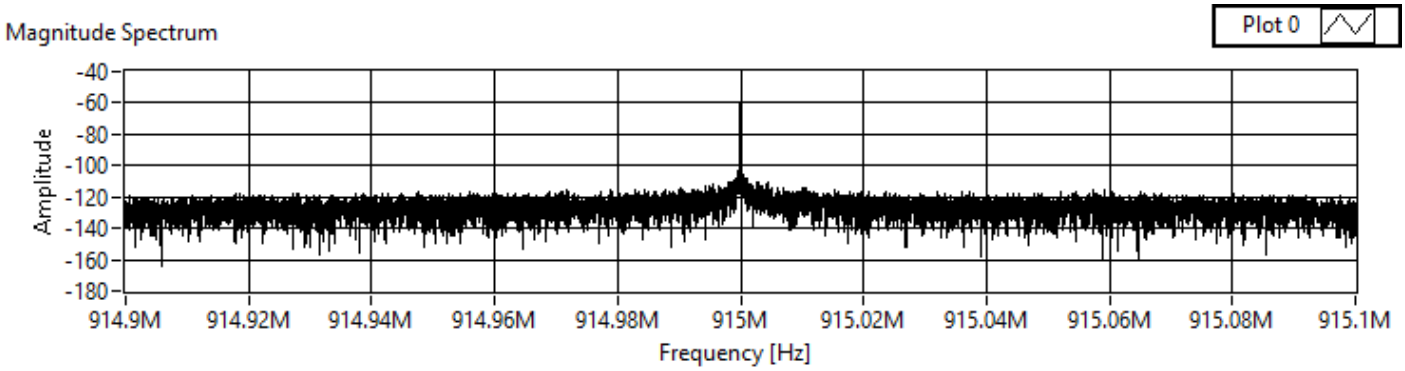


Figura 27: Espectro de potencia de canal libre, por la autora, 2018.

Tomando un barrido de frecuencias y potencia sobre el espectro mostrado, se obtuvo como resultado que la potencia de ruido promedio es del canal es de -118.298 (dBW).

Mientras que para el cálculo de la relación señal a ruido de cada una de las señales de información transmitidas, se empleó un algoritmo elaborado desde Matlab que permitió calcular la potencia promedio de cada experimento a partir de su espectro.

6. RESULTADOS

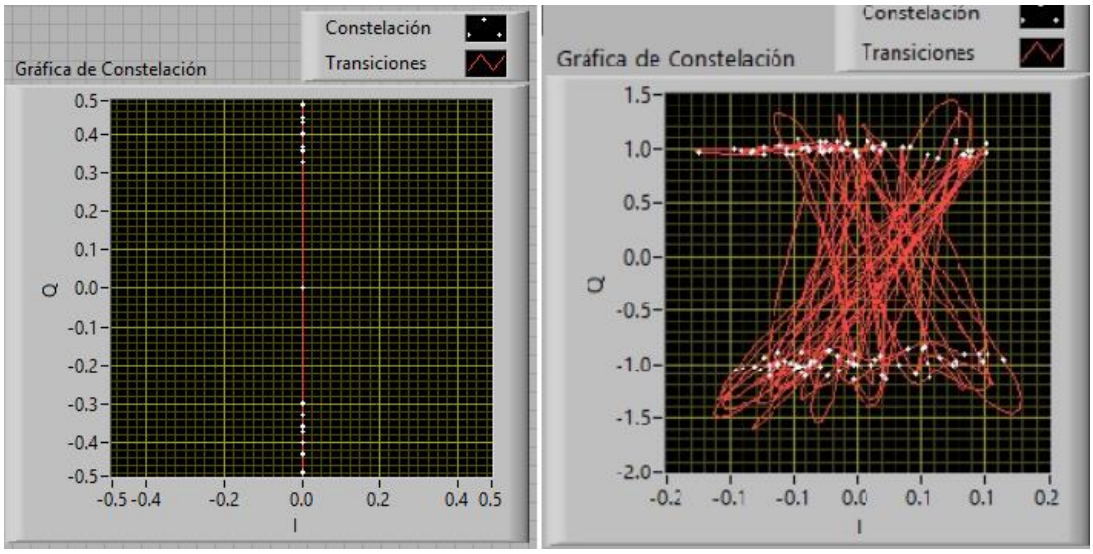
En este capítulo se presentaran los resultados obtenidos en la implementación de los experimentos. Se realizará un análisis del enlace inalámbrico establecido (intentando comparar los datos obtenidos con la teoría). Con el fin de observar los efectos que la atenuación tuvo sobre la implementación de las modulaciones.

Los parámetros iniciales en la configuración del transmisor, para todos los experimentos, son: Una tasa de transmisión de 500K [samples/second] en una frecuencia central de transmisión de 915 [MHz] y con 8 [samples/symbol].

Modulación BPSK

Los dispositivos NI-USRP se mantuvieron a una distancia de 5 metros de separación entre ellos. Dentro parámetros iniciales del experimento se involucró el aumento controlado de la ganancia desde el panel frontal del programa en el transmisor y el uso de los atenuadores incluidos en el kit del NI-USRP correspondiente a 30dB.

El sistema BPSK se está simulando en el NI-USRP y la figura 28 confirma que el diagrama de la constelación (a), se ajusta a la cifra teórica para transmitir con sólo dos posiciones 1 y -1.



a) *b)*

Figura 28: a) constelación en el Tx de modulación BPSK b) Constelación en el Rx de la modulación BPSK. Prácticas del NI-USRP, por la autora, 2018.

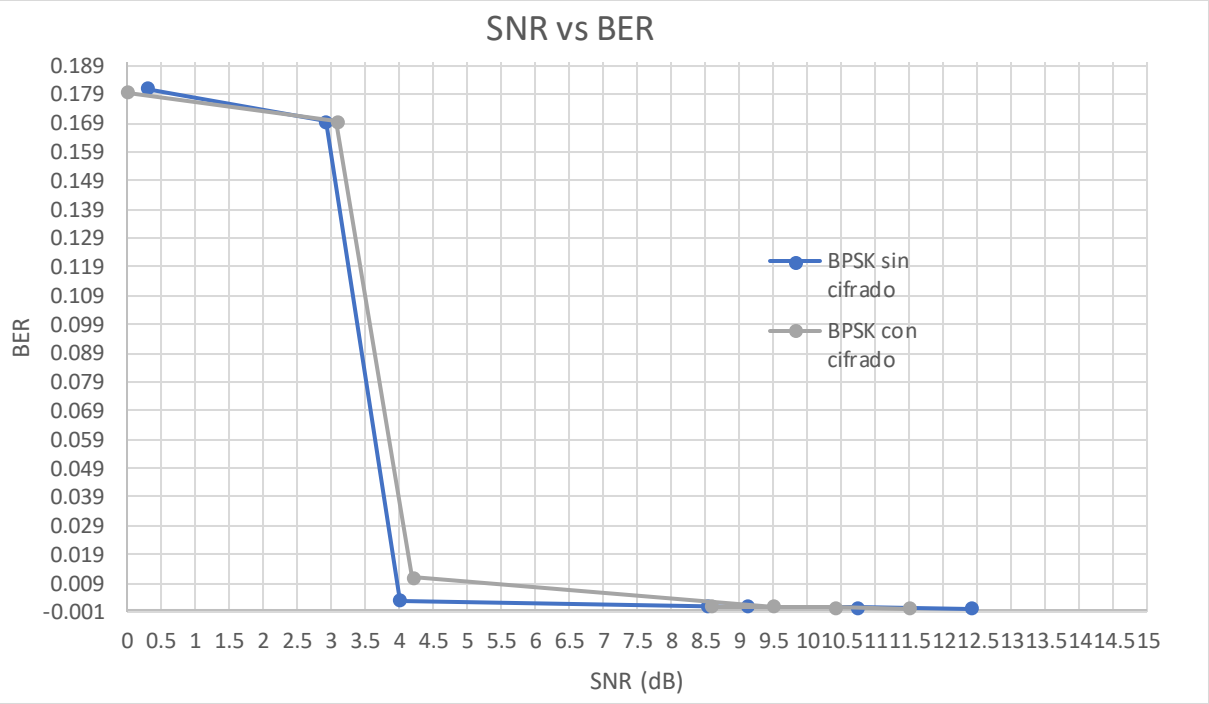
Mientras que el diagrama de la constelación (b) parece haber algunos problemas para la recepción que la señal, se observa la dispersión de los puntos de la

