Criptografía y seguridad informática

Análisis de la Máquina Enigma

Gianmarco Cafferata: 99423
Julián Ferres:
Uriel Kelman: 99616

2do. Cuatrimestre de 2020

Facultad de Ingeniería, Universidad de Buenos Aires

16 de febrero de 2021

Índice

1. Resumen

La Máquina Enigma es una de las herramientas criptográficas más famosas de la historia. Incluso Hollywood ha contado la historia alrededor de ésta famosa máquina, y cómo Alan Turing logró descrifrar su configuración logrando desencriptar los mensajes provenientes de las comunicaciones alemanas durante la Segunda Guerra Mundial. Tomando esto como punto de partida, el objetivo del siguiente informe es el de realizar una descripción completa de la Máquina Enigma, tanto de sus componentes como de su funcionamiento y, a partir de la implementación en código de la misma, obtener métricas acerca de lo que cuesta desencriptar un mensaje cifrado, combinando metodologías basadas en la fuerza bruta y en modelos estadísticos del lenguaje.

2. Introducción

La Máquina Enigma consiste básicamente en una herramienta para encriptar y desencriptar mensajes. Fue principalmente utilizada como método de protección de las comunicaciones alemanas en la Segunda Guerra Mundial. Su utilización en la práctica era bastante simple: a partir de un teclado con la distribución alemana QWERTZ, los alemanes tecleaban los mensajes que querían enviar y la máquina producía un criptograma. Luego, estos criptogramas eran enviados en sus comunicaciones, y quien recibía dicha comunicación podía desencriptar el mensaje tecleando caracter a caracter del criptograma en la máquina. A partir de entender cómo funcionan los distintos componentes que constituyen la máquina, se podrán apreciar las particularidades y la garantía de seguridad que ofrecía esta máquina para encriptar y desencriptar mensajes.

2.1. Máquina Enigma

2.1.1. Diseño general

La Máquina Enigma es un dispositivo electromecánico. Esencialmente, está compuesta por un teclado con distribución QWERTZ, un set de lámparas que representan los caracteres del diccionario, una serie de rotores (generalmente tres o cuatro) y un tablero de conexiones (conocido como *Plugboard*). Al presionar un botón del teclado, el caracter presionado es cifrado y el resultado puede ser observado en la lámpara asociada al caracter resultante del proceso. Asimismo, el criptograma puede ser descifrado introduciéndolo en el teclado de una máquina que tenga una configuración idéntica en sus elementos (tablero de conexiones y rotores) que la máquina que realizó el cifrado.

Las siguiente subsecciones se proponen analizar los distintos aspectos y componentes de la máquina.

Figura 1: Máquina enigma con sus componentes.

2.1.2. Flujo de corriente eléctrica

En la siguiente figura se esquematiza cómo es el
flujo de la corriente y el cableado interno dentro de la Máquina Enigma, desde que se presiona el caracter que se quiere codificar hasta que se enciende la luz que representa el caracter cifrado.

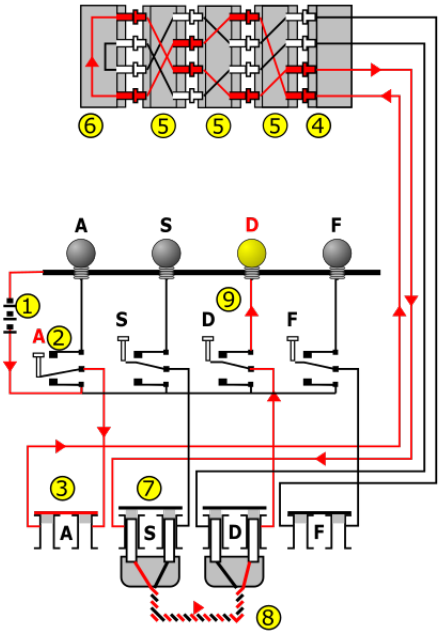


Figura 2: Flujo de corriente de la máquina.

La corriente comienza a fluir desde la batería [1] a través del switch de la tecla presionada [2] hacia el *plugboard*. El *plugboard* permite cambiar un caracter por otro mediante un cableo. Una vez que pasa por el *plugboard*, la corriente se dirige hacia la rueda de entrada [4] a los rotores. Para el caso de la letra A, no se realiza ningún cambio. Luego, atraviesa los rotores [5], y llega a un reflector [6], que refleja la señal para que atraviese nuevamente los rotores y la rueda de entrada, y vuelva al *plugboard*. En este caso, ingresa al tablero de conexiones a través de la entrada para la letra S, pero esta sí está conectada a la letra D a través de un cable [8] por lo que la corriente fluye hacia la lámpara asociada a dicha letra y a través de un switch [9] enciende la lámpara.

2.1.3. Rotor

El rotor es el elemento fundamental de la Máquina Enigma. En sí mismo, un rotor no realiza más que una sustitución de un caracter por otro. Su valor agregado radica en la sustitución realizada es de caracter polialfabético: debido a su rotación constante, una letra puede ser sustituida por varias a medida que se va ingresando en el teclado en mensaje que se desea encriptar.

