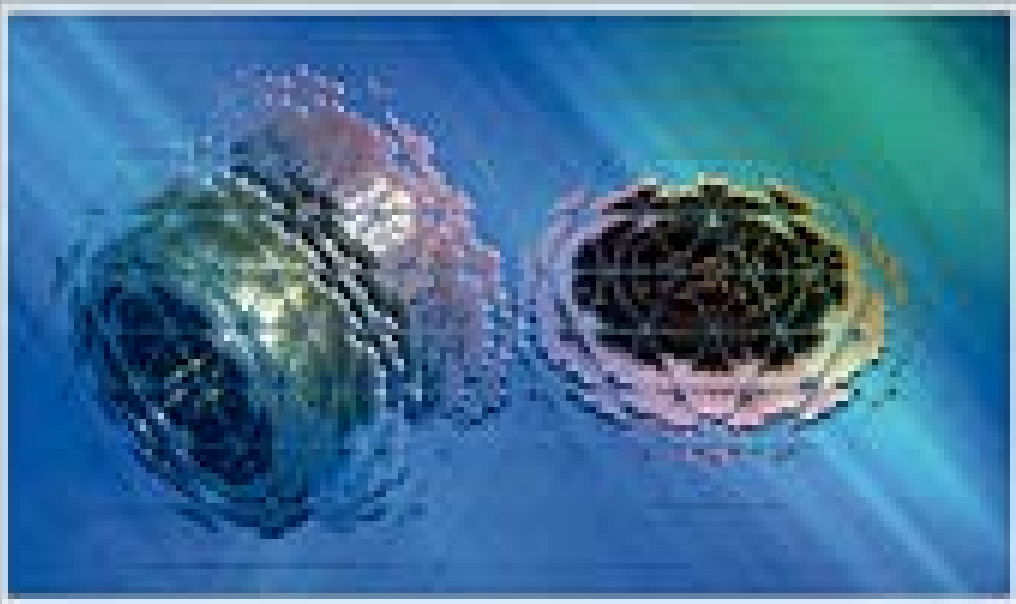
CIBERSEGURIDAD

Criptografía esencial

Principios básicos para el diseño de esquemas y protocolos seguros



María Isabel González Vasco
Ángel Luis Pérez del Pozo

Ra-Ma®
edU

Criptografía esencial

Principios básicos para el diseño de esquemas y protocolos seguros

María Isabel González Vasco
Ángel Luis Pérez del Pozo

Ra-Ma®
edU®
Conocimiento a su alcance
Bogotá - México, D.F.

González Vasco, María Isabel, *et al.*

Criptografía esencial/ María Isabel González Vasco y Ángel Luis Pérez del Pozo --.
Bogotá: Ediciones de la U, 2021
234 p. ; 24 cm
ISBN 978-958-792-293-6 e-ISBN 978-958-792-294-3
1. Informática 2. Seguridad informática 3. Ciberseguridad 4. Criptografía Tít.
621.39 ed.

Edición original publicada por © Editorial Ra-ma (España)
Edición autorizada a Ediciones de la U para Colombia

Área: Informática
Primera edición: Bogotá, Colombia, septiembre de 2021
ISBN. 978-958-792-293-6

Ediciones de la U es una empresa editorial que, con una visión moderna y estratégica de las tecnologías, desarrolla, promueve, distribuye y comercializa contenidos, herramientas de formación, libros técnicos y profesionales, e-books, e-learning o aprendizaje en línea, realizados por autores con amplia experiencia en las diferentes áreas profesionales e investigativas, para brindar a nuestros usuarios soluciones útiles y prácticas que contribuyan al dominio de sus campos de trabajo y a su mejor desempeño en un mundo global, cambiante y cada vez más competitivo.

Coordinación editorial: Adriana Gutiérrez M.
Carátula: Ediciones de la U
Impresión: DGP Editores SAS
Calle 63 #70D-34, Pbx (57+1) 3203510

Impreso y hecho en Colombia
Printed and made in Colombia

A María y Carlos,
que cada día me enseñan a descifrar mil mensajes secretos.
Maribel

A mis padres,
sin los que no sería la persona que soy,
de la que espero que estén orgullosos.