constelación con respecto a la constelación ideal que puede deberse al ruido de fase del canal. El problema podría solucionarse añadiendo un sistema de corrección, pero a pesar de la visible dispersión, la comunicación indica que la sincronización del sistema funciona bien.

Tabla 6
Paramentos y resultados del experimento con modulación BPSK.

$G_{\text{transmisor}}$ (dB)	P_{receptor} (dB) (sin cifrado)	P_{receptor} (dB) (con cifrado)
+30	-105.894	-106.791
+20	-107.567	-107.896
+10	-109.764	-109.716
+0	-109.196	-108.798
-30(+30)	-114.292	-114.096
-30(+20)	-115.384	-115.213
-30(+10)	-118.013	-118.285

Fuente: Archivo de la autora, 2018.



Gráfica 1: SNR vs BER para modulación BPSK. Por la autora, 2018.

En la gráfica 1 se puede observar el comportamiento del BER con respecto al SNR de la información cifrada y no cifrada. Se logra observar como la información en ambos casos logra obtener una SNR de hasta 12 dB con un error de bit mínimo de cero.

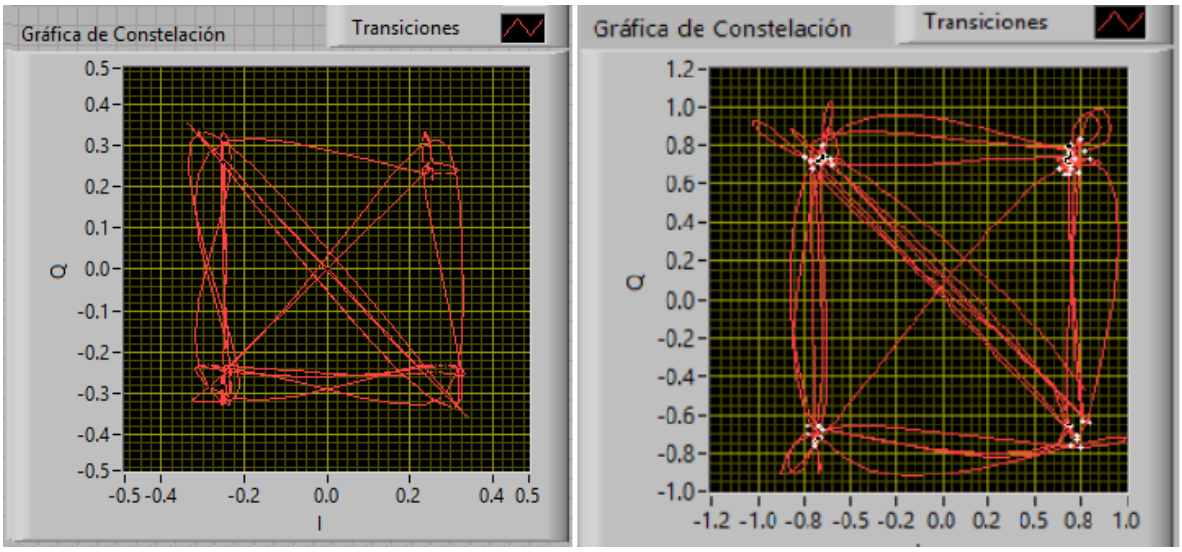
Para una mayor calidad en la trasmisión el valor del SNR debe ser cada vez mayor, esto indicaría que la potencia de la señal con información es más fuerte que el ruido.

La comparación del comportamiento de la transmisión del texto cifrado y no cifrado no tiene mucha variación en la modulación BPSK.

Modulación QPSK

Como se había explicado antes, cuando el sistema BPSK cambia a QPSK existen cuatro posiciones en el diagrama de constelación y comparando las características de la modulación BPSK con la QPSK se resalta el hecho de que con la misma potencia de la señal (que utiliza la modulación BPSK) puede doblar la tasa de transmisión o transmitir la misma señal ocupando la mitad del ancho de banda.

Se debe tener en cuenta que los parámetros iniciales propuestos para el transmisor deben ser los mismo que aparezcan en la interface del receptor, de lo contrario será imposible capturar la información enviada.



a) b)

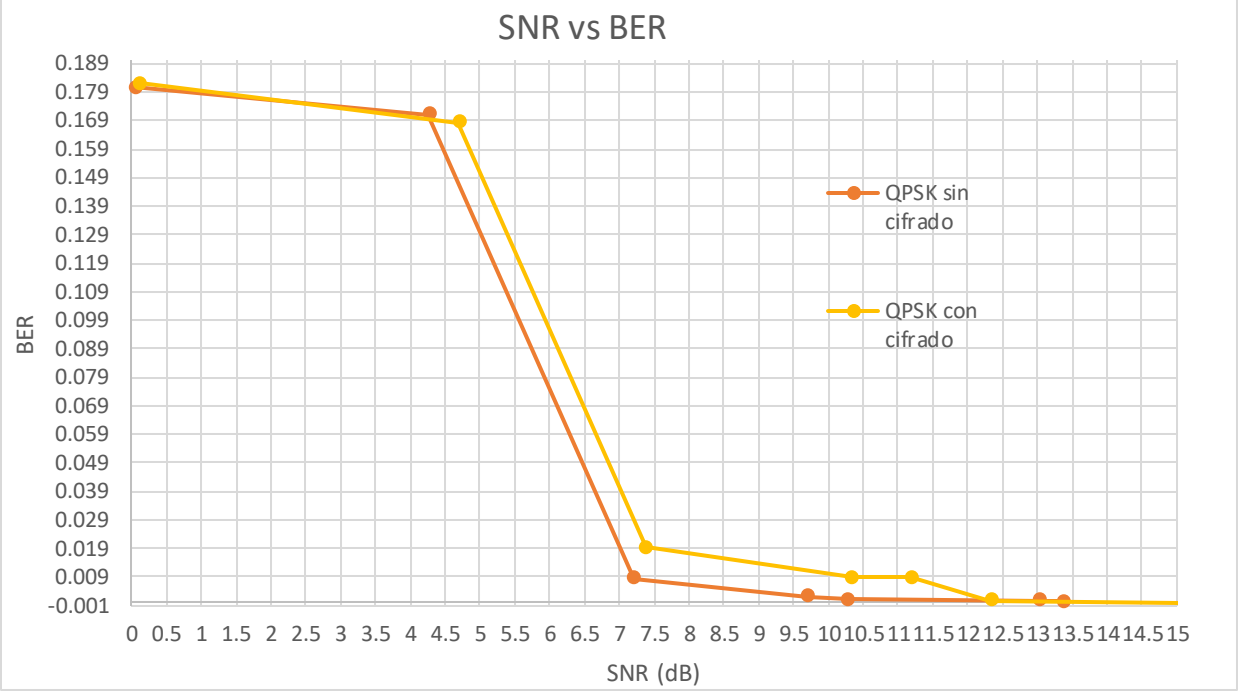
Figura 29: a) constelación en Tx de la modulación QPSK b) constelación en Rx de la modulación QPSK. Prácticas del NI-USRP, por la autora, 2018.

