SISTEMA CRIPTOGRÁFICO RSA PARA AUDIO.

Juan Felipe Rojas Cendales
Victor Alfredo Barragán Paez

Presentado a: Oswaldo Rojas Camacho

Teoría de la información y las telecomunicaciones

Universidad Nacional de Colombia
Facultad de Ingeniería, Departamento de ingeniería de sistemas e industrial
Bogotá, Colombia
2022

Indíce

1. Datos generales

1.1. Asignatura

Teoría de la información y las telecomunicaciones.

1.2. Docente de la asignatura

Oswaldo Rojas Camacho.

1.3. Título del proyecto

Sistema criptográfico RSA para audio.

1.4. Áreas a las que pertenece al proyecto

Telecomunicaciones, Sonido y Audio Digital, criptografía.

1.5. Autores del proyecto

Victor Alfredo Barragán Paez y Juan Felipe Rojas Cendales.

1.6. Fecha de presentación del proyecto

Lunes 21 de Noviembre de 2022.

2. Descripción general del proyecto

2.1. Resumen teórico

La criptografía es el uso de técnicas matemáticas con el fin de proteger y brindar seguridad a cualquier tipo de información que se desee transmitir., entre los algoritmos de criptografía moderna se encuentra RSA, un sistema de llave pública y privada para asegurar la transmisión de información entre dos entidades. En las telecomunicaciones, la información transmitida y manejada va desde textos, imágenes, audios, entre otros, estos tipos de información pueden digitalizarse para su manejo y representación computacional. Este proyecto desarrolla un sistema criptográfico en MATLAB basado en el algoritmo criptográfico de llave pública y llave privada RSA, para simular la comunicación entre dos entidades, manejar la información transmitida de manera digital y realizar encriptación o desencriptación de archivos de audio que se deseen transmitir dos entidades.

2.2. Planteamiento del problema

En una comunicación vía audio entre dos entidades se requiere utilizar el algoritmo de llave pública y llave privada RSA para cifrar y descifrar de manera segura la comunicación. La transmisión de audio que realizan aplicaciones de mensajería como Whatsapp o Telegram es una pieza fundamental en el funcionamiento de las aplicaciones y cotidiana en el uso de sus usuarios, por tanto, la información debe ser asegurada con el fin de protegerla y que esta sea reproducible solamente por el receptor deseado. Para esto es necesario garantizar la confidencialidad, usabilidad y disponibilidad del sistema criptográfico en general, también, es necesario implementar el algoritmo RSA desde la generación de llaves para ambas entidades en la comunicación hasta las funciones de cifrado y descifrado respectivas. Por último, en cuanto a la comunicación, es necesario manejar los archivos de audio y representarlos como señales y posteriormente vectores para realizar los procedimientos criptográficos.

2.3. Marco teórico

2.3.1. Telecomunicaciones

Las telecomunicaciones son los procesos de comunicación donde se transmiten y reciben cualquier tipo de información como textos, imágenes, sonidos en forma de señales utilizando medios tecnológicos que soportan el procesamiento de señales.

Las telecomunicaciones son a día de hoy parte vital de la infraestructura global en el proceso de transmisión de información, globalización, transmisión del

conocimiento y sociedad informática, dispositivos como los teléfonos móviles, televisiones, sensores son algunos ejemplos de aplicaciones en el campo de las telecomunicaciones que hacen parte del día común en la vida de las personas.

2.3.2. Audio

El audio es la representación de los sonidos en señales, es una señal eléctrica analógica (analógica al igual que la luz o el sonido) generada por el electromagnetismo y que oscila entre los 20 Hz y los 20000 Hz en donde puede ser percibida por la escucha humana.
A nivel práctico, es sencillo ejemplificar el sonido y audio con los micrófonos, en donde estos dispositivos reciben ondas sonoras que se transportan por el aire y que producen un movimiento en un diafragma generando así una señal eléctrica denominada audio que puede ser reproducible de manera inversa en el medio.

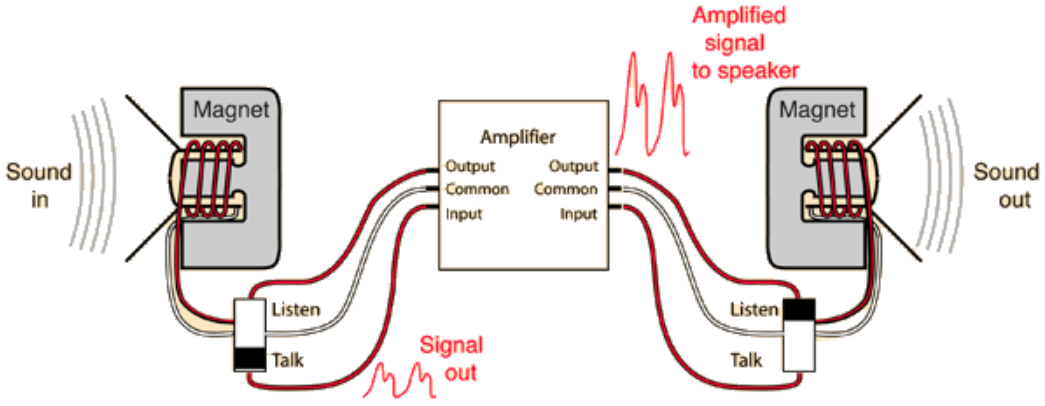

Figura 1: Funcionamiento de un micrófono.
Tomada de: http://hyperphysics.phy-astr.gsu.edu/hbase/Audio/mic.html

2.3.3. Digitalización de audio

La digitalización de audio es en esencia el proceso de convertir señales analógicas a digitales. Para este proceso, el conversor analógico/digital realiza dos operaciones en esencia: el muestreo de la señal y la cuantificación de la señal.
El muestreo de la señal analógica es el proceso que toma valores de la señal cada cierto intervalo de tiempo, este intervalo de tiempo está determinado por la frecuencia de muestreo que toma cierta cantidad de muestras para un segundo de la señal o en este caso un segundo de grabación de sonido.
No se debe confundir la frecuencia del audio mencionada anteriormente (entre 20 Hz y 20000 Hz) con frecuencias de muestreo que pueden llegar a ser hasta de 44100 Hz en los CD's. Entre más alta sea la frecuencia de muestreo más alta será la fidelidad y calidad de la digitalización con respecto al audio/sonido original.