A Angélica,
que ha querido ser mi Player 2
en el juego más importante de todos.
Ángel

ÍNDICE

AGRADECIMIENTOS

Querríamos expresar nuestro agradecimiento, en primer lugar, a nuestros alumnos, en especial a aquellos que han cursado la asignatura "Criptografía" del Grado en Ingeniería de la Ciberseguridad y la asignatura "Criptografía y Criptoanálisis" del Máster en Ciberseguridad y Privacidad de la Universidad Rey Juan Carlos. Gracias por padecernos con una sonrisa, criticarnos, animarnos, y ayudarnos a ver qué conceptos resultan más difíciles de entender dentro de la Criptografía moderna y qué dificultades confrontan aquellos que se acercan a esta disciplina por primera vez.

Gracias también a nuestros maestros (en el sentido más amplio de la palabra), por ayudarnos a enfrentarnos a esos mismos obstáculos y empujarnos al abismo maravilloso de la investigación en Criptografía Matemática.

Y, gracias, siempre, a nuestras familias, que han soportado estoicamente nuestra deliciosa e irritante obsesión por la Criptografía Matemática, sus métodos, sus aplicaciones, y sus desafíos constantes sin los que, seguro, seríamos mucho más aburridos.

María Isabel González Vasco
Ángel Luis Pérez del Pozo
Alcorcón, Madrid. Noviembre de 2020.

AUTORES

MARÍA ISABEL GONZÁLEZ VASCO

Doctora y Licenciada en Matemáticas por la Universidad de Oviedo, obteniendo en ambos casos el Premio Extraordinario. Desde 2003 es profesora del área de Matemática Aplicada de la Universidad Rey Juan Carlos, en el que es Titular desde marzo de 2009. Ha impartido cursos de Criptografía y Criptoanálisis en diferentes contextos (grado, postgrado y máster), y es coautora de CryptoGo, un juego de cartas para enseñar Criptografía simétrica.

Su área de trabajo es la Criptografía Matemática, cuyo fin es establecer los modelos adecuados para proporcionar demostraciones formales que sirvan para determinar el nivel real de seguridad de distintas herramientas criptográficas. En particular, en criptoanálisis (análisis crítico) destacan sus resultados identificando vulnerabilidades en esquemas de cifrado construidos a partir de teoría de grupos así como señalando problemas en protocolos para intercambio de clave en entornos multiusuario. Entre sus trabajos constructivos destacan los marcos formales para conseguir reutilizar claves manteniendo propiedades demostrables de seguridad, las propuestas para calcular la intersección entre dos conjuntos con garantías de privacidad y los diseños para establecimiento de clave entre varios usuarios con autenticación por contraseñas.

María Isabel González Vasco ha publicado dos libros, más de 50 artículos en revistas y actas de congresos especializados, así como dos patentes. Ha participado y dirigido numerosos proyectos de investigación, destacando su papel actual como codirectora del proyecto *Secure Communication in the Quantum Era* financiado por el programa *Science for Peace and Security* de la OTAN.

Es miembro del comité editorial de las revistas Journal of Mathematical Cryptology e International Journal of Computer Mathematics: Computer Systems Theory. Sirve de manera habitual como recensora de revistas de referencia en

Criptología (Journal of Cryptology, AAECC, Designs Codes and Cryptology, etc.) y participa frecuentemente en comités de programa de conferencias internacionales de referencia dentro de la criptología de clave pública (PKC, ACISP, ICITS). Además, ha formado parte del comité organizador de dos escuelas internacionales en Criptología Matemática (2008) y seguridad demostrable (2009), además de organizar en 2007 en Madrid el congreso internacional ICITS de seguridad basada en Teoría de la Información. A nivel nacional, pertenece periódicamente al comité de programa de la Reunión Española sobre Criptología y Seguridad de la Información, así como a distintos comités involucrados en las Jornadas Nacionales de Investigación en Ciberseguridad. Es, además, miembro de la IACR (International Association for Cryptologic Research) y vocal de la Junta de Gobierno de la Real Sociedad Matemática Española, a cuya comisión de publicaciones pertenece.

