Benemérita Universidad Autónoma de Puebla.

Facultad de Ciencias de la Computación.

Título de tesis:

Ocultación de la información mediante el ruido en audio (Esteganografía digital).

Que para obtener el Título de:

Licenciatura en Ingeniería en Ciencias de la Computación

Presentada por:

Carlos Sánchez Alvarez.

Asesor de Tesis:

Dra. Bárbara Emma Sánchez Rinza.

Puebla, Puebla. Octubre 2015.

Quiero dedicar esta tesis a mis Padres. Esto es para ustedes, para ti mamá **María Beatriz Alvarez Jiménez** y para ti papá **Efraín Sánchez Vázquez.**

AGRADECIMIENTOS

Quiero dar mis más sinceros agradecimientos a todas las personas que se involucraron y fueron parte de esta faceta de mi carrera profesional al contribuir a la realización de esta tesis:

A mi asesora de tesis la Dra. Bárbara Emma Sánchez Rinza quien me brindó su apoyo y consejos para realizar esta investigación. Así mismo por involucrarme a mundo de la investigación por confiar plenamente en mí, enseñando con su ejemplo profesional el cómo ser una mejor persona.

A mis sinodales: M.C. Carlos Adrián Antonio Martínez Camarillo y M.C Ana Patricia Cervantes Márquez por haberme acompañado brindándome su conocimiento y experiencia como profesores de la facultad de computación.

A mis padres y hermano, de quienes me siento extremadamente orgulloso y no los cambiaría por nada. Porque fueron el motor para luchar por este objetivo de vida y ser alguien en la vida, el camino no fue fácil pero se los demostré echándole ganas para terminar mi carrera profesional. Los tropiezos y las piedras en el camino fueron bastante, recordando las palabras que me dieron fuerza para no tirar la toalla; si fuera fácil cualquiera lo lograría. Les estoy profundamente agradecido por su apoyo incondicional y cariño. Motivándome en cada fase de mi vida personal y profesional, enseñándome valores para ser una mejor persona, además de decirles que son los máximo como padres no los cambiaría por nada, me enseñaron a que nada es fácil en esta vida pero tampoco imposible, me dieron la fuerza necesaria y la motivación que necesite para este gran proyecto de vida, mi carrera profesional.

A mis suegros la Sra. María Eugenia Zepeda Mateos y el Sor. José Rubén Huerta Sánchez y a mi esposa Christian Alicia Huerta Zepeda, por su apoyo incondicional ya que ustedes también formaron parte de esta etapa de mi vida, involucrándose en mis obstáculos que se me presentaron al finalizar mi carrera profesional, aconsejándome y motivándome para echarle ganas y no dejar mis objetivos.

Por ultimo a mis amigos: Víctor Fabián Valderrábano Martiñon, Lizbeth Ramos Ramírez, Viridiana Vega Cervantes, Katia Cecilia Flores y los que faltaron mencionar también. También a mis compañeros de trabajo y grandes amigos: Mtro. Fernando Armando Rosales Vera, Lic. Antonia Sánchez Medina y al Lic. Horacio Morales García, quienes de alguna forma me ayudaron a ser mejor persona en el ámbito profesional y laboral apoyándome con su amistad, consejos y ayuda incondicional, para no dejarme vencer y lograr este objetivo.

INDICE

INTRODUCCIÓN 1

CAPÍTULO I: 3
EL AUDIO Y EL RUIDO. 3
1.1 ¿QUE ES EL AUDIO? 3
1.1.1 Componentes Del Audio. 4
1.1.2. Parámetros Del Audio. 4
1.2 CALIDAD EN EL AUDIO DIGITAL 5
1.3 SISTEMA AUDITIVO HUMANO 6
1.4 MEDIOS QUE TRASMITEN EL SONIDO. 7
1.5 DIGITALIZACIÓN DEL SONIDO. 8
1.5.1 Conversión analógica - digital (ADC). 10
1.5.2 Conversión digital – analógico (DAC). 12
1.6 EDICIÓN DE SONIDO DIGITAL. 12
1.6.1 Modificación de la dimensión temporal. 13
1.6.2 Modificación de la amplitud mediante operaciones de multiplicación. 13
1.6.3 Modificación de la frecuencia. 14
1.7 LA VOZ HUMANA 15
1.7.1 Grabación y reproducción de audio. 15
1.8 ¿QUE ES RUIDO? 16
1.8.1 Términos que se le pueden asignar al ruido en los diferentes campos 17

CAPÍTULO II: 18
CRIPTOGRAFIA Y ESTEGANOGRAFIA 18
2.1 CRIPTOGRAFIA. 18
2.2 CLASIFIACION DE LA CRIPTOGRAFIA. 21
2.2.1. Época histórica. 21
2.2.2Según el algoritmo. 22
2.2.3 Según el procedimiento 23
2.3 ELEMENTOS PARA FORMAR UN CRIPTOSISTEMA REFERENTE A UN METODO DE CIFRADO. 23
2.4.1 Cifrado Polybios. 24
2.4.2 Encriptación Cifrado de Cesar. 25
2.4.3 Cifrado de Vigenére. 26
2.4.4 Cifrado de Playfair 27
2.4.5 Cifrado de Hill. 27
2.4.6 Cifrado de Vermam. 28
2.5 USO DE LA CRIPTOGRAFIA. 28
2.5.1 Confidencialidad en el cifrado. 28
2.5.2 Autentificación en el cifrado. 29
2.5.3 Verificación de la integridad en el cifrado. 30
2.5.4 Mecanismo de no repudio en el cifrado. 30
2.6 ESTEGANOGRAFIA. 30
2.6.1 Técnicas de la Esteganografía Digital. 32
2.6.2 Campos que implican la Esteganografía. 33
2.6.3 División de la Esteganografía. 34
2.7 FUNCIONAMIENTO DE LA ESTEGANOGRAFIA. 34
2.8 TIPOS DE METODOS PARA LA ESTEGANOGRAFÍA 35
2.8.1 Esteganografía por un método de Sustitución. 35
2.8.2 Esteganografía por un método de Inyección. 36
2.8.2 Esteganografía por un método de generación de un nuevo fichero. 36

CAPÍTULO III: 37
METODO DE CIFRADO E IMPLEMENTACIÓN 37
3.1 ESTEGANOGRAFIA ENFOCADA AL AUDIO, MEDIANTE UNA SEÑAL DE RUIDO. 37
3.2 Elementos necesarios para el desarrollo del método de cifrado digital 38
3.3 Clasificación para este método de cifrado. 40
3.4 Diseño del Método Esteganográfico enfocado al audio mediante una señal de ruido. 41
3.5 Implementación: Método Esteganográfico enfocado al audio mediante una señal de ruido generando el criptograma. 42
3.6Como quitar reducir el ruido con Adobe Audition CC 2014. 57
3.7 Descifrado del criptograma creado por el método esteganográfico enfocado a un audio mediante una señal de ruido. 63

CAPÍTULO IV: 67
RESUTADOS 67
4.1 METODO DE CIFRADO MODERNO TOMANDO UN ARCHIVO DIGITAL, UN AUDIO Y UNA APLICACIÓN DE EDICION DE AUDIO. 67
4.2 CRIPTOGRAMA GENERADO EN UN AUDIO, CIFRADO DE LA INFORMACION. 70
4.3 DESCIFRADO DE LA INFORMACION EN UN AUDIO, CRIPTOGRAMA. 71
4.4 ENFOQUE Y APLICACIÓN DEL PROYECTO. 72
4.5 INNOVACION DEL PROYECTO. 74
4.6 VIABILIDAD, IMPACTO ECONÓMICO, SOCIAL Y/O TECNOLÓGICO DEL PROYECTO. 76
4.7 OPINION Y REACCION DE USARIOS QUE UTILIZAN ALGUN TIPO DE DISPOSITIVO CONECTADO A INTERNET Y SE LES ENVIA EL CRIPTOGRAMA EN UN AUDIO. 81

CAPÍTULO V: 82
CONCLUSIONES 82

BIBLIOGRAFIA 84

RESUMEN.

En esta era de la conectividad electrónica universal, de virus, de hackers y fraudes electrónicos, no hay momento en que no importe la seguridad. En primer lugar al enorme crecimiento de los sistemas computacionales, móviles y sus interconexiones mediante redes ha hecho que organizaciones e individuos dependa cada vez más de la información almacenada y se trasmite a través de estos sistemas conectados en red. Esto a su vez ha aumentado la conciencia de la necesidad de proteger los datos y los recursos, garantizando la autenticidad de los datos y los mensajes protegiendo los sistemas frente ataques de red. En segundo lugar, las disciplinas de la criptografía y la seguridad de la red han madurado, dando como resultado aplicaciones prácticas, ya disponibles para la seguridad de red.

Ante esta situación y con la finalidad de minimizar los riesgos de la inseguridad de la información que se envía a través de la red de internet, es necesario optar por cifrar la información para proteger los datos antes de ser enviada por este medio mediante algún método de cifrado, si la información se llegara a perder o intentan robar, tengan información sin contenido claro. Además de generar una alternativa más para cifrar la información con este nuevo método de cifrado moderno involucrando un archivo digital como lo es un audio.

Además de que la mayoría de los métodos que existen de manera pública, para la codificación de la información, están enfocados a textos planos, casi todos tienen una forma parecida para cifrar la información es decir, alteran la información mediante combinaciones alfabéticas cada uno cumpliendo diferentes estándares para su cifrado y descifrado convirtiéndose en métodos de cifrado clásicos o antiguos. Son contados los métodos de codificación modernos que existen en la actualidad que involucran un archivo digital para cifrar información.

En resumen, la implementación de nuevas tecnologías trae de la mano, la introducción de nuevas oportunidades de negocio, así como también riesgos, amenazas y nuevos vectores de ataque, siendo requerido como parte de un proceso continuo, la revisión constante de los modelos de seguridad y como una alternativa están los métodos de cifrado para la seguridad de la información.

INTRODUCCIÓN

Como ya se sabe el ruido en términos generales es la sensación auditiva inarticulada desagradable, en el ambiente se define como algo molesto para el oído humano, un contaminante si este es excedido. En el ámbito de la comunicación sonora, se define como ruido, todo sonido no deseado que interfiere en la comunicación entre las personas o sus actividades. Desde ese punto de vista, en un audio (un tono musical, una melodía o una canción) puede ser calificada como ruido por aquella persona que en cierto momento no desee oírla.

En ocasiones, lo que grabamos puede contener ciertos ruidos de fondo en nuestro sonido, los cuales pueden ser debido al medio ambiente o ruidos producidos por el micrófono o el ordenador (especialmente, cuando el micrófono o instrumento de grabación, no es muy bueno).

Como es claro el ruido es considerado un contamínate ambiental, algo molesto y negativo, pero en este proyecto lo utilizaremos para algo positivo, para ocultar un mensaje, con el objetivo de pasar información (mensaje) desapercibida en la red, escondido en un audio con ruido. Hablando en términos computacionales y en el área de seguridad en redes, la ciencia de ocultar la información es estudiada por la criptografía y la esteganografía digital (audio). El propósito de este proyecto es generar un nuevo **método de cifrado moderno en un archivo digital**. Existen pocos métodos de cifrado que involucren para su proceso de cifrado un archivo digital, la mayoría de estos métodos están enfocados a textos planos mediante la alteración y cambio de posición de caracteres.

Los objetivos generales de este proyecto son:

- ✓ Ocultar información (grabación de voz) en un audio mediante una señal de ruido
- ✓ Poder enviar el criptograma formado por un audio y ser enviado por el canal de la red de internet, pasando desapercibida la información sin sospechas de contenido de información relevante.
- ✓ Informar algunos métodos de encriptación clásicos que son de exposición abierta al público, dando un resumen teórico de cómo funcionan cada uno de estos métodos de cifrado de la información, con el propósito de involucrarnos en el tema y entender los conceptos de cifrados.

Los objetivos específicos para este proyecto son:

- ✓ Investigar una aplicación de audio apropiada para manipular las señales de ondas de frecuencia de un audio, para la implementación del método de cifrado.
- ✓ Eliminar o Reducir el ruido de una grabación de voz.
- ✓ Generar la teoría, características y elementos de este nuevo método de cifrado digital tomando como referencia la encriptación y la esteganografía.

Este documento presenta la información divida en cinco capítulos, con la finalidad de involucrar y entender los conceptos que se tomaron en cuenta para cumplir con cada uno de los objetivos de esta investigación exponiendo y explicando la información tomada en cuenta para este proyecto. En el capítulo 1, se habla todo lo referente al audio (sonido) y el ruido. En el capítulo 2, se expone que es la criptografía y la esteganografía, su uso, su clasificación, se mencionan algunos ejemplos de métodos de cifrado y métodos esteganográficos, además de los elementos para formar su criptosistema referente a un método de cifrado. En el capítulo 3 se explica los elementos necesarios para generar este nuevo método de cifrado explicando paso a paso la implementación de este método de cifrado. En el capítulo 4 se abordan los resultados del proyecto y por último en el capítulo 5 se dan las conclusiones de la investigación.

La aplicación que se presentará en este documento es la herramienta "**Adobe Audition cc 2014**" que fue de gran apoyo para la implementación del proyecto.

CAPÍTULO I:

EL AUDIO Y EL RUIDO.

1.1 ¿QUE ES EL AUDIO?

El audio digital es la representación de señales sonoras mediante un conjunto de datos binarios. Un sistema completo de audio digital comienza habitualmente con un transceptor (micrófono) que convierte la onda de presión que representa el sonido a una señal eléctrica analógica [1].

Esta señal analógica atraviesa un sistema de procesado analógico de señal, en el que se puede realizar limitaciones en frecuencia, ecualización, amplificación y otros procesos. La ecualización tiene como objetivo contrarrestar la particular respuesta en frecuencia del transceptor utilizado de forma que la señal analógica se asemeje mucho más a la señal de audio [1].

Tras el procesado analógico la señal se muestrea, se cuantifica y se codifica. El muestreo toma un número discreto de valores de la señal analógica por segundo (tasa de muestreo) y la cuantificación asigna valores analógicos discretos a esas muestras, lo que supone una pérdida de información (la señal ya no es la misma que la original). La codificación asigna una secuencia de bits a cada valor analógico discreto. La longitud de la secuencia de bits es función del número de niveles analógicos empleados en la cuantificación. La tasa de muestreo y el número de bits por muestra son dos de los parámetros fundamentales a elegir cuando se quiere procesar digitalmente una determinada señal de audio [1].

Podemos definir tres aspectos de cualquier audio, primero debe haber una fuente de sonido; como cualquier onda mecánica, la fuente de ondas sonoras es un objeto en vibración. Segundo, la energía se transfiere desde la fuente en forma de ondas sonoras longitudinales. Y tercero, él sonido es detectado por el oído o por un micrófono [1]. El sonido son ondas producidas por las vibraciones de los objetos materiales.

Un audio digital se puede guardar, copiar y reproducir infinitamente sin perder calidad.

1.1.1 Componentes Del Audio.

- **Frecuencia** (altura): número de vibraciones por segundo, en el audio se mide en hercios (Hz), el oído humano pude oír entre 20 Hz y 20 Khz.
- **Amplitud** (intensidad y volumen): cantidad de fuerza o energía de sonido, la medida de la amplitud es logarítmica y se hace en **decibelios dB**, subir 3 dB duplica la potencia de sonido.

En la figura 1.1.1 se muestra dependiendo de la señal de audio, como se mide la frecuencia y amplitud.

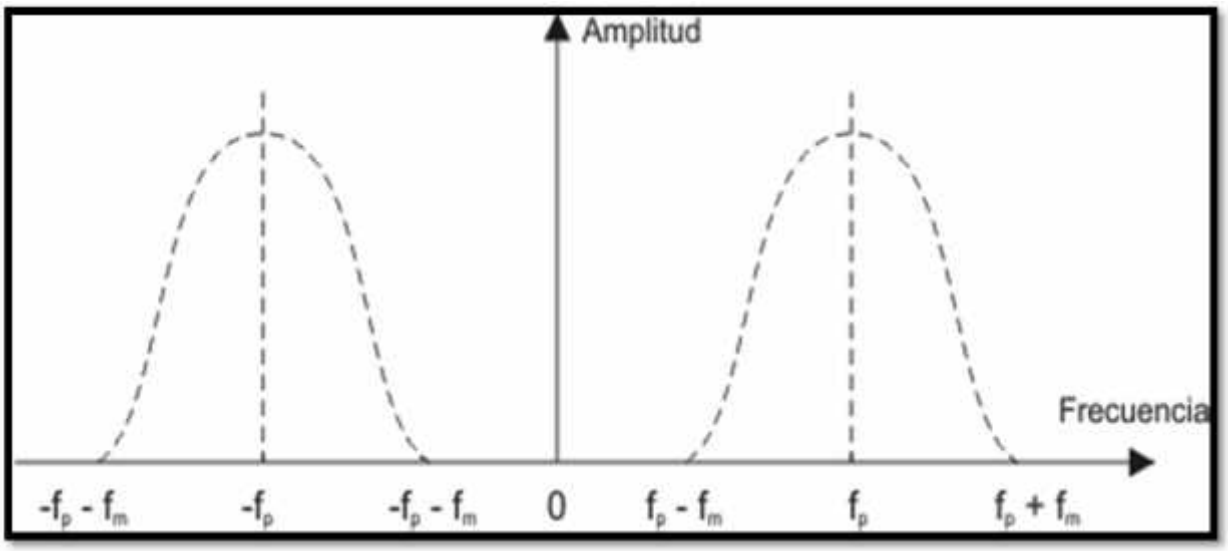

Figura 1.1.1 Medición de la amplitud y frecuencia de una señal de audio.

- **Ancho de banda:** es la diferencia de las frecuencias en las que se produce una caída de la amplitud del sonido determinada (se suele usar en 3 dB).
- **Ruido:** sonidos aleatorios que proceden de diversas fuentes y distorsionan o enmascaran el sonido fundamental. Se mide de dB.

1.1.2. Parámetros Del Audio.

Los parámetros básicos para describir la secuencia de muestras que representa el sonido son:

- El número de canales: 1 para mono, 2 para estéreo, 3 para el sonido cuadrafónico, etc. En la figura 1.1.2 se muestra cómo es que se propaga el sonido dependiendo de qué canal este activado salida mono o estéreo.

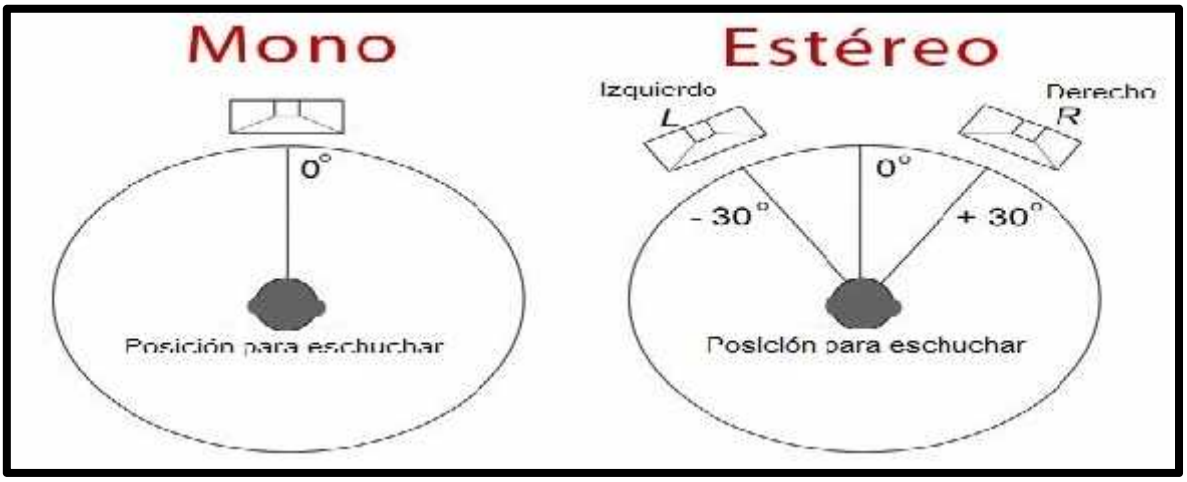

Figura 1.1.2 Representación gráfica de cómo es un de sistema de audio con salida mono y estéreo, así también de cómo se distribuyen las ondas de frecuencias en una persona.

- Tasa de muestreo: El número de muestras tomadas por segundo en cada canal.
- Número de bits por muestra: Habitualmente 8 o 16 bits.

Como regla general, las muestras de audio multicanal suelen organizarse en tramas. Una trama es una secuencia de tantas muestras, como canales correspondiendo cada canal. En este sentido el número de muestras por segundo coincide con el número de tramas por segundo. En estéreo, el canal izquierdo suele ser el primero.

1.2 CALIDAD EN EL AUDIO DIGITAL

La calidad del audio digital depende fuertemente de los parámetros con los que esa señal de sonido ha sido adquirida, pero no son los únicos parámetros importantes para determinar la calidad.

Una forma de estimar la calidad del sonido digital es analizar la señal diferenciada entre el sonido original y el sonido reproducido a partir de su representación digital. Según esta estrategia podemos hablar de una relación señal a ruido concreta.

Para los sistemas digitales con otro tipo de compresión la relación entre una señal de ruido puede indicar valores muy pequeños aunque las señales sean idénticas para el oído humano.

La razón es que la relación señal a ruido no es un buen parámetro de medida de la calidad de sonido debido a que la calidad que percibe el oyente está determinada por la respuesta del oído humano a las ondas sonoras, que no percibe

muchas de las posibles diferencias. Lógicamente si las señales son muy parecidas, el oído no las podrá diferenciar, pero también pueden ser muy distintas y ser percibidas como la señal original. Por lo tanto parece más apropiada la evaluación de la calidad de un sistema digital mediante parámetros de sensibilidad del oído humano y pruebas específicas con oyentes especializados. En la figura 1.2.1, se muestra cuando como se propaga una onda se sonido teniendo un obstáculo. [17]

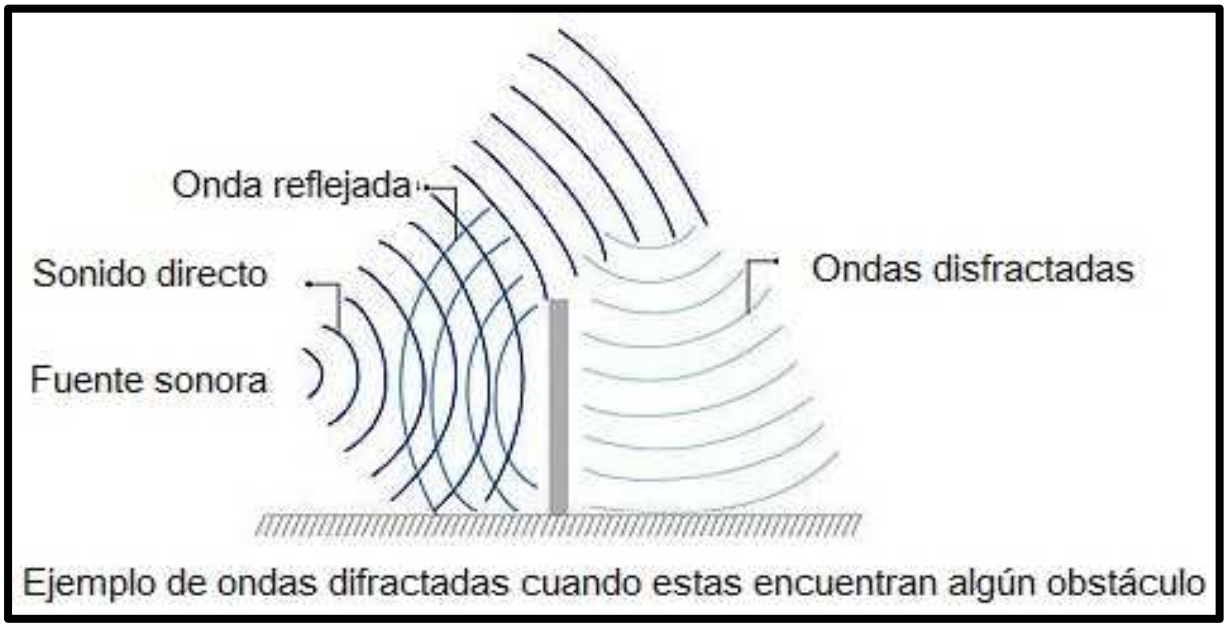

Figura 1.2.1 Ejemplo de ondas de sonido, cuando se encuentran con algún obstáculo.

1.3 SISTEMA AUDITIVO HUMANO

El sonido está asociado con nuestro sentido auditivo y, por lo tanto con la fisiología del oído y la psicología del cerebro que interpretan las sensaciones que llegan a los oídos. También hace referencia a la sensación física que estimula nuestros oídos mediante ondas longitudinales.

La estructura de nuestro sistema auditivo para la recepción del sonido es el que se describe a continuación. El tímpano, que es una membrana, vibrará en simpatía con las partículas de aire que la rodean y provocará la vibración de los huesos del oído interno. A continuación se muestra como está formado el órgano auditivo en la figura 1.3.1

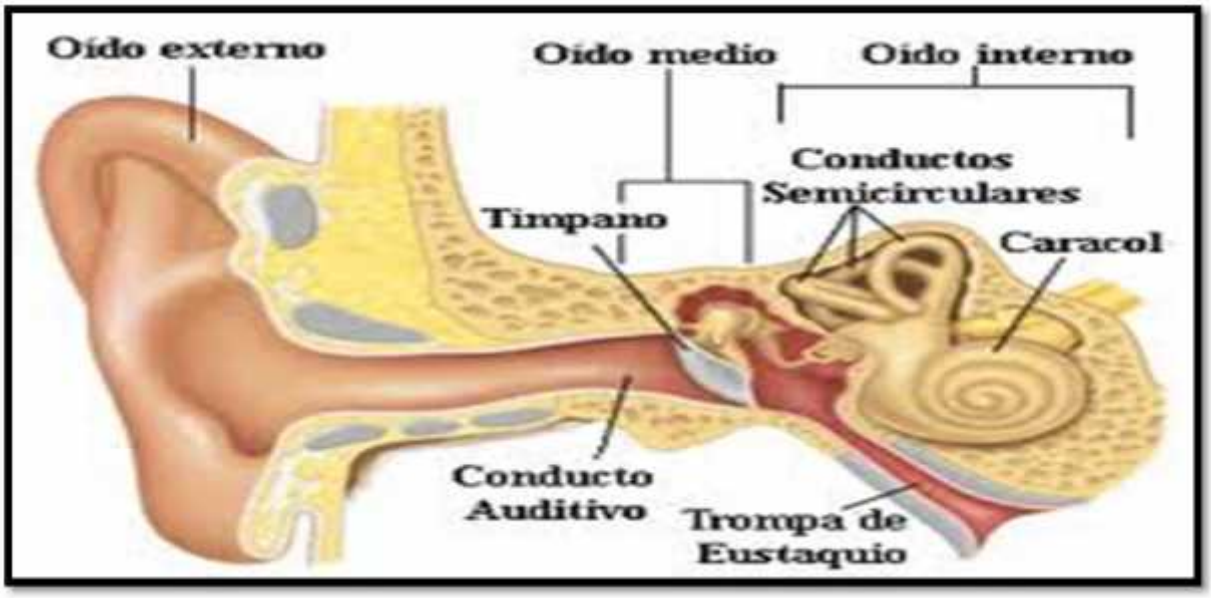

Figura 1.3.1 Sistema auditivo humano.

El elemento que transforma estos movimientos vibratorios en señales neuronales es la membrana basilar, dentro de la cóclea. La forma de la cóclea hace que las vibraciones que penetran en ella a través de la ventana oval alcancen de forma más intensa una zona más o menos profunda en función de su frecuencia. La membrana basilar está recubierta de pequeñas vellosidades conectadas a haces nerviosos que transmiten la información al cerebro. Como se puede apreciar por esta descripción, la información espectral del sonido (conjunto de frecuencias que componen la señal en un momento dado) llega ya desmenuzada a los centros auditivos del cerebro.

1.4 MEDIOS QUE TRASMITEN EL SONIDO.

La mayor parte de los sonidos que escuchamos se trasmiten a través del aire. No obstante, cualquier sustancia elástica, sea sólida, liquida, gaseosa o plasma, puede trasmitir el sonido. Comparado con los sólidos y líquidos, el aire es un conductor del sonido relativamente eficiente. El sonido de un tren distante puede escucharse con mayor claridad colocando una oreja contra el riel. De manera similar, cuando un reloj se encuentra sobre una mesa a una distancia que no se pueda captar en forma directa, este puede escucharse aplicando la oreja contra la mesa. La trasmisión del sonido requiere un medio; sin nada que comprimir y dilatar, no puede haber sonido [1]. En la figura 1.4.1 se muestra un objeto que trasmite un sonido.