Sin embargo, puede que una frecuencia de muestreo inadecuada produzca el aliasing, generando frecuencias falsas y un alteración del resultado más similar al original. Para lo anterior, es necesario tener en cuenta el teorema de Nyquist, donde: $f_m = 2 * f$. Es por este teorema que se tiene una estándar en los 44100 Hz como frecuencia de muestreo ya que son el doble de las frecuencias que son percibidas por la escucha humana.
La voz humana está en una frecuencia entre los 500 Hz y 3500 Hz por lo cual no es necesaria una frecuencia de muestreo superior a los 800 Hz para realizar procedimientos con este tipo de audios.

Posteriormente, se realiza un proceso de cuantificación de la señal en donde a las muestras obtenidas anteriormente se les mide el voltaje que corresponde a la amplitud de la muestra en cada instante y se les asigna un valor numérico discreto por aproximación, el concepto de digital. Con estos nuevos valores es posible transformar a sistema binario según un bitrate, en donde cada muestra irá representada en 16 bits según el estándar. Este proceso como es de imaginarse termina produciendo un error de cuantificación o ruido por el proceso de codificación y discretización.

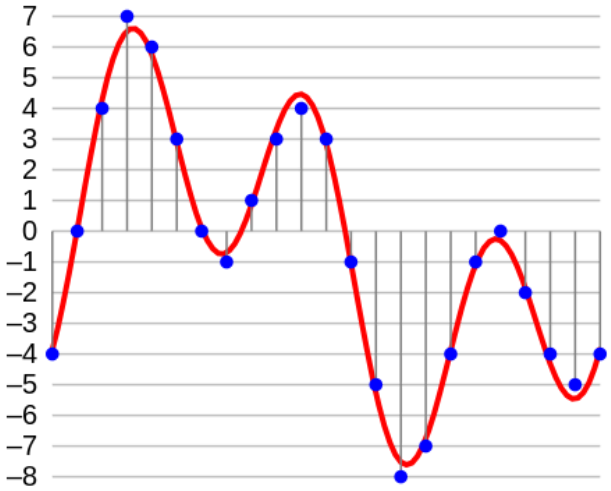

Figura 2: Muestreo y cuantificación de un sonido.
Tomada de: https://alexisound.com/sonido-digital/

Finalmente, es el codéc (codificador/decodificador) presente en el software que realizó estas operaciones el que permite determinar y manejar el tipo de almacenamiento de los datos. Almacenamientos como WAV o MP3 se diferencian por la compresión y el tamaño del archivo generado en donde los archivos WAV tienen una mayor calidad y por tanto mayor tamaño en bytes.

2.3.4. Criptografía

La criptografía es la disciplina que utiliza las matemáticas para el desarrollo de técnicas que se apliquen a la información y garanticen su seguridad. En cuanto a conceptos, la criptografía puede verse como el proceso de comunicación con adversarios presentes, siendo esto una batalla entre un code-master que cifra y un code-destroyer que descifra.
La criptografía es en esencia las actividades que se realizan para codificar o cifrar la información y asegurarla, esta rama hace parte de la criptología que combina estas actividades junto con las actividades de decodificación o desciframiento denominadas criptoanálisis.
Los objetivos prácticos de un sistema criptográfico aplicado a la comunicación de dos entidades son:

- Confidencialidad.
- Integridad.
- Autenticación.
- Disponibilidad.
- No repudio.

Según el principio de Kerckhoffs, es necesario que los sistemas criptográficos dependen de una llave/clave y no del sistema en sí mismo, es por lo anterior que las llaves en los sistemas criptográficos son una pieza fundamental y en ellas recae toda la integridad del sistema. Por tanto, el desarrollo histórico de algoritmos y sistemas criptográficos ha sido enfocado hacia el concepto de llave y cómo puede sacarse un mayor provecho a esta condición.

2.3.5. Sistemas criptográficos de llave pública/privada

Los sistemas criptográficos de llave pública y llave privada son un tipo de sistemas en la criptografía moderna que utilizan dos llaves por entidad para las actividades de cifrado y desciframiento. Estos sistemas poseen las siguientes características:

- Generación de dos llaves por entidad en la comunicación.
- La llave de desciframiento se mantiene privada.
- La llave de ciframiento se pública para el uso de la otra parte en la comunicación.
- Las llaves pública y privada comparten una relación matemática.
- Debe ser inviable el cálculo computacional de una llave privada conociendo solamente la llave pública, en esto recae la integridad del sistema.

Es sencillo comprender estos tipos de sistemas con una analogía a los sistemas postales antiguos. Alice y Bob desean intercambiar mensajes y para esto utilizan una caja en una oficina postal, Alice y Bob cuentan cada uno con una llave y un candado, la llave será privada y los candados son públicos. Cuando Alice desea dejarle un mensaje en la caja a Box, deja el mensaje en la caja, toma un candado público y cierra la caja. Posteriormente, Bob llega a la caja y la abre con su llave privada.