En la figura 29(b), la parte de recepción también presenta desviaciones en el diagrama de la constelación, que es una situación bastante similar a BPSK debido al ruido de fase y al ruido gaussiano blanco, entre otras cosas.

Tabla 7
Paramentos y resultados del experimento con modulación QPSK.

$G_{\text{transmisor}}$ (dB)	P_{receptor} (dB) (sin cifrado)	P_{receptor} (dB) (con cifrado)
+30	-104.923	-103.274
+20	-105.265	-105.975
+10	-108.016	-107.117
+0	-108.591	-107.958
-30(+30)	-111.089	-110.923
-30(+20)	-114.044	-113.613
-30(+10)	-118.261	-118.184

Fuente: Archivo de la autora, 2018.



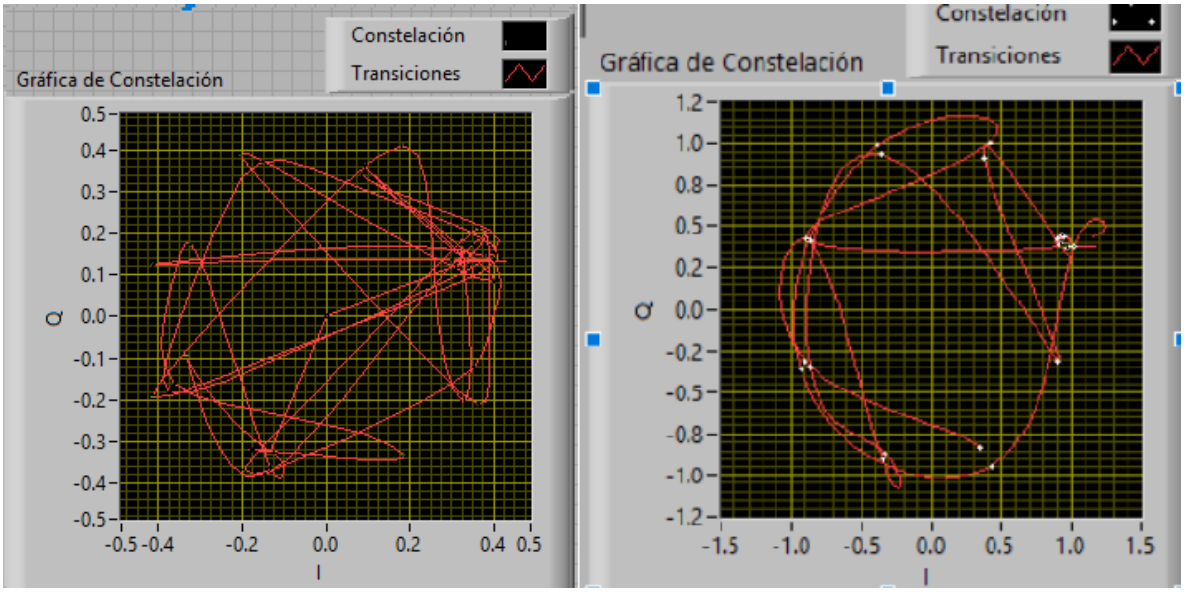
Gráfica 2: SNR vs BER para modulación QPSK. Por la autora, 2018.

A partir de los resultados representados en la gráfica 2, se observan los valores del BER obtenidos en relación a un SNR más alto. Estos datos fueron tomados usando los equipos NI-USRP en las diferentes modalidades del envío de información con o sin cifrado RSA y muestran un BER bastante bueno para un sistema de comunicación inalámbrico.

Modulación 8PSK

En el sistema M-ario de 8-PSK el diagrama de constelación debe tener ahora 8 posiciones diferentes. Los parámetros de funcionamiento del transmisor y receptor no sufrieron ninguna modificación, sin embargo para esta modulación, en particular, se encontraron diversos problemas para lograr una recepción con mediciones aceptables para el experimento.

En la constelación de la figura 30 se aprecia una notable diferencia entre la constelación ideal y la captada por el receptor. Este resultado no solo se ve reflejado en la imagen de la constelación sino que también la potencia del receptor es sumamente baja.



a) b)

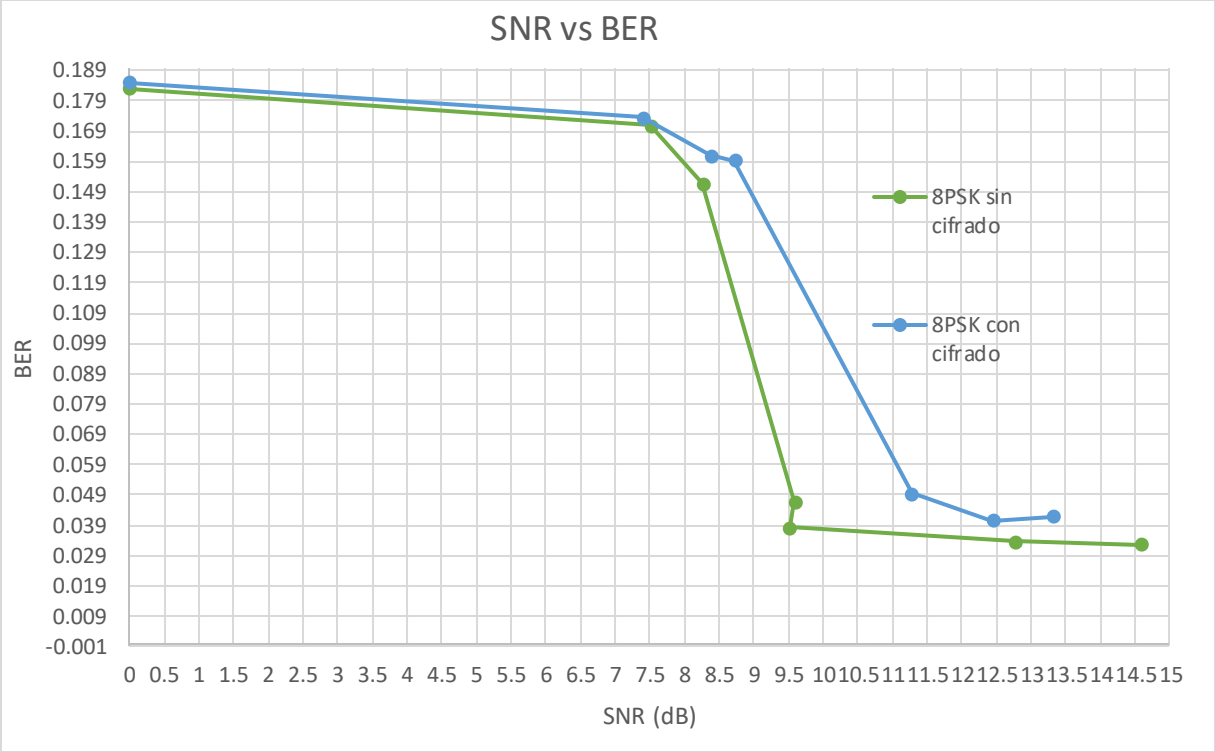
Figura 30: a) constelación en Tx para modulación 8PSK b) constelación en Rx para modulación 8PSK. Prácticas del NI-USRP, por la autora, 2018.