El rotor consiste básicamente en un disco metálico dentado [9] de aproximadamente 4 pulgadas de diámetro. En su interior, se encuentran 26 conexiones de alambre metálico [5] que conectan la entrada de 26 contactos con resorte [6] del lado derecho a 26 contactos planos en el lado izquierdo [4], estructura que se sostiene mediante un eje hueco [8] que atraviesa el interior. En el exterior se halla un anillo [3] con 26 letras o números y un *notch*, que consiste en una pequeña muesca posicionada en alguna de las letras. Este anillo puede rotar alrededor del disco y se traba en alguna posición mediante un arco con resorte[7]. Un cambio en la posición del anillo generará un cambio en la posición del *notch* y del alfabeto, relativo al cableo interno del rotor (es decir, agregará un $offset$ a la codificación que realice el rotor). La configuración de la posición del anillo es conocida como *Ringstellung* y su posición puede ser apreciada mediante una marca[2]. Por último, cada rotor posee en su sección izquierda al *notch* y en su sección derecha un trinquete[10]. Estos componentes son los que se combinan junto al mecanismo de avance para realizar una rotación.

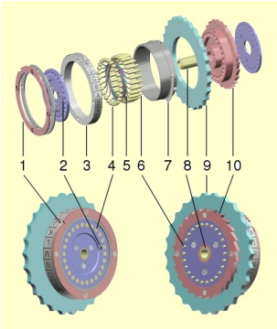


Figura 3: Máquina enigma con sus componentes.

(a) Vista izquierda del rotor con su único *notch*.

(b) Vista derecha del rotor con su trinquete dentado.

Figura 4: Vistas laterales del rotor.

Originalmente, la máquina que utilizaban la Armada y la Fuerza Aérea alemana poseía tres rotores. Luego, en 1938, la cantidad fue extendida a cinco rotores (cada uno con un *notch*, y se les asignaron los números romanos I, II, III, IV, V para distinguirlos. Más tarde, al set se agregaron los rotores VI, VII, VII, cuya particularidad era que tenían dos *notches* cada uno.

El cableo interno del rotor y su rotación son quienes realizan el encriptado. Cada uno de los rotores tiene su propia tabla de cifrado, la cual representa las conexiones que existen entre los pins de entrada en el lado derecho y los pins de salida del lado izquierdo. Por ejemplo, para los primeros cinco rotores, los

cuáles poseen únicamente un *notch*, sus tablas son las siguientes:

```
Entry = ABCDEFGHIJKLMNOPQRSTUVWXYZ
        ||||||||||||||||||||||||||
I     = EKMFLGDQVZNTOWYHXUSPAIBRCJ
II    = AJDKSIRUXBLHWTMCQGZNPYFVOE
III   = BDFHJLCPRTXVZNYEIWGAKMUSQO
IV    = ESOVPZJAYQUIRHXLNFTGKDCMWB
V     = VZBRGITYUPSDNHLXAWMJQOFECK
```

Figura 5: Tabla de cableo interno de rotores I a V.

Es importante tener en cuenta que este *mapping* entre letras no necesariamente (de hecho, rara vez sucederá) significa que una señal para la letra A proveniente del *plugboard* termine codificada como una E (si analizamos el rotor I). El resultado final dependerá además de la posición en la que se encuentre el rotor al momento en el que ingresa la señal (podría ingresar por cualquiera de los pines), además del *Ringstellung* que agregará un $offset$ a la salida.

Para realizar el encriptado de una señal correspondiente a un caracter proveniente del *plugboard*, se sigue el siguiente proceso. Cuando una tecla es presionada, los rotores avanzan antes de que la señal eléctrica los atraviese. A cotinuación, se procederá a ilustrar el proceso de encriptado mediante un ejemplo que utiliza al Rotor I. El anillo se corresponde con las letras encerradas en el campo gris; el cableo interno está encerrado por las dos columnas de letras encerradas en el campo blanco; la posición del rotor está indicada por la letra enmarcada en negro que se encuentra en el anillo exterior; la configuración del anillo o *Ringstellung* se indica con una pequeña marca negra al lado derecho de alguna letra del anillo gris; y por último los alfabetos que se encuentran a la derecha e izquierda del rotor representan los pines de entrada y salida respectivamente. Se considera la siguiente imagen:

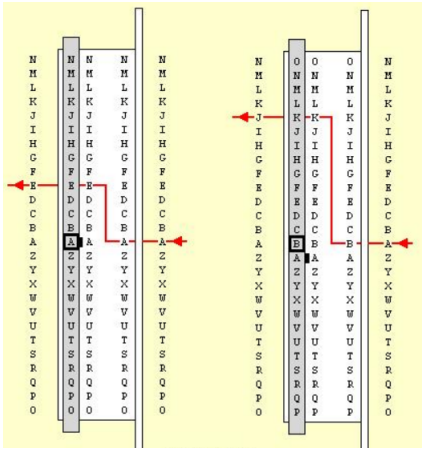


Figura 6: Cifrado seguido de la letra A en el Rotor I.

