This work is developed mainly in the area of group theory, monoid theory and cryptography. We will review both the construction of the braids and the groups of braids and cryptographic methods that base their security on issues related to the group of braids. Emphasis will be placed on the study of Garside monoids that will allow us to make a practical use of braids so that we can work with them from a computational point of view that allow the creation of algorithms involving them. They will also provide us solutions to the conjugacy problem and word problem.

We begin the work by reviewing basic concepts and results about groups necessary for the construction of the braid grop, such as quotient groups or group presentations.

We introduce the definition of monoid together with two kinds of monoids, free monoids and atomic monoids, that satisfy some characteristics. These monoids allow us to work with different monoid presentations. Under the hypothesis of working with a monoid that has a weighted presentation, it provides us a solution to the word problem and the divisibility problem.

Starting from an atomic monoid M and a subset $\Sigma \in M$, we define the monoid M_Σ. With this definition we can state a theorem of great relevance, since under the hypothesis that it presupposes we obtain in M_Σ a normal form, the property of cancellation, a solution to the word problem (inherited from the one obtained with the presentations) and a solution to the conjugacy problem. Furthermore, having the concept of an exhaustive set we are able to identify the monoid M_Σ with the monoid M from which it derives.

With monoids we get a set of highly useful results. Ultimately we are going to work with the braid group and we are interested in seeing how we can obtain results on groups from those obtained on monoids. Fraction groups and pre-Garside monoids are introduced for this purpose. A pre-Garside monoid is defined as a pair (M, Δ) where M is a monoid and Δ an element of M that fulfills certain properties. This element is called Garside element. A monomorphism is established between a pre-Garside monoid and its group of fractions, so that we can identify the pre-Garside monoid as a subset of the group of fractions. Thanks to this we get a normal form for the group of fractions as a product of a power of the Garside element and elements of the monoid. This normal form that we call the greedy normal form is what we use to work with the group of braids. Furthermore, the conjugacy problem in the fraction group can be reduced to a equivalent conjugacy problem in the monoid.

A Garside monoid is a pre-Garside monoid (M, Δ), where M is atomic and Σ is the set of divisors of Δ, fullfilling that for any two atoms s, t of M, the set

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

has a minimal element $\Delta_{s,t}$ (with respect to $\preceq$). A Garside monoid is exhaustive when $1 \in \Sigma$ and M have a presentation whose generators and relations belong to Σ. The exhaustive Garside monoid manages to gather the characteristics obtained, on the one hand, from the M_Σ monoid, and on the other, from the pre-Garside monoids. In this way, with the exhaustive Garside monoids, we obtain what we are looking for to be able to work with the group of braids, a normal form in the group of fractions, which in turn solves the word problem and a solution to the conjugate problem in the group of fractions. We also achieve other desirable properties such as cancellations or the existence and uniqueness of the greatest common divisor and least common multiple in M.

The mathematician Emil Artin was who in the first half of the 20th century coined the terms braid and braid group. He first gave a topological definition of the braid group and it was not until years later that he obtained an equivalent algebraic definition of the group of braids from an explicit group presentation. The algebraic definition is known as Artin's braid group and is the group generated by $n-1$ elements $\sigma_1, \sigma_2, ..., \sigma_{n-1}$ and the braid relations

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

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

The topological definition of braid is more intuitive and is made from the concept of geometric braid of n strands. We consider I as the interval $[0, 1]$. A geometric braid of n strands, with $n \geq 1$, is a subset $\mathcal{B} \subset \mathbb{R}^2 \times I$ formed by n topological intervals (subsets of $\mathbb{R}^2 \times I$ homeomorphs to the interval I) disjoint called strands in such a way that the projection $\mathbb{R}^2 \times I \to I$ establishes a homeomorphism of each thread in I and

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

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

Each strand of $\mathcal{B}$ intersects the plane $\mathbb{R}^2 \times \{t\}$ with $t \in I$ at a single point and connects a point $(i, 0, 0)$ with a point $(s(i), 0, 1)$ where $i, s(i)\ in \{1, 2, ..., n\}$. The sequence $(s(1), s(2), ..., s(n))$ is a permutation of the set $\{1, 2, ..., n\}$ called the underlying permutation of $\mathcal{B}$.

Through isotopies that are informally simply continuous deformations of one geometric braid in another, an equivalence relation is established. The set of equivalence classes associated with this relation are called braids of n strand.

Geometric braids can be represented by braid diagrams that are projections in the plane. Through the concatenation of the braid diagrams the product of braids is defined. The set of braids of n strands together with this operation form a group. Finally it is shown that this group is equivalent to Artin's group of braids.

We build the braid monoid using the braid group presentation as the monoid presentation. The braids of this monoid are called positive braids. The pair formed by the braid monoid and the Garside element Δ_n constitutes an exhaustive Garside monoid and the associated group of fractions is the braid group, being able to use all the results and characteristics mentioned above.

We review the basic concepts of cryptography and what the main cryptographic methods consist of, such as symmetric and asymmetric encryption, key exchange, digital signature or authentication.

In order to apply the use of the braid group in cryptography, we use cryptographic platforms, cryptographic protocols based on algebraic objects. If the algebraic object used is a group, this is called a platform group. The security of a cryptographic protocol then depends on the computational or theoretical difficulty of solving a group theory problem in the platform group. For a platform group G to be suitable for a group-based cryptographic protocol, G must possess certain properties that make the protocol both efficient to implement and secure. It must have a finite presentation. It also has to have a normal form to represent the elements in a unique way. It is desirable that the set of elements that can be represented with a certain maximum length grows exponentially with it. It is important that it presents a good diffusion when determining the normal forms of the products, that is, when finding the normal form of a product it is computationally hard to calculate the factors. Finally, the group must have a group problem complex enough that it cannot be solved computationally.

We review some cryptographic methods based on the braid group and the conjugacy problem or its variants, such as their algorithms. Among them are the Anshel-Anshel-Goldfeld and Ko, Lee et al key exchange schemes, which were the first attempts to use non-abelian groups as a platform group. An implementation of these is carried out and a study of the execution times is made by varying the parameters of the algorithms.

Finally, a section is dedicated to cryptanalysis of this type of methods. In

essence, to break these methods it is enough to solve the conjugacy problem. We are talking about various techniques to solve this problem computationally, since the solution provided by the Garside monoids is theoretical and cannot be calculated in practice. These are the calculation of the super summit sets, theEmbeddability length-based attacks, and the theoretical representation attacks. We also show a heuristic to solve the conjugate problem of which we carry out an implementation. We perform different runs of the algorithm for different conjugacy problems and show their exit rate. The results obtained by the original author's implementation are also shown.

Key words: Group, subgroup, symmetric group, quotient group, free group, group presentation, monoid, divisibility, equivalence, congruence, free monoid, atomic monoid, monoid presentation, weighted presentation, word problem, divisibility problem, normal form, conjugacy problem, cancelativity, comprehensive set, group of fractions, pre-Garside monoid, embeddability, Garside monoid, Artin's braid group, geometric braid, brand, isotopy, braid diagram, pure braid, cryptography, symmetric encryptation, asymmetric encryption, key exchange, digital signature, authentication, hash function, cryptographic hash function, Merkle-Damgard construction, Anshel-Anshel-Goldfeld scheme, Diffie-Hellman scheme, cryptanalysis, super summit sets, length-based attacks, theoretical representation attacks, heuristic.