La modulación 8-PSK es la más susceptible al error de bit debido a la cercanía de los puntos en la constelación esto se comprueba en los resultados mostrados por la gráfica 3 con la información enviada sin cifrar y cifrada por un canal real con ruido. De la cual se deduce que el texto cifrado es más susceptible al ruido debido a que contiene más bits de información.

Tabla 8
Paramentos y resultados del experimento con modulación QPSK.

$G_{\text{transmisor}}$ (dB)	P_{receptor} (dB) (sin cifrado)	P_{receptor} (dB) (con cifrado)
+30	-103.723	-104.984
+20	-105.541	-105.851
+10	-108.785	-107.021
+0	-108.709	-109.569
-30(+30)	-110.039	-109.915
-30(+20)	-110.789	-110.896
-30(+10)	-118.294	-118.293

Fuente: Archivo de la autora, 2018.

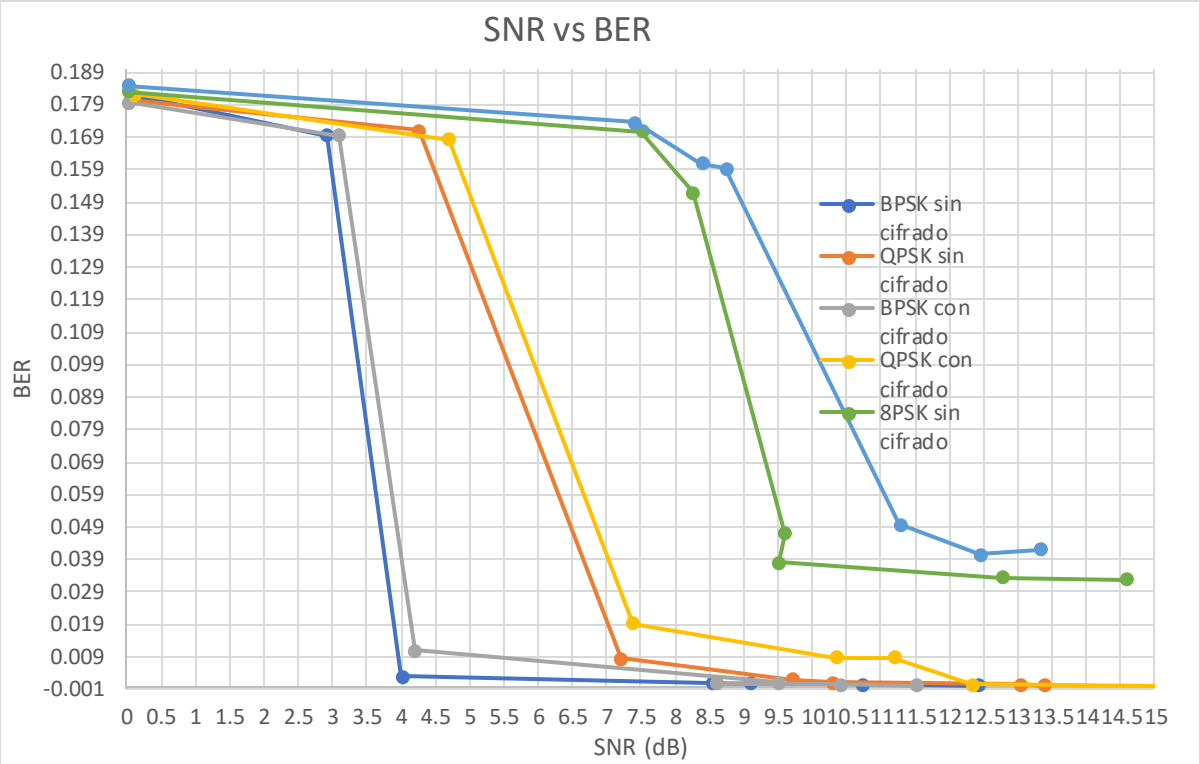


Grafica 3: SNR vs BER para modulación 8PSK. Por la autora, 2018.

En la gráfica 4 se puede observar de manera más detallada los beneficios de cada una de las modulaciones empleadas y sus diferentes comportamientos con respecto al cifrado de información.

Se confirma que la modulación BPSK es la más robusta de las modulaciones y que no hay una gran diferencia en la comparación de los resultados de la transmisión con texto cifrado y no cifrado, excepto por la modulación 8-PSK donde se observa que el

error de bit es sumamente alto para el texto cifrado, aun cuando la SNR de la señal es bastante buena.



Gráfica 4: SNR vs BER comparativo. Por la autora, 2018.

Las condiciones con las que se ejecutaron los ejercicios anteriores fueron un IQ rate de 200k (sampling/sec) con 8 (sampling/symbol) dando como resultado una tasa de transmisión:

$$Tasa\ de\ transmisión = \frac{200k\ sampling/sec}{8\ sampling/symbols} = 25000\ \frac{symbols}{sec}$$

Con sus respectivos anchos de banda:

Tabla 9:
Ancho de Banda para modulación M-PSK

Modulación	BW
BSPK	50kHz
QPSK	25kHz
8PSK	16.66Khz

Fuente: *por la autora, 2018.*

Tasa de transmisión

Las características del sistema de recepción y transmisión, empleadas para realizar los ejercicios de la comparación de la tasa de transmisión con la relación señal a ruido, fueron las siguientes:

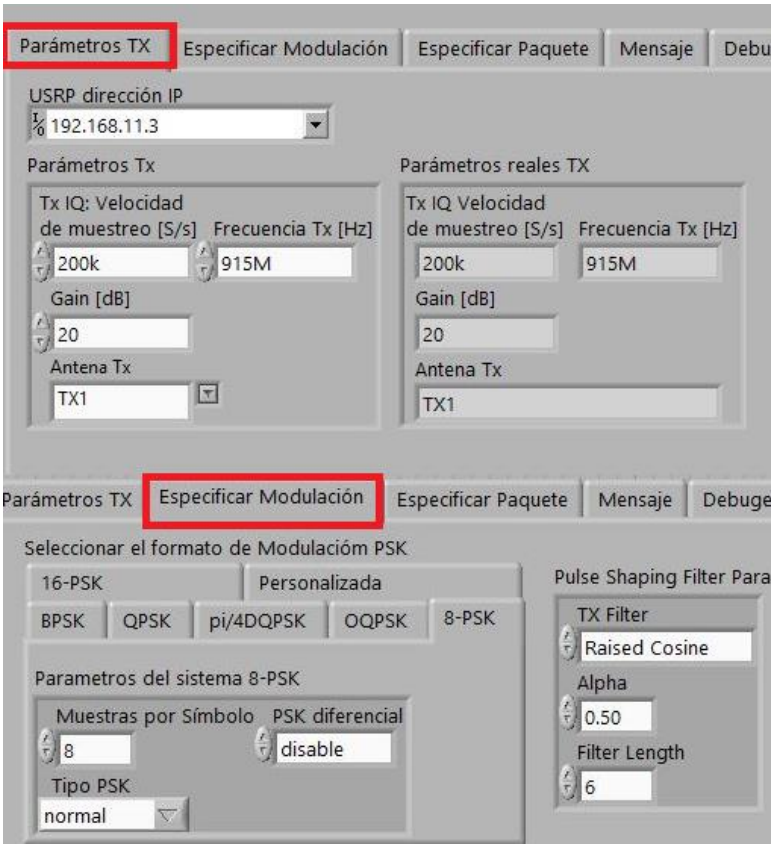
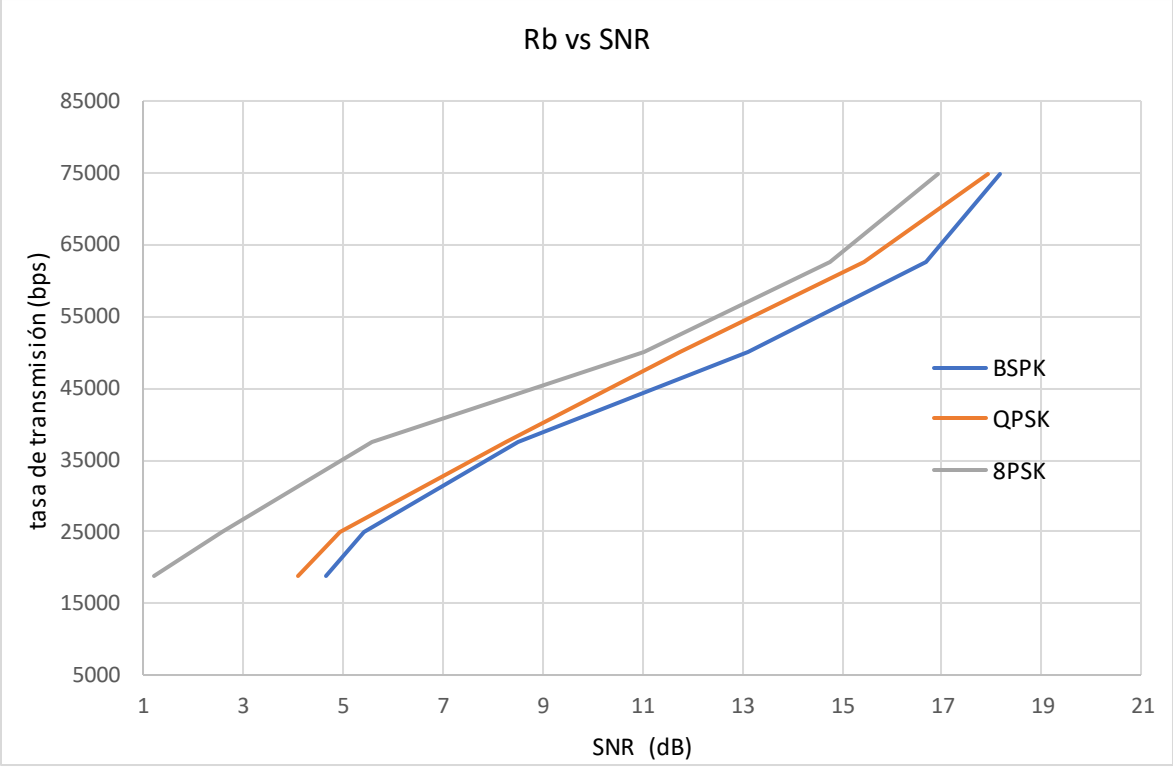


Figura 31: Parámetros para ejercicio Rb vs SNR. Prácticas del NI-USRP, por la autora, 2018.

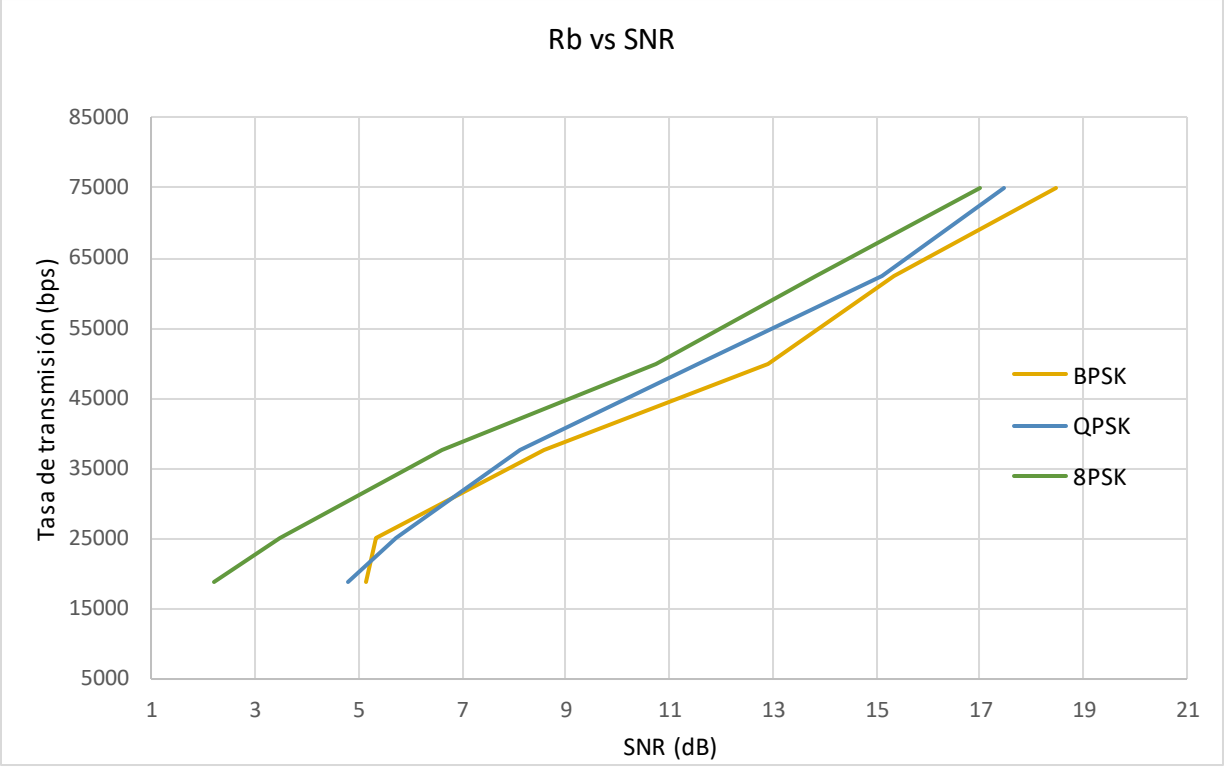
Se logró obtener una tasa de transmisión variable según las muestras por segundo que el programador introdujera en el apartado de configuración del NI-USRP, que junto con las muestras por símbolo que el sistema toma se obtuvieron las siguientes muestras para el caso de la recepción del paquete cifrado y no cifrado.



Gráfica 5: Rb vs SNR recepción de texto no cifrado. Por la autora, 2018.