La imagen de la izquierda muestra como se realiza el cifrado en el Rotor I cuando la letra A se presiona dos veces consecutivas. Nótese que la configuración del anillo del rotor es A-01, y la posición del rotor también es A. La señal de la letra A, proveniente del *plugboard*, arriba a la posición A e ingresa por el pin A, atraviesa el cableado interno pasando de la A a la E, y atraviesa el anillo para terminar saliendo por el pin E. Por su lado, en la imagen de la derecha, el rotor ha avanzado a la posición B. La señal arriba a la posición A, pero ahora ingresa por el pin B para ser redirigida al caracter K. Sin embargo, como todo el rotor ha avanzado una posición, la señal termina saliendo por la posición J hacia el rotor siguiente. Para este ejemplo no se ha tenido en cuenta una configuración del anillo que agregue un $offset$ al cifrado resultante. Consideremos los siguientes dos ejemplos:

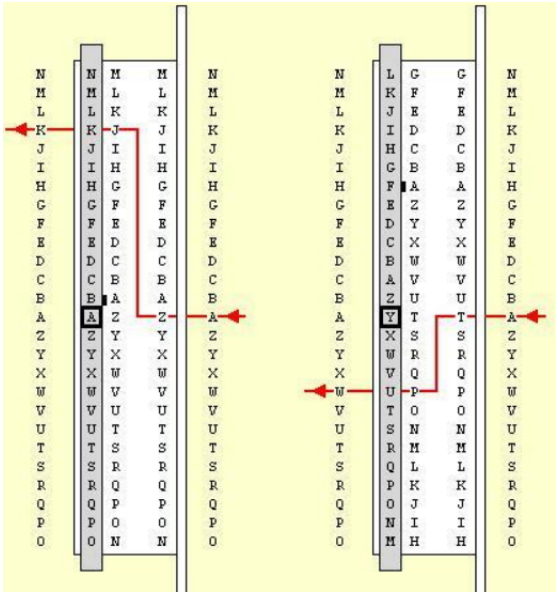


Figura 7: Cifrado de la letra A en el Rotor I con distintos *Ringstellung*.

En la imagen de la izquierda, la configuración del anillo es B-02. Como la posición del rotor es A, parecería ser que al ingresar por la posición A el cableado interno sería A-¿E. Sin embargo, el *Ringstellung* agrega un $offset$ al cableado y la señal ingresa por el pin Z y es redirigida al pin J. A su vez, el pin de salida J no coincide con la posición J ya que este $offset$ también afecta a los contactos de la salida, por lo tanto la señal finaliza saliendo por la posición K hacia el siguiente rotor.

La imagen de la derecha es el caso más complejo a analizar. En este caso, la configuración del anillo es F-06, y la posición del rotor es Y. La tecla presionada es nuevamente la A, y el pin de entrada al centro del rotor resulta ser la posición del rotor desplazada alfabéticamente en seis posiciones, es decir la letra T. Luego, el cableo interno del Rotor I redirige la señal hacia el pin P, que coincide con la posición U del anillo. Finalmente, como nos encontramos en la posición Y del rotor, la señal termina saliendo por la posición W hacia el rotor siguiente. Nótese que la salida está desplazada en siete posiciones alfabéticas: cinco entre

la A y la F por la configuración del anillo, y dos adicionales entre la Y y la A.

2.1.4. Mecanismo de avance

Cada vez que se presiona una tecla, se modifica la posición de al menos uno de los rotores de la máquina. Esto significa que se obtendrán cifrados diferentes cuando se presione la misma tecla en forma consecutiva. Aquí, en parte, radica el poder para encriptar la máquina: existen un número enorme de posibilidades de configuración y posicionamiento de los rotores que generan resultados distintos. El primero de los rotores avanza siempre que se presiona una tecla. El segundo, en cambio, avanza una vez por cada 26 avances del primer rotor, es decir cada 26 teclas presionadas. El tercero, el más lento de todos, avanza una vez por cada avance del segundo rotor, es decir una vez cada 676 teclas presionadas.

Figura 8: Mecanismo de avance de los rotores.

Al presionar una tecla, la barra de avance [1] se moverá hacia abajo y el eje del trinquete [2] y sus tres trinquetes [3] (uno por cada rotor) hacia arriba. Cada uno de estos tres trinquetes, que se mueven al unísono, intentará encastrarse con los dientes que recubren al rotor, para así generar un desplazamiento en el mismo. Por la forma en la que están dispuestos los rotores, solamente se podrá desplzar un rotor si el rotor de su derecha se encuentra en su posición *notch*, ya que en cualquier otro caso el anillo que recubre al *notch* impedirá la combinación entre el trinquete y los dientes del rotor. En el caso del rotor que se encuentra más a la derecha, ante la ausencia de un anillo que le impida accionar sobre los dientes del rotor, el trinquete siempre logrará moverlo y es por esto que el primero de los rotores avanza cada una de las veces que se ingresa una letra.

Con la descripción realizada, podría parecer que el sistema de rotores se comporta como un odómetro. Pero adicionalmente al movimiento producido en el caso en el que el rotor de la derecha se encuentre en la posición *notch*, existe una situación en la que un rotor que no es el de la derecha puede desplazarse dos veces seguidas. Esta situación sucede cuando, en el momento en el que un rotor debe avanzar porque el rotor de su derecha se encuentra en su posición *notch*, este también se encuentra en su posición de *turnover*. En este caso, el rotor avanzará dos veces consecutivas, en vez de esperar por un giro alfabético completo del rotor de su derecha.