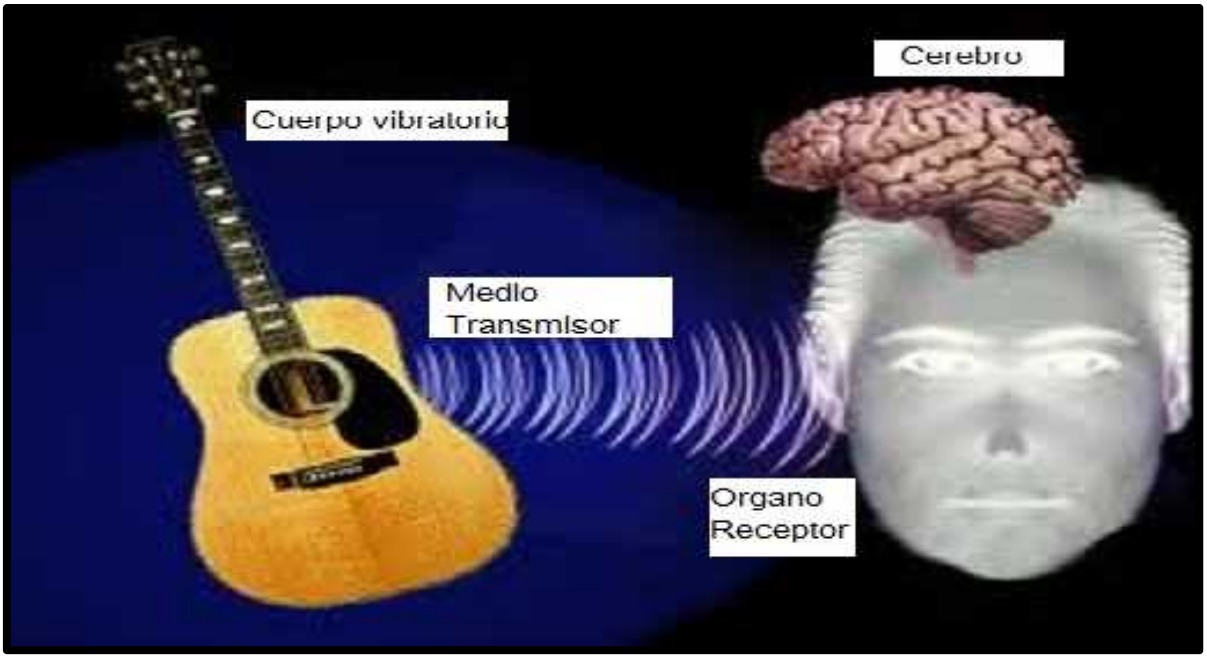

Figura 1.4.1 Ejemplo de un medio de trasmisión de sonido.

1.5 DIGITALIZACIÓN DEL SONIDO.

Nosotros no percibimos todas las ondas que se propagan a nuestro alrededor. Podemos comprobar que animales como perros y gatos son capaces de oír frecuencias que nosotros no alcanzamos. El ser humano es capaz de percibir, por término medio, los sonidos que hay en el espectro sonoro desde los 20 Hz a los 20 KHz; es decir, que el sonido más grave que podemos percibir es el que produce una cuerda al oscilar 20 veces por segundo, mientras que el más agudo es el que produce la misma cuerda si vibrase 20.000 veces por segundo. Por tanto, si queremos construir un sistema que grabe el sonido que nos rodea, no nos interesa que lo grabe todo, sino sólo aquellas porciones del espectro de frecuencias que podemos percibir.

La grabación digital no obtiene un registro de estas variaciones de frecuencia, sino que las analiza para extraer su descripción detallada. Como lo que llega a la membrana es una suma de frecuencias, estudiamos esta suma como una sola frecuencia, que tiene dos propiedades fundamentales: frecuencia y amplitud. ¿Cuál es la frecuencia de muestreo necesaria para efectuar un buen registro? La respuesta es sencilla: el doble de la máxima frecuencia de la señal original que queremos grabar si seguimos el teorema de Nyquist. Así, si lo que queremos es hacer un registro perfectamente fiel de todo el sonido que nos llega perceptible por

nuestro oído (20Hz – 20KHz), tenemos que tomar muestras al doble de la frecuencia máxima, 20 KHz. Así, esta frecuencia de muestreo debe ser de unos 44 KHz. [16]

El sonido, para su manejo en un sistema multimedia, ha de adquirirse por medios electrónicos. El primer elemento de la cadena es el micrófono, que convierte las variaciones de presión del medio en señales eléctricas. Éstas son después amplificadas para que alcancen los niveles adecuados para atacar las siguientes etapas del proceso.

La digitalización consiste en convertir los valores de intensidad de la señal en valores numéricos que la representen. Para ello se utilizan circuitos convertidores de analógico a digital ("ANALOG TO DIGITAL CONVERTER", o ADC) que llevan a cabo una conversión o lectura cada cierto tiempo. A cada lectura se la llama muestra y el número de muestras que se toman por segundo es la frecuencia de muestreo. Lógicamente, en algún momento esa misma señal o una versión mezclada, procesada o alterada de ella, ha de volcarse de nuevo al exterior en forma de sonido. Para ello se usa un convertidor de digital a analógico ("DIGITAL TO ANALOG CONVERTER" o DAC) conectado a un amplificador de salida y a un altavoz. A continuación se muestra el proceso que se lleva a cabo para digitalizar el sonido en la figura 1.5.1

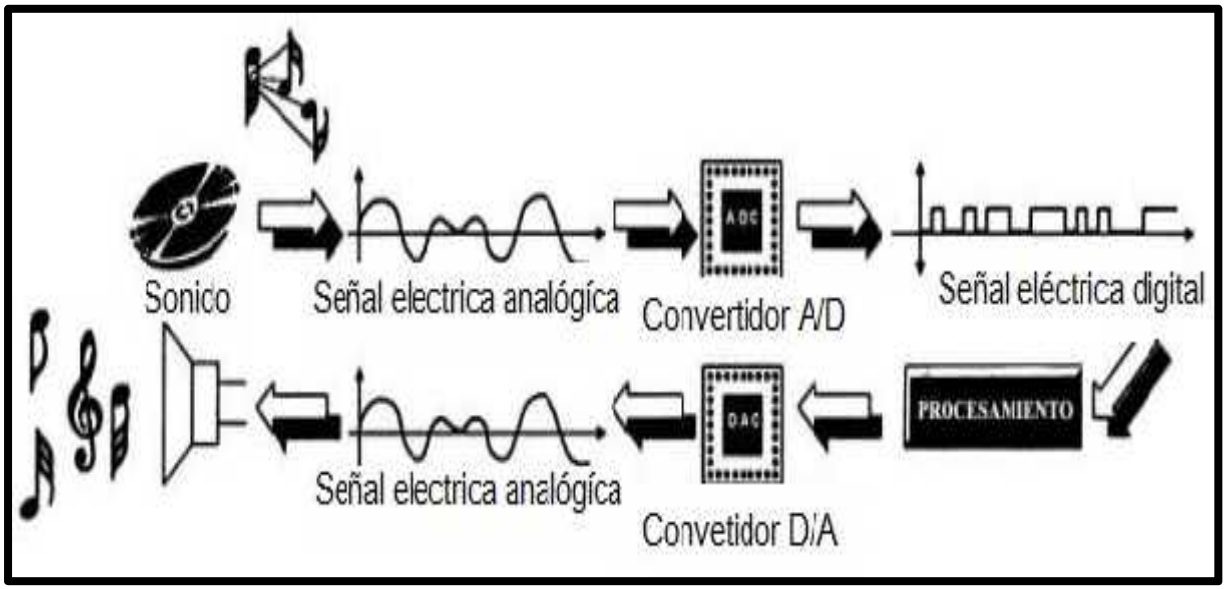

Figura 1.5.1 Proceso de digitalización del sonido (audio).

1.5.1 Conversión analógica - digital (ADC).

Dada una señal analógica, se van tomando valores discretos de su amplitud a intervalos de tiempo pequeños, evidentemente será más fiable la reproducción cuantas más muestras por segundo se tomen. A estos valores obtenidos se les asigna un valor digital que el computador puede entender y procesar como se requiera. Como se muestra en la figura 1.5.2

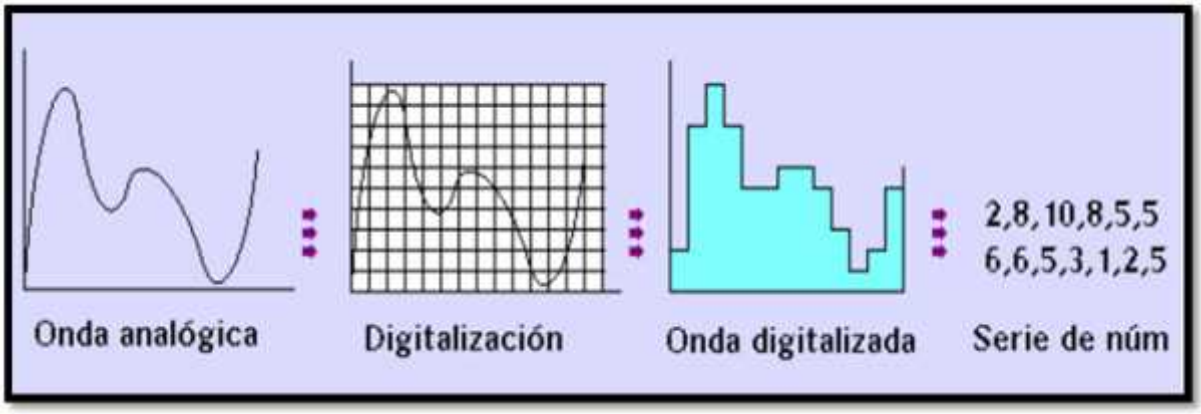

Figura 1.5.2 conversión A/D.

A cada muestra obtenida se le asigna un equivalente binario ya que es en este sistema en el que trabajan las computadoras, su unidad de información es el bit. Un bit solo puede tomar dos posibles valores "1" o "0", es lógico pensar que será necesario ampliar esta unidad de información para así poder asignar a cada valor de muestra tomada un equivalente binario. Por esta razón y dependiendo de la fidelidad con que queramos trabajar podemos utilizar palabras de 8 o 16 bits pudiendo obtener así 256 o 65536 combinaciones distintas y obtener mayor resolución.

- **Muestreo**, se van tomando valores discretos de la amplitud de una onda sonora a intervalos de tiempo pequeños.
- **Frecuencia de muestreo,** más frecuencia si se va a muestrear un sonido de más frecuencia. Como en la figura 1.5.3.

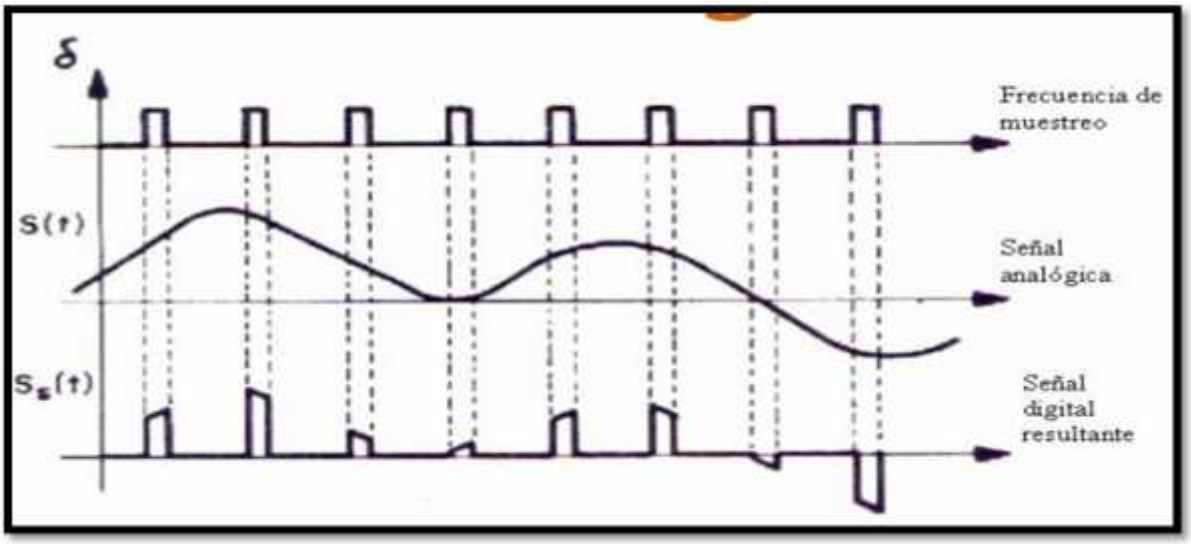

Figura 1.5.3 Frecuencia de muestreo de una señal analógica.

- **Resolución,** calidad del muestreo, más escalones

Para cuantificar la amplitud de onda muestreada, como se muestra en la siguiente figura 1.5.4.

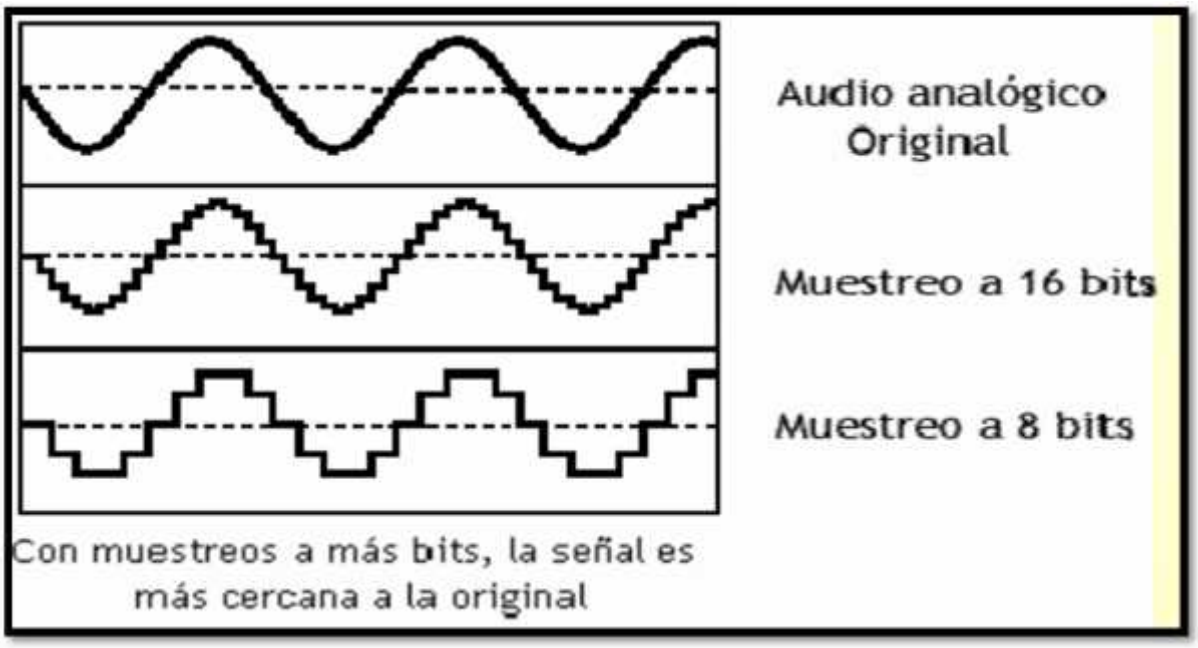

Figura 1.5.4 calidades del sonido y bit.

1.5.2 Conversión digital – analógico (DAC).

El proceso inverso es mucho menos complejo ya que solo se trata de ir poniendo los valores de las muestras en el mismo orden que fueron tomados y unos filtros electrónicos se encargan de convertir esa señal resultante de valores discretos en una señal analógica. Reconstrucción de una onda sonora a partir de los valores discretos de las muestras convenientemente filtrados. En la figura 1.5.5 se muestra el proceso de conversión A/C.

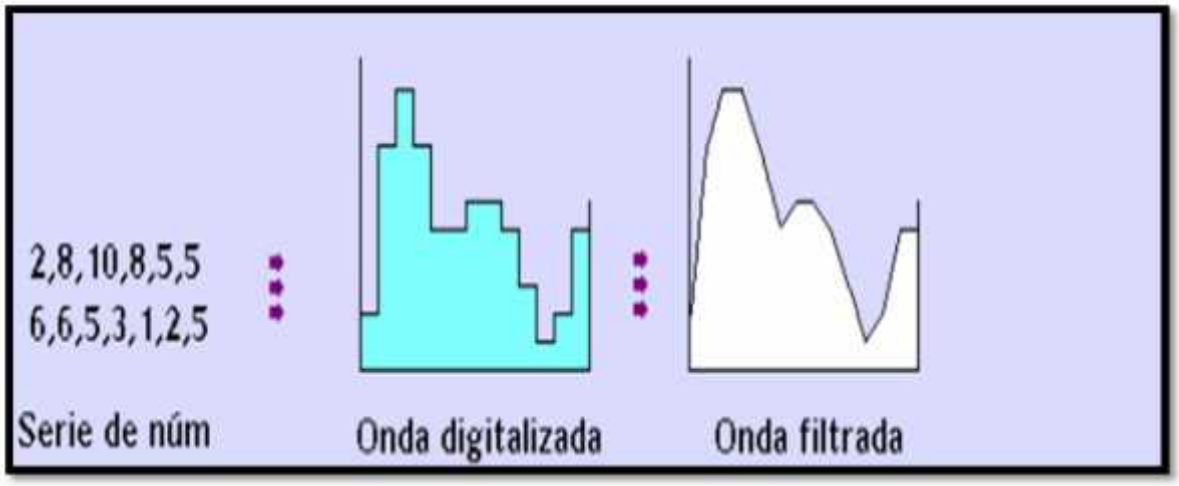

Figura 1.5.5 Conversión A/C.

1.6 EDICIÓN DE SONIDO DIGITAL.

Una de las mayores ventajas del sonido digital es la enorme flexibilidad que ofrece a la hora de editar el sonido. Una vez digitalizado el sonido y convertido en una secuencia de números, los programas de edición de sonido digital permiten aplicar operaciones matemáticas a dichos números para hacer todo tipo de modificaciones en el sonido original.

Se pueden clasificar las técnicas de edición de sonido digital atendiendo al aspecto del sonido que se modifica. Las propiedades del sonido que podemos modificar y las operaciones que podemos realizar sobre las mismas son:

1.6.1 Modificación de la dimensión temporal.

Cortar, copiar y pegar: lo que en la edición de sonido analógico se hacía cortando y pegando fragmentos de cinta magnética, se lleva a cabo ahora de manera sencilla con técnicas de manipulación directa. Para evitar ruidos en las transiciones, conviene seleccionar fragmentos con comienzo y final de valor nulo. O cambio de sentido: comenzar la reproducción de un sonido por el final y terminar por el principio.

Eliminar silencios: se define una amplitud por debajo de la cual el sonido se considera silencio, y se eliminan esos fragmentos. Puede servir para quitar las porciones inicial y final de una grabación, así como para eliminar las porciones de silencio entre sonidos. O Insertar silencios: de una duración determinada a partir de la posición del cursor.

1.6.2 Modificación de la amplitud mediante operaciones de multiplicación.

Modificar la ganancia: multiplicar las muestras por un número real. Al multiplicar por un valor entre 0 y 1 el nivel sonoro disminuye y si el valor es mayor que 1, aumenta.

Silenciar: multiplicar por cero las muestras de la zona seleccionada. O umbral de ruido: silencia las muestras por debajo de un determinado valor umbral. Permite eliminar el **ruido** de fondo, pero solo en aquellas porciones en las que no hay otros sonidos. También consigue que los ataques y decaimientos de los sonidos sean más bruscos. [16]

Normalizar: es un caso particular de modificación de la ganancia que obtiene la máxima amplitud posible sin que se produzca distorsión. Para ello, se recorre todo el fragmento de sonido y se registra la mayor amplitud de onda. Se calcula el cociente entre la mayor amplitud de onda posible y la mayor amplitud registrada. Finalmente, se multiplican todas las muestras por dicho cociente. [16]

Aplicación de envolventes: las envolventes son curvas que determinan la evolución temporal de la amplitud. Una envolvente puede especificar, por ejemplo, un aumento gradual del volumen al principio de un sonido, y una disminución brusca del mismo al final. O fundido de entrada y de salida (“fade in” y “fadeout”): son dos envolventes muy utilizadas. El fundido de entrada tiene valor inicial cero, y valor final uno y se usa para darle un comienzo progresivo al sonido. El fundido de salida tiene un valor inicial 1 y valor final 0 y sirve para darle un final progresivo al sonido. [16]

Modulación de la amplitud con una señal periódica: El efecto sonoro que se consigue es una variación cíclica del volumen (“trémolo”) o Inversión: hacer una reflexión de las muestras con respecto al eje horizontal, con lo que los valores positivos pasan a ser negativos y viceversa (cambio de fase). Se trata de un efecto sutil que se percibe mejor cuando se aplica a uno de los dos canales de un sonido estéreo. [16]

1.6.3 Modificación de la frecuencia.

Cambio de la frecuencia de reproducción: si un sonido muestreado a 44,1 KHz. se reproduce a 22,05 KHz. sonará una octava más grave y durará el doble de tiempo. El fichero original no se modifica.

Muestreo: a partir de las muestras de un sonido digital, aumentar o disminuir su frecuencia de muestreo, añadiendo o eliminando muestras respectivamente. Para pasar de 44,1 KHz. a 22,05 KHz. se elimina una muestra de cada dos. Antes de muestrear a una frecuencia más baja, conviene filtrar el sonido original y eliminar las frecuencias superiores a la mitad de la nueva frecuencia de muestreo. Para pasar de 22,05 KHz. 44,1 KHz., se crea por interpolación una nueva muestra entre cada dos. Hay que aclarar que este proceso no mejora la calidad del sonido, pero puede ser necesario por razones de compatibilidad entre programas o ficheros de sonido.

Transposición: es un término musical que significa subir o bajar la altura de una melodía uno o más semitonos. La transposición supone una variación de la duración del sonido: dura más cuanto más grave, y menos cuanto más agudo. O el “pitch bend” o modificación continúa de la frecuencia: es similar a la transposición, pero en vez de realizarse en intervalos discretos (semitonos) se lleva a cabo de forma continua. Se puede definir la evolución de la frecuencia en el tiempo mediante una envolvente. El efecto musical así obtenido se llama “glissando” y equivale a desplazar la mano izquierda sobre el mástil de una guitarra mientras suena una cuerda.

1.7 LA VOZ HUMANA

La voz humana es producida en la laringe, cuya parte esencial, la glotis, constituye el verdadero órgano de fonación humano. El aire procedente de los pulmones, es forzado durante la espiración a través de la glotis, haciendo vibrar los dos pares de cuerdas vocales, que se asemejan a dos lengüetas dobles membranáceas. Las cavidades de la cabeza, relacionadas con el sistema respiratorio y nasofaríngeo, actúan como resonadores.

La voz humana es el resultado de la vibración de las cuerdas vocales. En cada uno de estos casos una fuente en vibración trasmite una perturbación por el medio circundante, por lo general aire en forma de ondas longitudinales. La sonoridad del sonido depende de la amplitud de estas ondas; es decir, de cuanto aire se pone en movimiento. La altura del sonido está relacionada directamente con la frecuencia de las ondas sonoras, la cual es idéntica a la frecuencia de fuente vibrante. Las alturas producidas por las frecuencias inferiores se escuchan como notas bajas o graves, y las alturas superiores son producidas por las altas frecuencias [1].

1.7.1 Grabación y reproducción de audio.

Antes de que la computadora pudiera grabar, manipular y reproducir sonido, debe transformarse el sonido de una forma analógica audible a una forma digital aceptable por la computadora, mediante un proceso denominado conversión analógica - digital (ADC) y un software de edición de audio. Una vez que los datos de sonido se han almacenado como bytes en la computadora, puede hacerse uso de la potencia de la CPU de la computadora para transformar este sonido de miles de modos. Con el software adecuado es posible, por ejemplo, añadir reverberación o eco a la música o a la voz. Pueden eliminarse trozos de sonido grabado. Pueden mezclarse archivos de sonido, ajustarse el tono de la voz de manera que no pueda reconocerse y muchas cosas más. Finalmente, cuando se está dispuesto a escuchar el resultado, el proceso de conversión digital-analógica (DAC) transforma de nuevo los bytes de sonido a una señal eléctrica analógica que emiten los altavoces.

1.8 ¿QUE ES RUIDO?

El ruido es una mezcla de muchas frecuencias que tienen poca relación entre sí, y muestra un espectro de frecuencia continuo o casi continuo, es la sensación auditiva inarticulada generalmente desagradable. En el medio ambiente, se define como todo lo molesto para el oído. Desde ese punto de vista, la más excelsa música puede ser calificada como ruido por aquella persona que en cierto momento no desee oírla. En el ámbito de la comunicación sonora, se define como ruido todo sonido no deseado que interfiere en la comunicación entre las personas o en sus actividades. [4] En la figura 1.8.1 se muestra el medio ambiente de una ciudad y algunos factores que generan el ruido.

Figura 1.8.1 Factores ambientales que generan ruido.

Se llama contaminación acústica (o contaminación auditiva) al exceso de sonido que altera las condiciones normales del ambiente en una determinada zona. Si bien el ruido no se acumula, traslada o mantiene en el tiempo como las otras contaminaciones, también puede causar grandes daños en la calidad de vida de las personas si no se controla bien o adecuadamente.

El término contaminación acústica hace referencia al ruido (entendido como sonido excesivo y molesto), provocado por las actividades humanas (tráfico, industrias, locales de ocio, aviones, etc.), que produce efectos negativos sobre la salud auditiva, física y mental de las personas.

Este término está estrechamente relacionado con el ruido debido a que esta se da cuando el ruido es considerado como un contaminante, es decir, un sonido molesto que puede producir efectos nocivos fisiológicos y psicológicos para una persona o grupo de personas.

La mayor parte de los sonidos que escuchamos son ruidos. El impacto de un objeto que cae, un portazo, el estruendo de una motocicleta y muchos de los sonidos procedentes del tráfico en la calles de las ciudades son ruidos. El ruido corresponde a una vibración irregular del tímpano producida por la vibración irregular de algún objeto cercano. El sonido de la música tiene un carácter diferente, pues tiene tonos más o menos sostenidos, "notas" musicales. (Los instrumentos musicales pueden hacer ruido también) [2].

El ruido es sonido no deseado, y en la actualidad se encuentra entre los contaminantes más invasivos. El ruido del tránsito, de aviones, de camiones de recolección de residuos, de equipos y maquinarias de la construcción, de los procesos industriales de fabricación, de cortadoras de césped, de equipos de sonido fijos o montados en automóviles, por mencionar sólo unos pocos, se encuentran entre los sonidos no deseados que se emiten a la atmósfera en forma rutinaria.

El problema con el ruido no es únicamente que sea no deseado, sino también que afecta negativamente la salud y el bienestar humanos. Algunos de los inconvenientes producidos por el ruido son la pérdida auditiva, el estrés, la alta presión sanguínea, la pérdida de sueño, la distracción y la pérdida de productividad, así como una reducción general de la calidad de vida y la tranquilidad.

1.8.1 Términos que se le pueden asignar al ruido en los diferentes campos

El ruido, sonido inarticulado y confuso, alboroto no deseado por el receptor, que le molesta para escuchar el sonido que le interesa, o ninguno.

En el ámbito de la comunicación sonora: sonido o cualquier otro medio de información en el que ésta no sea clara e impida que el receptor sea capaz de identificar, individualizar o comprender, aunque sí se desee.

En la teoría de la información, se le considera una clase de información.

Ruido en informática, datos sin significado, generados simplemente como subproductos no deseados de otras actividades.

En comunicación, es la perturbación que afecta a la señal en el proceso comunicativo.

En la física, es el que propiamente se considera ruido, entendido como tal o en electrónica y en telecomunicaciones.

CAPÍTULO II:

CRIPTOGRAFIA Y ESTEGANOGRAFIA

2.1 CRIPTOGRAFIA.

Las raíces etimologías de la palabra criptografía son **Kriptos** que significa oculto y **Graphos**; que se traduce como escribir, lo que da una clara idea de su definición clásica: ciencia de escribir mensajes con clave secreta.

La criptografía nace al mismo tiempo que las computadoras. Durante la Segunda Guerra Mundial, en un ligar llamado Bletchley Park, un grupo de científicos entre los que se encontraba Alan Turing, trabajaba en en proyecto ULTRA tratando de descifrar los mensajes enviados por el ejército Alemán con los más sofisticados ingenieros en codificación ideados hasta entonces: la maquina ENIGMA y cifrado Lorenz. Este grupo de científicos diseño y utilizo el primer computador de las historia, denominado Colossus. [11]. En la figura 2.1.1 un bosquejo de la máquina ENIGMA.