La grafica 5 representa el comportamiento de la tasa de transmisión con respecto al SNR del paquete cifrado. Se observa que la relación entre los parámetros de transmisión es casi lineal, mientras más grande sea la tasa de transmisión mayor será la relación señal a ruido de la señal recibida.

En el caso de la modulación 8-PSK se observa una mayor sensibilidad por parte de la tasa de transmisión, debido a que el algoritmo de cifrado aumenta de manera significativa la cadena de bits para transmitir es necesario tomar en cuenta el tiempo de recepción empleado.



Gráfica 6: Rb vs SNR recepción texto cifrado. Por la autora, 2018.

Mientras que la gráfica 6 muestra los resultados para el texto no cifrado; se observa que todas las modulaciones tiene un comportamiento similar, con una SNR ascendente con respecto a la tasa de trasmisión.

7. Conclusiones

Una de los principales problemas con el enlace de transmisión fue la atenuación de la señal recibida por el receptor, posiblemente debido a las multitrayectorias de la señal; se pensó en colocar el transmisor y receptor NI-USRP lo más cerca posible para así evitar interferencias del medio que pudieran producir un retardo en la llegada de los símbolos o en el peor de los casos la llegada de una fase opuesta de la señal que pudiera ocasionaría su cancelación.

También se advirtió que si se desea aumentar la longitud del paquete transmitido hay que tener en cuenta el hecho de fijar un tiempo de captura más grande ya que si no es suficiente se puede perder la información y se obtendría un BER mucho más alto.

Se llevaron a cabo 6 tipos de muestras distintas para lograr capturar el análisis de la tasa de error de bit, las distintas potencias y tasas de transmisión recibidas, con el fin de analizar la sensibilidad máxima del NI-USRP en función de los distintos parámetros configurables de este proyecto, como el manejo de la ganancia en el transmisor y la atenuación al extremo de las antenas del dispositivo NI-USRP 2932, además de la variación en la tasa de transmisión para la segunda parte de los experimentos.

De lo cual se concluye que la modulación 8-PSK es la más susceptible al ruido del canal y con mayor probabilidad de error en una transmisión inalámbrica para una mayor tasa de transmisión, justo como la teoría nos dictamina, pues los puntos de la constelación se encuentran más cerca que cualquiera de las otras dos modulaciones empleadas, y aunque se considere que tiene mayores ventajas por la reducción del ancho de banda, habría que tener en cuenta que parámetros ayudan a resolver este inconveniente. La aplicación de un filtro de coseno alzado en la recepción aventaja un poco la situación, y en las aplicaciones de servicios, el FEC, también podría ser de ayuda.

De los experimentos realizados se obtuvo como conclusión que la atenuación impuesta en la transmisión afecta de manera directa a la calidad de la señal; el parámetro me mejor refleja esto es la relación señal a ruido, a su vez relacionado con la tasa de error de bits y la tasa de transmisión, debido a que el canal siempre habrá limitaciones por en ancho de banda y estos parámetros están ligados a esta condición. Para la diferencia de los parámetros de sensibilidad entre la información cifrada y no cifrada se puede concluir que al tener un mayor número de bits por transmitir, en el mensaje cifrado, es mayor el número de paquetes que se envía, pero

el comportamiento del canal y los parámetros no cambian demasiado, salvo por la modulación 8-PSK, con la que se obtuvo un BER más alto para una SNR bastante aceptable, esto debido posiblemente al aumento considerable de paquetes, debido al cifrado, recibidos por el transmisor.

Se identificaron los principales factores que afectan el enlace de comunicación, tales como la reflexión de la señal que elevaba el ruido del canal, la orientación del dipolo con respecto a su patrón de radiación y se propusieron procedimientos para superar las dificultades como despejar la zona de trabajo de posibles objetos reflectores de la señal y la implementación de un buen procesador en la PC para no invalidar la operación con el NI-USRP y una prueba de aislamiento para saber la mejor posición para la antena.

El estudio de la eficiencia de los parámetros de la tecnología de radio definido por software puede dar a conocer un panorama donde la interoperabilidad de los equipos no sea una dificultad a la hora de ejecutar un enlace ya que la posibilidad de una implementación con este tipo de tecnología en el ámbito de las telecomunicaciones, debido a sus aportes de ejecutar las operaciones del hardware a base de software, la tecnología SDR sería una excelente alternativa que suplantaría los inconvenientes de usar equipos de diferentes fabricantes.

El panorama, aún por explorar, puede englobar todas las tecnologías con las que es enviada la información y las bandas de frecuencias que utilizan y concuerdan con el ancho de banda de operación del NI-USRP 2932. Se podría iniciar el estudio de que tan factible es la operación de estos dispositivos en condiciones reales de propagación, con objetos reflejantes y distancias considerables para complementar la idea de llevar esta tecnología a la industria de las telecomunicaciones.

8. Referencias

[1] Ingeniería Inalámbrica de Pontificia Universidad Católica del Perú. [En línea]. (2016). Recuperado de: https://docplayer.es/13482746-Temario-modulo-1-ingenieria-inalambrica-8-h.html

[2] Gil, V. P. Pomares, B. J. Candelas, H. F .A. (2010). Codificación de la información en *Redes y transmisión de datos* (*p.* 58). Texto docente/Universidad de Alicante.

[3] Tomasi, W. (2003). Comunicaciones digitales, en *Sistemas de comunicaciones electrónicas (pp. 482 y 483),* 4ta edición. México: Pearson Educación.

[4] Gil, V. P. Pomares, B. J. Candelas, H. F .A. (2010). Codificación de la información en *Redes y transmisión de datos (p. 60)*. Texto docente/Universidad de Alicante.

[5] Juárez, O. (2016). *Estudio de Técnicas de Modulación Mediante Radios NI USRP (p.13)*. Trabajo de grado, Ingeniería en telecomunicaciones, Universidad Nacional Autónoma de México, México.

[6] Ganguly, S. (2017). IEEE ComSoc. [En línea]. Recuperado de: https://top.quora.com/What-are-the-advantages-of-differential-phase-shift-keying-DPSK-over-phase-shift-keying-PSK

[7] Millán, J. (2014). Comunicaciones radioeléctricas y servicios de radiodifusión en *Configuración de infraestructura de sistemas de telecomunicaciones (p. 33*). Ediciones Paraninfo.

[8] Generalidades sobre receptores de Universitat de les Illes Balears *(p. 2.6)*. [En línea]. (2007). Recuperado de: http://dfs.uib.es/GTE/education/telematica/sis_ele_comunicacio/Apuntes/Capitulo%202.pdf

[9] Ramírez, R. (2005). Transmisión de la señal digital en *Sistemas de radiocomunicaciones (p. 83*). Ediciones Paraninfo.

[10] Memon, T. D. (2009). 2nd International Conference on Computer, Control and Communication. [En línea]. Recuperado de: https://ieeexplore.ieee.org/document/4909180/

[11] Millán, J. (2014). Comunicaciones radioeléctricas y servicios de radiodifusión en *Configuración de infraestructura de sistemas de telecomunicaciones (p. 35*). Ediciones Paraninfo.

[12] Landeros S, Gonzales J. y Chavez S. (2013). *Análisis de la eficiencia de los estándares de transmisión de televisión digital por satélite en las bandas Ku y Ka*. Ingeniería Investigación y Tecnología, XIV (número 3), (p. 338).