2.1.5. Reflector

A diferencia del rotor, en donde una letra puede ser transformada en cualquier otra dependiendo de la posición y la configuración del anillo, el reflector posee conecciones de a pares. Esto significa que si la letra G está cableada a la letra P, entonces P también lo estara por la G. Si bien la tarea del reflector es simple, le agrega un grado de complejidad mayor al encriptado de un mensaje, ya que además de realizar la sustitución asociada al cableado, genera que la señal vuelva a atravesar los rotores por segunda vez en sentido contrario.

Figura 9: Reflector de la Máquina Enigma.

2.1.6. Plugboard

El *plugboard* se encuentra al frente de la máquina. Como se ha analizado previamente, la señal atraviesa el *plugboard* antes de llegar a la entrada del sistema de rotores y set de lámparas. Su función básica es la de realizar una sustitución simple entre letras antes de que la señal llegue al correspondiente destino. Su caracterísitica más importante es que la configuración puede ser modificada por el operador que va a utilizar la máquina, generando así un montón de combinaciones posibles y reforzando la seguridad criptográfica del criptograma final. La sustitución es entre pares: si por ejemplo se conectan las entradas U y J, toda señal que entre por la letra U será cambiada por una J y viceversa.

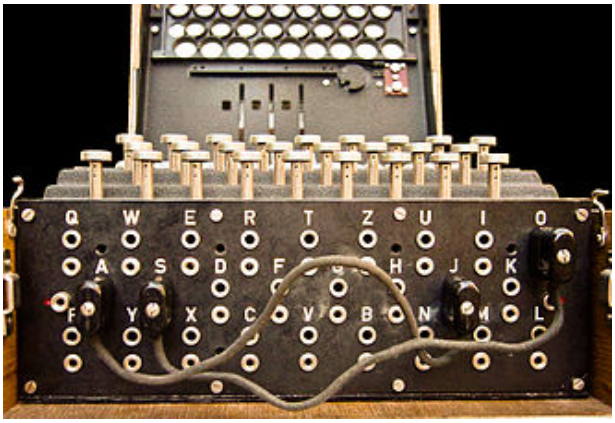


Figura 10: Plugboard de la Máquina Enigma.

2.2. Modelos de lenguaje

2.3. Divergencia de Kullback-Leibler

La divergencia de $Kullback - Leibler$ es una medida de similitud entre dos funciones de distribución probabilística. Siendo P y Q las funciones de distribución probabilística, se puede calcular cómo:

$$D_{KL}(P||Q) = \sum_i P(i) \cdot ln\frac{P(i)}{Q(i)} \tag{1}$$

Algunas propiedades de esta medida son:

- Es siempre positiva.
- Es nula solamente en el caso en el que $P = Q$.
- No es simétrica (no se trata de una medida de distancia).

Acá pensar de explicar un poco cómo aplica en nuestro caso, donde una distribución es el modelo de lenguaje y la otra la obtenida para lo que se desea desencriptar.

La transferencia dada para la realización del trabajo es la número 13. Su fórmula es la siguiente:

$$H_{13}(s) = \frac{s \cdot 207}{s^2 + s \cdot 207 + 4{,}562 \cdot 10^6}$$

La expresión canónica para el denominador de una función de transferencia cualesquiera es:

$$s^2 + \frac{w_0}{Q} + w_0^2$$

Nótese entonces que, a partir de esta expresión, $w_0^2 = 4{,}562 \cdot 10^6$, de lo cual resulta que $w_0 = 2135{,}883892$.

A su vez, conociendo el valor de w_0 es posible obtener Q. De la expresión canónica se sabe que $\frac{w_0}{Q} = 207$, de donde despejando se puede obtener $\frac{w_0}{207} = Q \rightarrow \frac{2135{,}883892}{207} = Q \rightarrow Q = 10{,}31827967$. Como Q es mayor a 0.5, las raíces de la ecuación canónica (que serán los polos de la función de transferencia) serán complejos conjugados.

Determinar los ceros y los polos de la función de transferencia resulta sencillo. Para hallar los ceros, basta hallar el valor para el cual se anula el numerador de la función. Es fácil divisar que el único cero que tenemos es el 0, siendo este un polo simple. Para determinar los polos de la función, debemos analizar cuáles son los valores de s para los cuáles se anula el denominador. Estos valores coinciden con las raíces de la ecuación:

$$s^2 + s \cdot 207 + 4{,}562 \cdot 10^6 = 0$$

de donde resulta que los polos son:

$$s_{1,2} = -103,5 \pm j25103{,}8$$

Para analizar el tipo de filtro, se observan dos aspectos distintos. En primer lugar, se analiza el comportamiento de la función de transferencia haciendo tender s hacia cero y hacia infinito.

$$\lim_{s \to 0} H_{13}(s) = \lim_{s \to 0} \frac{s \cdot 207}{s^2 + s \cdot 207 + 4{,}562 \cdot 10^6} = 0$$

$$\lim_{s \to \infty} H_{13}(s) = \lim_{s \to \infty} \frac{s \cdot 207}{s^2 + s \cdot 207 + 4{,}562 \cdot 10^6} = 0$$

Por otro lado, también es posible observar que la función de transferencia tiene la forma:

$$\frac{h_0 \frac{w_0}{Q} s}{s^2 + \frac{w_0}{Q} s + w_0^2}$$

Donde h_0 vale 1. Debido a la evaluación realizada para los límites de función de transferencia y de que esta tiene la forma nombrada, es posible estimar que el tipo de filtro acorde a la función de transferencia es un filtro de tipo pasabanda.