ÁNGEL LUIS PÉREZ DEL POZO

Licenciado en Matemáticas en 2001, con premio extraordinario por la Universidad Complutense de Madrid y Doctor en Matemáticas en 2005 por la misma universidad. Durante un año fue Profesor Ayudante en el Departamento de Biomatemática de Universidad Complutense. Desde septiembre de 2007 su carrera académica ha estado vinculada a la Universidad Rey Juan Carlos, donde ha ocupado plazas de Profesor Visitante y Profesor Ayudante Doctor, que es la que ostenta en la actualidad. Durante este periodo ha impartido clases en varias titulaciones científico-técnicas de asignaturas como Matemática Discreta, Álgebra Lineal, Lógica y Estrcuturas Algebraicas. En los últimos años ha sido también profesor de Criptografía en el Grado en Ingeniería de la Ciberseguridad y de Criptografía y Criptoanálisis en el Máster en Ciberseguridad y Privacidad, ambos impartidos por la URJC. Desde 2012 a 2014 trabajó como consultor de seguridad senior en las empresas Solium e Innovation for Security, ambas vinculadas al grupo BBVA.

Su línea de investigación principal es la Criptografía Matemática, dentro de la que ha realizado trabajos en las áreas del criptoanálisis de esquemas basados en grupos, el cifrado broadcast, los protocolos de computación muliparte para el cálculo privado de la intersección de conjuntos, el intercambio de claves de grupo y los esquemas de compartición de secretos. Ha publicado más de 20 artículos en revistas indexadas y actas de congresos internacionales y es coautor de dos patentes. Ha participado en varios proyectos de investigación con financiación nacional e internacional, entre los que puede destacarse el proyecto *Secure Communication in the Quantum Era* en el marco del programa *Science for Peace and Security* de la OTAN. Colabora habitualmente con miembros del Departamento de Informática de la Univesità degli Studi di Salerno, en la que ha realizado varias estancias de investigación. Ha participado en diversas actividades para la divulgación de la Criptografía, entre las que destacan un taller dentro del curso de verano Mates por todas partes de la UNED y varios talleres apoyados en el juego CrytpoGo.

PRÓLOGO

El ecosistema en el que discurren nuestras vidas hoy en día es *computacional*. Está, en efecto, poblado de múltiples dispositivos de diferentes dimensiones, pesos, costes, consumos energéticos y propiedades específicas, que comparten la capacidad de almacenar información en formato digital, elaborarla y transmitirla a través de redes de diversa naturaleza.

Un ecosistema radicalmente distinto del de hace algunas décadas. Los instrumentos físicos analógicos para la reproducción de música o vídeo, por ejemplo, han desaparecido, suplantados por un único tipo de dispositivo, que trata los datos representados únicamente de un modo, en digital. Y muchas actividades que requerían alguna forma de interacción real, son a menudo sustituidas por operaciones equivalentes y más rápidas que el usuario efectúa a través de uno de esos dispositivos con el que está conectado a la red y que requiere simplemente cómputo y comunicación.

Vivimos, por tanto, en un ecosistema en el que muchísimas actividades han perdido *fisicalidad* y existen sólo en forma de transacciones digitales o de objetos representados mediante un flujo de bits que puede ser procesado y transmitido. En este nuevo ecosistema, los problemas de seguridad y de privacidad no han desaparecido: tenemos la necesidad de garantizar para todas las actividades reproducidas digitalmente las mismas propiedades de seguridad que garantizábamos en el mundo físico.

En el mundo físico, a menudo, eran de ayuda distintos tipos de soportes: candados y cajas fuertes para proteger material sensible, papeles especiales resistentes a falsificaciones para elaborar billetes bancarios y documentos importantes, sobres opacos para proteger nuestra oferta en una subasta, cabinas en los colegios electorales para proteger la privacidad de nuestro voto, procedimientos de identificación para reconocer nuestra identidad, procedimientos de autenticación para certificar la autoría de documentos y actos... y la lista podría continuar alargándose. Y estos

soportes eran para nosotros tranquilizadores: teníamos *confianza* en ellos porque nos garantizaban, con buenos resultados, las propiedades de seguridad y de privacidad que deseábamos en el ejercicio de nuestra actividad.