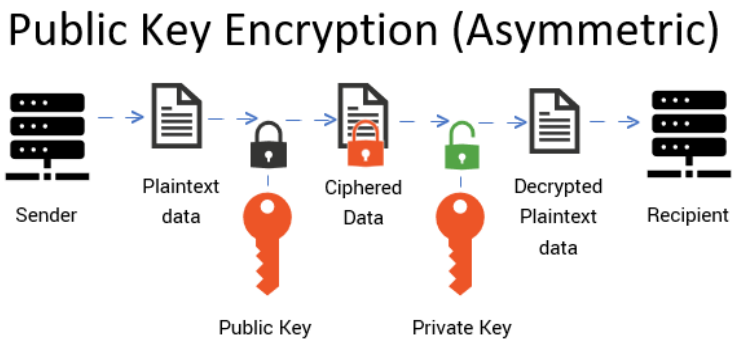

Figura 3: Sistemas criptográficos de llave pública/privada.
Tomada de:
https://cheapsslsecurity.com/p/what-is-public-key-and-private-key-cryptography-and-how-does-it-work/

2.3.6. RSA

El algoritmo criptográfico de llave pública y privada RSA surgió en 1977 y lleva ese nombre por las iniciales de sus creadores (Ronald, Adi y Leonard), la patente se volvió pública en el año 2000.
RSA mantiene su integridad en la incapacidad computacional actual de calcular las llaves privadas a partir de las públicas, un problema de factorización de enteros. La fase previa de RSA es la generación de las llaves para cada entidad, para esto es necesario seguir el siguiente algoritmo:

1. Generar dos primos grandes de manera pseudoaleatoria.
2. Computar la multiplicación de los primos y la multiplicación de los primos menos uno.
3. Seleccionar un entero pseudoaleatorio entre 1 y la multiplicación de los primos menos uno como la llave pública.

4. Computar la llave privada como el inverso multiplicativo modular de la llave pública y la multiplicación de los primos menos uno.
5. Publicar la llave pública y guardar la llave privada.

Las actividades de ciframiento y desciframiento utilizan las llaves, el mensaje o la información, la multiplicación de los primos y la función de exponenciación modular para generar el resultado.

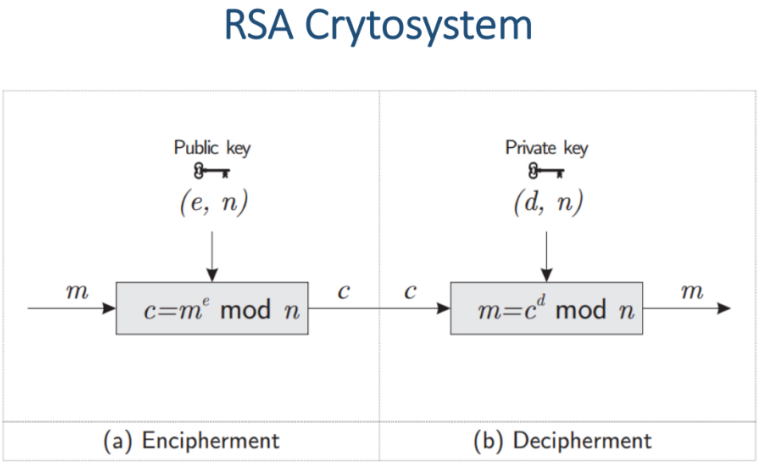

Figura 4: RSA.
Tomada de: [4]

2.4. Objetivo general

El desarrollo de este proyecto pertenece al objetivo general de las telecomunicaciones y la criptografía, desarrollar un sistema capaz de realizar la transmisión (simulada) de la información, el procesamiento de señales y la utilización de técnicas matemáticas y algoritmos criptográficos para garantizar la seguridad de la información.

2.4. Objetivo específico

El desarrollo de este proyecto tiene como objetivo específico realizar en MATLAB una transmisión (simulada) de audio digitalizado utilizando un criptosistema de llave pública/privada RSA para cifrar y descifrar el contenido del audio generando la respectiva graficación y reproducción de la señal y su contenido durante los procesos de digitalización y criptografía que realice el sistema.

3. Desarrollo del proyecto

3.1. Dibujo esquemático del proyecto

Se presentan los diagramas de flujo para las funciones utilizadas durante los procesos principales de emisión, criptografía y recepción de audio:

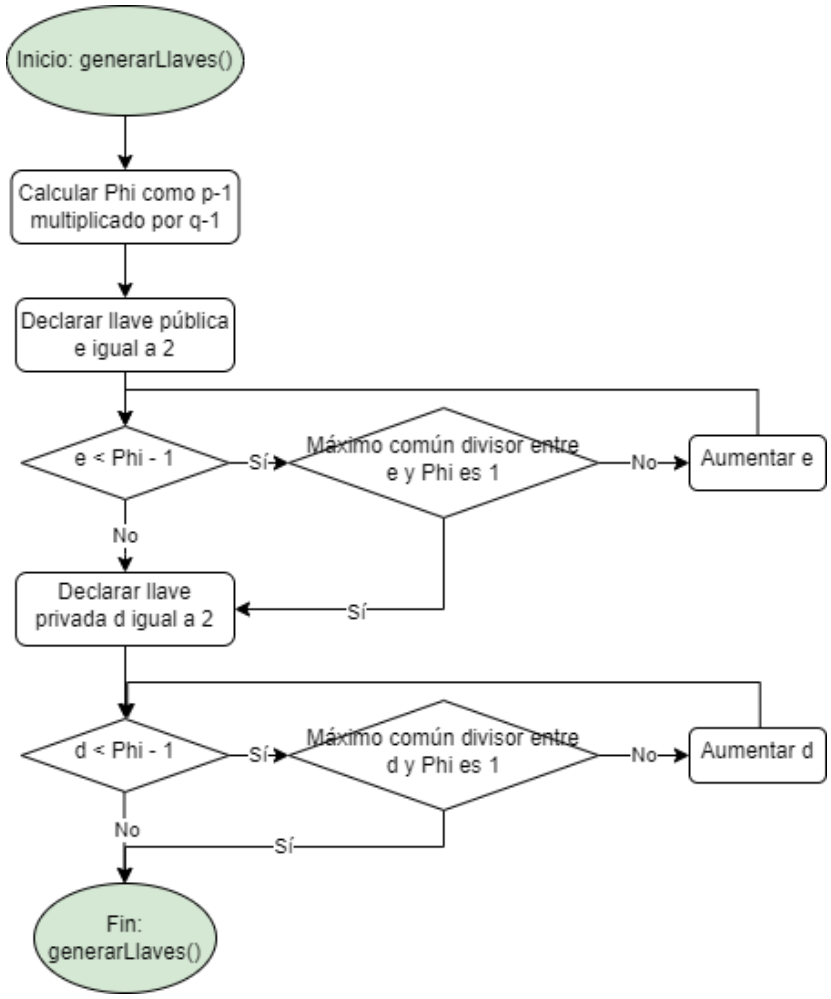

Figura 5: Diagrama de Flujo para la función generar llaves.