[13] Ruido de Universitat de les Illes Balears *(p. 2.1)*. [En línea]. (2007). Recuperado de: http://dfs.uib.es/GTE/education/telematica/sis_ele_comunicacio/Apuntes/Capitulo%203.pdf

[14] Mera, S. (2007). *Estudio del ruido a altas frecuencias en transistores de efecto de campo de silicio germanio (SiGe) (pp. 28-30)*. Trabajo de grado, Ingeniería en comunicaciones y electrónica, Instituto Politécnico Nacional. México.

[15] Vega, C. Zamanillo J. y Casanueva, A. (2007). Ruido en *Sistemas de telecomunicaciones (p. 262)*. Textos universitarios, Universidad de Cantabria.

[16] Cortes, G. (2011). *Calculo del ancho de banda (p.108)*. Revista Negocios de Seguridad.

[17] España, M. C. (2003). La red telefónica conmutada en *Servicios avanzados de telecomunicaciones (p. 93*). Ediciones Díaz de Santos.

[18] Tomasi, W. (2003). Comunicaciones digitales en *Sistemas de comunicaciones electrónicas* (pp. 467-523) (4ta edición). México: Pearson Educación.

[19] PROMAX. (2014). Manual del buen instalador [Mensaje en un blog]. *El blog de PROMAX. Recuperado de: https://blogdepromax.wordpress.com/2014/06/26/manual-del-buen-instalador-i-el-ber/*

[20] Pallares, J. (2009). *VII Congreso Instaladores PROMAX*. (pp. 11- 21), PROMAX.

[21] Fraundez, M. (2001). Emisores, Receptores y Antenas en *Sistemas de Comunicaciones (p. 63)*. 1era. Edición: Marcombo.

[22] Ettus Research, VERT400 Antenna en *Catalog Pruduct*. Recuperado de: https://www.ettus.com/product/details/VERT400

[23] Fraundez, M. (2001). Emisores, Receptores y Antenas en *Sistemas de Comunicaciones (pp. 64-69)*. 1era. Edición: Marcombo.

[24] Pinar, I. y Murillo, J. J. (2011). *Laboratorio de Comunicaciones Digitales Radio Definida por Software (p. 11)*. (1a edición). Depto. Teoría de la señal y comunicaciones. Universidad de Sevilla.

[25] National Instruments. Software Defined Radio Device en *Products*. Recuperado de: https://www.ni.com/es-mx/shop/select/usrp-software-defined-radio-device

[26] Montero, J. P. (2014). *Implementación de un sistema de comunicación basado en Software Radio (pp. 28 -30)*. Depto. Tecnología Electrónica y de las Comunicaciones, Universidad Autónoma de Madrid.

[27] Liu, P. (2014). *Development of an ice-penetrating software-defined radar using the universal software radio peripheral platform*. Trabajo de grado, Maestría en ciencias e ingeniería eléctrica (pp. 23-28). Universidad del estado de Pensilvania, Pensilvania.

[28] National Instrument Support (2013). *Introduction to Software-Defined Radio with LabVIEW and USRP* (p. 4). Manual de introducción.

[29] Marin, E. (2013). *Security analysis of an implantable cardioverter defibrillator (p. 8)*. Trabajo de grado, Maestría en Ingeniería Eléctrica, Universidad Católica de Lovaina, Lovaina

[30] Bolaños, L. A. y Ruiz, A. A. (2015). *Diseño de un algoritmo para el análisis y monitoreo de parámetros de señales LTE 4G utilizando la plataforma de radio definida por software (USRP)* (pp. 41-44). Trabajo de grado, Ingeniería en electrónica, Universidad Politécnica Salesiana, Ecuador.

[31] National Instrument Support (2013). *Introduction to Software-Defined Radio with LabVIEW and USRP* (pp. 7-12). Manual de introducción.

[32] IBM Knowledge Center. *Cifrado* en MQ Version 7.0.1 documentation. Recuperado de:https://www.ibm.com/support/knowledgecenter/es/SSFKSJ_7.0.1/com.ibm.mq.csqzas.doc/sy10500_.htm

[33] Ramió, J. (2014). ¿Qué son los principios de Kerckhoffs? en *Criptored* [En línea]. Recuperado de: http://www.criptored.upm.es/thoth/material/texto/pildora007.pdf

[34] De Luz, S. (2010). Criptografía: Algoritmos de cifrado de clave simétrica en *Redes@Zone* [En línea]. Recuperado de: https://www.redeszone.net/2010/11/04/criptografia-algoritmos-de-cifrado-de-clave-simetrica/

[35] Quero E., García A. y Peña J. (2007). *Mantenimiento de portales de la Información: explotación de sistemas informáticos* (pp. 101 y 12). Editorial: Paraninfo.

[36] Facultad de ingeniería (2010). *Fundamentos de Criptografía de Laboratorio de redes y seguridad* [En línea]. Recuperado de: http://redyseguridad.fi-p.unam.mx/proyectos/criptografia/criptografia/index.php/5-criptografia-asimetrica-o-de-clave-publica/54-rsa-rivest-shamir-adelman

[37] LabView Digital Modulation Documentation Help. *MT Generate System Parameters VI*. Recuperado de: https://documentation.help/LabView-Digital-Modulation/MT_Generate_System_Parameters.html.

[38] Juárez, O. (2016). *Estudio de Técnicas de Modulación Mediante Radios NI USRP (p. 43)*. Trabajo de grado, Ingeniería en telecomunicaciones, Universidad Nacional Autónoma de México, México.

[39] LabView Digital Modulation Documentation Help. *MT Generate Filter Coefficients VI*. Recuperado de: https://translate.google.com/translate?hl=es-419&sl=en&tl=es&u=https%3A%2F%2Fdocumentation.help%2FLabView-Digital-Modulation%2FMT_Generate_Filter_Coefficients.html&anno=2

[40] Jaimes, O. (2017). *Turbo envío: una estrategia de retransmisión rápida para enviar paquetes en redes inalámbricas ad hoc (pp. 33 y 34)*. Trabajo de grado, Maestría en Ingeniería eléctrica-telecomunicaciones, Universidad Nacional Autónoma de México, México.

[41] LabView Digital Modulation Documentation Help. *MT Demodulate PSK VI*. Recuperado de: https://documentation.help/LabView-Digital-Modulation/MT_Demodulate_PSK.html