En el ecosistema computacional en el que vivimos hoy no disponemos de todo esto. Pero disponemos de un *potentísimo instrumento matemático* que nos permite dar respuesta a los problemas de seguridad y de privacidad que surgen en el nuevo contexto: este instrumento es la *Criptografía*.

La Criptografía moderna proporciona, en efecto, *técnicas matemáticas* útiles para proteger la información digital, los sistemas de procesado y la computación distribuida de ataques adversarios. Permite garantizar la *confidencialidad* de las comunicaciones, la *integridad* de los mensajes intercambiados y la *autenticación* de los mensajes y los participantes en juego. Y, es más, permite la creación de protocolos que implementan de forma segura bases de datos distribuidas, autenticadas y persistentes, que implementan dinero digital, que soportan subastas electrónicas o juego on-line, que implementan formas de voto electrónico. En general, la Criptografía moderna se convierte en el instrumento que *corrobora la confianza* en la actividad y los procesos que hemos reproducido o creado desde cero en el mundo digital.

Este volumen presenta a los estudiantes, de forma sencilla, los principios y las técnicas básicas de la Criptografía moderna. De los preliminares de teoría de números y teoría de la complejidad a la seguridad demostrable y los protocolos avanzados, el tratamiento es siempre riguroso y preciso. Está escrito con riqueza de detalles por dos excelentes criptógrafos, figuras de referencia en la comunidad científica nacional y bien conocidos y apreciados en la comunidad internacional, como atestigua su curriculum vitae. La Profesora María Isabel González Vasco y el profesor Ángel Pérez del Pozo llevan años comprometidos con la investigación básica, con publicaciones en actas de importantes conferencias y prestigiosas revistas, así como con la enseñanza y la divulgación de la Criptografía a través de libros, proyectos y programas de trabajo que unen a entidades públicas y privadas.

He tenido el placer de colaborar con ellos durante cerca de 15 años. Aprecio profundamente su capacidad científica, profesionalidad y cualidades humanas: el cuidado que ponen en su trabajo y la atención que prestan a las personas con las que interactúan los convierten en un sólido punto de referencia.

Sin ninguna sombra de duda, escrito con competencia y pasión, este texto puede ser verdaderamente útil a los estudiantes: podrán apreciar la importancia de la Criptografía, aprender sus elementos básicos y ser capaces de utilizarla en todos los contextos en los que resulte necesario.

Salerno, a 20 de octubre de 2020
Paolo D'Arco,
Professore Associato, Universitá degli studi di Salerno, Italia.

PREFACIO

La Criptografía, ciencia (y arte) de la gestión, transmisión, almacenamiento y procesado de información en entornos hostiles, es una disciplina fascinante en la que confluyen las Ciencias de la Computación, las Matemáticas, la Física y distintas áreas de Ingeniería. Resulta sorprendente analizar su evolución a lo largo de la historia, viendo cómo se ha desarrollado en paralelo a los diferentes sistemas de comunicación. Las primeras civilizaciones desarrollaron, a medida que avanzaban en nuevas formas de lenguaje y transmisión de mensajes a distancia, métodos más o menos ingeniosos para restringir el acceso a la información. Así, la llamada *Criptografía simétrica, clásica* o *de clave secreta,* se considera tan antigua como el lenguaje. Algunos jeroglíficos egipcios (datados hacia el 1900 a.C.) ya utilizaban simbología que era sólo conocida por ciertas clases de sacerdotes, en un intento de limitar el acceso al contenido de inscripciones consideradas delicadas. Hay también multitud de ejemplos de métodos de cifrado elementales utilizados por las antiguas civilizaciones del Mediterráneo, generalmente utilizados para enviar órdenes a los ejércitos manteniendo cierto nivel de confidencialidad. Este tipo de Criptografía clásica se cimenta en el principio de que sólo aquellos que conocen cierta información restringida (la clave) podrán tener acceso a los mensajes transmitidos a través de un cierto sistema de comunicación. En contraposición, la llamada *Criptografía asimétrica* o *de clave pública*, surge en los años setenta del siglo pasado partiendo de un escenario abierto en el que no podemos suponer el intercambio "seguro" de secretos a priori. En los últimos años, la proliferación de métodos y dispositivos para comunicarnos en entornos cada vez más complejos ha supuesto un reto fascinante para el desarrollo de herramientas criptográficas. También, esta proliferación ha traído la necesidad imperiosa de disponer de métodos formales para la validación de herramientas criptográficas que permitan perfilar con precisión cuál es más adecuado para cada contexto.