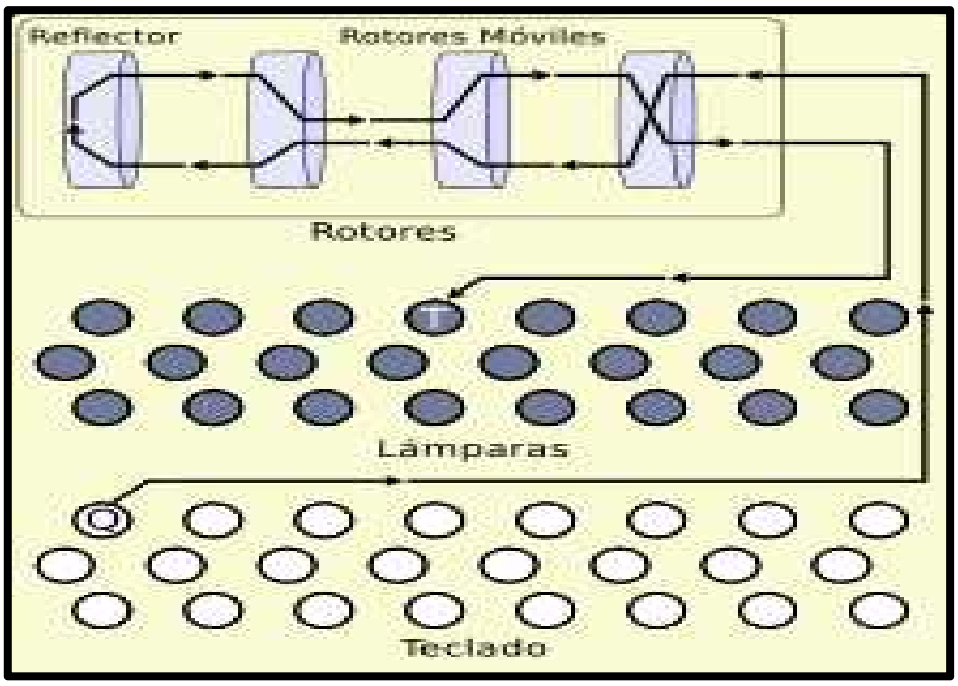

Figura 2.1.1 Esquema de la máquina de ENIGMA [11].

Desde entonces hasta hoy ha habido un crecimiento espectacular de la tecnología criptográfica, si bien la mayoría de estos avances se mantienen y se seguirán manteniendo algunos en secreto, financiadas fundamentalmente por la NSA (Agencia Nacional de Seguridad de los EE.UU), la mayor parte de las investigaciones hasta hace relativamente poco tiempo han sido tratadas como secretos militares, sin embargo, en los últimos años, las investigaciones serian llevadas a cabo en universidades de todo el mundo y gracias a esto se ha logrado que la criptografía sea una ciencia al alcance de todos, convirtiéndose en una piedra angular de asuntos tan importantes como el comercio electrónico, la telefonía móvil, o las nuevas plataformas de contenidos multimedia.[11]

Todo sistema computacional que procesa, almacena o trasmita información tiene que cumplir una seria de requisitos. En primer lugar, ha de preservar la información frente alteraciones no deseadas, debido a fallos en el software o en el hardware por agentes externos, interrupciones en el suministro eléctrico. En segundo lugar, evitar el acceso no autorizado tanto del sistema como de su contenido de información. Finalmente, el sistema debe garantizar que la información esté disponible cuando sea necesario. Estos tres conceptos quedan recogidos en los conceptos de integridad, confidencialidad y disponibilidad de la información respectivamente. Un sistema interconectado constituye el caso más general y extendido. De hecho, hoy por hoy, cualquier ordenador está conectado algún red y cada vez más dispositivos son auténticas computadoras como: consolas de videos juegos, teléfonos celulares, reproductores multimedia, etc.

Enviando y recogiendo información del exterior constantemente. Esto hace que las redes de los ordenadores sean más complejas, y presenten auténticos desafíos en cuestiones de la seguridad de la información.[11]

Las primeras técnicas que podemos considerar criptográficas o de ocultación fueron creadas en ese contexto, para permitir el envió de información de manera segura entre partes. Además, en cada época la tecnología determina en gran medida el potencial de ataque, por lo que un mayor avance tecnológico implicaba mayor capacidad bélica y por ende, superioridad de poder. A raíz de esto y en términos generales, podemos decir que la mayoría de los avances de la ciencia y la tecnología que se dieron en las distintas etapas de la evolución social, estuvieron motivados por objetivos militares, para luego trasladarse a el ámbito civil (quien

conocía el forjado del hierro podía construir mejores espadas, quien conocía la pólvora podía crear explosivos, etc.) [3].

Pese al acuerdo general en cuanto a lo que hoy representa conceptualmente en las ciencias de la computación se ha tratado de llegar a una definición completa e integral de la criptografía.

En un primer intento de acercarnos al concepto definiremos a la criptografía como un conjunto de técnicas basadas en la matemática y aplicadas por medio de la informática que utilizan distintos métodos con el objetivo de ocultar datos ante observadores no autorizados, mediante el uso de un algoritmo y al menos una clave.

La criptografía actual permite, principalmente, proteger la información contra accesos no autorizados lo que garantiza su confidencialidad, a la vez provee mecanismos para asegurar la autentificación, la integridad y no el repudio, (una propiedad que evita que pueda negarse a la responsabilidad sobre una acción tomada), su aplicación principal se da tanto en las redes informáticas como en los datos almacenados en medios fijos y extraíbles. Al parecer en la criptografía, es natural que surja como la necesidad de analizar la información protegida para determinar si será posible recuperarla aunque no se conozca el sistema utilizado para ocultarla, o bien para obtener la clave, así nace el criptoanálisis, que definiremos con el estudio de los sistemas criptográficos con el objetivo de descubrir las debilidades que en ellos pudiera encontrarse, a fin de romper su seguridad sin que sea necesario conocer su clave o secreto utilizado.

El conjunto de criptografía y criptoanálisis conforma una disciplina científica que denominamos criptología. Se suele incluir además de la criptología a la **esteganografía**, que permite que la información pase desapercibida en su medio habitual, y también su complemento. Para adentrarnos en el tema más adelante hablaremos de los métodos de encriptación más importantes resumiendo como función y su mecanismo para codificar la información.

2.2 CLASIFIACION DE LA CRIPTOGRAFIA.

No existe una manera de clasificar a la criptografía y sus técnicas relacionadas, debido a los múltiples aspectos de escribir. No obstante, es posible realizar divisiones según la época histórica, el tipo de algoritmo y la forma en la que se procesa la información.

La criptografía consistía en algoritmos basados en caracteres (símbolos, letras y números) que sustituían caracteres o se intercambian entre sí, siempre cambiando uno por otro. De estos algoritmos criptográficos, lo más sofisticado que hacían era secuencias que se repetían. [4]

Conforme avanza el desarrollo de la tecnología, es posible que los métodos de codificación, se estén relacionando con los archivos digitales, como la imagen, video y el audio. Sin embargo se apoyan con métodos, formulas y algoritmos para cifrar la información, es decir, de la esteganografía, puesto que ya no está enfocada a un texto plano, como los métodos de encriptación que a continuación se presentan, que solo se altera el texto mediante combinación del mismo alfabeto. La esteganografía se enfoca en los medios digitales para procesar la información y ocultarla, más adelante hablaremos del tema.

2.2.1. Época histórica.

Desde los inicios de las sociedades, la comunicación tanto oral como escrita, fue un proceso indispensable. El hombre organizado en grupos y comunidades para mejorar sus probabilidades de supervivencia, comprendiendo desde siempre que la información podía derivar en conocimiento y este en poder [3]

Una característica intrínseca del ser humano ha sido la existencia de conflictos entre personas, a veces con origen en cuestiones territoriales o de recurso naturales, o por motivos religiosos o ideológicos. Esto se derivó en el uso de las fuerzas y de la existencia de ataques, violencia y guerras, donde el más poderoso resulta ser el vencedor. En muchos casos, la victoria dependía de un motivo muy evidente: con cuanta información contaba uno [3].

En base a de estas necesidades y dependiendo de cada época es como se realizaron los métodos de codificación, un ejemplo de codificación antigua es la Ecitala, proveniente de la antigua Grecia.

2.2.2Según el algoritmo.

Si tenemos en cuenta el tipo de algoritmo utilizado para las operaciones del cifrado (solo para sistemas modernos), se pueden clasificar en algoritmos simétricos (o clave secreta) y algoritmos asimétricos (o de clave pública).

Los simétricos tienen la característica de utilizar la misma clave para realizar operaciones de cifrado y descifrado, requiriendo una sola clave por cada par de entidades a comunicar. En figura 2.2.1 se muestra una representación gráfica de un algoritmo simétrico.

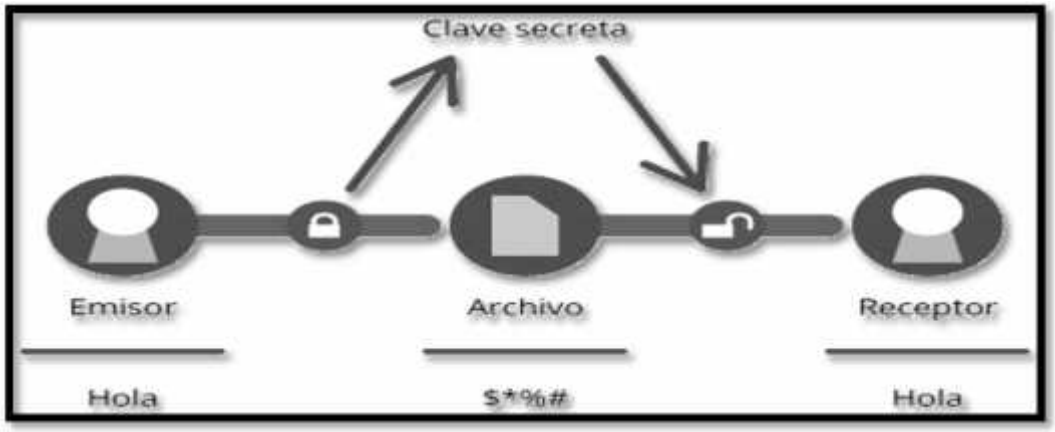

Figura 2.2.1 Algoritmo simétrico.

Los asimétricos utilizan, en cambio, una clave para cifrar distinta y complementaria a la que utilizan para descifrar. Esto implica que un mensaje cifrado con una clave solo puede ser descifrado con otra, y viceversa. En figura 2.2.2 se muestra una representación gráfica de un algoritmo asimétrico.

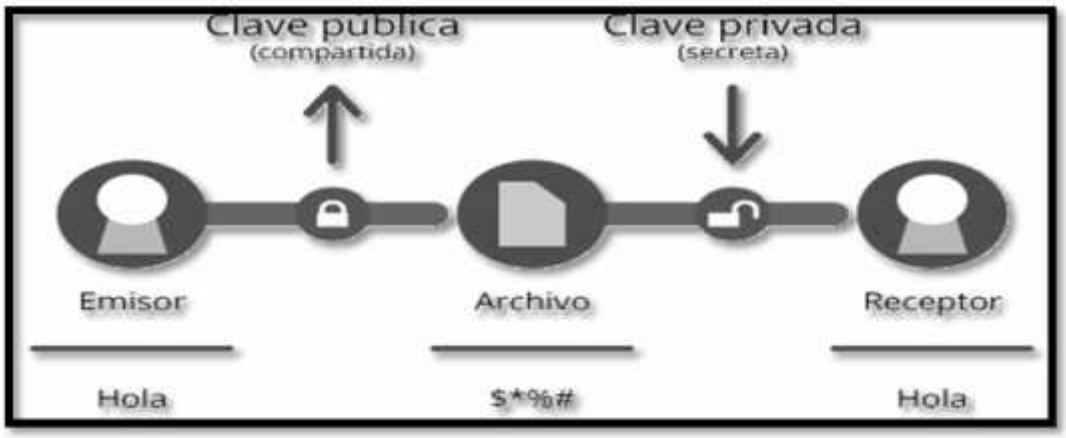

Figura 2.2.2 Algoritmo Asimétrico.

2.2.3 Según el procedimiento.

La forma de procesar la información es una categoría que, tal como la anterior, solo aplica a los sistema modernos (y estrictamente hablando, solo de algoritmos simétricos), pudiendo así dividir los algoritmos en aquellos que dan tratamiento de la información bloques de datos y aquellos que lo hacen tomar bit por bit, llamados algoritmos de flujo. La esteganografía o empleo de canales subliminales, consiste en ocultar en el interior de una información, aparentemente inocua, otro tipo de información (cifrada o no). En donde se involucra un archivo digital para el procesamiento de cifrado de la información.

2.3 ELEMENTOS PARA FORMAR UN CRIPTOSISTEMA REFERENTE A UN METODO DE CIFRADO.

Mediante un conjunto de componentes se puede formar un, criptosistema y este puede cumplir para diversas funciones. Para que un método pueda ser un criptosistema debe cumplir con un:

- ✓ **Emisor**: quien realiza el proceso criptográfico.
- ✓ **Receptor**: quien realiza el proceso de descifrado.
- ✓ **Medio**: canal utilizado para intercambiar la información.
- ✓ **Algoritmo**: conjunto de trasformaciones aplicadas al mensaje para obtener el criptograma.
- ✓ **Mensaje**: información que se desea ocultar.
- ✓ **Clave**: (o llave) pieza de información que se aplica al algoritmo. Permite transformar el mensaje en criptograma y viceversa. Al conjunto de todas estas claves se le llaman espacio de claves.
- ✓ **Criptograma**: mensaje trasformado. También llamado mensaje cifrado.
- ✓ **Protocolo**: conjunto de reglas que permiten intercambiar información entre entidades. Es claro que la encriptación se encarga de ocultar información de terceros, y depende de la época, algoritmo y metodología. La criptografía clásica abarca desde sus primeros tiempos hasta mediados del siglo xx y finaliza en la segunda guerra mundial y la encriptación se basaba en texto plano. A continuación se dará a conocer algunos métodos de criptografía clásica, basada en una encriptación enfocada a un texto plano.

Además de estos elementos definiremos a un Criptosistema como una quíntupla (**M, C, K, E, D**) donde:

- **M** representa todo el conjunto de todos los mensajes sin cifrar (lo que se denomina texto claro, o plaintext) que puedan ser enviados.
- **C** representa el conjunto de todos los posibles mensajes cifrados, o criptogramas.
- **K** representan el conjunto de claves que pueden ser empleadas en el criptosistema.
- **E** conjunto de trasformaciones de cifrado o familia de funciones que se aplica a cada elemento **M** para obtener un elemento de **C.**
- **D** es el conjunto de trasformaciones de descifrado.

Todo criptosistema debe cumplir la siguiente condición:

$$D_K\left(E_K(m)\right) = m$$

Es decir, si se tiene un mensaje **m,** lo ciframos la clave **k** y luego lo descifamos empleando la misma clave **k,** para obtener de nuevo el mensaje original **m.** [7]

2.4.1 Cifrado Polybios.

Hacia mediados del siglo II a.C., el historiador gripo Polybos diseño un sistema basado en una tabla donde hacia corresponder a cada letra del alfabeto con un par de letras según su ubicación de fila y columna, por lo que el criptograma era ese conjunto de pares de letras (por ejemplo, la letra A quedaría representa por AA, la M como CB, etcétera). Podemos considerar desventajoso el hecho de que la longitud del texto cifrado sea el doble que la del texto sin cifrar. En la figura 2.4.1 se muestra la tabla de descifrar y cifra con en cifrado Polybios. [3].

	A	B	C	D	E
A	A	B	C	D	E
B	F	G	H	I/J	K
C	L	M	N/Ñ	O	P
D	Q	R	S	T	U
E	V	W	X	Y	Z

Figura 2.4.1 tabla para cifrar con Polybios.

2.4.2 Encriptación Cifrado de Cesar.

En el siglo I a.C., apareció el cifrado de Cesar, nombrado así en honor al emperador Julio Cesar. Este cifrado aplica al texto un desplazamiento fijo de tres caracteres, modo de trasformación. El alfabeto de cifrado es entonces el mismo que el texto original, solo que desplazado hacia la derecha. En la figura 2.4.2 se muestra como es el cifrado de cesar.

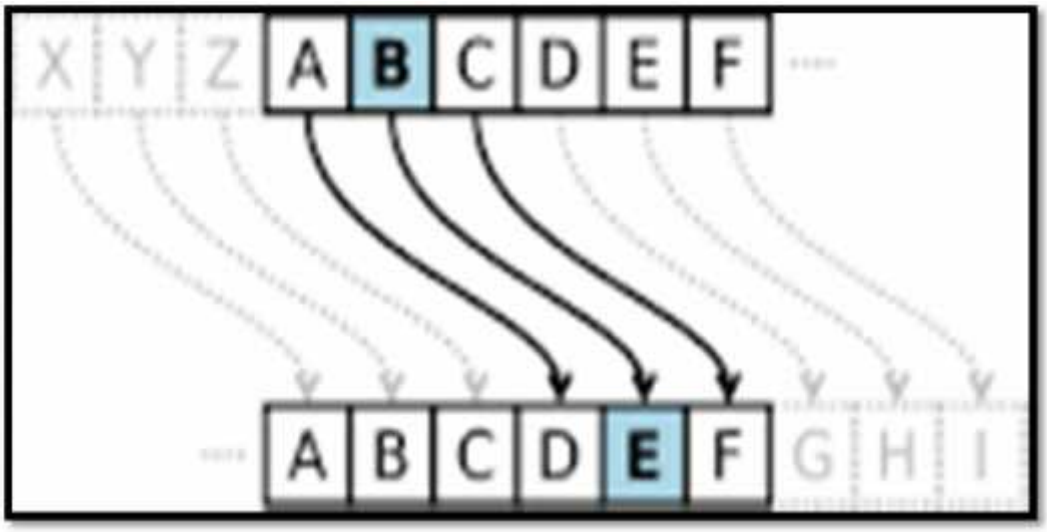

Figura 2.4.2 Cifrado de Cesar (3 corrimientos hacia la derecha).

La principal desventaja es que se conoce por el desplazamiento de corrimientos, deja de ser problemático en la decodificación. Modificando un poco el método se resolvería este problema, es decir, que no fuera un número estático el corrimiento en este caso tres corrimientos, si no que entre el receptor y emisor este

corrimiento fuera dinámico, cambiando los corrimientos y solo ellos acordaran cuantos corrimientos se ocuparan para el cifrado y descifrado. Este método fue base para algunos otros métodos más de cifrado.

2.4.3 Cifrado de Vigenére.

Este método también es utilizado para un texto plano, realizado por el criptologo francés Blaise de Vigenére (1523- 1596), se basa en el mismo principio que el de Cesar pero con desplazamiento de caracteres indicado por un número relacionado con un carácter de la clave escrito de manera cíclica debajo del mensaje [3].

Para obtener el criptogramas utiliza una tabla asociada, o bien el método analítico. Si utilizamos la tabla buscaremos, cada letra del mensaje en la primera fila y su correspondiente letra de la clave en la primera columna, y en su intercesión se encontrara la letra del criptograma. Para realizar el descifrado, identificamos cada letra de la clave en la primera fila y buscamos en la columna correspondiente la letra del criptograma. Al desplazarnos horizontalmente desde esta hacia la primera columna, obtendremos la letra correspondiente al texto claro [3].

En figura 2.4.3 se muestra la tabla vigenère y un ejemplo de cómo se cifra mediante este método.

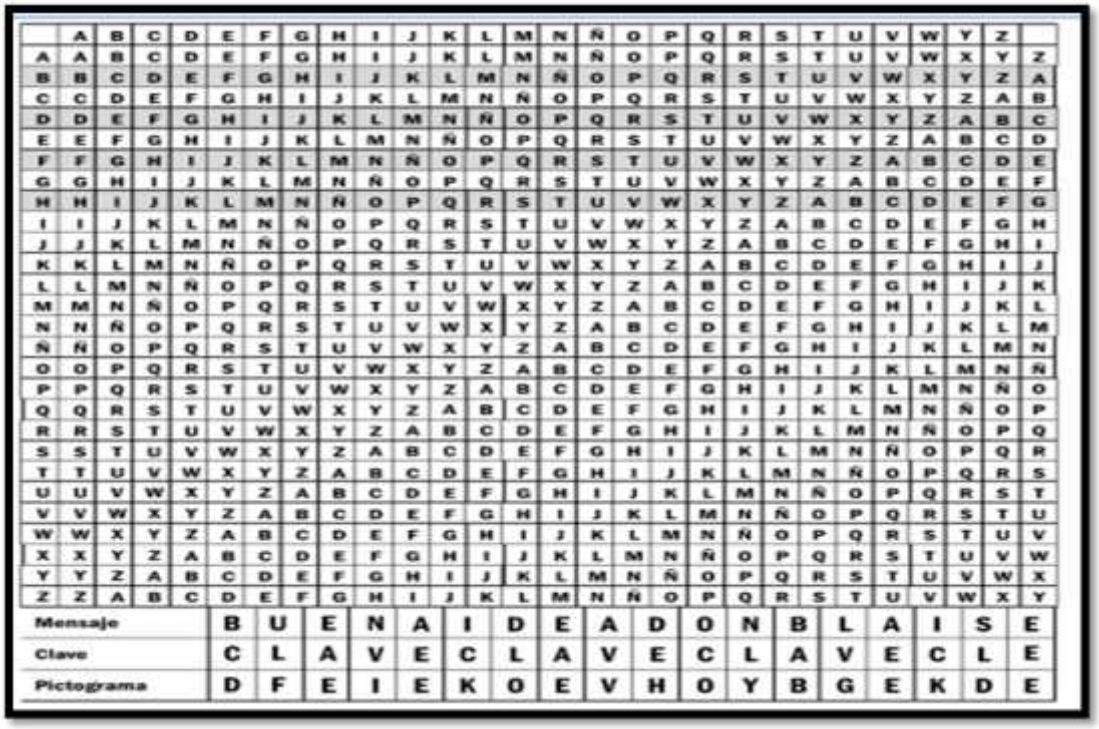

Figura 2.4.3 Ejemplo del cifrado Vigenére y tabla [3].

2.4.4 Cifrado de Playfair.

Creado por el Charles Wheatstone, para realizar comunicación secreta por telégrafo y fue nombrado así por el científico escoces Lord Lyon Playfair quien lo impulso su utilización. Este cifrado toma de a dos letras de mensaje y se trasforma en otras dos diferentes, a partir de un conjunto de reglas y una matriz de 5x5 (suficiente para albergar todas las letras del alfabeto inglés y casi todas del español). [3].

Las reglas para transformar dos caracteres de mensaje (**m1 y m2**) en sus correspondientes del criptograma (**c1 y c2**) son las siguientes:

Si **m1 y m2** están en la misma fila, **c1 y c2** son letras de su derecha (si están en un extremo, se toma circularmente).

Si **m1 y m**2 están en la misma columna, **c1 y c2** son letras de abajo (también de manera circular).

Si **m1 y m2** están en distintas filas y columnas, **c1 y c2** corresponden a las letras de la diagonal opuesta (formando un cuadro entre el cuatro).

Si **m1 y m2** son iguales, se inserta un carácter sin significado entre ellos para evitar la repetición y luego se aplican las demás reglas.

Si la cantidad de letras es impar, se agrega una letra sin significado al final de texto.

2.4.5 Cifrado de Hill.

Creado por matemático Lester Hill, este método utiliza el uso de matrices el cual utiliza cifrado por sustitución poligráfica.

Este cifrado implica operar con matrices, para lo cual debe asegurase que la matriz K (clave) tenga inversa. Entonces se calcula.

$$K \cdot 1 = T_{Adj(K)} / |K| \bmod n$$

Donde:

Adj(k) es la matriz adjunta

T es la matriz traspuesta

IKI es el determinante (no puede ser cero ni tener factores en común con n)

En caso de que el texto del mensaje no sea múltiplo del bloque N, solo se llena con caracteres predefinidos. [3].

2.4.6 Cifrado de Vermam.

Creado por Gilbert Vermam, cifrado por sustitución binaria que utilizaba el código de los estereotipos (Baudot, de 5 bits). Este aplica operación XOR y una secuencia aleatoria obtenida en una base a una clave (K) que es previa compartida por las dos partes. Por ser la función XOR reversible (aplicándose nuevamente), en este algoritmo para cifrar es lo mismo para descifrar. En la figura 2.4.4 se muestra un esquema de lo que es este cifrado. [3].

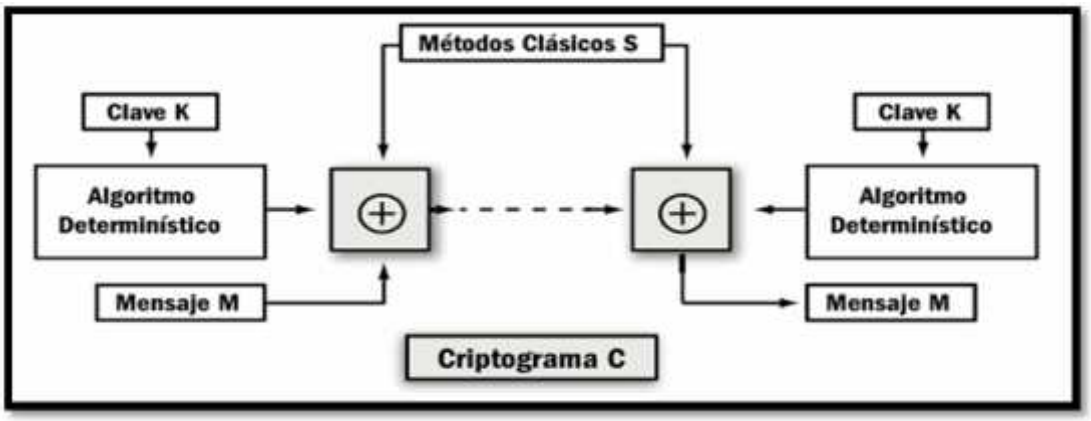

Figura 2.4.4 Cifrado de Verman requiere idealmente, secuencias totalmente aleatorias el intercambio para las claves [3].

2.5 USO DE LA CRIPTOGRAFIA.

Como leímos en los temas anteriores nos da una idea de los posibles usos de la codificación, y entendemos que, el uso de la criptografía es principalmente la ocultación de la información, mediante el uso y aplicación de técnicas ya mencionadas. Para el resguardo de información en secreto entre dos o más partes (emisor (es) – receptor (es)). Además de que la información debe ser secreta, tiene que haber elementos como la **confidencialidad**, **autentificación**, **verificación de integridad** y **mecanismo de no repudio**. Dependiendo del mecanismo del método de encriptación y el uso que se le está dando, todos los integrantes que lo ocupen deben tener en cuenta los elementos mencionados anteriormente.

2.5.1 Confidencialidad en el cifrado.

La confidenciada o privacidad de la información es el uso o aplicación de la criptografía. Implica básicamente el mantener en secreto una información determinada (un mensaje para ser trasmitido en un canal de comunicación inseguro, un documento almacenado en un medio no confiable, etc.). El objetivo, está claro,

es que solo aquellas personas que estén autorizadas tenga acceso a la información resguardada (esto es, cifrada) [4].

2.5.2 Autentificación en el cifrado.

La autentificación en la actualidad, es uno de los mecanismos más utilizados en la red para la seguridad de la información, precisamente para tener segura la información que se queda almacena en la red, como datos persónales, documentos, fotos, etc. Un ejemplo es Facebook, las direcciones de correo electrónico, aplicaciones donde se almacena información personal, documentos y fotos. Otro ejemplo es Dropbox, aplicación para guardar documentos. Si no existiera la autentificación cualquier persona podría acceder a nuestra información pudiéndola cambiar de manera mal intencionada, ocasionado problemas y robo de información.

En la figura 2.5.1 se muestra una forma de identificación en la redes como lo es el logueo.

Figura 2.5.1 En la red, para autentificarse lo que se utiliza es el logueo.

Hablar de autentificación o identificación implica hablar de la corroboración de la identidad de una entidad (una persona, una computadora, un sector de una compañía o empresa, etc.).

Puede entenderse como la autentificación como un uso a aplicación relacionado con el de la identificación. Esta función aplica a ambas partes o entidades participantes en una comunicación y a la información en si mimas. Sépase que dos partes, al comenzar una comunicación, deberán identificarse entre ellas. La información trasmitida deberá ser autentificada respecto del origen (fecha de origen, contenido, fecha de envió o transmisión, etc.) por estas razones, este aspecto de la criptografía es comúnmente dividido en dos clases principales:

autentificación de entidades y autentificación de origen de datos. Esto último incluye implícitamente la verificación de integridad de datos [4].

2.5.3 Verificación de la integridad en el cifrado.

La verificación de la integridad, surge como debido a las nuevas formas de ataques como: hackers, virus y troyanos. Solo con lanzar algún virus podrían acceder a la información almacenada en la red o computadora conectada a la red. Con la verificación de la integridad sirve de apoyo para saber si la persona que quiere acceder a la información no es una maquina (o virus), defendiendo una vez más la seguridad de los datos.

Estos mecanismos, entonces, ataca al problema de la alteración no autorizada de datos o información. Para asegurar la integridad de un documento por ejemplo, debe tener la habilidad de detectar la manipulación de esta información, es decir, de sus contenidos, por partes no autorizadas, sabiendo que dentro de lo que se entiende por manipulación debe contemplarse lo que se agregue, elimine o sustituya la información [4].

2.5.4 Mecanismo de no repudio en el cifrado.

Este uso o aplicación consta de la implementación de un mecanismo o técnica – mediante funcionalidades criptográficas, por supuesto, para prevenir que una identidad niegue un envió previo de información, un mensaje, una acción, etc.