9. ANEXO

Diagrama de bloques de transmisor

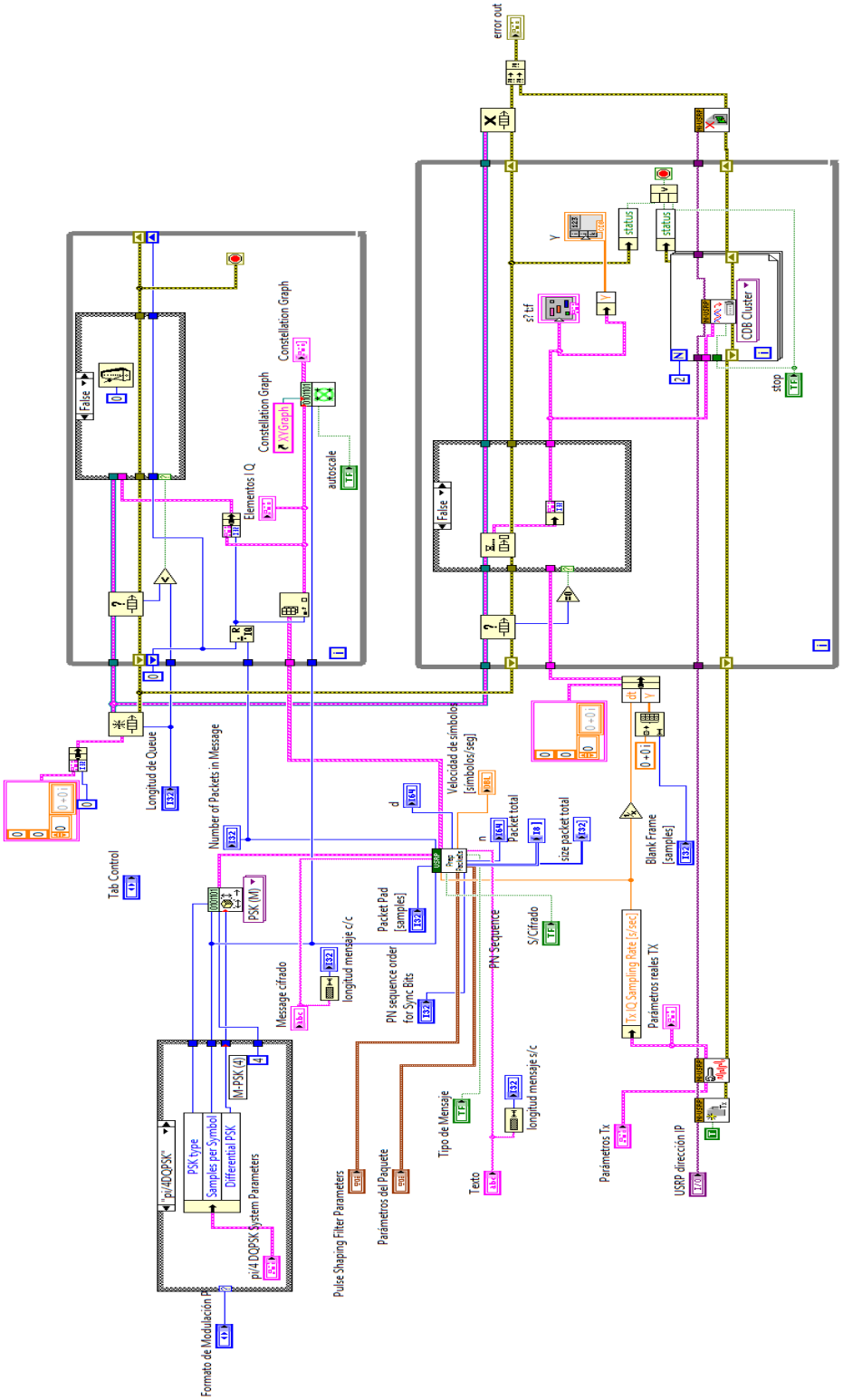
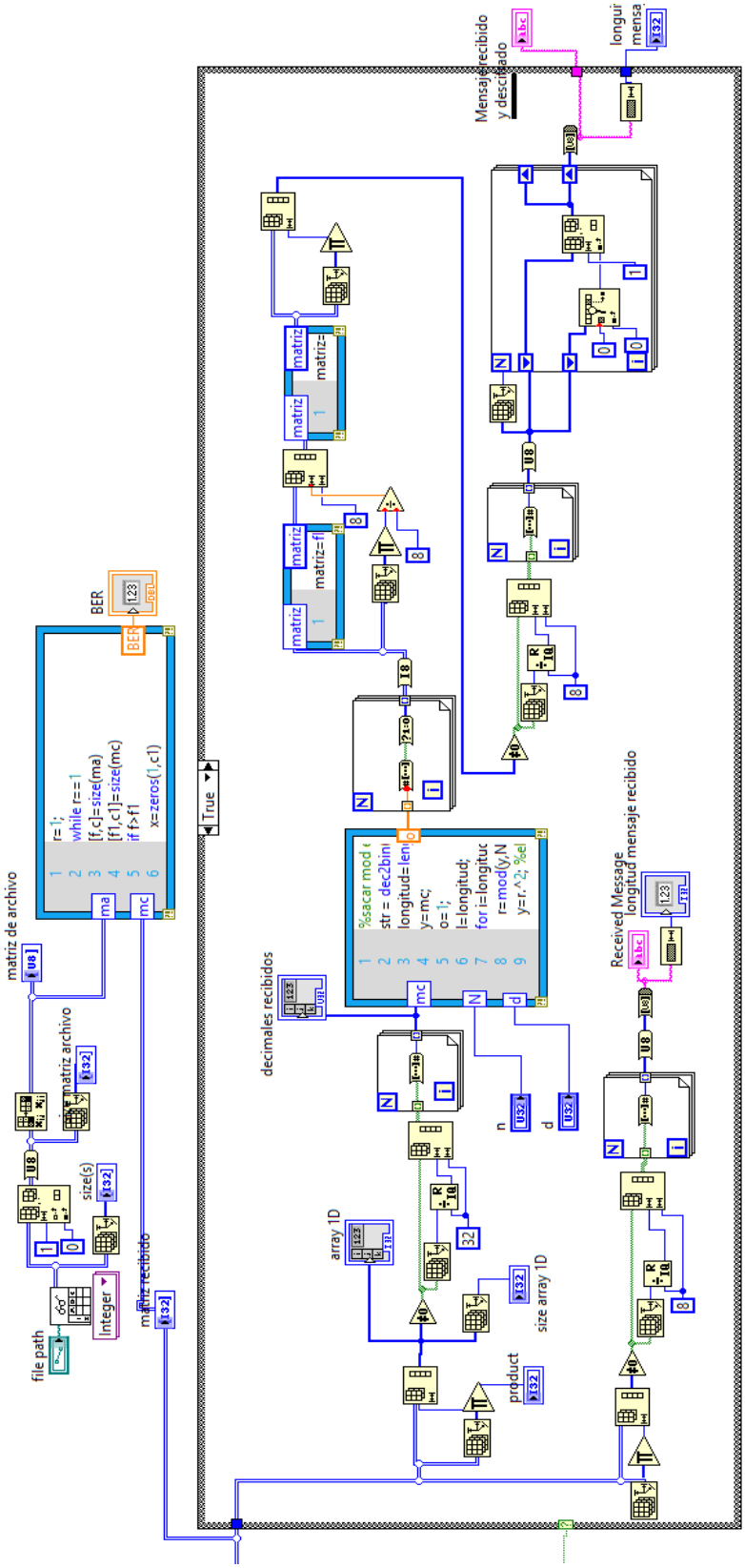


Diagrama de bloques del código de cifrado



10. ACRÓNIMOS:

NI-USRP: National Instrument- Universal Software Radio Peripheral.

BPSK: Binary Phase-Shift Keying.

QPSK: Quadrature Phase-Shift Keying.

8-PSK: 8-Phase-Shitf Keying.

CDMA: Acceso Multiple por Divsión de Código

WiMAX: Worldwide Interoperability for Microwave Access

WLAN: wirless local area network

DVB: Digital Video Broadcasting

GSM: Global System for Mobile

LTE: Long Term Evolution

MIMO: Multiple-Input Multiple-Output

PLL: Pashe Locked Loop

VCO: Voltage Controlled Oscillators

LO: Local Oscillators

POO: Programacion Orientada a Objetos

VI: Virtual Instrument

DAC: Digital- Analogic Converter

FEC: Forward Error Correction.