Por último, podemos responder cuál es la frecuencia f_0. Sabemos que:

$$w_0 = 2 \cdot \pi \cdot f_0$$

de donde sale que $f_0 = \frac{w0}{2 \cdot \pi}$. Para los valores obtenidos:

$$f_0 = \frac{2135{,}883892}{2 \cdot \pi} = 339{,}9364793$$

2.4. Diagramas de Bode de la transferencia

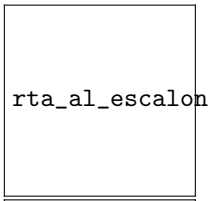
A continuación es posible observar los diagramas de módulo y fase para la transferencia propuesta. Tal como fue descrito en la sección anterior, el diagrama de Bode que se corresponde con la ganancia en dB refleja que la transferencia se corresponde con la de un filtro de tipo pasabanda: la ganancia de la señal crece para un determinado rango de frecuencias, teniendo la ganancia máxima en w_0, y atenuando la señal cuanto más nos alejamos de la frecuencia de corte.

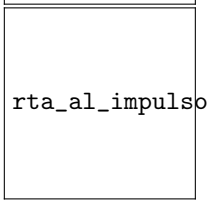
bode_modulo.png

bode_fase.png

2.5. Respuesta al escalón y respuesta al impulso

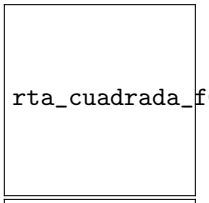
A continuación es posible encontrar la respuesta al escalón y la respuesta al impulso para la transferencia dada. Como se ha dicho previamente, el circuito es de tipo pasabandas, por lo tanto dejará pasar algun rango de frecuencias intermedias cuando se produzca el salto en el escalón. El gráfico de la señal comenzará en 0 ya que el circuito no deja pasar las altas frecuencias, luego dará un salto debido a que pasarán algunas frecuencias intermedias, y finalmente la señal se irá atenuando con el tiempo debido a que el circuito no dejar pasar la señal continua ya que ésta tiene frecuencia nula (no oscila). Esta atenuación será oscilante ya que los polos de la transferencia son complejos conjugados, y debido a que $Q = 10{,}31827967$ habrá aproxidamente una decena oscilaciones hasta que se termine de atenuar la señal por completo.

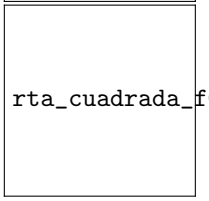




2.6. Respuesta a ondas cuadradas de distintas frecuencias

En esta sección es posible encontrar la respuesta del filtro a distintas ondas cuadradas cuya diferencia es la frecuencia para la cual se producen los flancos ascendentes y descendentes. Una onda cuadrada es una señal periódica y como tal es posible descomponerla en una serie que resulta ser una sumatoria de senos y cosenos que oscilan a distintas frecuencias. Como nuestro filtro es un pasa banda, solamente deja pasar las frecuencias intermedias y por lo tanto las distintas respuestas serán todas oscilantes. Además de esto, sus gráficos varían según la frecuencia elegida. Para un décimo de la frecuencia de corte f_0, se produce un patrón de oscilaciones que se repiten para cada período de la frecuencia de corte original. Para una cuadrada de frecuencia f_0, se produce una oscilación que aumenta su amplitud hasta llegar a un equilibrio, ya que son coincidentes la frecuencia de la onda cuadrada y la frecuencia de corte. Por último, se encuentra el gráfico para una onda cuadrada que multiplica por diez la frecuencia f_0, para la cual podemos ver como en los distintos períodos de la señal cuadrada se producen aumentos y decrementos en la amplitud sucesivamente, logrando así la forma que se encuentra en la tercer figura.





2.7. Búsqueda de un circuito que cumpla con la transferencia

Como se ha determinado anteriormente, la función de transferencia se corresponde con la de un circuito de tipo pasabandas de segundo orden. Un circuito que cumple con este tipo de transferencia es el Infinite Game Multiple Feedback Band-Pass, es decir la versión del IGMF pasabanda. Su configuración es la siguiente:

Ahora, planteando ecuaciones de nodos para el circuito es posible hallar cuál es el valor genérico para la transferencia. Sean V_1 y V_2 las tensiones de entrada y salida respectivamente; sea $H(s) = \frac{V_1}{V_2}$ la función de transferencia que se quiere encontrar; y sean p y q los dos nodos del circuito. Es posible plantear las siguientes ecuaciones de nodos:

$$\frac{V_1}{R_1} + V_2 \cdot s \cdot C_1 = V_p \cdot (\frac{1}{R_1} + \frac{1}{R_2} + s \cdot C_1 + s \cdot C_2) - V_q \cdot s \cdot C_2 \tag{2}$$

$$\frac{V_2}{R_3} = -V_p \cdot s \cdot C_2 + V_q \cdot (s \cdot C2 + \frac{1}{R_3}) \tag{3}$$