2.6 ESTEGANOGRAFIA.

La esteganografía o empleo de canales subliminales, consiste en ocultar en el interior de una información, aparentemente inocua, otro tipo de información (cifrada o no). Este método ha cobrado bastante importancia últimamente debido a que permite burlar diferentes sistemas de control. Supongamos que un disidente político quiere enviar un mensaje fuera de su país, evitando la censura. Si lo codifica, las autoridades jamás permitirán que el mensaje atraviese las fronteras independientemente de que puedan acceder a su contenido, mientras que si ese mismo mensaje viaja camuflado en el interior de una imagen, un video o un audio, tendrá más posibilidades de llegar a su destino.

Podemos decir que la criptografía y la esteganografía son técnicas diferentes, e incluso complementarias. Mientras que la primera se encarga de hacer el mensaje ilegible frente agentes no autorizados, sin preocuparse de que este pueda tener un aspecto claramente reconocible, la segunda provee para hacer que la información resulte indetectable. [11]

Desde el punto de vista formal, la esteganografía toma un mensaje ***anfitrión***, y lo modifica hasta encontrar otro ***mensaje huésped*** que queremos ocultar, de forma que únicamente aquellos que conozcan el proceso seguido para su ocultación puedan recuperarlo de manera satisfactoria. En función de la naturaleza del mensaje anfitrión (una imagen, un fragmento de sonido o un video), cambiara radicalmente el concepto del significado y por lo tanto los procesos de modificación que permitirá alojar al huésped sin despertar sospechas [11].

La esteganografía es considerada una rama de la cristología en la que se utilizan técnicas para ocultar mensajes dentro de otros mensajes (portadores) de manera que no se pueda detectar su existencia. Esto crea un canal encubierto (cover chanel), para la trasmisión de la información secreta que permita a ciertos usuarios recuperar los mensajes sólo si saben cómo estos fueron guardados dentro del portador, pasando desapercibidos para otros usuarios que tengan acceso al canal [3].

Un ejemplo histórico de la esteganografía hasta la antigüedad. Los griegos utilizaban tablas de madera recubiertas de cera sobre las cuales escribían con objetos punzantes y luego raspaban para poder escribir de nuevo (recuérdese la expresión “tubula rusa”). Se conoce que fueron ocultados los mensajes escritos directamente sobre la madera, que posteriormente se cubría con cera. De parte de Heródoto también conocemos la utilización de tatuajes en el cuero cabelludo de un esclavo que, sin evidenciarlo y ya con el cabello crecido, contenía un mensaje o una información secreta (por ejemplo, una advertencia a Grecia respecto de planes de invasión por parte de los persas.) En la figura 2.6.1 se muestra como fue tabula rusa.

Figura 2.6.1 Esteganografía antigua, ocultación de la información mediante escritura en la tablilla cubierta con cera.

Así como sucede en la criptografía, podemos distinguir entre la esteganografia clásica y la moderna, donde la seguridad de la primera se basa en el secreto del canal y la técnica usada; y en la segunda se usan canales digitales además de los archivos de texto, imágenes, música, videos y demás [3].

2.6.1 Técnicas de la Esteganografía Digital.

En lo que se refiere a Esteganografia, etimológicamente, la palabra proviene del griego steganos (oculto) y graphos (escritura), y se puede definir como una técnica para ocultar información de un canal encubierto con el propósito de prevenir la detección de un mensaje oculto [5].

La esteganografía, se enfoca en ocultar la información mediante medios digitales como un audio, una imagen o un video. Mediante un tratamiento o técnica en donde se puede introducir la información (mensaje) y ocultarlo de alguna manera.

Y en la mayoría de estos archivos se busca insertar bits en las zonas de los archivos o paquetes de datos de red, que una vez recuperados representen un mensaje codificado ya sea en el mismo formato o en otro.

Las técnicas modernas incluyen, por ejemplo el uso de ocultamiento de datos en una imagen a modo de marca de agua, los algoritmos de trasformación específicos

y la inserción de datos en los bits menos significativos de imágenes y otros archivos multimedia que representan escalas (de colores, sonidos, etc.). Por ejemplo en;

- **Una imagen;** cuando se trata de representar imágenes, esta se subdivide en una matriz de m x n pixeles y para cada uno de ellos se almacena un valor entero, que representa un nivel de gris si es una imagen monocromática o un vector de tres valores si es una imagen de color, que representa usualmente los niveles de rojo (R), verde (G) y azul (A) del pixel en cuestión. Introduciendo la información que se quiera ocultar en un fragmento del pixel alterando un poco la información de la imagen mediante un algoritmo.
- **Un video;** para este caso se añade una tercera dimensión, correspondiente al tiempo para poder añadir información que se quiere ocultar.
- **Un audio;** en este archivo los niveles de presión del aire se miden en un número fijo de veces por segundo (frecuencia de muestro) y se aproxima a un número de enteros presión.

En la siguiente tabla se puede ver los diferentes niveles de seguridad en función de la forma en la que se construya el esquema del método de cifrado. [3].

Nivel de protección	**1**	**2**	**3**	**4**
Uso de algoritmo	si	si	si	si
Uso de clave	no	si	si	si
Influencia de la clave en la distribución de bits del mensaje	no	no	si	si
Influencia de la clave en la distribución y selección de bits del mensaje.	no	no	no	si

2.6.2 Campos que implican la Esteganografía.

Se pueden observar distintos actores implicados en el campo de la esteganografía, los cuales se describen adelante:

1. ***Objeto contenedor***: Se trata de la entidad que se emplea para portar el mensaje oculto.
2. ***Estego-objeto***: Se trata del objeto contenedor más el mensaje encubierto.
3. ***Adversario***: Son todos aquello entes a los que se trata de ocultar la información encubierta.

4. ***Estegoanálisis***: Ciencia que estudia la detección (ataques pasivos) y/o anulación (ataques activos) de información oculta en distintas tapaderas, así como la posibilidad de localizar la información útil dentro de la misma (existencia y tamaño) [5].

2.6.3 División de la Esteganografía.

A grandes rasgos la esteganografía se divide en dos:

- Esteganografía lingüística.
- Esteganografía técnica.

Por esteganografía lingüística se entiende que es la que cuyo portador es un texto escrito, mientras que la esteganografía técnica utiliza cualquier otro tipo de portador, sea audio, imágenes, video, etc. [5].

2.7 FUNCIONAMIENTO DE LA ESTEGANOGRAFIA.

En esteganografía tanto el emisor como el receptor tienen su respectiva función para realizar el proceso de cifrado y descifrado de la información, como se muestra en la figura 2.7.1

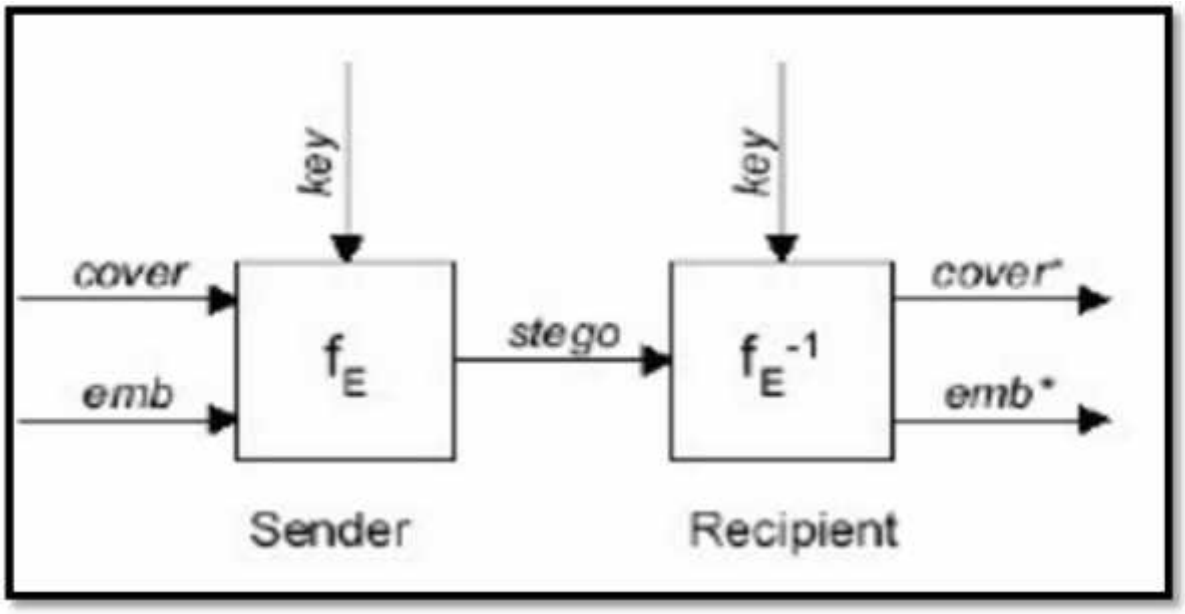

Figura 2.7.1 Funcionamiento de un algoritmo mediante la esteganografía.

$$\boldsymbol{D} \quad :$$

$$f \quad = F \qquad p \quad e$$

$$f \quad ^{-1} = F \qquad p \quad e$$

$$c \quad = 0 \qquad d \quad e \qquad e \; m \qquad (a \quad)$$

$$e \quad = M \qquad e$$

$$k \quad = P \qquad d \; f$$

$$s \quad = 0 \qquad c \quad e \; m \qquad e$$

$$s \qquad = E$$

$$r \quad ip \quad = R$$

2.8 TIPOS DE METODOS PARA LA ESTEGANOGRAFÍA

Los métodos que existen en la actualidad para hacer esteganografía son:

- Sustitución.
- Inyección.
- Generación de nuevos ficheros.

2.8.1 Esteganografía por un método de Sustitución.

Cada fichero que es creado contiene áreas de datos no usadas o que no son importantes. Estas áreas pueden ser remplazadas sin aparentes cambios visuales o estructurales de fichero original.

Esto permite esconder información sensible dentro del fichero y tener aun la certeza que el fichero original no ha sufrido ninguna mutación. Este método del bit menos significativo (LSB) sustituye el ultimo byte, del tal forma que podemos repetir este mismo proceso con cada byte sin que el ojo humano aprecie diferencia alguna.

El método LSB funciona mejor en fichero que tenga ruido, es decir fotos que tengan muchos colores y figuras. Cuando más ruido tenga el fichero más difícil será que una persona sea consistente de la manipulación realizada.

El método de sustitución no incrementa el tamaño de la imagen sin embargo debemos tener en cuenta el tamaño del mensaje que queremos ocultar.

2.8.2 Esteganografía por un método de Inyección.

Este método implica encajar el mensaje secreto directamente en el objeto portador. El problema reside en que generalmente esto hace que el fichero crezca de tamaño que el fichero original.

2.8.2 Esteganografía por un método de generación de un nuevo fichero.

Esta técnica implica coger el mensaje y usarlo para generar un nuevo fichero desde la nada. Una de las ventajas de este método es que no existe un fichero original con el que comparar.

CAPÍTULO III:

METODO DE CIFRADO E IMPLEMENTACIÓN

3.1 ESTEGANOGRAFIA ENFOCADA AL AUDIO, MEDIANTE UNA SEÑAL DE RUIDO.

El oído humano es extremadamente sensible a cambios en los patrones de audio, pero no tanto como para percibir cambios dentro de una misma frecuencia. A la hora de ocultar un mensaje en audio, es importante saber el medio por el cual se va a trasmitir el mensaje, ya que no es lo mismo entre los medios digital – digital (entre ordenadores) o entre aire – digital (micrófono).

Cuando se quiere ocultar información sensible dentro de un fichero de sonido, se suele utilizar las siguientes cuatro técnicas:

- **Codificación Low-Bit.** El mensaje puede ser almacenado en fichero de sonido de la misma manera técnica LSB hace las imágenes.
- **Spread Spectrum**. Es el método de ocultar un mensaje de baja señal dentro de otro de señal mayor. Este método añade ruido aleatorio para completar perfectamente la ocultación final.
- **Echo Data Hiding.** Este método usa el eco de un fichero de sonido para ocultar en él, la información secreta.
- **Máscara perceptual**. Este método usa el concepto de ocultar un sonido tras otro de la misma frecuencia.

Ahora bien, la esteganografía oculta la información en un mensaje secreto (información que se pretende ocultar), en otro mensaje público (para este caso un audio base). Con el propósito de trasmitir el mensaje, puede que alguien trate de espiar por el canal (en las redes de comunicación entre dos o más personas como: Messenger, correos electrónicos, inbox, etc.) tratando de robar información sea para el propósito que sea y cuando el conocimiento de dicha información constituya una amenaza para una organización determinada (emisor (es) – receptor(es)), podemos utilizar la esteganografía.

Con el objetivo de utilizar la esteganografía digital en un audio, se explicara cómo se puede crear un método más de encriptación involucrando una señal de ruido en una grabación de voz. En los temas siguientes se explicara cada uno de los elementos y el proceso que conllevara dicha encriptación de la información.

3.2 Elementos necesarios para el desarrollo del método de cifrado digital

Para poder formar cualquier método de encriptación es necesario contar con los elementos necesarios para poder formar un criptosistema. A continuación se detalla cada uno de ellos que nos ayudara a darnos una idea general de este proyecto:

- ✓ **Emisor:** Organización o persona, que pretende enviar un mensaje secreto ya cifrado mediante algún dispositivo que tenga acceso a la red. Como se muestra en la figura 3.2.1
- ✓ **Receptor**: Organización o persona, a la cual se le hará llegar el mensaje mediante la red cifrado, permitiendo descifrar. Como se muestra en la figura 3.2.1
- ✓ **Medio**: El medio para cual está enfocado este nuevo método es la red (internet), como canal de comunicación, si en el trascurso la información es robada o perdida, solo tendrán un audio con ruido y no más información. Como se muestra en la figura 3.2.1

Figura 3.2.1 Emisor y receptor que utilizan algún dispositivo para almacenar, enviar información, mediante el canal de red, la información será enviada mediante un criptograma en un audio.

- ✓ **Algoritmo**: Se utilizara una señal de ruido para poder trasponer en un audio base y la grabación de voz (mensaje que se pretende esconder), mediante un editor de audio para este caso la aplicación que se utilizará es **Adobe Audition cc 2014.** En figura 3.2.2 se muestra la aplicación para poder manipular y editar el audio.

Figura 3.2.2Adobe Audition CC 2014 (versión 2014.0) aplicación para poder general nuestro algoritmo mediante la edición de audio generando archivos de audio e formato mp3.

- ✓ **Mensaje**: Grabación de voz almacenada en un audio, eliminando ruido si lo hay cuando se grabe la voz, esta grabación de voz será creada con la aplicación de audio mencionada anteriormente en la figura 3.2.2.
- ✓ **Clave**: (llave) Una señal de ruido por ejemplo el ruido generado en el medio ambiente.
- ✓ **Criptograma**: Va a estar formado, unificando el audio base, la grabación de voz y la señal de ruido.

Este nuevo método, pretende ocupar una señal de ruido, como clave de trasformación para poder cifrar la información, cualquier persona que escuche algún audio que contenga ruido, lo podrá escuchar poco tiempo, ya que el ruido es un contaminante auditivo y molesto para el que lo oye. Aquí se ocupa precisamente como un distractor para intrusos que no tienen por qué saber la información de la organización que establece la comunicación.

3.3 Clasificación para este método de cifrado.

Para poder definir qué tipo de método es, describiremos los elementos que se utilizaran y en base a eso podremos concluir el tipo clasificación del método de cifrado.

Podemos decir, que será un método de **codificación simétrico**, pues la misma señal de ruido que se va ocupar para cifrar, es la misma que se va quitar para descifrar, además de la aplicación de edición de audio Adobe Audition CC 2014, por ese motivo se dice que es un algoritmo simétrico. En la figura 3.3.1 se muestra el gráfico del algoritmo simétrico enfocado a este método. También sería un método de codificación moderno por la utilización de archivos digitales, gracias a la esteganografía.

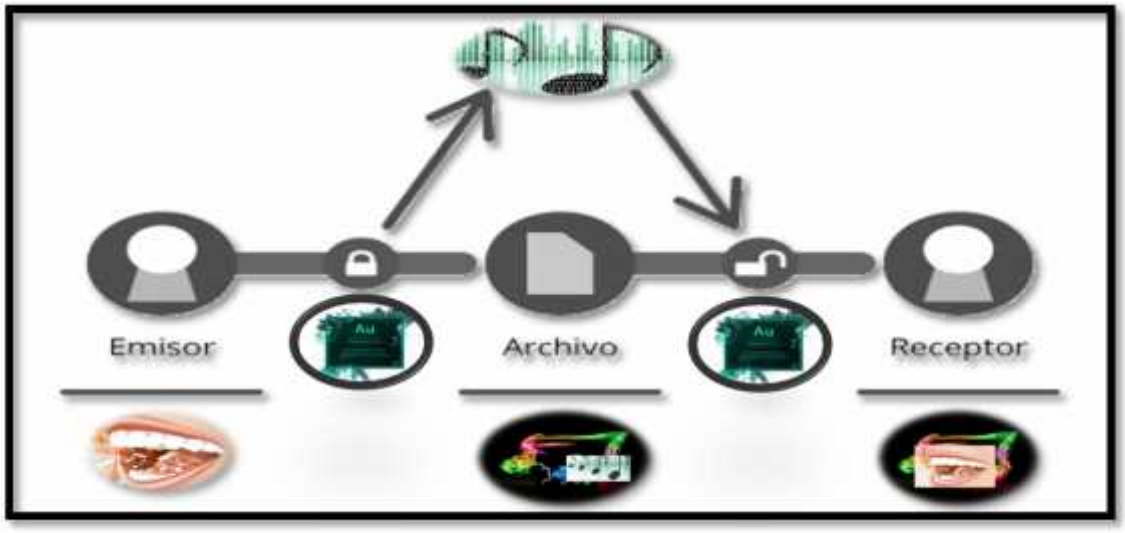

Figura 3.3.1 Ocultación de la información mediante una señal de ruido en un audio, un Algoritmos Simétrico.

Este método esteganográfico también es un método por **inyección,** ya que se va a introducir en el objeto portador que es el audio, la grabación de voz (mensaje) y nuestro ruido (llave o clave). Como se va agregar más información a nuestro objeto portador tiende a crecer un poco el tamaño del archivo. Este método implica encajar el mensaje secreto directamente en el objeto portador.

3.4 Diseño del Método Esteganográfico enfocado al audio mediante una señal de ruido.

En este apartado, se explicara paso a paso el proceso de encriptación, como es que funciona, lo que se pretende hacer, utilizando una señal de ruido. Para la realización del método se requiere de un editor de audio, para este caso, el editor Adobe Audition CC 2014 con el que se va a trabajar. Los pasos que se deben seguir son:

- ✓ Pasó 1: se debe tener un audio base, es decir un fondo musical, el cual dependerá del tamaño de la información que se quiera ocultar (Tiempo de duración del audio).
- ✓ Pasó 2: grabar la información que se pretenda ocultar con alguna aplicación, quitarle el ruido posible a dicha grabación y que quede en un formato que se pueda manipular, para este caso se trabajara con formato mp3.
- ✓ Pasó 3: unificar con una aplicación de edición de audio, el paso 1 y paso 2, para tener un solo archivo con los dos elementos.
- ✓ Pasó 4: con una señal de ruido (esta varía dependiendo del tipo de voz de la persona. Si la persona tiene la voz suave se necesitaría una señal de ruido no tan fuerte, pero si es caso contrario la señal de ruido tendría que ser más fuerte), para ocultar la información (grabación de voz) con dicha señal de ruido. En la figura 3.4.1, se muestra un bosquejo de este método de encriptación.

Figura 3.4.1 Bosquejo de encriptación, para la ocultación de la información en un audio mediante una señal de ruido, tomando una aplicación de edición de audio para su desarrollo y algoritmo.

3.5 Implementación: Método Esteganográfico enfocado al audio mediante una señal de ruido generando el criptograma.

- **Paso 1**: contar con el audio base almacenada en su computadora donde se va a trabajar, es decir el fondo musical con extensión .mp3, el cual dependerá del tamaño de la información que se quiera ocultar (Tiempo de duración del audio del mensaje).
- **Paso 2:** contar con la grabación de voz almacenado también en la computadora, esta grabación será la información que se pretenda ocultar, es decir, el mensaje, la grabación de voz no debe tener ruido, se debe escuchar solamente la voz clara y entendible, en formato .mp3 para poder ser manipulada con el editor de audio. Para este proyecto la misma aplicación de edición de audio Adobe Audition CC 2014 la ocupamos para grabar la voz.
- **Paso 3:** contar con la señal de ruido con extensión .mp3, la señal de ruido que se utilizó para este proyecto fue tomada y grabada del medio ambiente, del ruido generado por el tráfico vehicular en los autos, y calles de la ciudad de Puebla. Para mayor comodidad se recomienda hacer una carpeta donde se tengan almacenados los 3 archivos para localizarlos de manera fácil. Una vez cumpliendo los 3 pasos anteriores iremos al paso 4.
- **Paso 4:** edición de audio unificando el archivo del paso 1 y 2.En esta parte se hace uso total de nuestra aplicación de edición de audio, para poder cifrar la información. En figura 3.5.1, se muestra la pantalla grafica de la aplicación de audio.

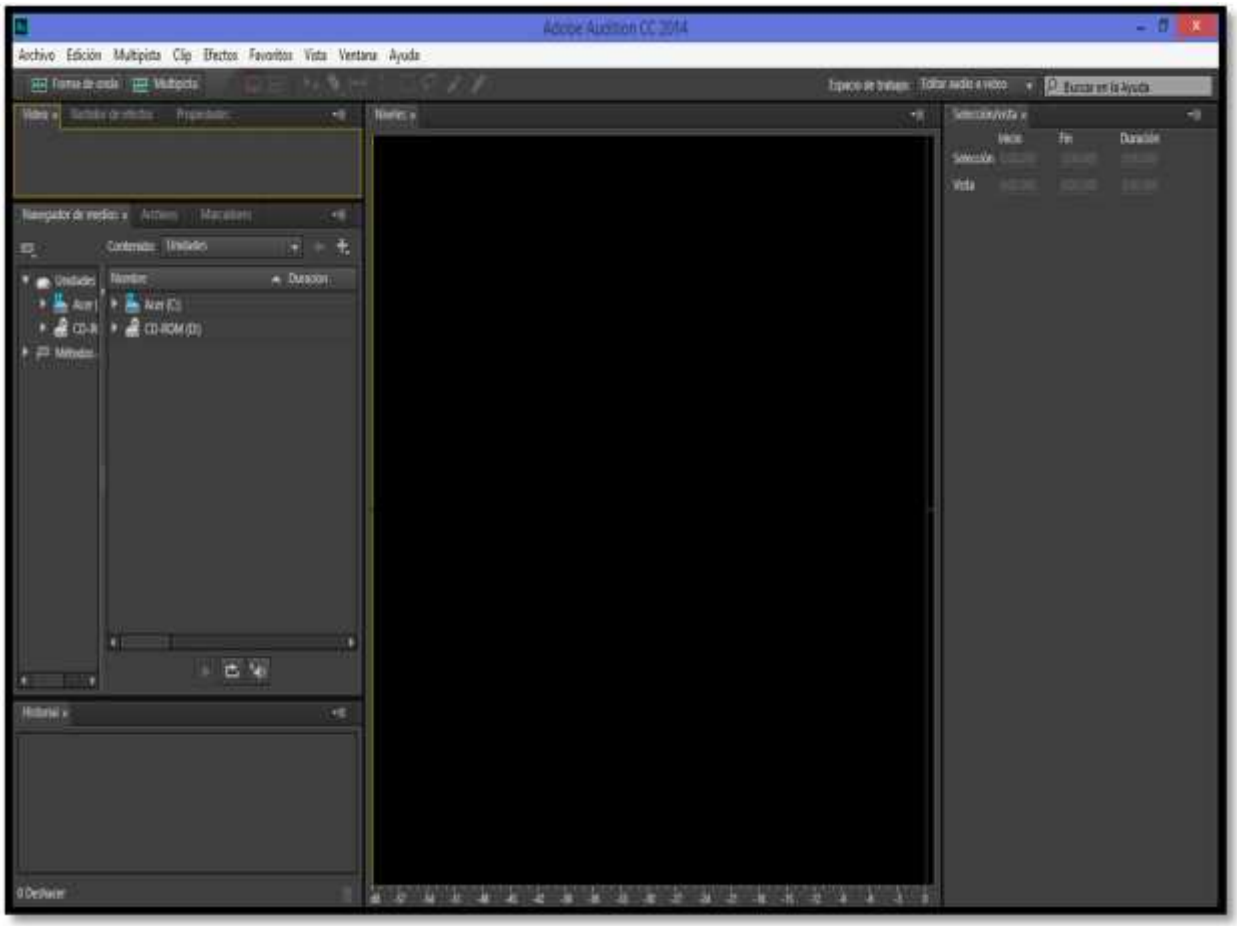

Figura 3.5.1. Aplicación **Adobe Audition CC 2014**, Pantalla principal de la aplicación.

Mediante el editor de audio, se tiene que unificar el paso 1 y paso 2, es decir se va a ser una edición para unificar el audio base que se tiene como fondo musical y la grabación de voz (mensaje). Teniendo como resultado de esta edición de audio, un archivo de audio en formato mp3, nombrándolo p1y2.mp3, para comodidad y saber que en ese archivo está el paso 1 y 2. A continuación se muestra cada una de las pantallas de la aplicación para poder realizar este proceso:

Primero abrir el archivo que contiene el audio base con el fondo musical como se muestra en la figura 3.5.2.

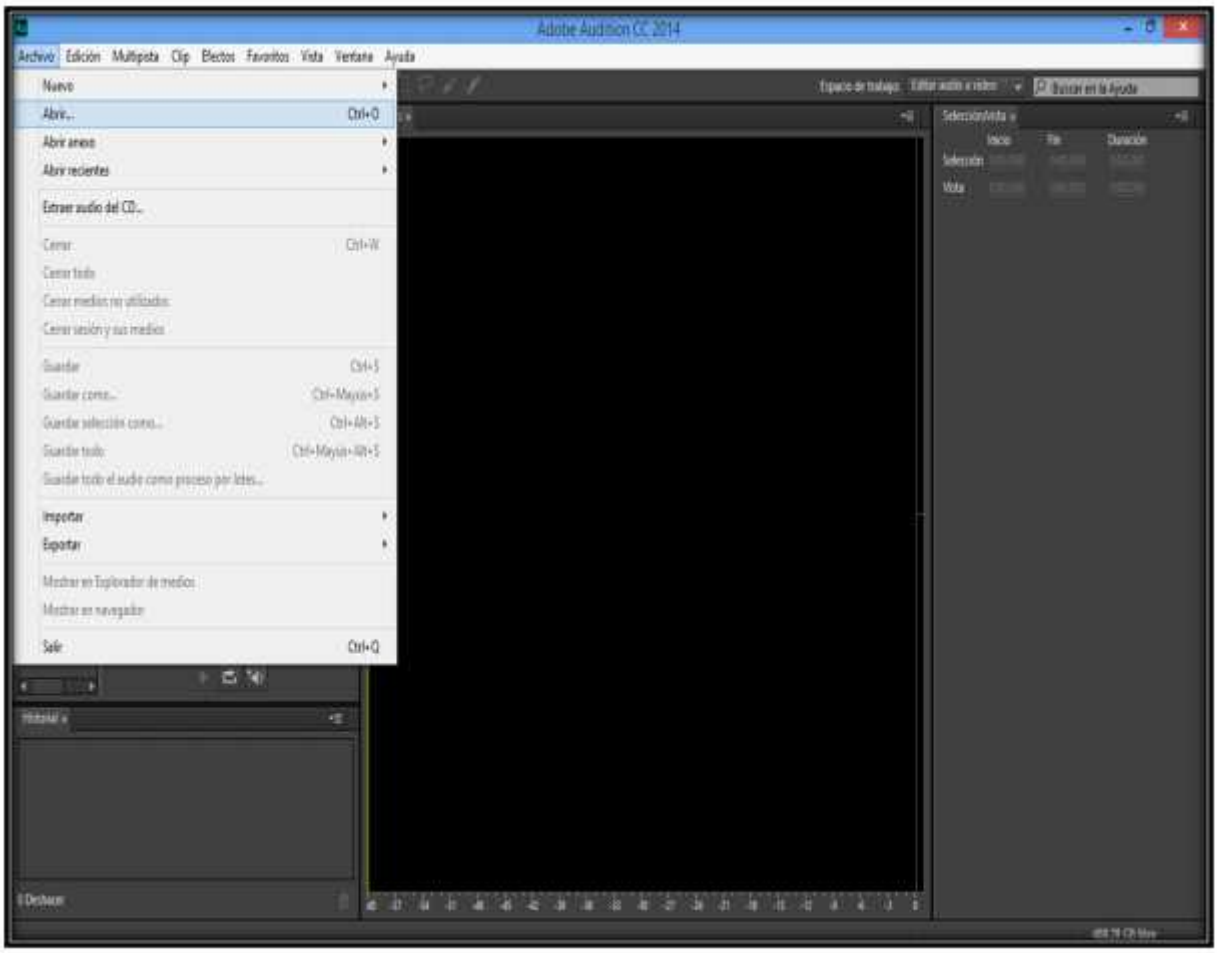

Figura 3.5.2 Para Abrir o guardar cambios de un audio, se puede en las opciones de Archivo.