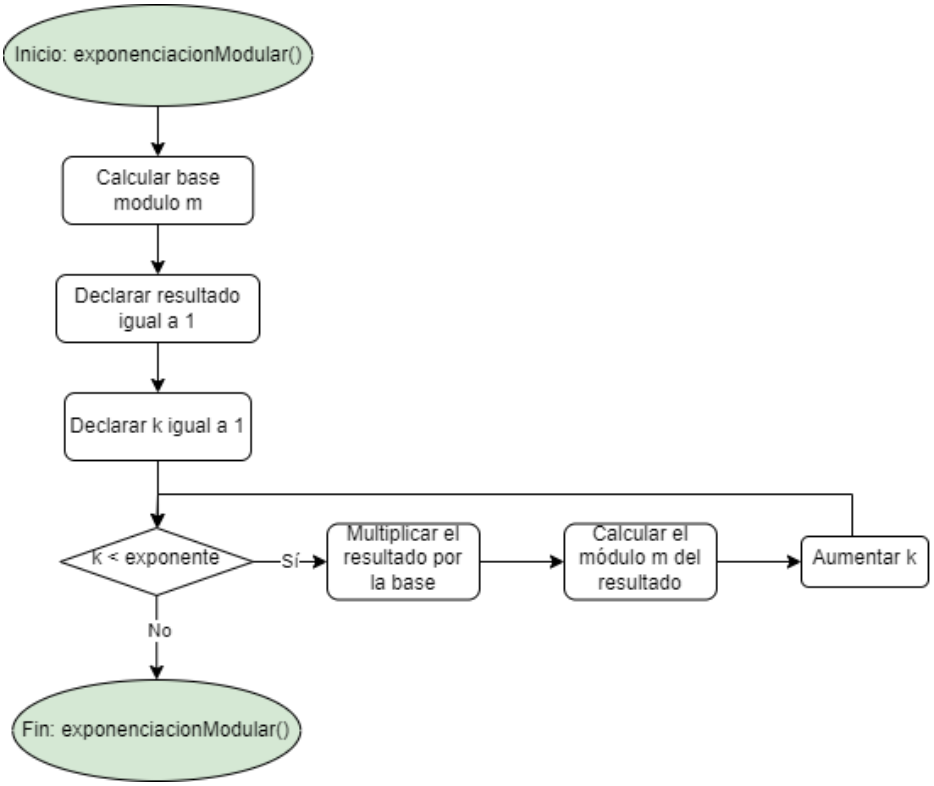

Figura 6: Diagrama de Flujo para la función exponenciación modular.

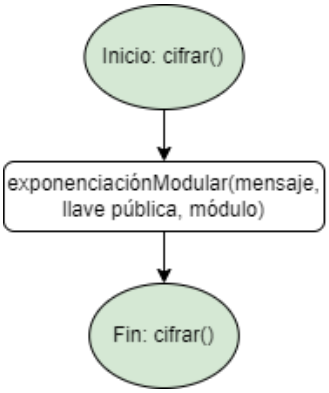

Figura 7: Diagrama de Flujo para la función cifrar.

Figura 8: Diagrama de Flujo para la función descifrar.

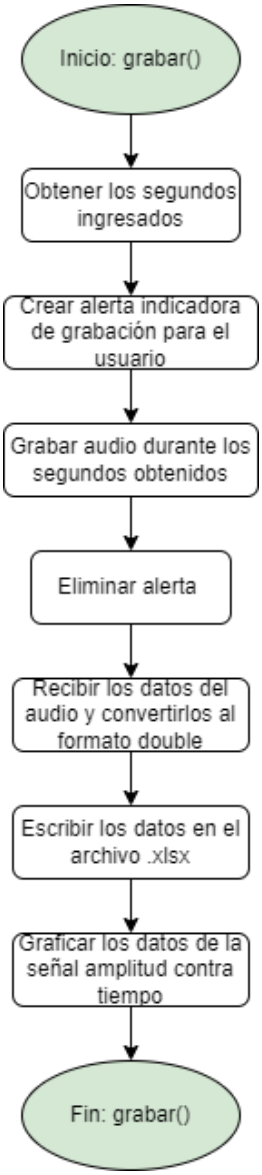

Figura 9: Diagrama de Flujo para la función grabar.