Esta obra es uno de los libros con más contenido matemático de la colección de Ingeniería de la Ciberseguridad de la editorial RAMA. Dicho contenido, minimalista en cierto sentido, es a nuestro juicio fundamental para cualquier ingeniero en ciberseguridad. Igual que no es posible ser un excelente arquitecto sin poder validar la calidad y robustez de los materiales de construcción, resulta impensable que un experto en ciberseguridad pueda desempeñar su labor sin conocer cómo funcionan las piezas básicas con las que se implementan soluciones en este ámbito: las herramientas criptográficas. Perseguimos pues con este volumen distintos objetivos:

- Familiarizar al lector con la terminología y nociones fundamentales que se utilizan en Criptografía moderna,
- Presentar los paradigmas de Criptografía simétrica y asimétrica, su filosofía y las primitivas esenciales que permiten conseguir los objetivos básicos de *confidencialidad, integridad* y *autenticación*.
- Exponer, de manera sencilla y comprensible, las nociones elementales de *seguridad demostrable,* de modo que el lector pueda comprender demostraciones matemáticas sencillas de seguridad y entienda las implicaciones prácticas de los teoremas en este campo.
- Permitir al lector asomarse al fascinante mundo de los protocolos criptográficos, ver distintos ejemplos de diseños adaptados a aplicaciones actuales en los que la Criptografía juega un papel esencial (y, a menudo, insospechado).

El material que presentamos se estructura en cinco capítulos. Cada uno finaliza con un breve test sobre los contenidos expuestos, y con una lista de lecturas sugeridas para profundizar en los temas tratados a lo largo del capítulo. Comenzamos en el Capítulo 1 dando una breve introducción a distintos fundamentos matemáticos y computacionales necesarios para la comprensión del resto del libro. Esta introducción es suficiente, pero en modo alguno exhaustiva, si bien seguramente sea prescindible para la mayoría de los lectores que hayan cursado asignaturas básicas de Álgebra Lineal, Matemática Discreta y Programación. El Capítulo 2 se centra en Criptografía simétrica o de clave secreta, dedicándose el Capítulo 3 a la Criptografía asimétrica o de clave pública. En ambos casos proporcionamos descripciones teóricas de diferentes tipos de construcciones, ilustrando dichas definiciones con ejemplos concretos cuidadosamente seleccionados. La seguridad demostrable, centrada en el caso asimétrico, se introduce en el Capítulo 4, donde hablamos fundamentalmente de seguridad para esquemas de cifrado. El Capítulo 5 contiene una muestra ilustrativa de diferentes tipos de herramientas criptográficas, quizá menos conocidas, pero sin duda esenciales para muchas aplicaciones actuales.

Finalizamos con un breve apéndice que contiene las soluciones a los tests presentados al final de cada capítulo.

1

PRELIMINARES

1.1 FUNDAMENTOS MATEMÁTICOS

Para afrontar el estudio de la Criptografía de manera seria es imprescindible manejar con soltura algunas nociones matemáticas. Muchas de ellas no están presentes en las enseñanzas previas a los estudios universitarios. En esta primera sección revisamos las que son necesarias para seguir el resto del libro.

1.1.1 Conjuntos, funciones y estructuras algebraicas

Definición. **[Conjunto. Pertenencia]** Un *conjunto* se define, de manera informal, como una colección de objetos, que reciben el nombre de *elementos* de ese conjunto. Se dice también que esos objetos *pertenecen* al conjunto.

Una opción habitual para describir un conjunto es enumerar sus elementos, que se escriben entre llaves y separados por comas. Así, por ejemplo, podemos escribir el conjunto A formado por los 5 primeros números impares positivos como $A = \{1,3,5,7,9\}$. Para denotar que 3 pertenece al conjunto A podemos escribir $3 \in A$ mientras que $6 \notin A$ quiere decir que 6 no es un elemento de A.