Para abrir cualquier archivo de audio en la aplicación nos vamos Archivo/Abrir, nos abrirá una ventana para poder seleccionar el archivo con el que se va a trabajar y se da aceptar, para nuestro caso el primer archivo que vamos abrir siempre es el fondo.mp3 (archivo del paso 1). Y se abrirá un recuadro de archivo con el nombre de nuestro archivo junto con su grafica de onda esta se pueden ver en Db o Hz. En la figura 3.5.3 se muestra cómo es que la aplicación da la información de un archivo de audio al abrirlo.

Figura 3.5.3. Aplicación **Adobe Audition CC 2014,** Al abrir un archivo de audio en formato mp3, la aplicación genera dos ventanas; una (recuadro rojo) muestra el nombre de nuestro archivo de audio y la otra (recuadro azul) muestra la gráfica de ondas de frecuencias generadas por la información del audio.

Una vez que ya abrimos el archivo del paso 1 (fondo.mp3), en la primera ventana de la aplicación del lado izquierdo aparece el nombre de nuestro archivo que se abrió, es decir, fondo.mp3, seleccionamos el nombre del archivo después damos clic derecho con el ratón y nos aparecerá un recuadro con varias opciones le daremos clic a la opción **Insertar en multipista/Nueva sesión de multipista,**se abrirá una ventana con el nombre de **Nueva sesión multipista,** esta ventana es para poder nombrar a nuestro proyecto de edición de audio un nombre (el nombre del proyecto será p1y2, para saber que ya se involucraron los archivos del paso 1 y 2) y poder trabajar la edición de dos o más archivos de audio, así como se muestra en la figura 3.5.4.

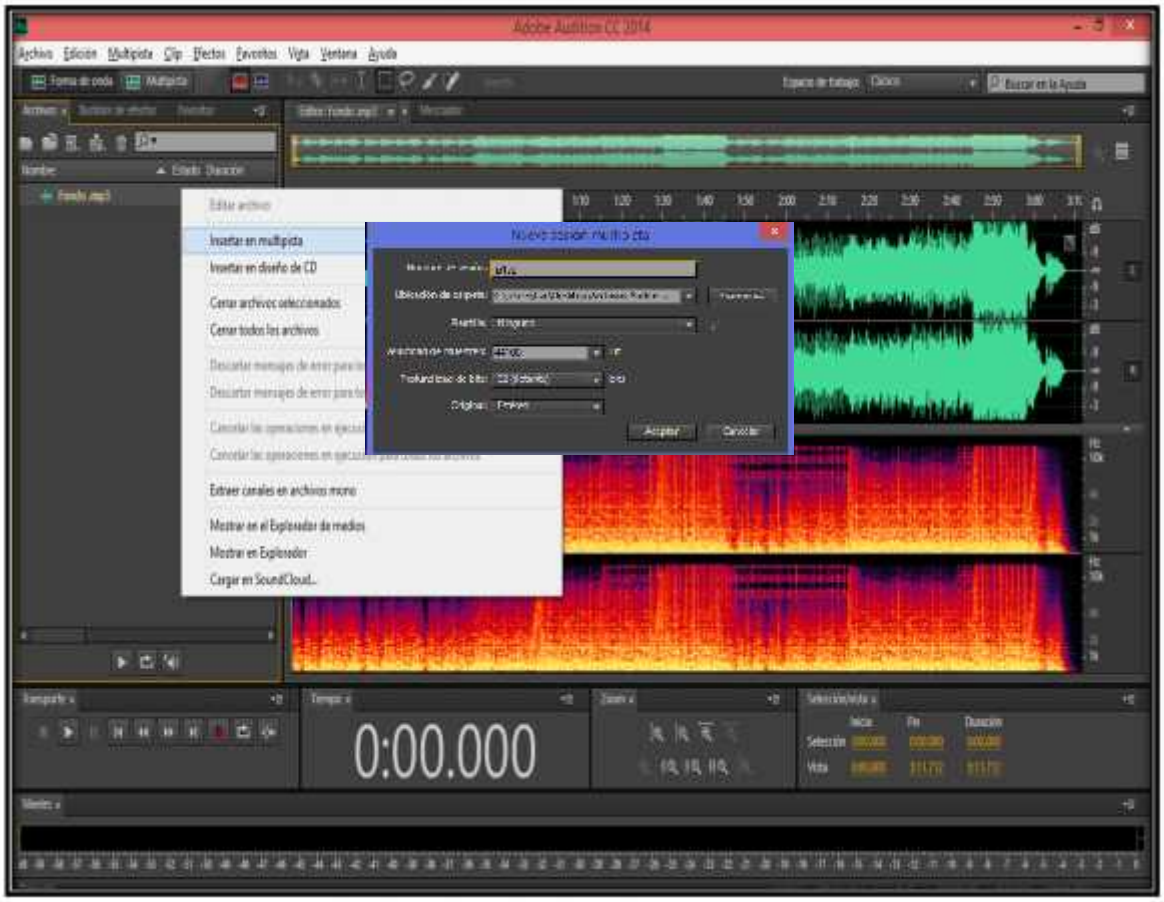

Figura 3.5.4 Aplicación **Adobe Audition CC 2014,** opciones para editar dos archivos de audio.

Una vez que le indicamos el nombre de nuestra sesión multipista, se creará el proyecto de edición y se agregará su nombre en al recuadro de lado izquierdo de la aplicación, y en el recuadro de lado derecho se agregará dos paneles de pistas 1, 2, 3, 4, 5, 6 y 7 como se muestra en la figura 3.5.5; solo se ocupara el panel de la pista 1, el cual contiene la información de las ondas de frecuencia de nuestro archivo fondo.pm3 y el pista 2 se arrastrará el nombre de nuestro archivo que contiene la grabación de voz para obtener la información de sus ondas de frecuencias y poder manipular dichas ondas. Antes de arrastrar nuestro archivo a la pista 2 hay que abrir el archivo Grabación de voz.mp3 (archivo del paso 2), y empezar la edición acomodando los dos archivos de manera que se le dé tiempo para que inicie la música de fondo luego y de inmediato se empiece a escuchar la grabación de voz con el fondo musical y al terminar la grabación, también se le dé tiempo al fondo musical para que nuestro audio termine con el fondo musical, y no con la grabación de voz.

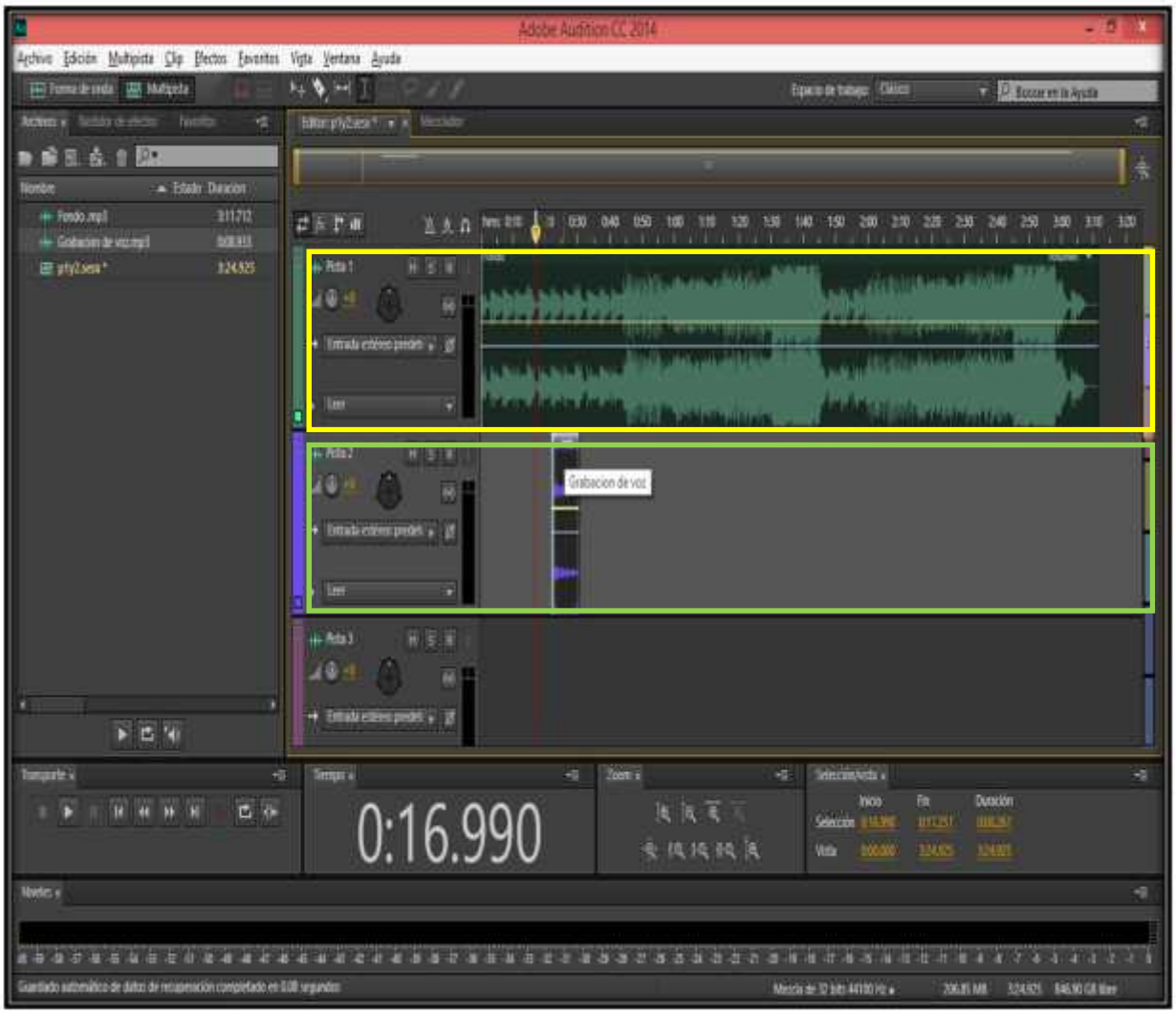

Figura 3.5.5. Aplicación **Adobe Audition CC 2014,** proyecto de sesión de dos audios.

En el recuadro amarillo, se muestra las gráficas de las ondas de frecuencias del archivo de audio fondo.mp3 y en el recuadro verde, se muestra la gráfica de ondas de frecuencias generadas por el archivo de grabación de voz.

Para hacer la edición de los audios y poder unificarlos, el programa **Adobe Audition CC 2014,** cuenta con cada una de las opciones para poder manipular sus ondas de frecuencias de manera que uno le convenga, para poder realizar estas opciones de edición es importante que nuestros archivos no se estén reproduciendo ni en pause deben estar en stop, si no es así, no dejara editar los archivos, estas opciones son:

Opción **selección**: sirve para obtener una trama de frecuencias de onda de tiempo deseada, como se muestra en la figura 3.5.6

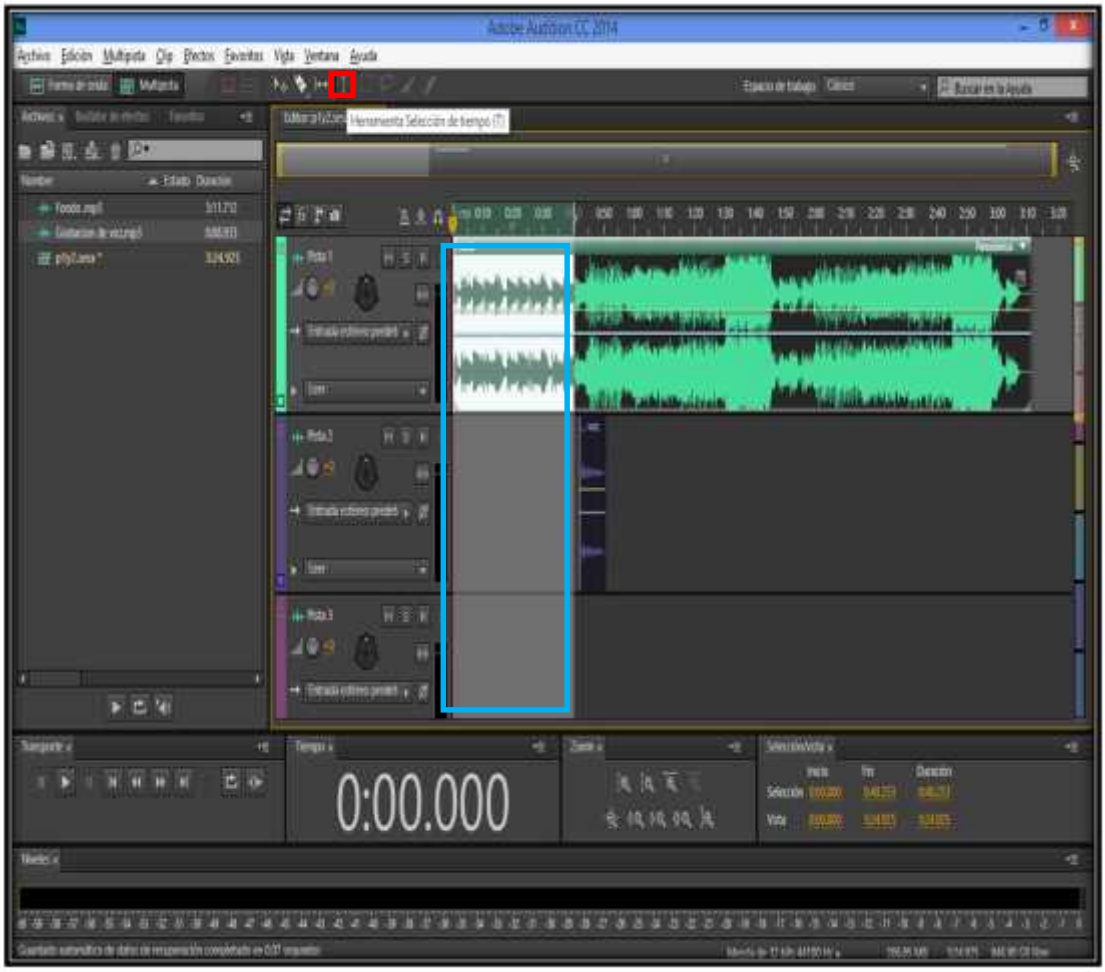

Figura 3.5.6. Programa **Adobe Audition CC 2014**, para seleccionar una trama de tiempo.

Para seleccionar una trama de tiempo le damos clic en la opción de herramienta selección de tiempo enmarcada en la figura con un cuadro rojo y con el cursor del ratón, seleccionamos la trama que deseamos editar, en la figura se muestra con un recuadro azul la trama de tiempo que se seleccionó.

Opción **Copiado**; para copiar una trama la seleccionamos, se hace mediante el comando **Ctrl + c** con botones del teclado. Como se muestra en la figura 3.5.7

Opción **Pegado**; una vez seleccionada la trama y presionado el comando de copiado, se pega la trama mediante el comando **Ctrl + v** con botones del teclado. Como se muestra en la figura 3.5.8.

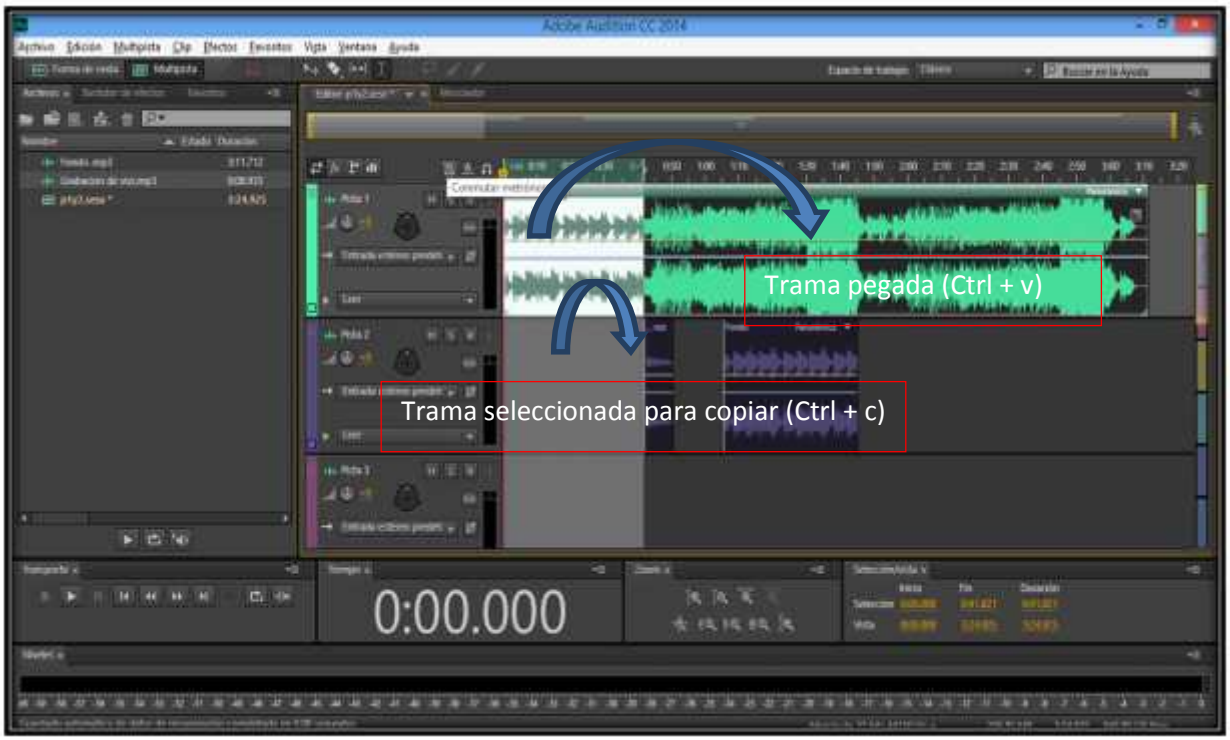

Figura 3.5.7. Programa **Adobe Audition CC 2014,** se muestra como se pegó una trama que se copió de la pista 1 en la pista 2.

Opción **Pegado, Suprimir o borrar**; solo seleccionamos la trama que se desea eliminar y le damos la tecla suprimir y listo la trama seleccionada se borra. Después con las opciones de selección, copiar y pegar movemos la grabación de voz, para que quede acomodada como si fuera una canción dándole tiempo a que inicie el fondo musical después de unos segundos que inicie la grabación de voz, antes de que termine la grabación de voz también hay que darle unos cuantos segundos para que el audio termine con el fondo musical. Si es necesario reducir el fondo musical hay que cortar el audio de fondo musical a modo que se adecue la duración de la grabación de voz y finalmente lo exportamos para guardar el archivo en formato nombrándolo p1y2.mp3 ya que este archivo lo ocuparemos para el paso 5, realizando con esto el paso 4. En la figura 3.5.9 se muestra como quedo el archivo nuevo de audio con el nombre p1y2.mp3.

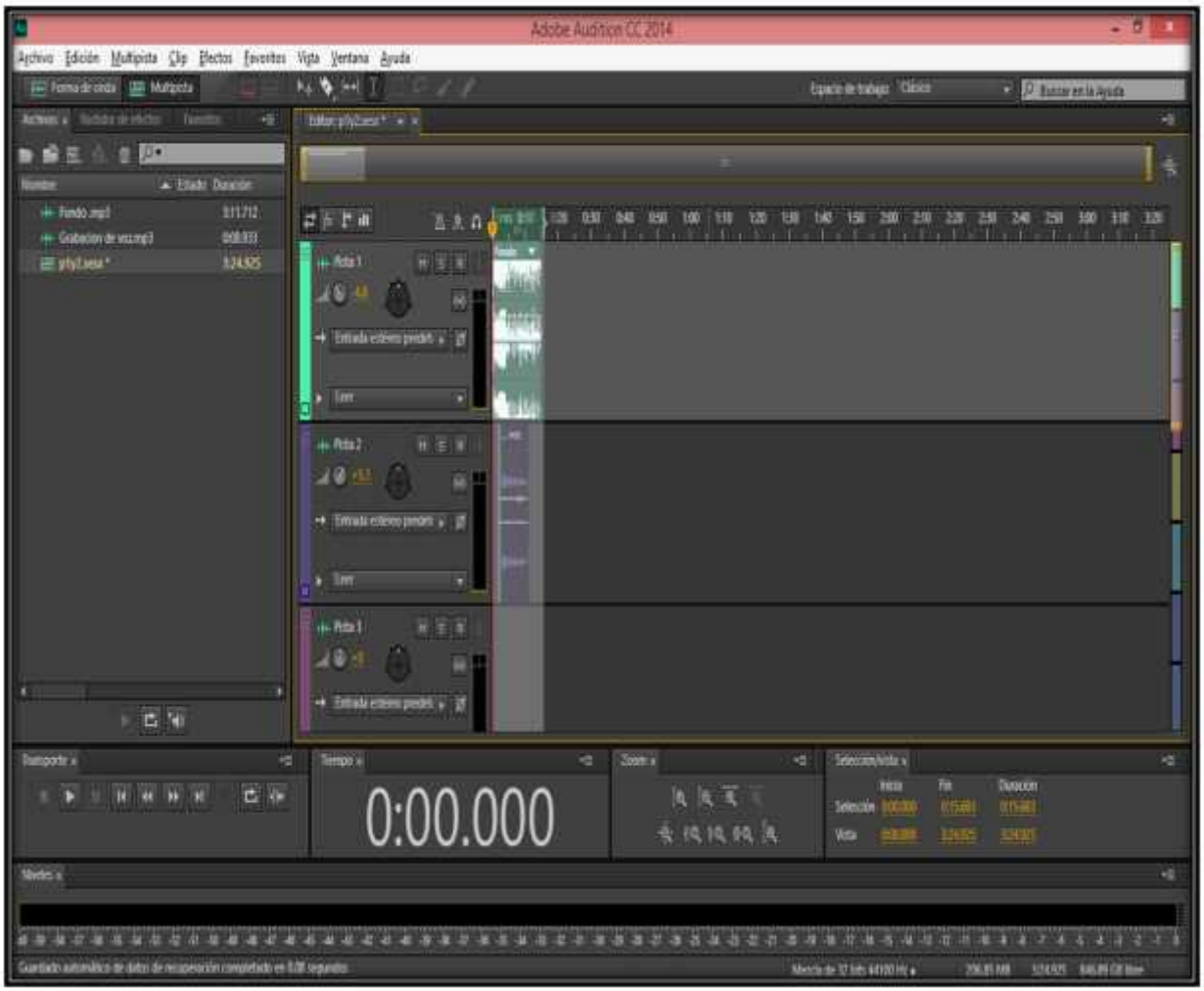

Figura 3.5.8. Programa **Adobe Audition CC 2014** realizando el paso 4.

Para el paso 4 la edición de la grabación de voz y el fondo musical generando el archivo p1y2.mp3 para el paso 5, una vez bien acomodada las señales de ondas de frecuencias de los dos audios, se tiene que generar solo una señal de ondas de frecuencias de tiempo mediante las opciones del programa **Multipista/Mezclar sesión en un archivo/sesión completa,** como se muestra en la figura 3.5.9 Después de haber unificado en una sola señal de frecuencias los archivos del paso1 y 2, es exporta el archivo en formato mp3, con el nombre p1y2.mp3 fue así nombrado así para comodidad y realización del algoritmo. En la figura 3.1.10 se muestra gráficamente las opciones para exportar un archivo y guardarlo en formato mp3.

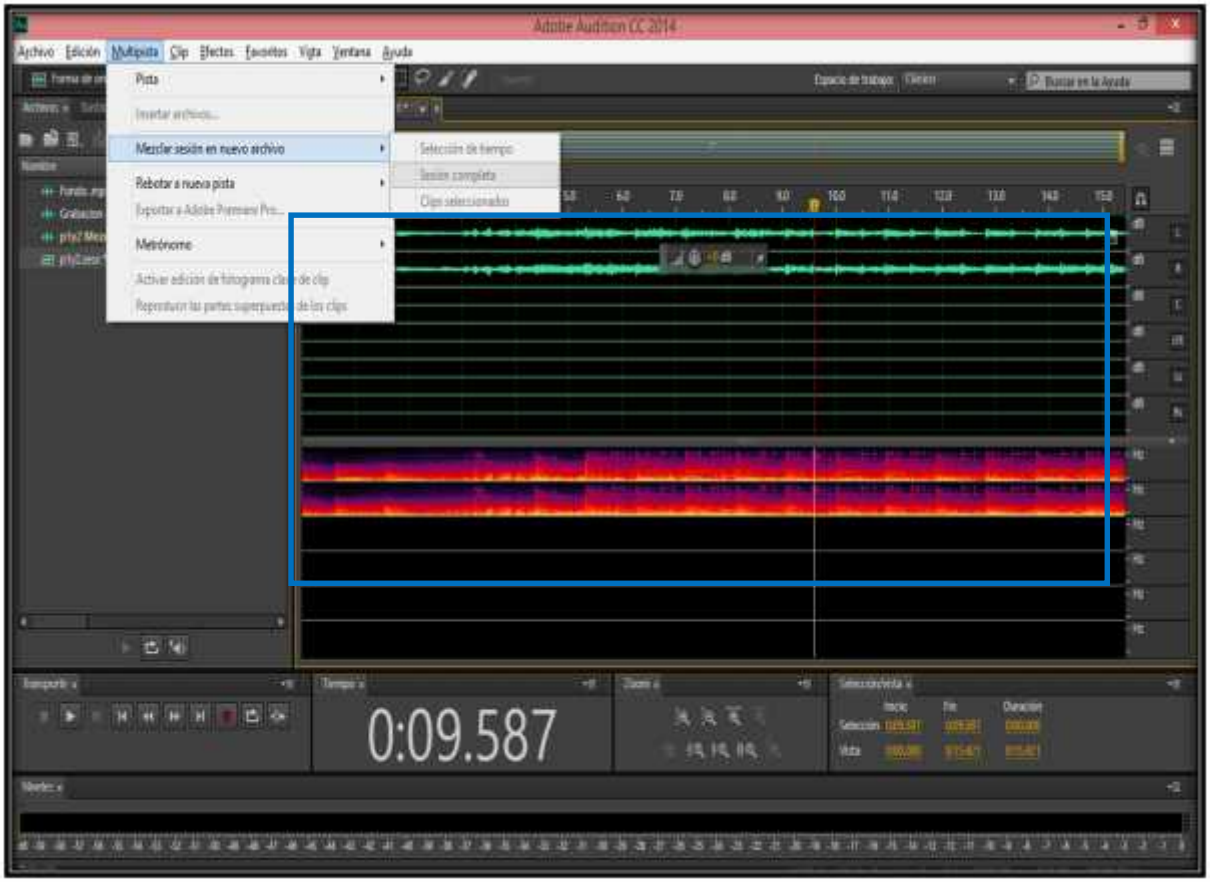

Figura 3.5.9. Programa **Adobe Audition CC 2014,** resultado de la edición de audios del **paso 4**.

Unificando los archivos del paso 1 y 2 quedando una señal de ondas de frecuencias como se muestra en el recuadro azul, para generar un nuevo audio que ocuparemos en el paso 5.

