Este trabajo se desarrolla mayoritariamente en el área de la teoría de grupos, teoría de monoides y criptografía. Haremos una revisión tanto de la construcción de las trenzas y los grupos de trenzas como de métodos criptográficos que basen su seguridad en problemas relacionados con el grupo de trenzas. Se hará hincapié en el estudio de los monoides de Garside que nos permitirán hacer un uso práctico de las trenzas de forma que podremos trabajar con ellas desde un punto de vista computacional y que permiten la creación de algoritmos que las involucren. También nos proporcionará soluciones para el problema del conjugado y el problema de palabra.

Comenzamos el trabajo repasando conceptos y resultados básicos sobre grupos necesarios para la construcción del grupo de trenzas como pueden ser los grupos cocientes y las presentaciones de grupos.

Introducimos la definición de monoide junto con dos tipos de monoides, los monoides libres y los monoides atómicos, que cumplen características específicas cada uno. Estos monoides nos permiten trabajar con diferentes presentaciones de monoide. Bajo las hipótesis de trabajar con un monoide que posea una presentación ponderada nos aporta una solución al problema de palabra y al problema de divisibilidad.

Partiendo de un monoide atómico M y un subconjunto suyo Σ, definimos el monoide M_σ. Con esta definición podemos enunciar un teorema de gran relevancia, ya que bajo las hipótesis que presupone obtenemos en M_Σ una forma normal, la propiedad de cancelatividad, una solución al problema de palabra (heredada de la obtenida con las presentaciones) y una solución al problema del conjugado. Además, teniendo el concepto de conjunto exhaustivo somos capaces de poder identificar el monoide M_Σ con el monoide M del que deriva.

Con los monoides conseguimos un conjunto de resultados de gran utilidad. En última instancia nosotros vamos a trabajar con el grupo de trenzas y nos interesa ver como podemos obtener resultados sobre grupos a partir de los que se obtienen sobre monoides. Con este fin se introducen los grupos de fracciones y los monoides pre-Garside. Un monoide pre-Garside se define como un par (M, Δ) donde M es un monoide y Δ un elemento de M que cumple ciertas propiedades. Ha dicho elemento se le denomina elemento de Garside. Entre un monoide pre-Garside y su grupo de fracciones se establece un monomorfismo, de forma que podemos identificar el monoide pre-Garside como un subconjunto del grupo de fracciones. Gracias a esto conseguimos una forma normal para el grupo de fracciones como producto de una potencia del elemento de Garside y elementos del monoide. Esta forma normal a la que llamamos forma normal greedy es la que utilizamos para trabajar con el grupo de trenzas. Además, se puede reducir el problema del conjugado

en el grupo de fracciones a un problema del conjugado equivalente en el monoide.

Un monoide de Garside es un monoide pre-Garside (M, Δ) donde M es atómico y siendo Σ el conjunto de divisores de Δ se tiene que para cualesquiera dos átomos s, t de M, el conjunto

$$\{a \in \Sigma \mid s \preceq a,\ t \preceq a\}$$

tiene un elemento mínimo $\Delta_{s,t}$ (con respecto a $\preceq$). Un monoide de Garside es exhaustivo cuando $1 \in \Sigma$ y M posee una presentación cuyos generadores y relaciones pertenecen a Σ. El monoide de Garside exhaustivo consigue reunir las características obtenidas, por una parte, del monoide M_Σ, y por otra, de los monoides pre-Garside. De esta forma con los monoides de Garside exhaustivos obtenemos lo que buscamos para poder trabajar con el grupo de trenzas, una forma normal en el grupo de fracciones, que a su vez resuelve el problema de palabra y una solución al problema del conjugado en el grupo de fracciones. También conseguimos otras propiedades deseables como son la cancelatividad o la existencia y unicidad de máximo común divisor y mínimo común múltiplo en M.

Fue el matemático Emil Artin quien en la primera mitad del siglo XX acuño los términos de trenza y grupo de trenzas. Primero dió una definición topológica del grupo de trenzas y no fue hasta años después que obtuvo una definición algebraica equivalente del grupo de trenzas a partir de una presentación de grupo explicita. La definición algebraica se conoce como grupo de trenzas de Artin y es el grupo generado por $n-1$ elementos $\sigma_1, \sigma_2, ..., \sigma_{n-1}$ y las relaciones de trenza

$$\sigma_i \sigma_j = \sigma_j \sigma_i,$$

para todo $i, j \in \{1, 2, ..., n-1\}$ con $|i - j| \geq 2$ y

$$\sigma_i \sigma_{i+1} \sigma_i = \sigma_{i+1} \sigma_i \sigma_{i+1},$$

para todo $i \in \{1, 2, ..., n-2\}$.