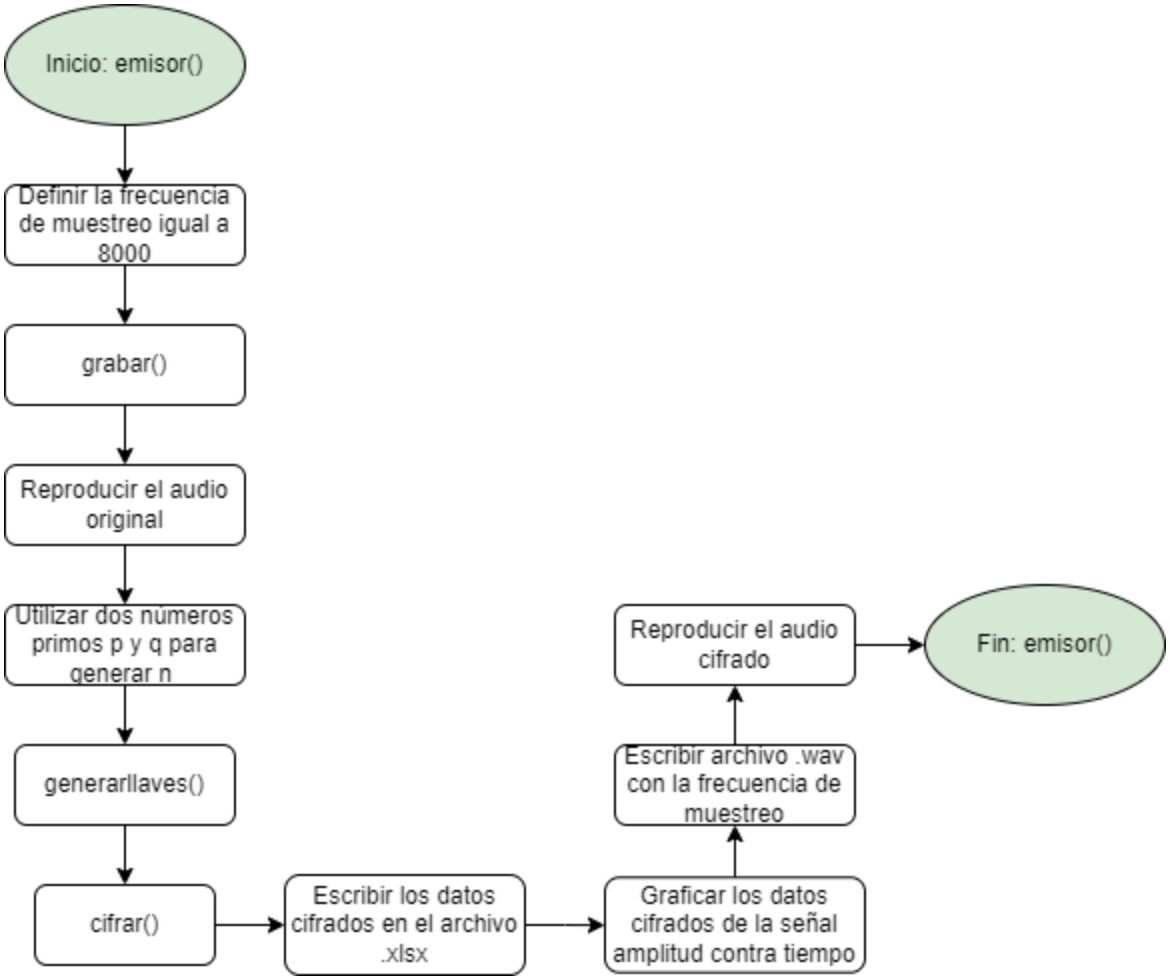

Figura 10: Diagrama de Flujo para la función emisor.

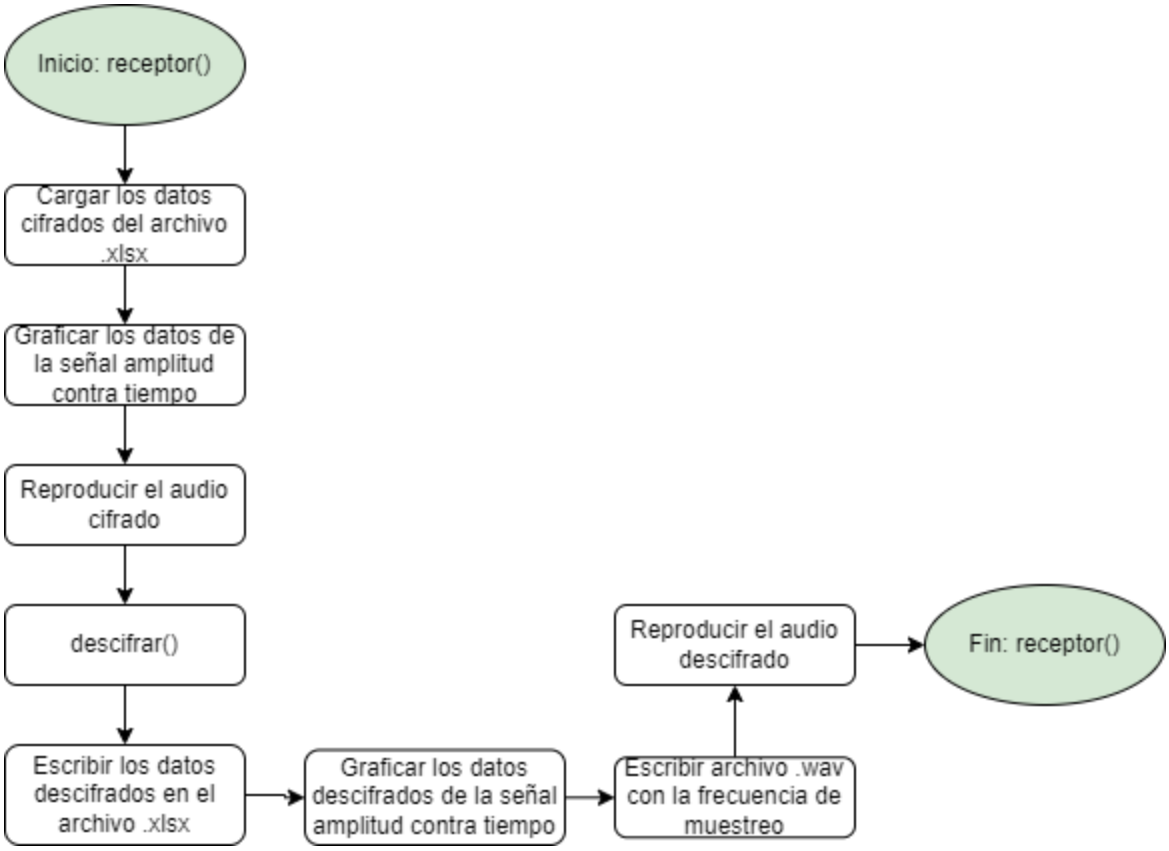

Figura 11: Diagrama de Flujo para la función receptor.