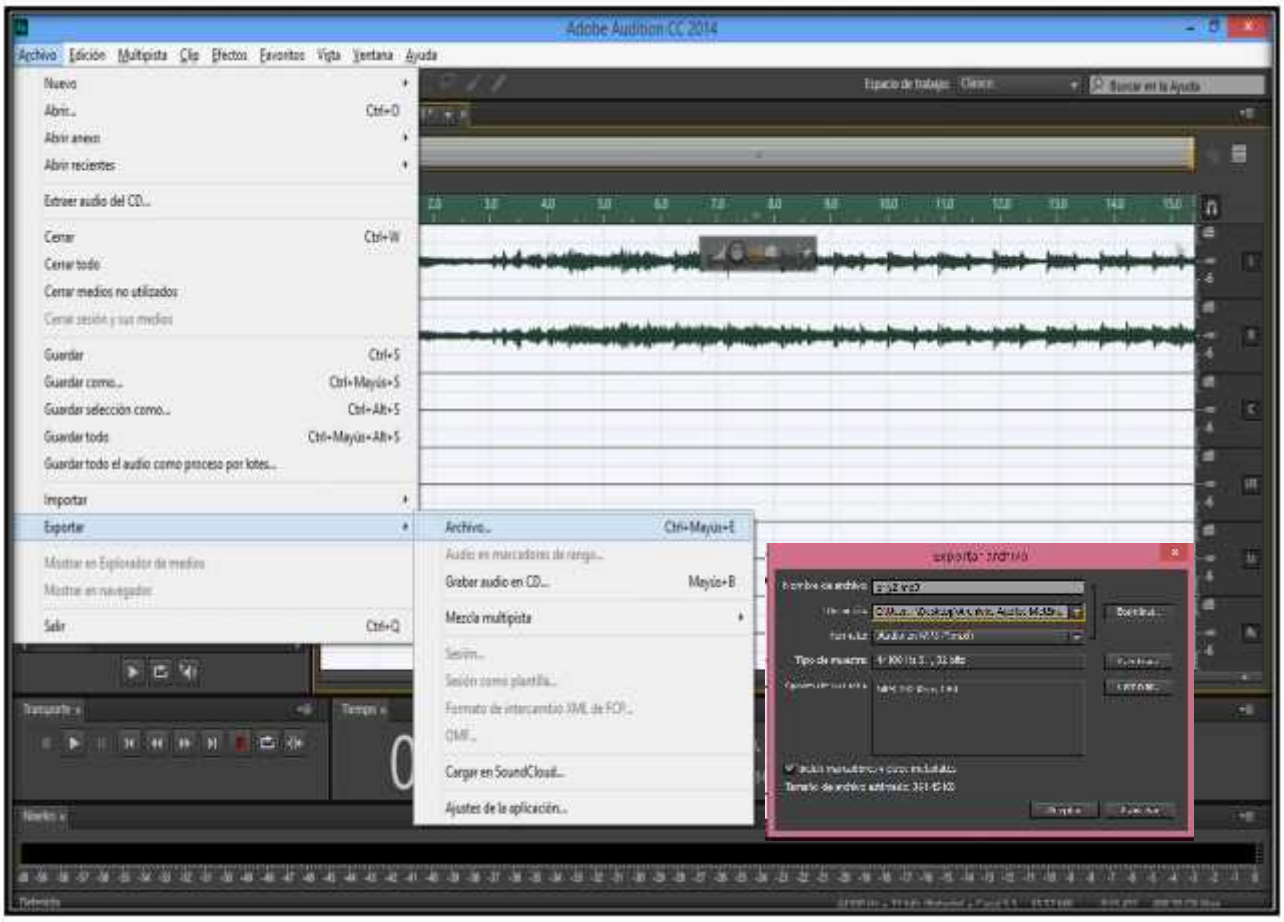

Figura 3.5.10. Programa **Adobe Audition CC 2014,** para exportar a un archivo de audio en el programa de edición de audio.

Para exportar a un archivo de audio en el programa de edición de audio, iremos a la opción dando clic en **Archivo/Exportar/Archivo.** Se abrirá una ventana para indicarle el nombre del archivo, para este caso será p1y2.mp3, la ubicación de donde se desea guardar el archivo y el formato en el que se va a guardar, seleccionaremos .mp3 y damos aceptar, con esto tendremos el archivo creado del paso 4 en formato mp3.

Paso 5: Para este caso se abren dos archivos; uno es el archivo p1y2.mp3 resultado del paso 4 y el otro archivo la señal de ruido almacenada en formato.mp3, que contiene ruido del tráfico de la ciudad de puebla, como se muestra en la figura 3.5.11. Para hacer nuestra segunda y última sesión de edición de audio y concluir con este último paso el método de cifrado.

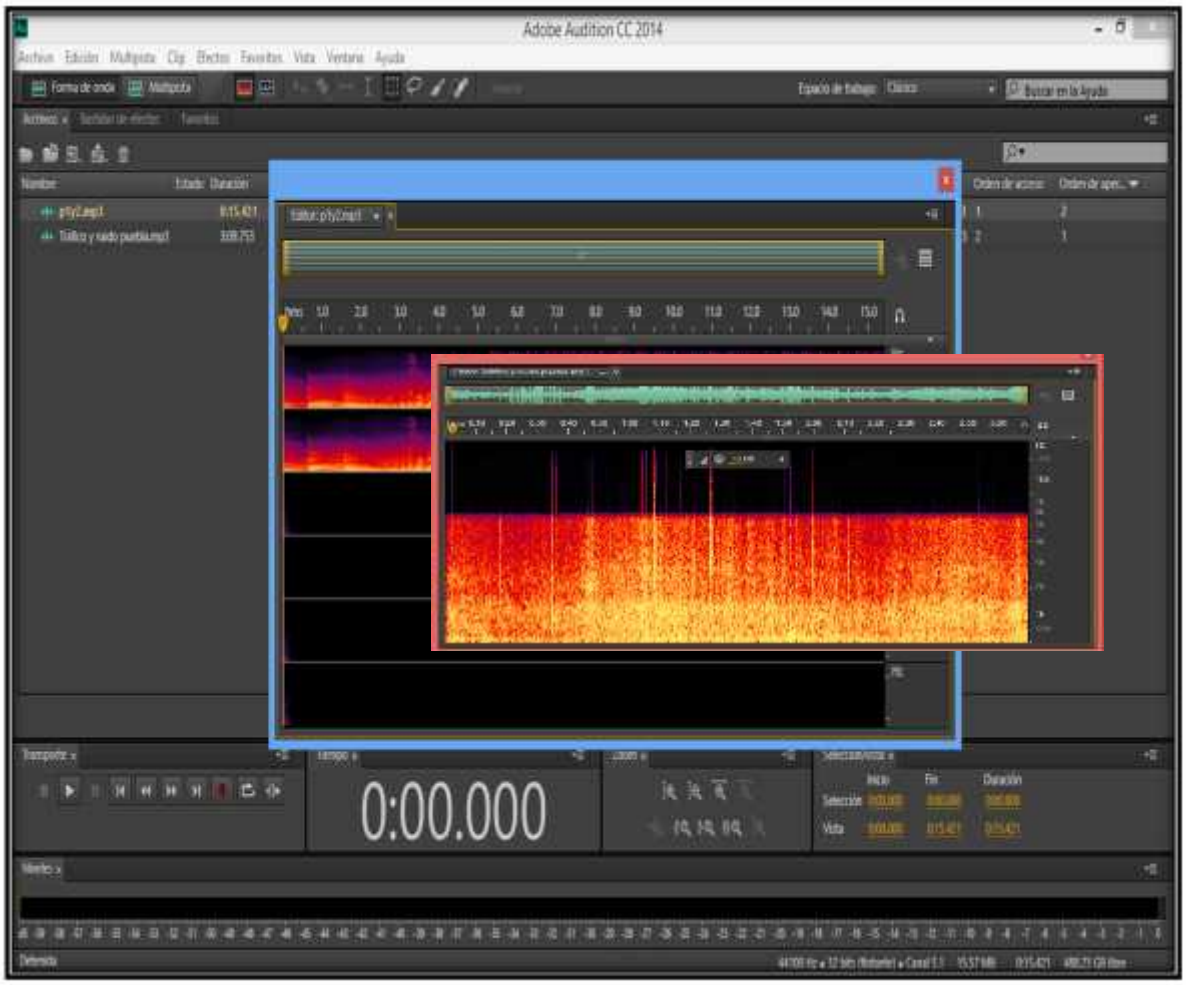

Figura 3.5.11 Programa **Adobe Audition CC 2014,** en la figura se muestra la información de la señal de onda de frecuencia de nuestros dos archivos finales que van a ser necesarios para generar el paso 5.

En el paso 5 el objetivo es generar el criptograma, es decir nuestro archivo de audio ocultando la información (grabación de voz) involucrando toda una trama de señal de ruido por arriba de la señal generada en el archivo del paso 4. Para esto vamos a editar el archivo del paso 3, la señal de ruido del tráfico de puebla a modo de hacerle un espacio en la parte de debajo de la señal de ondas de frecuencias formada por la información generada de dicha señal, esto lo realizamos con la **herramienta de cuadro de selección** tal y como se muestra en la figura 3.5.12

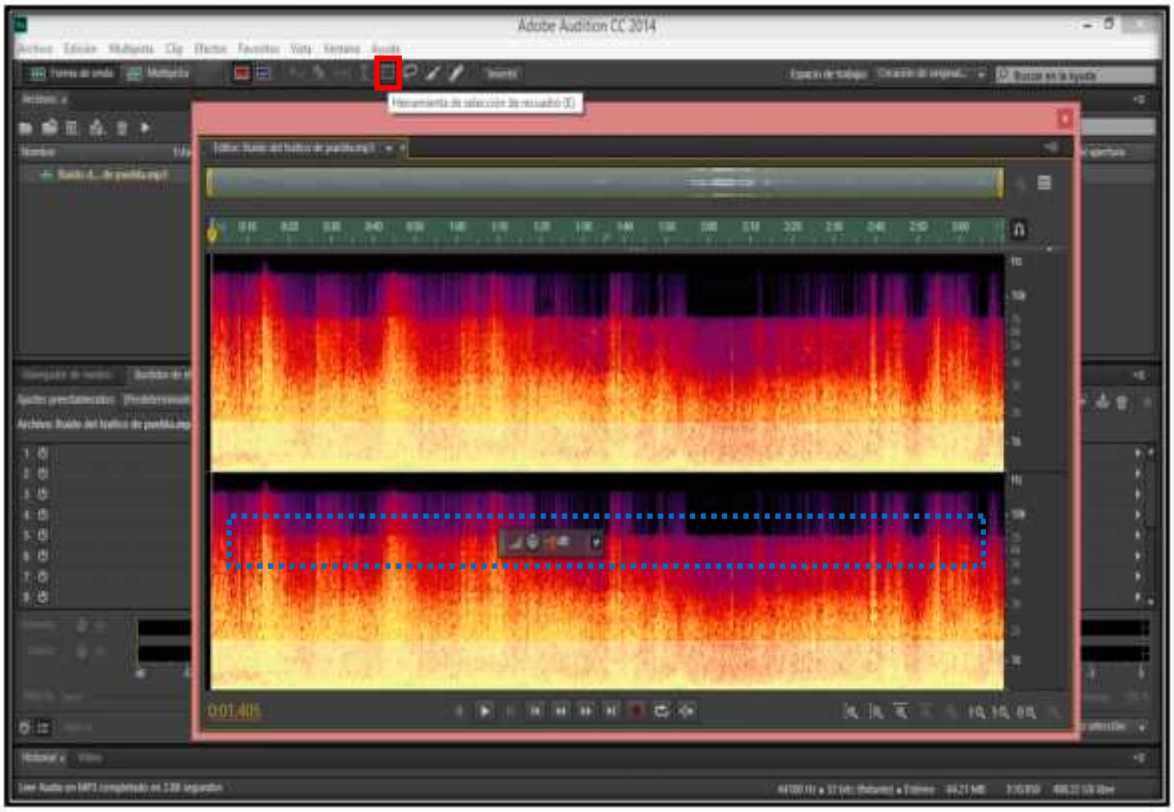

Figura 3.5.12. Programa **Adobe Audition CC 2014** realizando el paso 5.

Para el paso 5, la edición de nuestra señal de ruido, está en formato mp3, seleccionamos la herramienta marcada en recuadro dándole clic, y posteriormente seleccionamos con el cursor, la parte más baja de la señal, tal como se muestra en la imagen en el recuadro punteado de color azul una vez seleccionado. Esa señal se borrara con la tecla **supr** para introducir en ese espacio nuestro archivo del paso 1 y 2, como se muestra en la figura 3.5.13

Figura 3.5.13 Programa **Adobe Audition CC 2014** realizando el paso 5, eliminación de trama de ruido.

El paso 5, eliminación de trama de ruido, para dejar espacio, para introducir las ondas de frecuencia digitales de nuestro archivo generado en paso 4, dependiendo de su señal hay que suprimir dicho espacio en la señal de ruido, para poder ingresar en ese espacio limpio la señal de archivo del paso 4, va a ser necesario subirle el volumen a la señal de ruido para que al pegar la frecuencias de ondas se escuche más ruido y no la información, como se muestra en la figura 3.5.14

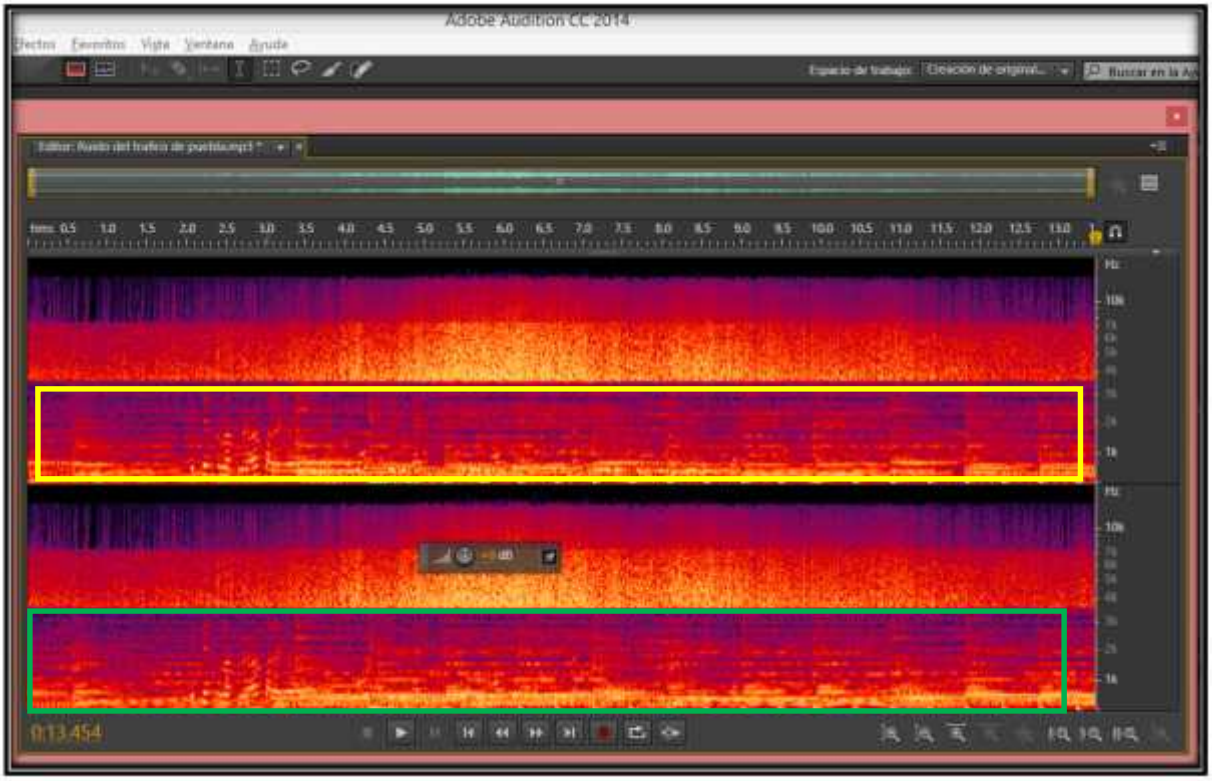

Figura 3.5.14 Programa **Adobe Audition CC 2014** realizando el paso 5, en la imagen se muestra que ahora el espacio que se eliminó.

Se muestra que ahora el espacio que se eliminó, mediante cuadro de selección en ese espacio se tiene que pegar toda la señal de ondas de frecuencias generadas por el fondo musical y la grabación de voz, formando con este nuestro criptograma de manera satisfactoria, lo que está en recuadro amarillo en la señal de ruido y lo que están recuadro verde es la información que se está ocultando.

Con esto se finaliza el algoritmo, de encriptación antes de guardar los cambios hay que escuchar que efectivamente se tenga un audio sin información preliminar, solo un audio con ruido y con la mínima información de grabación de voz.

Nota: todas las opciones de edición las tiene el programa **Adobe Audition CC 2014**, como: abrir archivo nuevo, exportar, recortar, pegar, seleccionar, importar, grabar la voz y las opciones necesarias para mejorar la calidad de un audio y la grabación de voz.

3.6Como quitar reducir el ruido con Adobe Audition CC 2014.

El programa de edición **Adobe Audition CC 2014**, dispone de una opción que permite reducir el ruido de un archivo de audio. Lo que en realidad hace el programa es eliminar determinadas frecuencias, en las que se encuentran ondas de ruido. Pero al eliminar esas frecuencias, se están eliminando partes de la grabación que comparten las frecuencias en donde se encuentra el ruido, el resultado, tras aplicar este efecto puede ser un fragmento limpio y nítido o bien un fragmento con un sonido algo metalizado. Somos nosotros los que hacemos la valoración si el resultado nos compensa o no. Esto se origina cuando grabamos la voz o algún acontecimiento en el medio ambiente, siempre se generan señales de ruido. Para poder reducir el ruido mediante esta aplicación de edición de audio.

Si el ruido se encuentra introducido en la grabación de voz de nuestro audio, y no está separada drásticamente como en el procedimiento del método de encriptación, se puede reducir el ruido y mejorar nuestra grabación de voz.

Para estos casos se hace de la siguiente manera: primero abrimos nuestro archivo, después las opciones **Vista/visualización de ondas de frecuencias,** como se muestra en la figura 3.6.1.

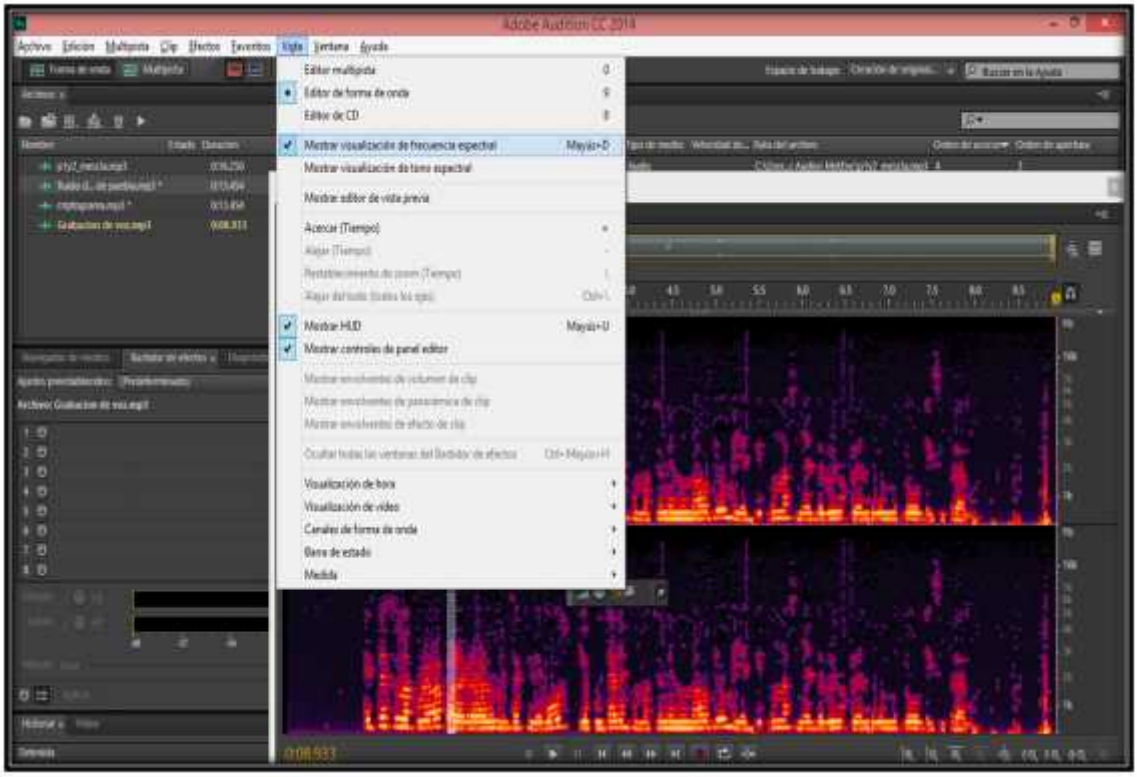

Figura 3.6.1 Programa **Adobe Audition CC 2014 reducción de ruido en un audio.**

Ahora con la Herramienta de Selección de Recuadro seleccionaremos el Ruido, el cual podemos escuchar presionando la barra espaciadora. Le damos clic derecho a la selección y se procede a dar clic en Capturar Perfil de Reducción de Ruido y daremos clic, automáticamente captura el programa la impresión de sonido. En la figura 3.6.2 se muestra este pequeño proceso.

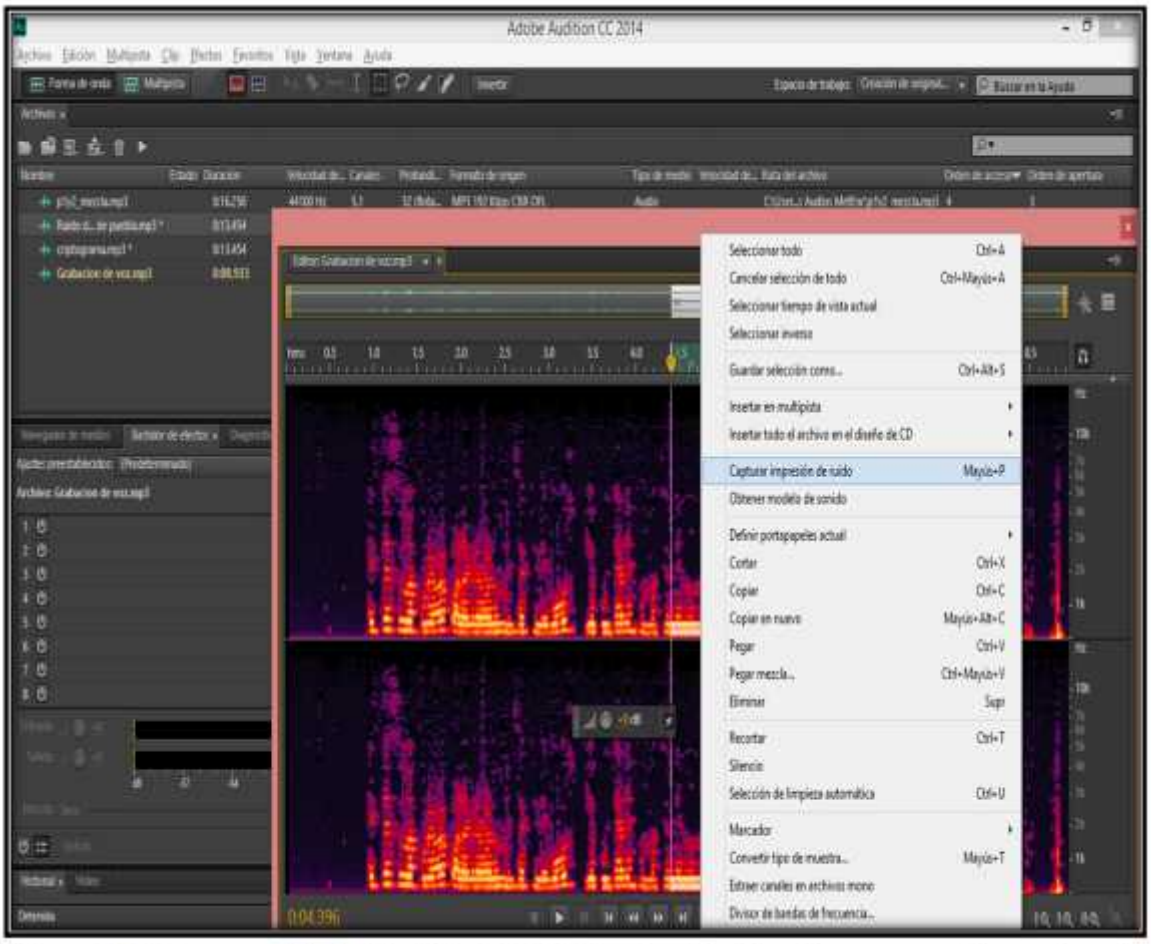

Figura 3.6.2 Programa **Adobe Audition CC 2014 reducción de ruido en un audio,** captura de impresión de sonido**.**

Seleccionamos toda la pista de audio, y una vez seleccionada iremos a la ventana de **Efectos/Restauración/Reducción de Ruido/Reducción de ruido (proceso),** hacemos clic en esta última. Como se muestra en la figura 3.6.3.

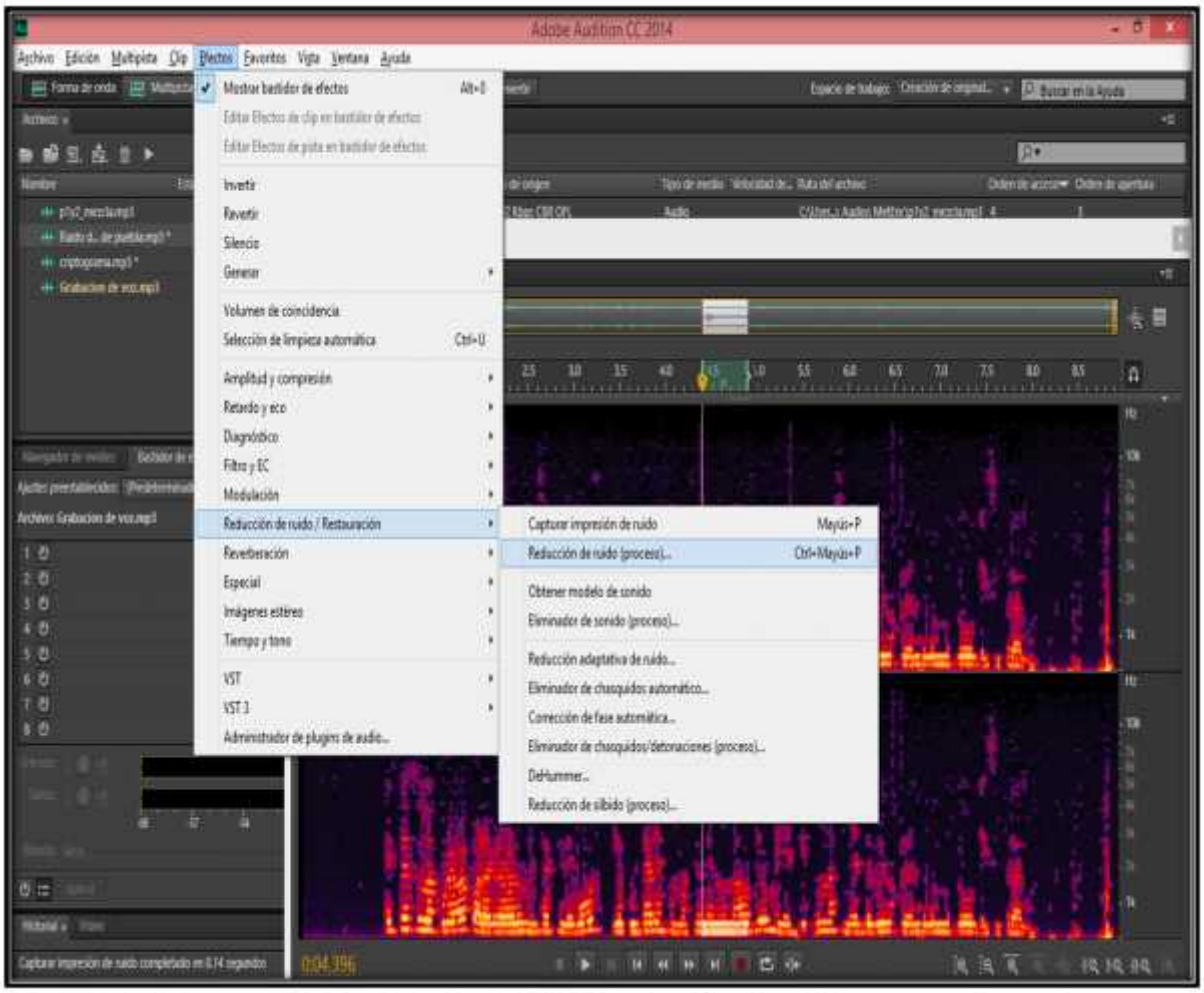

Figura 3.6.3 Programa **Adobe Audition CC 2014 reducción de ruido en un audio,** opciones para reducir el ruido en un audio**.**

Nos aparecerá una ventana que nos muestra varias opciones para reducir el ruido, Seleccionamos el botón Seleccionar toda la Fila si el ruido se repite en todo el sonido, como se muestra en la figura 3.6.4. Después jugamos con los demás valores hasta eliminar el ruido y damos aceptar.