La definición topológica de trenza es más intuitiva y se hace a partir del concepto de trenza geométrica de n hebras. Una trenza geométrica de n hebras, con $n \geq 1$, es un subconjunto $\mathcal{B} \subset \mathbb{R}^2 \times I$ formado por n intervalos topológicos (subconjuntos de $\mathbb{R}^2 \times I$ homeomorfos al intervalo $[0, 1]$) disjuntos llamados hebras de tal manera que la proyección $\mathbb{R}^2 \times I \to I$ establezca un homeomorfismo de cada hebra en I y

$$\mathcal{B} \cap (\mathbb{R}^2 \times \{0\}) = \{(1, 0, 0), (2, 0, 0), ..., (n, 0, 0)\},$$

$$\mathcal{B} \cap (\mathbb{R}^2 \times \{1\}) = \{(1,0,1),(2,0,1),...,(n,0,1)\}.$$

Cada hebra de $\mathcal{B}$ interseca con el plano $\mathbb{R}^2 \times \{t\}$ con $t \in I$ en un único punto y conecta un punto $(i,0,0)$ con un punto $(s(i),0,1)$ donde $i, s(i) \in \{1,2,...,n\}$. La sucesión $(s(1),s(2),...,s(n))$ es una permutación del conjunto $\{1,2,...,n\}$ llamada permutación subyacente de $\mathcal{B}$.

A través de isotopías que informalmente no son más que deformaciones de una trenza geométrica en otra se establece una relación de equivalencia. Al conjunto de clases de equivalencia asociadas a esta relación se les denomina trenzas de n hebras.

La trenzas geométricas las podemos representar mediante diagramas de trenza que son proyecciones en el plano. A través de la concatenación de los diagramas de trenza se define el producto de trenzas. El conjunto de trenzas de n hebras junto con esta operación forman un grupo. Finalmente se demuestra que este grupo es equivalente al grupo de trenzas de Artin.

Construimos el monoide de trenzas utilizando la presentación del grupo de trenzas como presentación de monoide. A las trenzas de este monoide se les llama trenzas positivas. El par formado por el monoide de trenzas y el elemento de Garside Δ_n constituye un monoide de Garside exhaustivo y el grupo de fracciones asociado es el grupo de trenzas, podiendo utilizar todas los resultados y características mencionados anteriormente.

Realizamos un repaso sobre conceptos básicos de criptografía y en que consisten los principales métodos criptográficos como son el cifrado simétrico y asimétrico, el intercambio de llaves, la firma digital o la autenticación.

Para poder aplicar el uso de grupo de trenzas en criptografía utilizamos las plataformas criptográficas, protocolos criptográficos basados en objetos algebraicos. Si el objeto algebraico utilizado es un grupo, a este se le llama grupo plataforma. La seguridad de un protocolo criptográfico depende entonces de la dificultad, computacional o teórica, de resolver un problema de teoría de grupos en el grupo de plataforma. Para que un grupo de plataforma G sea adecuado para un protocolo criptográfico basado en grupos, G debe poseer ciertas propiedades que hagan el protocolo tanto eficiente de implementar como seguro. Debe poseer una presentación finita. Además tiene que tener una forma normal para representar los elementos de forma única. Es deseable que el conjunto de elementos que se pueden representar con una cierta longitud máxima crezca exponencialmente con esta. Es importante que presente una buena difusión al determinar las formas normales de los productos, es decir, que al encontrar la forma normal de un producto es complejo computacionalmente calcular los factores. Por último, el grupo ha de contar con un problema de grupo lo suficientemente complejo como para

que no se pueda resolver computacionalmente.

Repasamos varios métodos criptográficos basados en el grupo de trenzas y el problema del conjugado o variantes suyos, como sus algoritmos. Entre ellos se encuentran los esquemas de intercambio de llave de Anshel-Anshel-Goldfeld y Ko, Lee et al, que fueron los primeros intentos de usar grupos no abelianos como grupo plataforma. De estos se realiza una implementación y se hace un estudio de los tiempos de ejecución variando los parámetros de los algoritmo.

Por último se dedica un apartado al criptoanálisis de este tipo métodos. En esencia para romper estos tipos de métodos basta con resolver el problema del conjugado. Hablamos de varias técnicas para resolver este problema computacionalmente, puesto que la solución que nos aportan los monoides de Garside es teórica y no se puede calcular en la práctica. Estos son el cáculo de los super conjuntos cumbre, los ataques basados en longitud y los ataques teóricos de representación. También mostramos una heurística para resolver el problema del conjugado de la cual llevamos a cabo una implementación. Realizamos diferentes ejecuciones del algoritmo para diferentes problemas del conjugado y mostrar su tasa de acierta. También se muestran los resultados obtenidos por la implementación del autor original.