Por propiedades de los amplificadores operacionales, sabemos que las tensiones de entrada de ambos debe ser igual. A partir de esta propiedad se deduce que $V_q = 0$, por lo tanto las ecuaciones de nodos son:

$$\frac{V_1}{R_1} + V_2 \cdot s \cdot C_1 = V_p \cdot (\frac{1}{R_1} + \frac{1}{R_2} + s \cdot C_1 + s \cdot C_2) \tag{4}$$

$$\frac{V_2}{R_3} = -V_p \cdot s \cdot C_2 \tag{5}$$

De la ecuación cuatro es posible despejar V_p obteniendo:

$$V_p = -\frac{V_2}{s \cdot R_3 \cdot C_2} \tag{6}$$

Reemplazando el valor obtenido de V_p en (5) dentro de (3):

$$\frac{V_1}{R_1} + V_2 \cdot s \cdot C_1 = -\frac{V_2}{s \cdot R_3 \cdot C_2} \cdot (\frac{1}{R_1} + \frac{1}{R_2} + s \cdot C_1 + s \cdot C_2) \tag{7}$$

De donde distribuyendo el denominador del valor reemplazado se obtiene:

$$\frac{V_1}{R_1} + V_2 \cdot s \cdot C_1 = -V_2 \cdot (\frac{1}{s \cdot R_1 \cdot R_3 \cdot C_2} + \frac{1}{s \cdot R_2 \cdot R_3 \cdot C_2} + \frac{C_1}{R_3 \cdot C_2} + \frac{1}{R_3}) \tag{8}$$

Pasando el segundo término de la parte izquierda de la igualdad y luego sacando factor común, se llega a lo siguiente:

$$\frac{V_1}{R_1} = -V_2 \cdot (\frac{1}{s \cdot R_1 \cdot R_3 \cdot C_2} + \frac{1}{s \cdot R_2 \cdot R_3 \cdot C_2} + \frac{C_1}{R_3 \cdot C_2} + \frac{1}{R_3} + s \cdot C_1) \quad (9)$$

Operando llegamos a que:

$$\frac{V_1}{R_1} = -V_2 \cdot \frac{R_1 \cdot C_1 + R_2 \cdot C_1 + s \cdot R_1 \cdot R_2 \cdot C_1^2 + s \cdot R_1 \cdot R_2 \cdot C_1 \cdot C_2 + s^2 \cdot R_1 \cdot R_2 \cdot R_3 \cdot C_1^2 \cdot C_2}{s \cdot R_1 \cdot R_2 \cdot R_3 \cdot C_1 \cdot C_2}$$

De donde sale la siguiente igualdad:

$$\frac{V_1}{V_2} = -\frac{R_1 \cdot C_1 + R_2 \cdot C_1 + s \cdot R_1 \cdot R_2 \cdot C_1^2 + s \cdot R_1 \cdot R_2 \cdot C_1 \cdot C_2 + s^2 \cdot R_1 \cdot R_2 \cdot R_3 \cdot C_1^2 \cdot C_2}{s \cdot R_2 \cdot R_3 \cdot C_1 \cdot C_2}$$

Invirtiendo, es posible llegar a la fórmula de la transferencia:

$$\frac{V_1}{V_2} = -\frac{s \cdot R_2 \cdot R_3 \cdot C_1 \cdot C_2}{R_1 \cdot C_1 + R_2 \cdot C_1 + s \cdot R_1 \cdot R_2 \cdot C_1^2 + s \cdot R_1 \cdot R_2 \cdot C_1 \cdot C_2 + s^2 \cdot R_1 \cdot R_2 \cdot R_3 \cdot C_1^2 \cdot C_2}$$

De la cual finalmente obtenemos la fórmula canónica para la misma:

$$\frac{V_2}{V_1} = -\frac{s \cdot \frac{1}{R_1 \cdot C_1}}{s^2 + s \cdot (\frac{1}{R_3 \cdot C_1} + \frac{1}{R_3 \cdot C_1}) + \frac{1}{R_2 \cdot R_3 \cdot C_1 \cdot C_2} + \frac{1}{R_1 \cdot R_3 \cdot C_1 \cdot C_2}}$$

Ahora bien, la transferencia obtenida es negativa. Para poder obtener un circuito pasabanda de segundo orden que cumpla con la transferencia propuesta basta con agregar un amplificador operacional y dos resistencias de la misma magnitud en forma de configuración inversora, de forma tal de invertir la transferencia con ganancia 1 quedando la transferencia para el IGMF positiva:

$$\frac{V_2}{V_1} = \frac{-s \cdot \frac{1}{R_1 \cdot C_1}}{s^2 + s \cdot (\frac{1}{R_3 \cdot C_1} + \frac{1}{R_3 \cdot C_1}) + \frac{1}{R_2 \cdot R_3 \cdot C_1 \cdot C_2} + \frac{1}{R_1 \cdot R_3 \cdot C_1 \cdot C_2}}$$

2.8. Definición de los valores para el armado del circuito

Los componentes normalizados que se elegirán son aquellos que nos permiten tener una transferencia lo más parecida posible a la transferencia propuesta. Para esto, se eligen valores normalizados para los capacitores (serie del 10 %, serie E12) y los resistores (serie del 1 %, serie E96), especificados en los requerimientos para el armado del circuito. Estos valores son:

- R1 = 5.9kΩ
- R2 = 54.9Ω
- R3 = 412kΩ
- R4 = 10kΩ
- C1 = 0.82uF

- C2 = 0.012uF

Reemplazando en la fórmula que hemos obtenido en la sección anterior para un IGMF con la señal invertida, la transferencia queda como:

$$H(s) = \frac{V_2}{V_1} = \frac{-s \cdot \frac{1}{5{,}9k\Omega \cdot 0{,}82uF}}{s^2 + s \cdot (\frac{1}{412k\Omega \cdot 0{,}82uF} + \frac{1}{412k\Omega \cdot 0{,}012uF}) + \frac{1}{54{,}9\Omega \cdot 412k\Omega \cdot 0{,}82uF \cdot 0{,}012uF} + \frac{1}{5{,}9k\Omega \cdot 412k\Omega \cdot 0{,}82uF \cdot 0{,}012uF}}$$

De aquí, realizando las cuenta correspondiente resulta que la transferencia para los componentes normalizados es:

$$H(s) = \frac{s \cdot 206{,}6969822}{s^2 + s \cdot 205{,}2253532 + 4534796{,}495}$$

Notar que para realizar la cuenta no se tuvo en cuenta la resistencia R4 (la que forma parte de la configuración inversora que nos permite invertir la salida), debido a que no es necesario ya que su única función es formar parte del inversor y su valor no afecta a la transferencia normalizada.

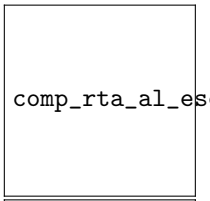
Ahora bien, uno de los requerimientos pedidos es que tanto resistencias como capacitores se encuentren en un determinado rango de valores. A pesar de esto, algunos de los valores hallados no se encuentran dentro de los valores permitidos. Para poder utilizar estos valores, se busca demostrar que las corrientes a las salidas de los operacionales y la corriente de entrada a través de la fuente no superan los 5 mA, de forma tal que podrán soportar la corriente sin dañarse ni presentar comportamientos que alteren el filtro. Para dicho propósito, se realizó una simulación de circuito LTSpice utilizando como señal de entrada una onda senoidal de amplitud 5 con la frecuencia para la cual nuestro circuito deja pasar más cantidad de señal (f_0). Los resultados obtenidos para las 3 corrientes se pueden ver en el siguiente gráfico:

demostracion.jpg

Como es posible observar, las distintas corrientes no superan el límite de los 5 mA, por lo tanto es posible realizar el armado del circuito con los valores de componentes presentados anteriorme

2.9. Comparación entre la transferencia para el circuito normalizados y la transferencia original

A fines de realizar una comparación entre ambas transferencias, a continuación podemos encontrar los mismos gráficos que se obtuvieron en la sección 2.2. En estos gráficos se encuentran solapados la transferencia original y la normalizada.

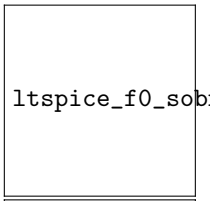


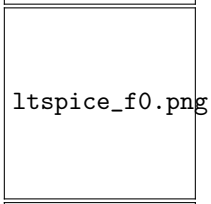
A partir de los gráficos, es posible llegar a la conclusión de que, a pesar de que la transferencia cambió levemente debido a que se debió normalizar el circuito utilizando valores de componentes específicos, la diferencia entren los distintos diagramas para la transferencia original y la transferencia normalizada es prácticamente nula, conservando perfectamente la característica de ser un filtro pasabanda.

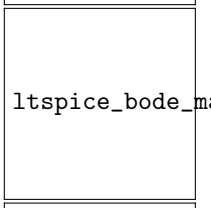
2.10. Simulación del circuito en LTSpice.

En la siguiente figura es posible apreciar el circuito para el cual se realizaron las simulaciones en LTSpice. Nótese que los valores de los componentes se corresponden con los hallados anteriormente, y que se eligió una resistencia de 10kΩ para la configuración inversora de forma tal de invertir la salida del IGMF.

Tal cual había sucedido anteriormente para los diagramas de Bode de la función de transferencia original en comparación a la función de transferencia normalizada, los diagramas poseen una diferencia prácticamente nula, esta vez solapando los de la transferencia original contra los obtenidos a partir de los datos generados en la simulación. Los diagramas son los siguientes:







Notemos que, para todos ellos, las diferencias de los diagramas obtenidos en la simulación a comparación de los diagramas obtenidos utilizando la librería *sympy* del lenguaje de programación Python es prácticamente nula.

3. Mediciones sobre el circuito

3.1. Materiales

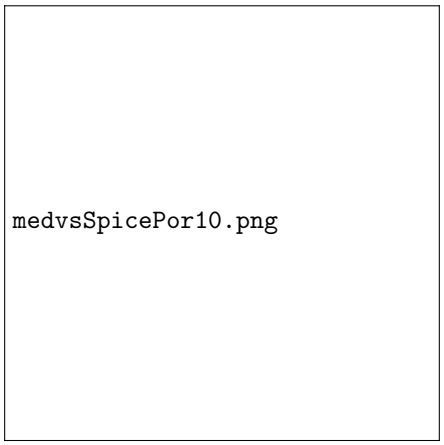
Para realizar las mediciones sobre el circuito armado a partir de la transferencia normalizada se utilizaron los siguientes materiales:

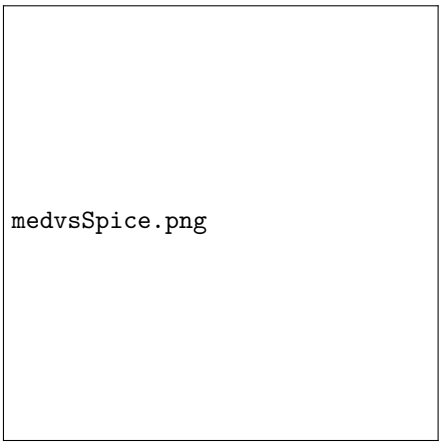
- Una resistencia de 5.9kΩ
- Una resistencia de 54.9Ω
- Cuatro resistencias de 100kΩ
- Tres resistencia de 10kΩ
- Un capacitor de 0.82uF

- Un capactior de 0.012uF
- Multímetro Sonel CMM-40
- Osciloscopio Siglent SDS 1102CML
- Fuente de tensión Kaise HY3005D
- Generador de funciones Topward 8140
- Cables banana-coco
- Puntas de osciloscopio (2)
- Cables unipolares para protoboard
- Protoboard
- Amplificador operacional TL081 (2)

3.2. Respuesta del circuito a señales cuadradas

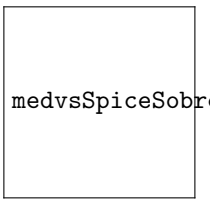
Una de las mediciones realizadas sobre el circuito fue sobre señales cuadradas con distintas frecuencias, tomando las mismas especificaciones desarolladas en la sección 2.4, a fines de realizar una comparación con los resultados obtenidos en la simulación en LTSpice. Para esto, se midieron las señales de entrada y salida del circuito con el osciloscopio, exportando los datos obtenidos a un archivo con formato *csv* a fines de poder graficar las respuestas obtenidas con el lenguaje de programación Python. A continuación, podemos encontrar los gráficos correspondientes a la comparación entre la respuesta obtenida con las mediciones en contraste con la simulación realizada en LTSpice.





Como es posible observar en lo gráficos, las respuestas a las cuadradas coinciden bastante con las respuestas obtenidas en la simulación. Existen algunas pequeñas diferencias cuyo motivo principal radica en los materiales utilizados (por ejemplo, la resistencia original de 412kΩ fue reemplazada por una puesta en serie de 4 resistencias de 100kΩ y una de 10kΩ). A su vez, el generador de ondas también introduce un pequeño error ya que el período de las ondas, su

valor pico-pico y el offset de las mismas no es exactamente el mismo que para las simulaciones.



3.3. Barrido en frecuencia

Además de analizar como responde el circuito a ondas cuadradas de distintas frecuencias, se realizó un barrido en frecuencia a fines de determinar como se comporta el circuito ante distintas frecuencias. Para esto, se definió una tensión fija de entrada y se midió la tensión de salida para distintas frecuencias, calculado la caída en dB de la salida respecto de la entrada. Los resultados de este barrido pueden observarse en la siguiente tabla:

Frecuencia(Hz)	Vpp(in)(mV)	Vpp(out)(mV)	Caìda dB
170	840	64	-22,3619862415599
214,186578482128	840	80	-20,4237859813988
269,858178834594	840	144	-15,3183358793326
340	840	384	-6,79896123388702
361	840	820	-0,2093086735633
428,373156964257	840	480	-4,86076097372589
539,716357669188	840	176	-13,5753323649546
680	840	96	-18,8401610604463
856,746313928514	840	64	-22,3619862415599
1079,43271533838	840	64	-22,3619862415599

Como es posible observar en la tabla, la menor caída en dB se da para una tensión pico-pico de $820mV$. A partir de este valor, es posible aproximar el error relativo de la frecuencia de corte encontrada realizado el barrido respecto a la frecuencia de corte obtenida realizando el análisis previo al armado y medición sobre el circuito. De este modo, el error relativo es:

$$\epsilon = \frac{361 - 339}{339} \cdot 100 = 6{,}48\,\%$$

4. Conclusiones

Durante el desarollo del trabajo práctico ha sido posible llevar a cabo el proceso de análisis de una transferencia propuesta junto con el armado de un circuito asociado a la misma. En primer lugar, se analizaron las características fundamentales del circuito (el tipo de filtro, su frecuencia de corte, sus polos y ceros, etc); luego, se determinó un circuito acorde a la transferencia, además de los valores de los componentes para armarlo. Finalmente, se realizaron una serie de mediciones sobre el mismo.
El trabajo práctico ha permitido poner en juego una serie de diversos conceptos

vistos en la materia. Analizando la respuestas al impulso, al escalón y los diagramas de Bode se ha podido determinar cómo responde el circuito para distintas frecuencias. A su vez, se logró resolver el desafío del armado del circuito, eligiendo uno de los circuitos más conocidos conocidos que existen: el IGMF de tipo pasa banda. A su vez, fue posible aprender a usar un simulador como LTSpice, comprobando que las simulaciones arrojan prácticamente los mismos resultados que los obtenidos vía el lenguaje de programación Python (del cual se utilizó la librería sympy). Por último, todo el análisis realizado en primera instancia en software pudo ser bajado a la práctica armando el circuito con los componentes normalizados en una protoboard y luego realizando distintas mediciones. Estas demostraron que el circuito armado se comporta casi en su totalidad en forma igual a los resultados que arrojó la etapa de análisis previo.