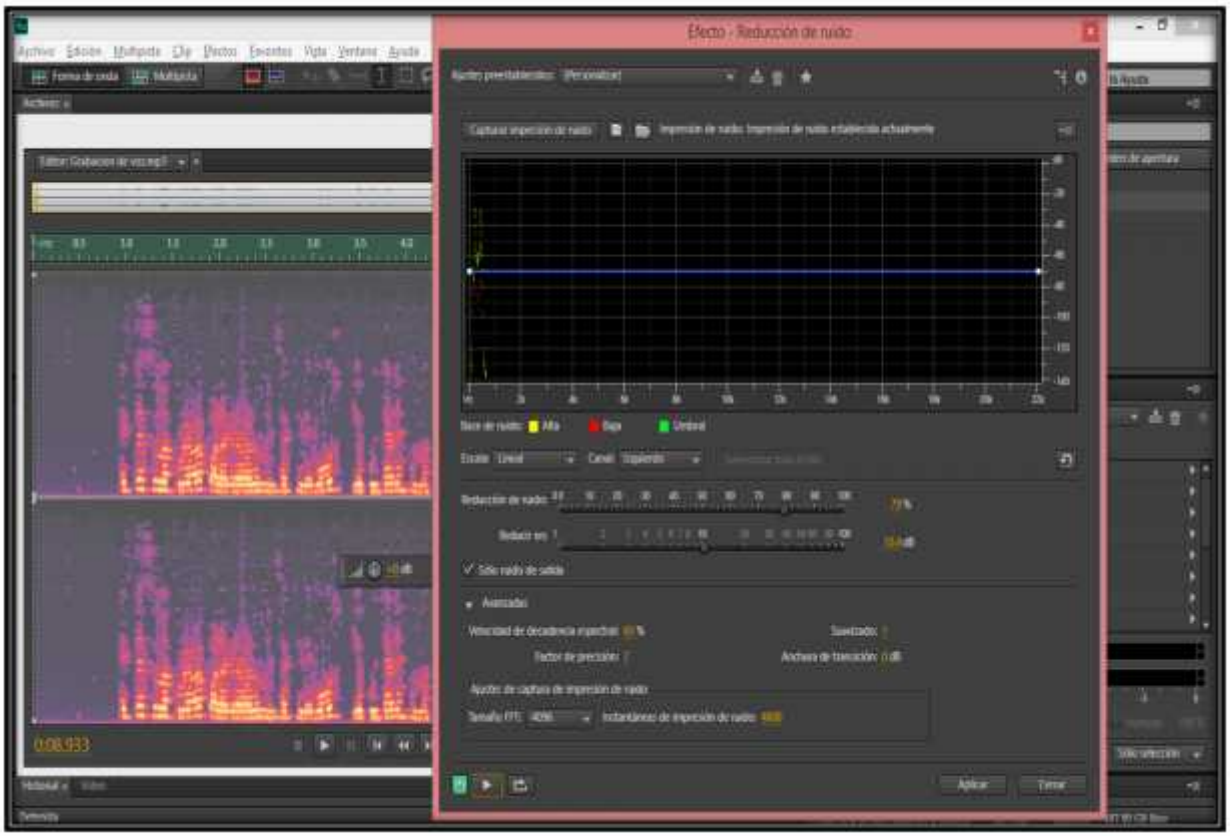

Figura 3.6.4 Programa **Adobe Audition CC 2014 reducción de ruido en un audio,** paso final para reducir el ruido en un audio**.**

El efecto Reducción de ruido/Restauración. Reducción de ruido reduce significativamente el ruido de fondo y de banda ancha con una reducción mínima de la calidad de la señal. Este efecto permite eliminar una combinación de ruido, incluido el silbido de cinta, el sonido de fondo del micrófono, zumbido de línea de potencia o cualquier ruido constante en una forma de onda.

La cantidad adecuada de reducción de ruido depende del tipo de ruido de fondo y de la pérdida aceptable de calidad de la señal restante. En general, puede aumentar la relación señal-ruido en un valor comprendido entre 5 y 20 dB y mantener una alta calidad de audio.

Para obtener los mejores resultados con el efecto Reducción de ruido, debe aplicarlos a audio sin desplazamiento de DC. Con desplazamiento de DC, este efecto puede introducir chasquidos en pasajes tranquilos. (Para eliminar un desplazamiento de DC, seleccione Favoritos - Reparar desplazamiento de DC).

Y listo hemos aprendido a eliminar ruido de una forma sencilla y práctica, ahora solo guardaremos el archivo y lo podremos utilizar. Como se puede ver en la figura 3.6.5

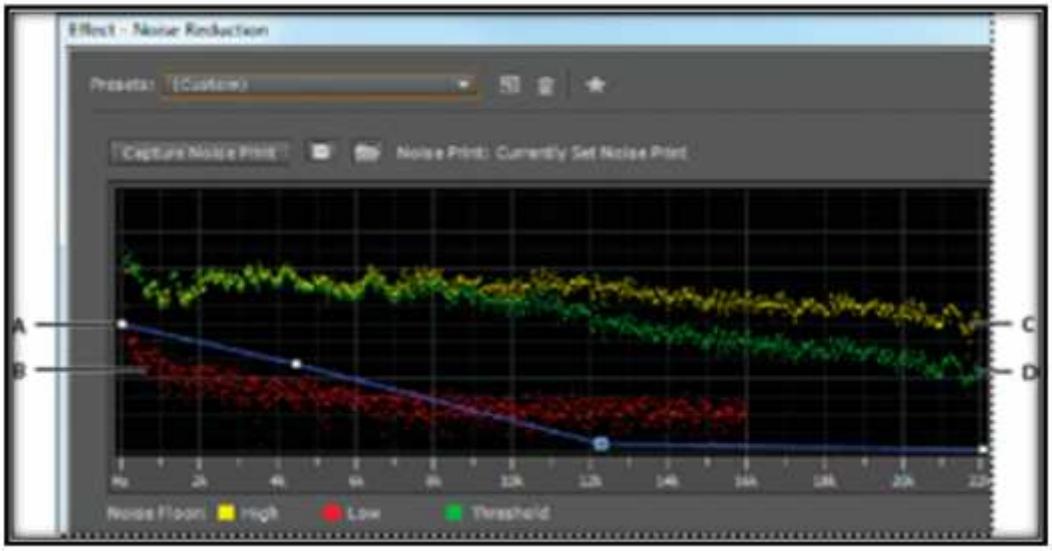

Figura 3.6.5 Programa **Adobe Audition CC 2014 reducción de ruido en un audio.**

Evaluación y ajuste de ruido con el gráfico Reducción de ruido: A. Arrastre los puntos de control para variar la reducción en diferentes rangos de frecuencia B. Ruido de amplitud baja. C. Ruido de amplitud alta D. Límite bajo el cual se produce la reducción de ruido.

Una vez realizando estos cambios antes de guardarlos se puede escuchar cómo quedó nuestro audio reduciendo las frecuencias generadas por el ruido, damos aceptar y los cambios estarán guardados y se podrá exportar en un formato de audio para este caso .mp3.

Otra forma de reducir estas señales de ruido es haciéndolo trama por trama, esta es más tediosa pero es la mejor, ya que como se está trabajando trama por trama, se le da un tiempo dedicado a cada frecuencia de ruido y se reduce de una manera notable, esto sirve de mucho cuando se tiene una grabación de voz en un archivo digital por ejemplo .mp3, como ya se sabe cuándo se graba la voz siempre la grabación contará con ruido generado por el medio ambiente o por el mismo instrumento de grabación. Para este proyecto fue de mucha ayuda, ya que se eliminó el ruido de la grabación de voz teniendo como resultado una voz digital más limpia. Este proceso se realiza mediante la opción **herramienta pincel correcto puntual (B)**, además de que se genera un curso de selección con un grosor de selección deseado para selección de un simple punto hasta una circunferencia más grande desde medidas que uno desee, en la figura 3.6.6 se muestra la opción**.**

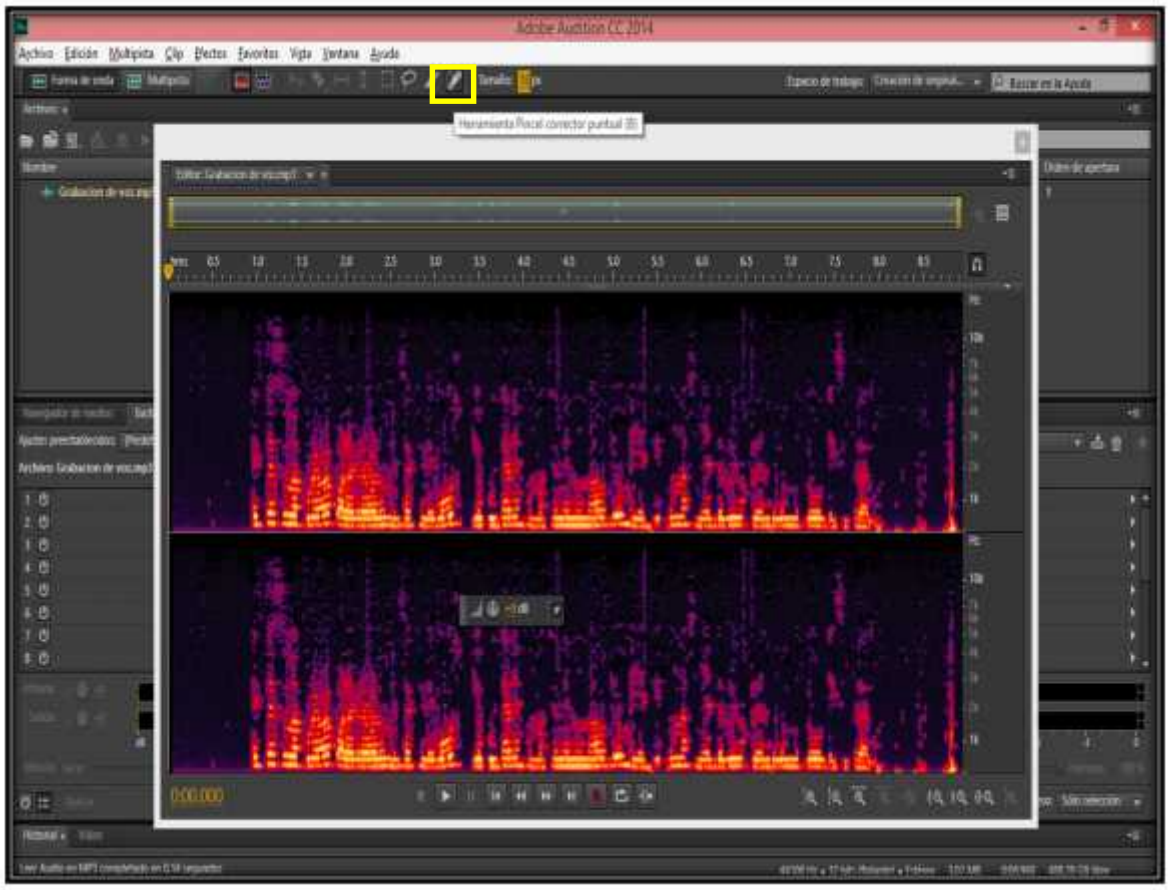

Figura 3.6.6 Programa **Adobe Audition CC 2014 reducción de ruido en un audio.**

En el recuadro amarillo se muestra la ubicación de esta opción para reducir el ruido manualmente, en el modo de visualización espectral, existe una forma de eliminar de manera rápida y sencilla los sonidos pequeños de fondo que ensucian el audio con señales de ruido como: toses, chasquidos, siseos, sirenas, timbres de celular, pasos, respiración, entre otros sonidos secuenciales.

Mediante la opción de Pincel corrector puntual se logra realizar la limpieza de la pista en fragmentos pequeños y perfeccionándolos de manera manual, pero si lo que se pretende es eliminar un sonido secuencial de manera prolongada, por ejemplo, el sonido de una sirena mientras hay una voz de un locutor delante, y el sonido se prolonga durante toda la pista de audio, se puede crear un modelo de sonido tomando como punto de referencia la selección realizada, además se puede usar posteriormente en ediciones similares. La **herramienta Pincel corrector puntual** funciona solamente en modo de visualización espectral como se puede ver la figura 3.6.7.

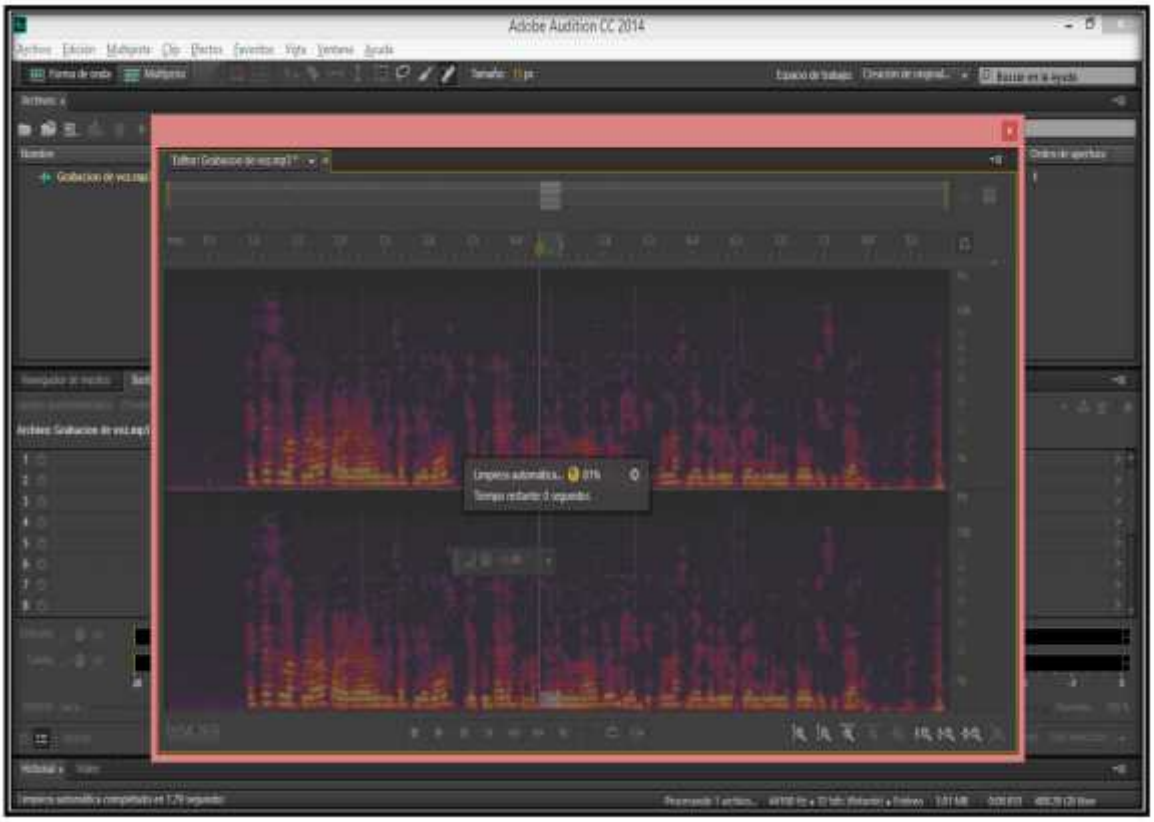

Figura 3.6.7 Programa **Adobe Audition,** selección de un pequeño fragmento de frecuencia aplicando la opción **herramienta pincel correcto puntual.**

3.7 Descifrado del criptograma creado por el método esteganográfico enfocado a un audio mediante una señal de ruido.

Mediante un algoritmo de cifrado, la información de alguna manera se codifica para ocultarla, la esteganografía toma algún archivo digital como base para introducirle información y ocultarla como se hizo en este proyecto. Todo algoritmo criptográfico tiene como resultado un criptograma, dicho algoritmo debe tener su inversa, es decir poder descifrar el criptograma teniendo acceso total a la información que se ocultó.

Para este nuevo método de encriptación y con la ayuda de la aplicación de audio, se realizó el proceso de descifrado siguiendo los siguientes pasos en la aplicación **Adobe Audition:**

Paso 1: Una vez que se tiene el criptograma en formato mp3, se abre este criptograma de audio con la aplicación **Adobe Audition**, como se muestra en la figura 3.7.1

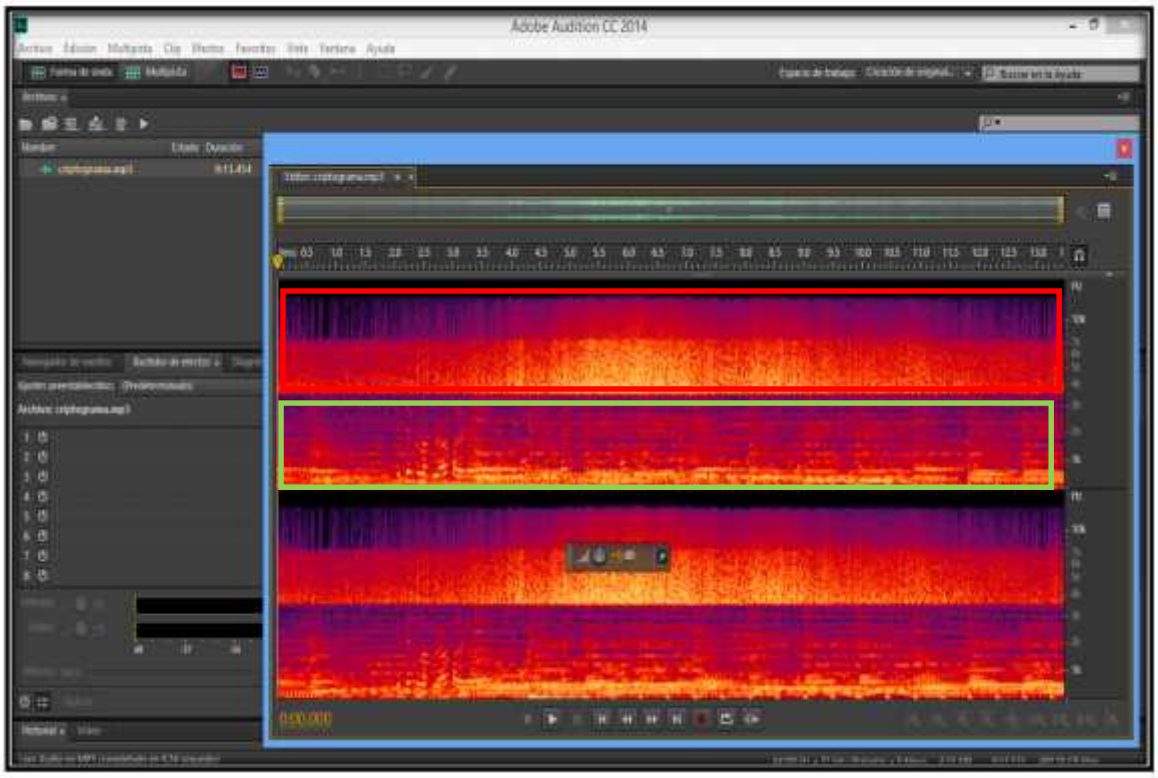

Figura 3.7.1 Proceso de descifrado, Abrir el criptograma con la aplicación de audio **Adobe Audition.**

Paso 2: Una vez que ya se abrió el archivo de audio que contiene nuestro criptograma, muestra las señales de onda que genera la información de nuestro criptograma y se observara en dicha grafica como la señal esta partida en dos. La **parte superior** es nuestra señal generada por nuestra clave o llave de encriptación, es decir la señal de ruido, y en **la parte inferior** se muestra la gráfica generada por nuestro audio base y nuestra grabación de voz, recordando que la grabación de voz es la información que se ocultó. En la figura 3.7.2 se muestra en recuadro rojo la parte superior y con verde la parte interior descritas anteriormente.

Para descifrar la información, seleccionamos con un clic, la opción del programa de audio **Herramienta de selección de recuadro,** después seleccionamos mediante esta herramienta el recuadro que encuentra en la parte superior de nuestra señal de onda formada por el criptograma, así como se muestra en la figura 3.7.3.

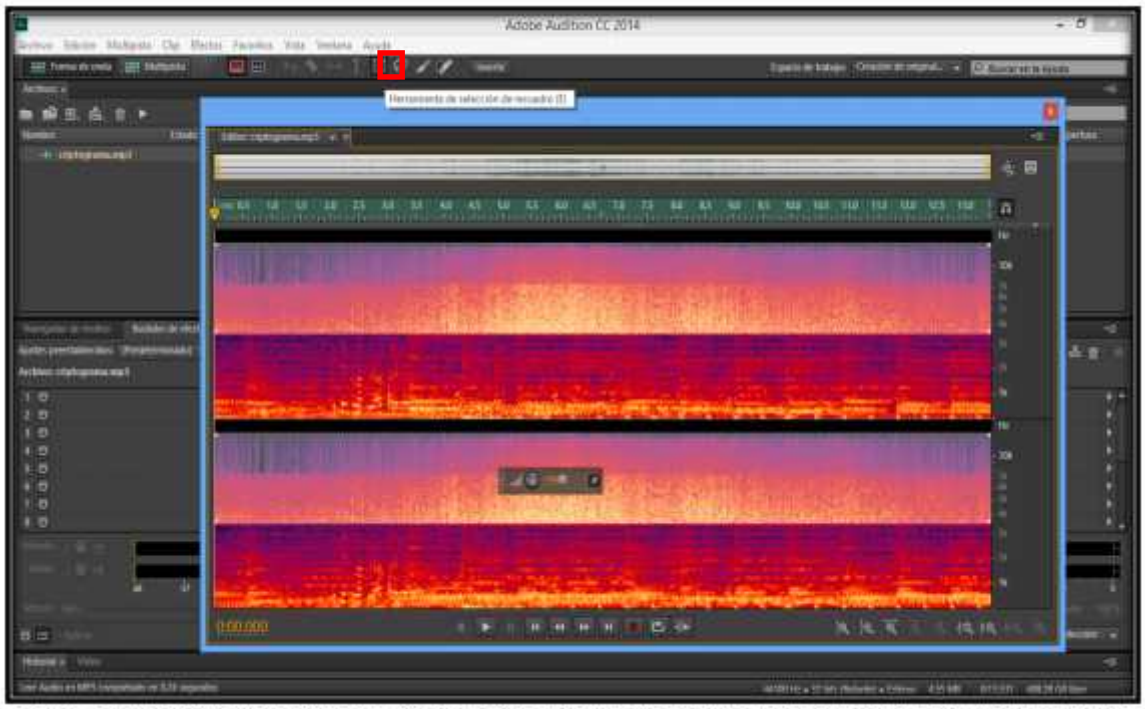

Figura 3.7.2opción de selección de recuadro, mostrada mediante el cuadrito rojo y con el cursor seleccionamos y arrastramos hasta abarcar toda la parte superior del rectángulo superior formado por la información de ondas del criptograma.

Después de haber seleccionado, lo único que se tiene que hacer es eliminar dicha información del criptograma, mediante la tecla **supr**, tal y como se muestra en la figura 3.7.3

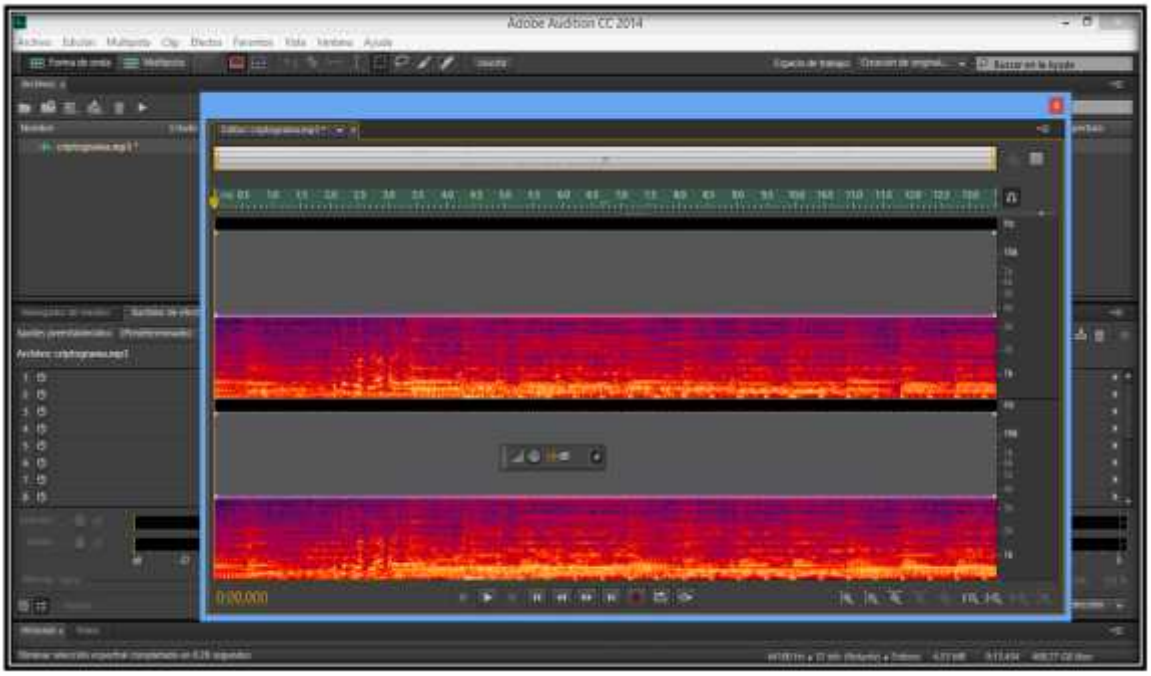

Figura 3.7.3 Selección de recuadro y eliminación de ondas formadas por nuestra llave de encriptación, es decir el ruido en el criptograma.

Como se puede ver en la imagen 3.7.3, al eliminar la señal de la parte superior se queda la señal de ondas de la parte inferior, la cual contiene nuestra llave de encriptación, es decir, nuestra señal de ruido, quedando las ondas de frecuencia de la parte inferior la cual contiene la información relevante, la grabación de voz, con esto se cumple satisfactoriamente el proceso de descifrado de la información de este algoritmo de encriptación.

CAPÍTULO IV:

RESUTADOS

4.1 METODO DE CIFRADO MODERNO TOMANDO UN ARCHIVO DIGITAL, UN AUDIO Y UNA APLICACIÓN DE EDICION DE AUDIO.

En este capítulo se verá todo lo relacionado en el proceso de desarrollo de este proyecto y junto con la recolección de información se logró el objetivo principal de esta investigación, crear un método de cifrado moderno enfocado a un archivo digital, un audio mediante una aplicación de audio para su creación y desarrollo.

En este proyecto se informa sobre el uso de la codificación de la información enfocada al audio (esteganografía), las metodologías y métodos que se utilizan en la codificación mediante los medios digitales y los métodos enfocados a textos planos para poder conocer más a fondo el tema conociendo los métodos que existen, su funcionamiento y mecanismos de cifrar información, con el objetivo de grabar voz (mensaje) y ocultarla introduciendo alguna señal de ruido. Después quitar la señal de ruido para escuchar el mensaje, haciendo una nueva codificación utilizando las fuentes digitales que para este caso un audio y una señal de ruido, para muchos es algo incómodo escuchar y para ese caso algo benéfico ocultar la información.

La base teórica, sirvió para tener más en claro el cómo crear un método de cifrado de información, así como los elementos necesarios que tiene que cumplir para ser un método de encriptación. En primera instancia también la teoría fue de gran apoyo realizar el análisis de datos reuniendo las características y elementos que se tomaron en cuenta para la teoría e implementación, reuniendo cada una de las propiedades para su desarrollo, dándole así sus características y clasificación para este nuevo método de cifrado de información en un audio.

Al pasar, a la parte de implementación de este método de cifrado, se fue analizando y verificando para llegar al objetivo principal, crear un método de cifrado de información, mediante el cifrado y descifrado de la información. Para esto la clave de desarrollo para la implementación del método fue la aplicación de edición de audio. Se mencionó en primera instancia que se utilizaría la aplicación **AudaCity**

mostrada en la figura 4.1.1.Al ir realizando los pasos del algoritmo, se vio la necesidad de cambiar la aplicación de forma inmediata, por las siguientes cuestiones;

- La aplicación estaba limitada al manejo de frecuencias de onda.
- Debido a que era un software libre y gratuito algunas cosas se realizaban de forma básica y limitada.
- La información que generaba por un archivo de audio, gráficamente hablando, las ondas de frecuencia se mostraban muy básicas y por este motivo no se podía manipular de manera correcta las ondas de frecuencia.
- Debido a esto no se estaba llegando ni a un 70% de avance práctico de desarrollo del algoritmo, con esta aplicación se pudo crear el criptograma. Pero no de manera óptima para después descifrar la información debido a su forma básica y limitada de manejo de frecuencia de onda de un audio.
- Para reducir el ruido solo lo hace de manera general, es decir toda una trama del audio, al practicar esto involucraba todo el audio, por ende, afectaba la información que no se pretendía afectar como la grabación de voz esto ocasiono que al querer descifrar la información en procedimiento fuera un total fracaso.

Figura 4.1.1 Aplicación de edición de audio AudaCity, aplicación gratuita que permite hacer ediciones de audio.

Aplicación de edición de audio AudaCity, aplicación gratuita que permite hacer ediciones de audio básicas como unir dos audios, mejorar su calidad, manipular las señales de onda de forma básica. Es una aplicación buena pero para este proyecto no sirvió.

Al ir analizando las características que tenía que cubrir la aplicación adecuada para el proyecto, se encontró la aplicación de audio **Adobe Audition CC** tomando la versión más actual **2014,** esta aplicación ya no fue software libre como la mencionada anteriormente, esta ya es de licencia, pero al ser de licencia las opciones de edición de audio son más completas y no son tan limitadas en todos los sentidos, la información de ondas de frecuencias que se muestran de un archivo de audio son más complejas y completas como la gráfica de información se puede visualizar en Db decibelios y Hz mostrando más información relevante de ruido y detalles generados por las información de ondas de frecuencias tal como se muestra en la figura 4.1.2.

Figura 4.1.2 Aplicación de edición de audio **Adobe Audition CC 2014.**

Así es como la aplicación muestra gráficamente la información generada por un audio en formato mp3. Se puede apreciar que en la gráfica de la parte superior muestra la gráfica general de información de ondas formada por un audio mp3 en Db y en la parte inferior se muestra a más detalle en Hz, la información formada por dicho audio la cual sirvió de más utilidad para el desarrollo práctico del proyecto.