3.2. Material utilizado

3.2.1. MATLAB

MATLAB [6] es una plataforma de programación para el desarrollo de sistemas de cómputo con aplicaciones en análisis de datos, procesamiento de señales, robótica, algoritmia, aprendizaje de máquina, entre otros. MATLAB cuenta con un lenguaje de programación propio, IDE de escritorio u online y está supervisado por la multinacional MathWorks.
El IDE de MATLAB para escritorio fue utilizado durante el desarrollo del proyecto, al igual que la totalidad del código fuente, incluyendo funciones de criptografía, programa principal e interfaz gráfica, está desarrollado en el lenguaje de programación MATLAB.

3.2.2. RSA Notebook

En el material utilizado también se utilizó un Notebook del lenguaje Python con la implementación de RSA con fines de aprendizaje y académicos [7]. Este

notebook funcionó como un apoyo y soporte ante la implementación de RSA en un lenguaje de programación diferente. Este Notebook fue desarrollado previamente por los mismos integrantes de este proyecto como un proyecto propio bajo la temática y el curso de Matemáticas Discretas.

3.3. Descripción de la implementación

El sistema criptográfico desarrollado cuenta con una interfaz gráfica principal que permite al usuario la grabación de voz, procesos de criptografía sobre los audios, reproducción de los audios y graficación de señales. El primer módulo de la aplicación corresponde al emisor y la encriptación en donde es posible realizar las siguientes acciones:

- Grabación de voz según un número de segundos definido por el usuario.
- Graficar la señal original.
- Reproducir el audio de la grabación original.
- Encriptar los datos del audio.
- Graficar la señal encriptada
- Reproducir el audio obtenido al encriptar la grabación original.

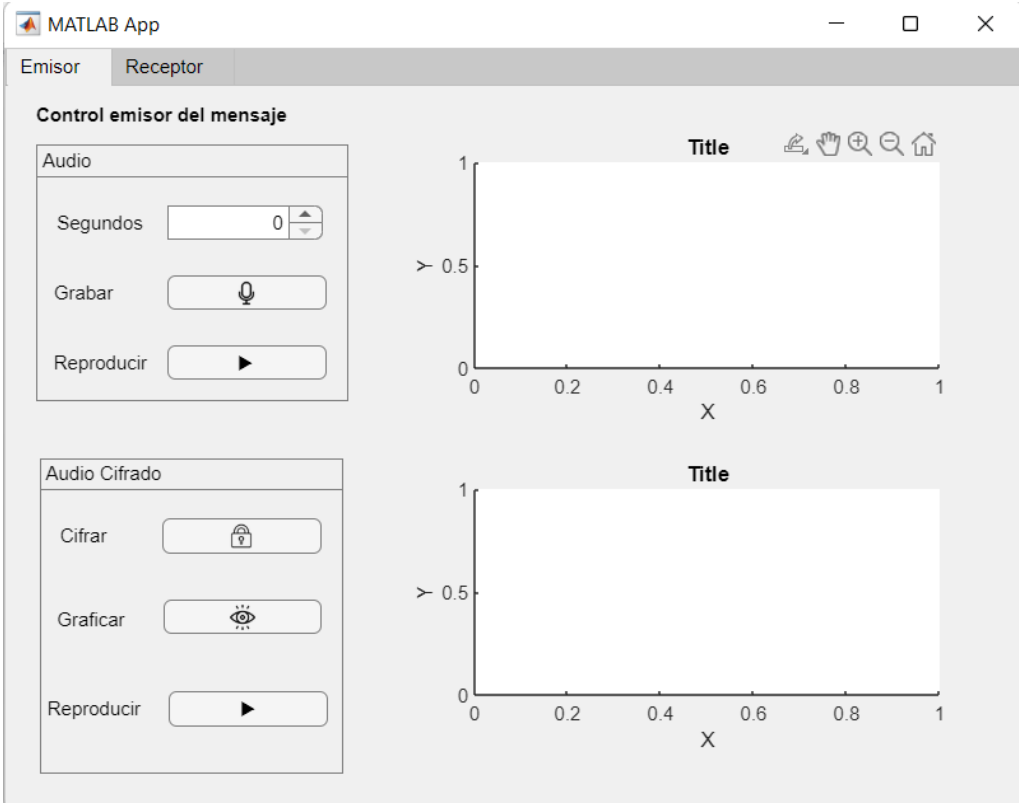

Figura 12: Interfaz gráfica del módulo emisor/encriptar.

El segundo y último módulo corresponde al receptor y la desencriptación en donde es posible realizar las siguientes acciones:

- Cargar el archivo .xlsx con los datos de la grabación encriptada.
- Graficar la señal encriptada.
- Reproducir el audio encriptado.
- Desencriptar los datos del audio encriptado.
- Graficar la señal original reconstruida.
- Reproducir el audio original obtenido al desencriptar la grabación cargada.

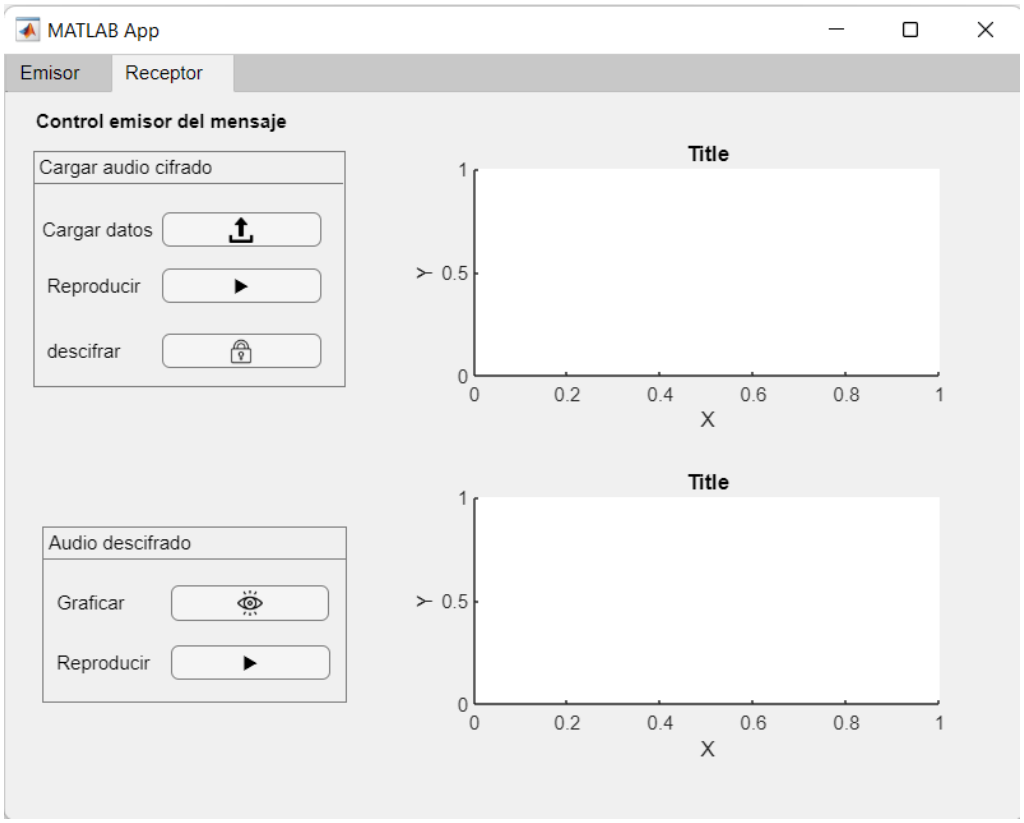

Figura 13: Interfaz gráfica del módulo receptor/desencriptar.

.

La interfaz gráfica utiliza de fondo las funciones presentadas anteriormente para el algoritmo RSA en los diagramas de flujos. También, los flujos de emisor y receptor se encuentran distribuidos entre los distintos botones y acciones que tiene y realiza la interfaz gráfica.

4. Análisis de resultados y conclusiones

4.1. Resultados obtenidos

Los resultados obtenidos fueron un sistema de grabación de audio pensado para la grabación de voz humana, adaptable a un número de segundos definido por el usuario, intuitivo y amigable con el usuario durante el proceso. Además, la graficación de la señal generada a partir de la grabación y muestreada como se presenta en la siguiente gráfica:

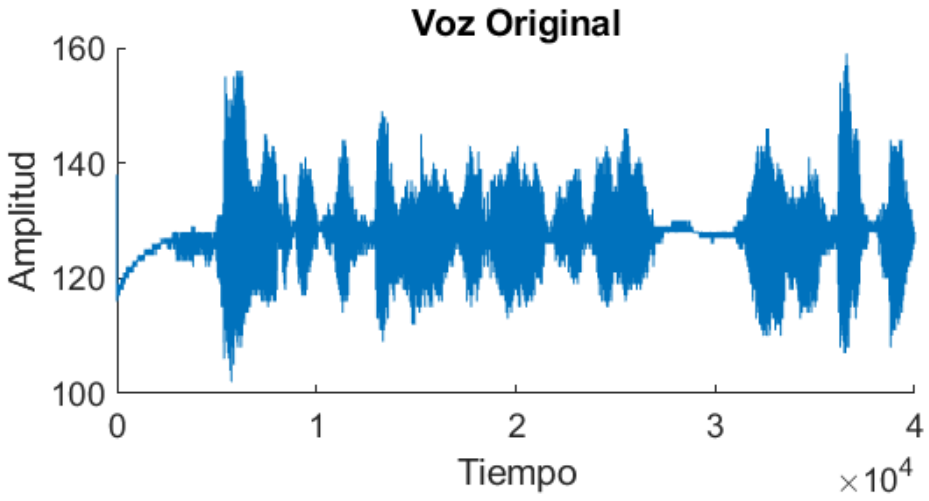

Figura 14: Gráfica de la voz original muestreada.

Durante el proceso de encriptación se generaron dos llaves para el receptor, una pública y una privada ejemplificando el proceso que realiza RSA para la generación de llaves. También, se cifraron los datos de la señal original obteniendo una nueva señal cifrada como se presenta en la siguiente gráfica:

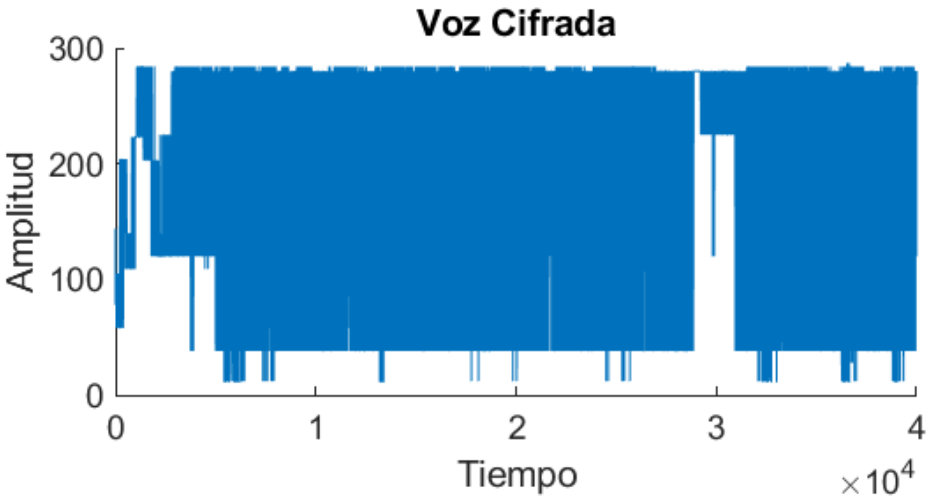

Figura 15: Gráfica de la voz cifrada.