Además de proporcionar más información relevante de las onda de frecuencias generadas por un audio, las opciones de edición son las completas en cuestiones de quitar ondas de frecuencias generadas por ruido, puesto que se puede hacer de manera manual trama por trama o general todo el audio por

completo como se mencionó en el capítulo 3. También se pudo manipular mediante selección de recuadro una parte de cualquier lugar de la gráfica de ondas y pegarla en un lugar destino que uno deseara, lo cual en la aplicación AudaCity no lo permitía, estaba demasiada limitada de opciones de edición.

Gracias a la aplicación **Adobe Audition CC 2014,** se logró realizar los pasos de este nuevo algoritmo de cifrado en un audio mediante una señal de ruido, ya que la implementación fue basada en esta aplicación. Logrando verificar el análisis de datos para crear el criptograma, es decir, la información oculta en el audio. Así como después descifrar la información, recuperando satisfactoriamente la información oculta. Viendo como en cada paso del algoritmo las ondas de frecuencias se fueron modificando verificando la calidad del sonido llegando al objetivo de cada paso del algoritmo de cifrado de manera exitosa, esto explicado a gran detalle en el capítulo 3.

4.2 CRIPTOGRAMA GENERADO EN UN AUDIO, CIFRADO DE LA INFORMACION.

Tomando en cuenta la información recolectada de los capítulos 1, 2 y parte del 3 se reunieron las características y elementos para crear este nuevo método de cifrado actual generando un criptograma en una archivo de audio, pero para poder llegar a este paso fue necesario el análisis y recolección de datos que conlleva un método de cifrado, reuniendo sus propios elementos y describiendo cada uno de ellos, la clasificación que tendrá este método de encriptación generando su propia base teórica. Después se generó la base teórica y la implementación del método.

La implementación fue generada mediante la aplicación de audio **Adobe Audition CC 2014,** gracias a la completa información que proporcionó como las ondas de frecuencias generadas por un archivo de audio, y las opciones avanzadas para poder manipular y editar un audio se logró ocultar la información en un audio, creando el algoritmo con sus respetivos pasos para llegar a formar un criptograma en un archivo digital de audio. En la figura 4.2.1 se muestra la información de ondas de frecuencias generadas por el criptograma de este método de cifrado, esta información es parecida para cualquier criptograma de diferente información, solo cambiara la gráfica de la parte inferior dependiendo de la información generada por la ondas de frecuencias de la grabación de voz y fondo musical.

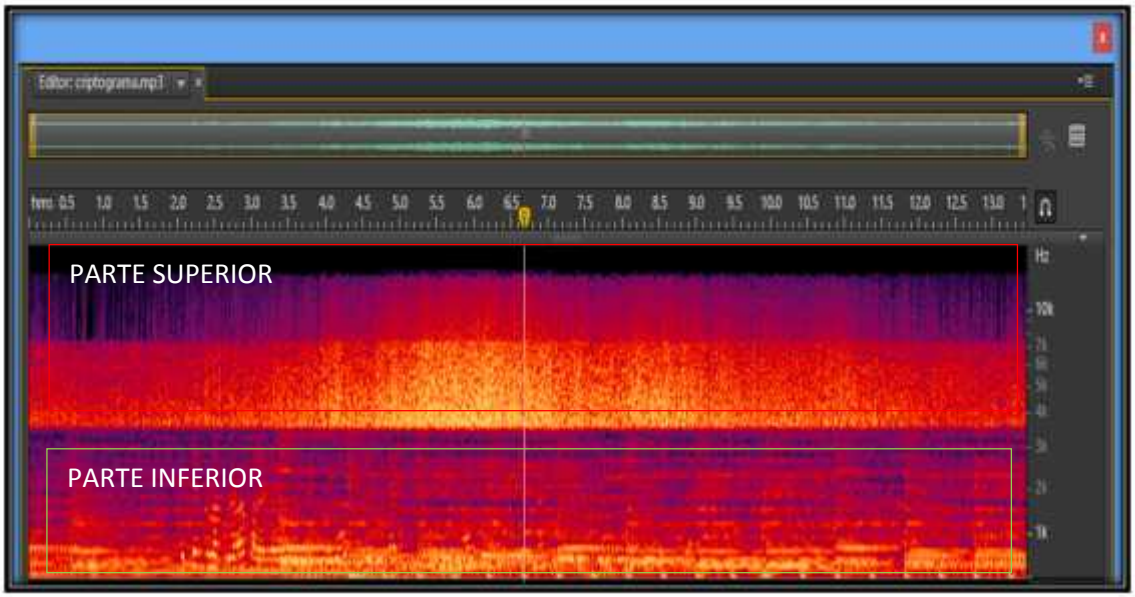

Figura 4.2.1 Ondas de frecuencias generadas por el criptograma.

Como se puede ver la figura la 4.2.1 al realizar los pasos de este método de encriptación el criptograma formado tendrá una información de ondas parecidas a las que muestra la imagen quedando en la parte superior la información de la clave de encriptación del algoritmo, para este caso la señal de ruido y en la parte inferior la información a cifrar, es decir la grabación de voz.

4.3 DESCIFRADO DE LA INFORMACION EN UN AUDIO, CRIPTOGRAMA.

En cualquier método de cifrado de información enfocado a cualquier archivo sea texto plano o un archivo digital, en este tipo de métodos se oculta la información en un archivo llamado criptograma, pero el algoritmo también debe contar con su respectivo procedimiento para descifrar dicho criptograma, accediendo a la información que fue cifrada en el criptograma. Cualquier método de cifrado cuenta con este procedimiento, para este nuevo método de cifrado digital, se logró de manera exitosa crear los pasos para descifrar la información mencionada a gran detalle en el capítulo 3, quedando como resultado un archivo de audio con una información de frecuencias de ondas menores a las generadas por el criptograma como se muestra en la figura 4.3.1. Teniendo como resultado acceso total a la información oculta, es decir, la grabación de voz.

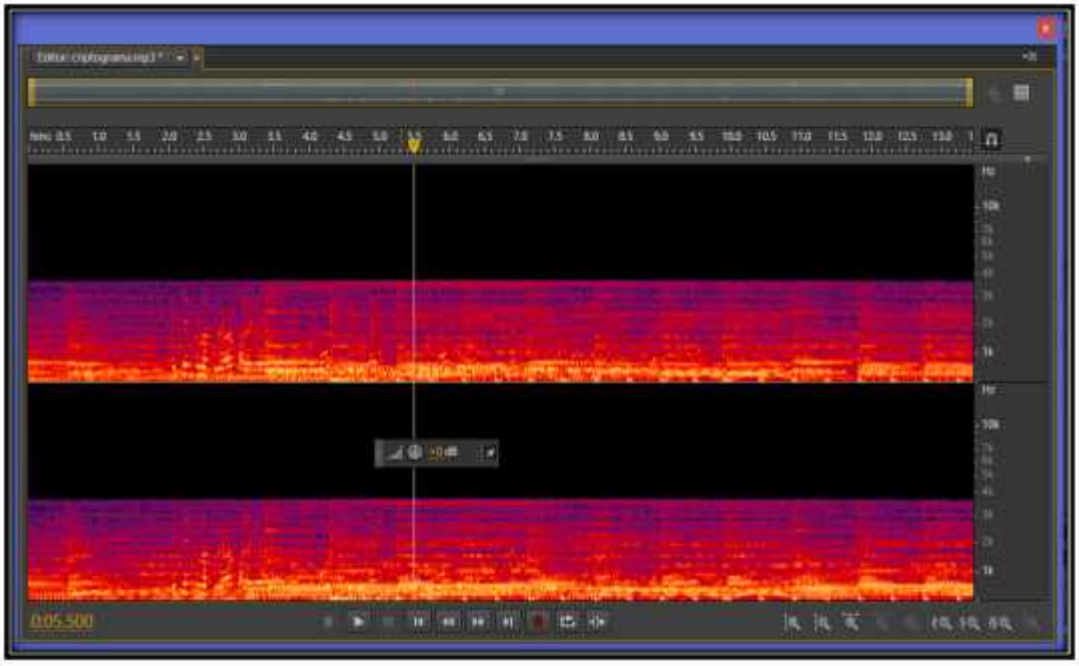

Figura 4.3.1 Ondas de frecuencias generadas al descifrar el criptograma.

4.4 ENFOQUE Y APLICACIÓN DEL PROYECTO.

Este proyecto está enfocado al área de seguridad de redes minimizando la inseguridad de la información que es trasmitida a través del internet y los peligros que se presta al enviar información por este medio, puesto que no es segura la integridad de la información y el uso inapropiado de la misma, aportando una alternativa más para cifrar la información pudiéndola enviar por la red de internet. Si por alguna situación en el canal de envió se pierde la información de manera intencionada o no intencionada, tengan información irrelevante sin importancia, si se pierde o extraen el archivo enviado, solo será un archivo digital sin importancia, no proporcionando la información. Este tipo de métodos de cifrado sirven como alternativa para proteger la información que se envía a través de la red quedando una barrera entre la información que se envía por este medio como se muestra en la figura 4.4.1.

Figura 4.4.1 Un algoritmo de encriptación sirve para poder trasmitir información enmascarada mediante un canal de comunicación.

Gracias a los formatos digitales y a Internet, podemos transferir información de todo tipo a otras personas sin necesidad de realizar envíos físicos. Además, los PCs nos permiten almacenar enormes cantidades de documentos sin que tengamos que preocuparnos por el espacio que ocupan, facilitándonos en gran medida la localización rápida de datos específicos.

Sin embargo, todas estas ventajas poseen, algún inconveniente. En primer lugar, si enviamos documentos que posean una importante clave, puede resultar conveniente hacer conciencia de que efectivamente los remitentes somos nosotros, despejando toda posible duda sobre una suplantación de identidad. Por otra parte, aunque los ficheros confidenciales no vayan a ser enviados a otros usuarios, es importante que aprendamos a protegerlos contra miradas indiscretas.

La aplicación que se le puede dar a este proyecto, es como una opción más de cifrado moderno de información involucrando un archivo digital para su proceso, esto mediante organizaciones de 2 o más personas que busquen alternativas para poder enviar la información y muchas veces han sido atacados mediante la red por intrusos intentando acceder a su información envidada por algún dispositivo de almacenamiento de información conectado a internet. En la figura 4.4.2 se hace una ilustración de como un hacker intenta robar la información que se envía a través de un dispositivo conectado a la red.

Figura 4.4.2 Robo de información a través de internet, de manera hackeada o perdida de la información mediante el canal de envió mediante internet.

4.5 INNOVACION DEL PROYECTO.

Esta investigación sirvió para crear un método de encriptación generando su propia teoría, recordando que para su implementación, se involucró una aplicación de audio, para manipular las ondas de frecuencias de un archivo digital de audio mp3. Mediante esta aplicación se realiza ediciones de frecuencias de ondas, tomando como clave de encriptación ondas de frecuencias de ruido.

Si bien ya se realizó cada uno de los procedimientos necesarios para realizar este nuevo metodo de encriptación, una innovación a futuro podría ser la creación de un sistema computacional introduciendo el algoritmo para poder procesar archivos de audios. El sistema fuera capaz de realizar el cifrado de manera automática y no manual como se hace en esta investigación.

Pensando en el desarrollo del sistema computacional capaz de cifrar la información en un archivo digital, la idea para el sistema seria que contara con las siguientes opciones, para trabajar con archivos digitales en formato mp3:

- El sistema tendrá la capacidad de grabar la voz, recordando que esta es la información que se va a cifrar.
- Dar opciones de fondo musical para la construcción del criptograma, o seleccionar algún fondo deseado.
- El ruido quedaría fijo, generado por el tráfico de la ciudad, teniendo la opción de poder subirle volumen, para que tape la grabación de voz.

- Una vez teniendo estos tres archivos listos dentro del sistema, tendrá una opción de cifrar, involucrando el metodo que se creó en este proyecto, el sistema será capaz de cifrar la información de manera automática.
- Una vez que se tenga el criptograma, poder cargar el archivo de audio y con una opción de descifrar, poder acceder a la información cifrada de manera automática, tomando en cuenta el procedimiento creado por esta investigación. En la figura 4.5.1 se muestra un bosquejo de la estructura que tendría que desarrollar para este sistema computacional criptográfico.

Figura 4.5.1 Idea mediante el bosquejo para el sistema de cifrado de información mediante este nuevo método de cifrado moderna para archivos de audio en formato mp3.

4.6 VIABILIDAD, IMPACTO ECONÓMICO, SOCIAL Y/O TECNOLÓGICO DEL PROYECTO.

Hoy en día el uso de la red y de la gran cantidad de dispositivos que se pueden conectar a internet, beneficia en gran cantidad al acceso de información tanto para el almacenamiento e intercambio de información entre estos dispositivos, así como el crecimiento de servicios públicos que ocupan este medio para realizar trámites como; pagos bancarios, ventas en línea, procesos de registro, o simplemente utilizan la conexión de red para comunicarse por alguna plataforma de chat en donde constantemente se intercambia información y en ocasiones la información que se almacena y se envía puede ser de suma importancia que si por alguna razón cae en manos equivocadas puede tener consecuencias graves dañando la integridad de los datos personales, promoviendo a realizar fraudes, a robar créditos de información, usurpación de identidad, entre otras situaciones en donde se puedan robar la información por la red perjudicando de manera maliciosa. Debido a estos acontecimientos de robo y accesos no autorizados de información, se crearon métodos de cifrado de información para poder combatir la inseguridad que existe en la red, ocultando la información mediante un proceso de cifrado y descifrado para la protección de la información que se intercambia por la red, asegurando que solo las personas que conozcan el de método cifrado que se está utilizando y lo sepan aplicar puedan acceder a la información de manera satisfactoria, de no ser así solo tendrán información que no se entiende, en caso de robo o pérdida de la información que se está enviando. Referente a esto se han tomado medidas para la seguridad en la red mediante métodos de cifrado que ayudan a minimizar riesgos en la información.

Las necesidades de la seguridad de la información en una organización han sufrido dos cambios fundamentales en las últimas décadas. Antes de la expansión del uso del equipamiento de procesamiento de datos, la seguridad de la información que una organización consideraba valiosa se proporcionaba, por un lado por medios físicos, como el uso de armarios con cierre de seguridad para almacenar documentos confidenciales y, por otro, medios administrativos, como los medios de protección de datos personales que se usan en el proceso de contratación.

El segundo cambio que afecto la seguridad fue la introducción de sistemas distribuidos y el uso de redes y herramientas de comunicación para transportar datos de un dispositivo y el computador. Las medidas de seguridad de la red son necesarias para proteger la información durante la trasmisión. De hecho el término de seguridad de red, es engañoso, en cierto modo, ya que prácticamente todas las empresas, las instituciones gubernamentales y académicas no solo en el estado de Puebla, sino que en cualquier parte del mundo cada días es más el uso de sistemas utilizados para los procesos de recolección de datos para generar algún evento en donde se involucre el envió de información mediante la red. Formando un grupo de redes conectadas para la comunicación e intercambio de información.

Para justificar lo mencionado anteriormente se explicara mediante sencillos ejemplos de comunicación entre dos usuarios que utilizan la red, como medio de comunicación e intercambio de información, la mayoría de las empresas de Puebla optan por utilizar, introducir equipos de cómputo y dispositivos inteligentes para establecer intercambio de información para algún proceso administrativo de trabajo donde la inseguridad de la red que pone en riesgo la información donde por ejemplo:

- Un usuario A envía archivo al usuario B. El archivo contiene información confidencial que se debe proteger (datos personales, registros de nómina, números de cuenta, claves interbancarias, etc.). El usuario C no está autorizado a leer el archivo, observara la transmisión y capturara una copia del archivo durante la trasmisión Ø Un administrador de red, D, trasmite un mensaje a un computador o dispositivo, E, que se encuentra bajo su gestión. El mensaje ordena al computador E que actualice un fichero de autorización para incluir las identidades de nuevos usuarios a los que se va proporcionar acceso A.
- Un empleado es despedido sin previo aviso. El jefe de personal envía un mensaje a un sistema servidor de red para validar la cuenta del empleado. Cuando la invalidación se lleva a cabo, el servidor ha de notificar la confirmación de la acción del archivo del empleado. El empleado intercepta el mensaje y lo rastrea el tiempo suficiente para un último acceso al servidor y recuperarlo, así, información confidencial. A continuación, se envía el mensaje, se lleva a cabo la acción y se notifica la confirmación. La acción del

empleado puede pasar inadvertida durante un periodo de tiempo considerable.

- Un cliente envía un mensaje a un corredor de bolsa con instrucciones para realizar diferentes transacciones. Más tarde, las inversiones pierden valor y el cliente niega haber mandado ese mensaje.

Estos son algunos ejemplos de violación de información, que ocurren en dispositivos que están interconectados en la red, habiendo más que estos mencionados.

Cada día es más común encontrarnos que las empresa Poblanas trasforman y actualizan sus procesos administrativos y de servicios en sistemas computacionales que tienen la necesidad de estar conectados en la red, involucrando dispositivos y computadoras para llevar a cabo dichos procesos en donde se intercambia la información que quizá antes se tenía en papel, ahora ya todo se está convirtiendo en información digital, y la información cada vez más se envía más por este medio que es la red de internet, pero en el trascurso de traslado la información se puede perder de manera intencionada o no intencionada, si esto pasa la información puede ser eliminada y/o actualizada.

En el desarrollo de un mecanismo, un método de cifrado particular siempre deben tener en cuenta los posibles ataques a esas características de seguridad. Después de diseñar los mecanismos de seguridad, es necesario decir donde usarlos, tanto que respecta a la ubicación física para este caso sería en el internet, enfocado a que la información que se envía a través de este medio, se transporte de manera cifrada hasta que llegue al receptor, minimizando el riesgo de los ataques pasivo o activos en el trascurso del traslado de la información, y si existiera un ataque mediante el cifrado digital de la información no tenga vulnerabilidades de acceso de información.

Los Gobiernos, entidades militares, instituciones financieras, los hospitales y las empresas privadas acumulan una gran cantidad de información confidencial sobre sus empleados, clientes, productos, investigación y su situación financiera. La mayor parte de esta información es recolectada, tratada, almacenada y puesta a la disposición de sus usuarios, en computadoras y trasmitida a través de las redes entre los ordenadores.

En caso de que la información confidencial de una empresa, sus clientes, sus decisiones, su estado financiero o nueva línea de productos caigan en manos de un competidor; se vuelva pública de forma no autorizada, podría ser causa de la pérdida de credibilidad de los clientes, pérdida de negocios, demandas legales o incluso la quiebra de la misma. Por lo que proteger la información confidencial es un requisito del negocio, y en muchos casos también un imperativo ético y una obligación legal. Para el individuo común, la Seguridad de la Información tiene un efecto significativo respecto a su privacidad, la que puede cobrar distintas dimensiones dependiendo de la cultura del mismo. El campo de la Seguridad de la Información ha crecido y evolucionado considerablemente en los últimos años. Convirtiéndose en una carrera acreditada a nivel mundial. La misma ofrece muchas áreas de especialización, incluidos la auditoría de sistemas de información, Planificación de la continuidad del negocio, Ciencia Forense Digital y Administración de Sistemas de Gestión de Seguridad por nombrar algunos.

La Seguridad Informática es un concepto de Seguridad que nació en la época en la que no existían las redes de banda ancha, los teléfonos móviles o los servicios de internet como las redes sociales o las tiendas virtuales. Es por ello que la Seguridad Informática suele hacer un especial énfasis en proteger los sistemas, es decir, los ordenadores, las redes y el resto de infraestructuras de nuestra organización. La Seguridad Informática es un concepto fundamentalmente técnico. El problema del enfoque de la Seguridad Informática es que suele perder de vista otros aspectos importantes para una organización y, en la mayoría de las ocasiones, cuando nos hablan de Seguridad Informática nos parece algo completamente alejado de nuestra actividad diaria.

La nueva tendencia respecto de la implementación de gran cantidad de dispositivos móviles y redes inalámbricas como parte de la nueva infraestructura tecnológica, también ha requerido que los profesionales en seguridad, ajusten nuevamente sus procedimientos y desarrollen un conjunto de técnicas y controles capaces de velar por la seguridad de la información con ellos relacionada.

La seguridad informática mediante la esteganografía y el cifrado de la información, métodos alternativos para minimizar los riesgos e intenta proteger el almacenamiento, procesamiento y transmisión de información digital. La navegación por la web del vendedor puede ser una conexión no cifrada, pero cuando se utiliza el carrito debemos pasar a servidor seguro.

Las infracciones de seguridad afectan a las organizaciones de diversas formas. Con frecuencia, tienen los resultados siguientes:

- Pérdida de beneficios.
- Perjuicio de la reputación de la organización.
- Pérdida o compromiso de la seguridad de los datos.
- Interrupción de los procesos empresariales.
- Deterioro de la confianza del cliente.
- Deterioro de la confianza del inversor.

Las infracciones de seguridad tienen efectos de gran repercusión. Cuando existe una debilidad en la seguridad, ya sea real o sólo una percepción, la organización debe emprender acciones inmediatas para garantizar su eliminación y que los daños queden restringidos. Muchas organizaciones tienen ahora servicios expuestos a los clientes, como los sitios Web. Los clientes pueden ser los primeros en observar el resultado de un ataque. Por lo tanto, es esencial que la parte de una compañía que se expone al cliente sea lo más segura posible. Para minimizar y evitar acceso y robo de información no autorizados hay que involucrar los mecanismos del cifrado de información en nuestros mecanismos de intercambio de información en la red de internet y esta investigación se puede tomar como opción más de cifrado moderno.

El impacto económico y tecnológico es prevenir la inseguridad de la información que se envía por algún medio de red. Este medio de comunicación es utilizado por diferentes factores sociales como; la distancia, ocupaciones profesionales, trabajo, etc. Es decir, que por alguna razón no se pueden comunicar de manera personal y la comunicación se tiene que realizar mediante la red, involucrando él envió de datos importantes como números de cuentas, números telefónicos, direcciones, datos personales, claves de seguridad, información confidencial, en fin muchas cosas de suma importancia, si esa información llega por error a personas no autorizadas podría ocasionar problemas graves. Cuando se trata de envió de información en la red, es importante saber que la información que se envía por este medio, no es segura ya que se puede perder, robar o incluso manipular por terceras personas. Hoy por hoy tiene más poder quien más información controla, por lo que permite que los ciudadanos empleen técnicas de cifrado para proteger su intimidad limitada de forma efectiva. No cabe duda que la información se está convirtiendo en la mayor fuente de poder que ha conocido la humanidad, y la codificación de la información se ha convertido en una herramienta esencial para su control.

Es necesario que los ciudadanos de pies a cabeza conozcan sus ventajas e inconvenientes, sus peligros y leyendas que existen al enviar la información mediante la red. Se aportara al desarrollo tecnológico con la creación de un método más de encriptación ya no clásico, sino un método moderno involucrando un medio digital para su proceso de codificación, beneficiando a toda persona que quiera establecer seguridad en la información que envía día a día en este medio tan grande como lo es la red y sus aplicaciones derivadas. Tomando como una opción más para cifrar la información en un archivo digital para este caso un audio y se pueda tomar como una alternativa más para le cifrado de la información.

4.7 OPINION Y REACCION DE USARIOS QUE UTILIZAN ALGUN TIPO DE DISPOSITIVO CONECTADO A INTERNET Y SE LES ENVIA EL CRIPTOGRAMA EN UN AUDIO.

Se realizaron pruebas diciéndoles a algunos destinatarios que se le iba a enviar una información de suma importancia y esa información les llegaría mediante un audio. Se logró observar la reacción al escuchar la información cifrada en dicho audio, es decir el criptograma. Las reacciones y comentarios de la mayoría fueron las siguientes:

- Me llego un audio mal solo es puro ruido, lo eliminare y envíame la información
- Tuve que eliminar la información que me enviaste solo se escucha audio con ruido.
- Al parecer la información esta se dañada solo se oye ruido, no se escucha nada de información.
- No entendí nada se oye ruido.

CAPÍTULO V:

CONCLUSIONES

Este proyecto de tesis, se llevó a cabo mediante una recolección de datos que sirvieron para formar bases teóricas de los métodos de encriptación y esteganográficos que han sido revelados de manera pública dando a conocer sus mecanismo de funcionamiento, aportando con esto desarrollar nuevos métodos de cifrado modernos en donde ya no se involucran archivos de texto plano, sino involucrando archivos digitales para su procesamiento y tratamiento de la información. Mediante esta investigación realizada se logró de manera exitosa todos los objetivos para la creación de un nuevo método de cifrado en un audio, tomando una señal de ruido digital.

Se concluye que todo este proceso de investigación sirvió para cumplir los objetivos generales y específicos del proyecto de investigación de manera exitosa, dichos objetivos fueron;

Objetivos generales:

- ✓ Se logró de manera satisfactoria ocultar información en un audio mediante una señal de ruido
- ✓ Al enviar el criptograma formado por un audio, se envió mediante el canal de red de internet, y se logró pasar desapercibida la información sin sospechas de contenido de información relevante.
- ✓ Se recolectó información de los métodos de encriptación clásicos que son de exposición abierta al público, informando teóricamente como funciona cada uno de estos métodos de cifrado, para ir involucrándonos con el tema y entender a más detalles los conceptos de cifrado enfocados a textos planos.

Objetivos específicos

- ✓ Se investigó la aplicación de audio, la cual manipula de manera apropiada las señales de ondas de frecuencias, mediante la edición de un audio. Esta aplicación sirvió para realizar la implementación del método de cifrado en un archivo digital.
- ✓ Se logró mediante la aplicación de audio, eliminar el ruido de una grabación de manera satisfactoria.

- ✓ Se generó la teoría reuniendo las características y propiedades de este nuevo método de cifrado de la información moderno en un archivo digital, un audio.

Al tener la base teórica y práctica se cumplen con las propiedades y características que tiene que cumplir cualquier método de cifrado de información, con esto se establece un método de cifrado de manera exitosa.

Mediante este tipo de proyectos también se busca fomentar con más investigaciones donde se solucionen con algún método de cifrado la inseguridad que existe al enviar información mediante la red, puesto que en intercambio de información y el almacenamiento que existe en los dispositivos conectados a internet no es segura, mientras que la información llega a su destino, esa información en el trayecto se puede perder, la pueden robar o manipular terceras personas y estas personas pueden ocasionar problemas si la información involucra datos personales importantes. Para este y otro tipo de problemas existen los métodos de cifrado de información, para minimizar los riesgos de la información que se envía en la red de internet.

BIBLIOGRAFIA

[1] Douglas C. Giancoli, (*Física para ciencias e ingenierías con física moderna*), Cuarta edición, Prentice hall ,978-607-442-303-7
[2]Paul G. hewitt, (*Conceptos de física*), Novena edición, Limusa, 968-18-4180-8.
[3]Federico Pacheco (Criptografía) ,1ra edición, Red Users, 978-1949-35-9.
[4]Ariel Maiorano (CRIPTOGRAFÍA Técnicas de desarrollo para profesionales), 1ra edición, AlfaOmega, 978-987-23113-8-4.
[5] Sánchez Rinza Barbara E., Morales Salgado Maria del R., Cortez Olguin Cristian O., Avances de investigación aplicada en ciencias de la computación, "Security system for sending information containing hidden voice data by steganography (siove) using matlab". ISBN 22773754.
[6] Sánchez Rinza Barbara E., Cano C. M., Avances de investigación aplicada en ciencias de la computación, "Steganography algorithm marb of carriers on charts". ISBN 9786074871234.
[7] Pino C. Gil, "Seguridad informática. Técnicas criptográficas.", Primera edición. Editorial Alfaomega, México, 1997. ISBN 970-15-0328-7.
[8] Gómez V. Álvaro, "Enciclopedia de la Seguridad Informática", Primera edición, Editorial Alfaomega, México, 2007. ISBN 978-970-15-1266-1.
[9] Olanrewaju R.F., Khalifa O., Abdul R. H., "Increasing the Hiding Capacity of Low-Bit Encoding Audio Steganography Using a Novel embedding Technique", World Applied Sciences Journal 21., 2013, ISSN: 1818-4952.
[10] Johnson N. F., Jajodia S., "Exploring Steganography: Seeing the Unseen", 1998.
[11] William Stalling (Fundamentos de redes de seguridad Aplicaciones y Estanadares), Segunda edición, Editorial Pearson Prentice hall, Madrid, 2004.ISBN 84-205-4002-1.
[12] José Fabián Roa Buendía (Seguridad Informática), Primera edición, Editorial McGraw-Hill, Madrid, 2013. ISBN 978-84-481-8569-5.
[13]https://senaintro.blackboard.com/bbcswebdav/institution/semillas/228101_2_VIRTUAL/OAAPs/OAAP4/aa2/oa4/manual_audition.pdf
[14]https://creative.adobe.com/es/products/audition
[15]http://www.monografias.com/trabajos93/contaminacion-ambiental-ruido-salud-y-bioetica/contaminacion-ambiental-ruido-salud-y-bioetica.shtml#ixzz3QjBXKHbL
[16]http://ocw.innova.uned.es/mm2/tm/contenidos/pdf/tema3/tmm_tema3_sonido_digital_presentacion.pdf
[17]http://webquery.ujmd.edu.sv/siab/bvirtual/BIBLIOTECA%20VIRTUAL/TESIS/03/CMN/ADCP0001180.pdf