Finalmente, el proceso de desencriptación utiliza la llave privada para descifrar los datos cargados de la señal cifrada obteniendo una reconstrucción de la voz original como se presenta en la siguiente gráfica:

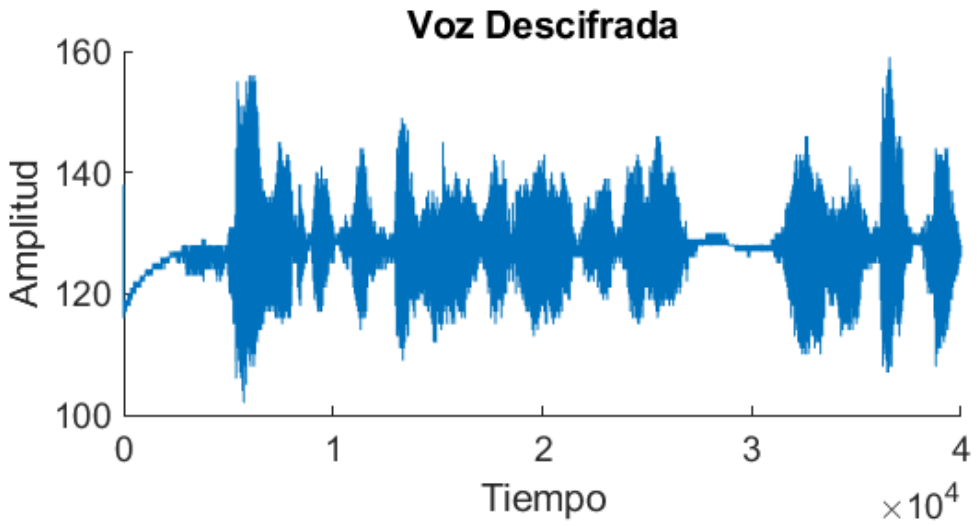

Figura 15: Gráfica de la voz original descifrada.

Entre otros resultados obtenidos que no pueden ser presentados en este documento se encuentran la reproducción de la grabación, voz encriptada y voz reconstruida descifrada.

4.2. Conclusiones

Como conclusión general, el desarrollo de este proyecto nos enfrentó a la profundidad de desarrollos existentes en los campos de las telecomunicaciones, la teoría de la información y la seguridad de la misma. La simulación de un proceso relativamente poco sofisticado como la digitalización del audio y la seguridad de los datos demostró ser un proceso complejo que requiere conocimientos muy teóricos en los diferentes campos como el teorema de Nyquist o la aritmética modular. MATLAB nos permitió realizar una interfaz gráfica clave para el desarrollo del flujo en nuestro proceso de transmisión y un código fuente sólido y bien estructurado capaz de realizar los procesos de criptografía, graficación, grabación, entre otros. El proyecto tenía como objetivo general el garantizar la seguridad del audio transmitido y en los resultados obtenidos encontramos que fue posible realizar el sistema criptográfico que nos garantizara este requerimiento.
Como conclusiones específicas en el desarrollo del proyecto encontramos:

- En el proceso de digitalización de audio, la definición de una frecuencia de muestreo apropiada es clave para conseguir resultados coherentes y evitar el

aliasing. El teorema de Nyquist tiene como finalidad determinar esa frecuencia de muestreo apropiada dada la frecuencia de la señal continua original.

- RSA, aunque sus aplicaciones sean más que todo académicas, nos permite desarrollar un sistema criptográfico fácil de comprender y confiable en donde la seguridad recaerá sobre las llaves, cumpliendo con el principio de Kerckhoffs.
- MATLAB nos permite realizar diversas aplicaciones en su lenguaje de programación y complementarlas con interfaces gráficas sencillas de diseñar y adaptar a códigos fuentes modulares.

4.3. Aprendizaje

El aprendizaje generado por este proyecto no solo ha dejado conceptos teóricos reforzados en cuanto a las telecomunicaciones y el algoritmo criptográfico RSA, sino también, sobre la programación práctica y digitalización de los mismos. MATLAB demostró ser confiable y poderoso para el desarrollo de cualquier tipo de proyectos, RSA demostró ser un algoritmo criptográfico sencillo y confiable para fines académicos y la digitalización de sonido a pesar de ser un campo ampliamente estudiado, es sin duda alguna un campo donde se pueden identificar trabajos futuros con respecto al hardware actual, personalización, omnipresencia, inteligencia artificial, entre otros.

5. Bibliografía

[1] Colaboradores de Wikipedia. (2022, 25 octubre). *Telecomunicación*. Wikipedia, la enciclopedia libre. https://es.wikipedia.org/wiki/Telecomunicaci%C3%B3n

[2] Creus, M. (2021, 24 agosto). *Digitalización de sonido: de analógico a digital*. Comograbar.com. https://www.comograbar.com/digitalizacion-de-sonido/

[3] La digitalización del sonido. (2017, 25 enero). Musicalecer. Creación, edición y producción musical. https://musicalecer.com/el-sonido-digital/la-digitalizacion-del-sonido/

[4] Part 1 Introduction. (2022). En Camargo Mendoza, J.E, Introducción a la criptografía y la seguridad de la información. Universidad Nacional de Colombia.

[5] Part 6 Public Key Cryptosystems. (2022). En Camargo Mendoza, J.E, Introducción a la criptografía y la seguridad de la información. Universidad Nacional de Colombia.

[6] MATLAB - El lenguaje del cálculo técnico. (s. f.). MATLAB & Simulink. https://la.mathworks.com/products/matlab.html

[7] GitHub - Feliperojas2601/DM2-RSA-Project: Discrete Maths 2 RSA implementation Project. (2020). GitHub. https://github.com/Feliperojas2601/DM2-RSA-Project

6. Anexos

Se entregan como anexos a este documento el código fuente del software realizado en MATLAB, los diseños de la aplicación en diagramas de flujo como un archivo XML, una presentación general del proyecto y un video demostración del funcionamiento del mismo.