Definición. **[Contenido. Subconjunto]** Dados dos conjuntos A y B, diremos que A está *contenido* en B si todo elemento de A es también elemento de B; también se dice que A es un *subconjunto* de B y se escribe $A \subseteq B$.

Definición. **[Conjunto vacío]** Necesitaremos un conjunto caracterizado por la propiedad de no tener elementos. A ese conjunto lo llamaremos *conjunto vacío* y utilizaremos el símbolo $\varnothing$ para representarlo. Es fácil convencerse de que, dado

como hemos definido la relación de contenido, siempre se cumple que $\varnothing \subseteq A$ para cualquier conjunto A.

Ejemplo. **[Conjuntos numéricos]** Será frecuente que trabajemos con conjuntos formados por números, que seguramente el lector ya conocerá. El más sencillo es el formado por los *números naturales*, los "números de contar". Consideraremos que 1 es el primer número de este conjunto; así escribiremos

$$\mathbb{N} = \{1, 2, 3, 4, \ldots\},$$

donde los puntos suspensivos indican que este conjunto nunca termina de enumerarse ya que es infinito. A continuación tenemos el conjunto de los *números enteros*, que se obtiene añadiendo a $\mathbb{N}$ el 0 y los números negativos. Se denota

$$\mathbb{Z} = \{\ldots, -2, -1, 0, 1, \ldots\}.$$

El conjunto de los *números racionales* se denota $\mathbb{Q}$ y está formado por las fracciones cuyo numerador y denominador son números enteros, siendo el denominador distinto de 0. Dos fracciones se consideran iguales con la noción habitual de equivalencia, es decir, si el producto cruzado de ambas coincide. Los números enteros se pueden considerar fracciones con denominador 1. Todo número racional tiene una expresión en base 10, que puede tener decimales. Esa parte decimal puede ser finita o infinita pero periódica. Si consideramos todos los números que tienen expresión decimal, siendo esta finita, infinita periódica o infinita no periódica, obtenemos el conjunto de los *números reales* $\mathbb{R}$. Algunos ejemplos de números reales que no son racionales son $\sqrt{2}, e, \pi, \ldots$ Usaremos $\mathbb{R}^+$ para referirnos al conjunto de los números reales positivos, es decir, aquellos $x \in \mathbb{R}$ tales que: $x > 0$. Nótese que cada uno de estos conjuntos está contenido en el siguiente; así pues:

$$\mathbb{N} \subseteq \mathbb{Z} \subseteq \mathbb{Q} \subseteq \mathbb{R}.$$

Otra forma de describir un conjunto, en lugar de mediante enumeración, es especificando las propiedades que cumplen sus elementos. Así, por ejemplo, el conjunto $B = \{x \in \mathbb{R} : 3 \leq x < 6\}$ es el formado por los números reales del intervalo $[3, 6)$ y $\mathcal{P} = \{x \in \mathbb{N} : x \text{ es primo}\}$ es el conjunto infinito formado por los *números primos* (recordemos que un número entero p es primo si $p \geq 2$ y sus únicos divisores positivos son 1 y p).

Definición. **[Cardinal]** Dado un conjunto cualquiera A, se llama *cardinal* de ese conjunto a su número de elementos. Se denota como $|A|$. Por ejemplo, $|\{1, 3, 5, 7, 9\}| = 5$. Cuando un conjunto tiene infinitos elementos, diremos que su cardinal es *infinito* y escribiremos $|A| = \infty$.

Los conjuntos numéricos de los ejemplos anteriores tienen todos cardinal infinito, así como el conjunto $\mathcal{P}$ del ejemplo anterior, el formado por los números primos. Es posible dar una definición más sofisticada bajo la cual no todos los conjuntos infinitos tienen el mismo cardinal, hay algunos más "grandes" que otros, pero no la necesitamos para los objetivos de este libro. Por último, el cardinal del vacío, por definición, es $|\varnothing| = 0$.

Definición. **[Operaciones con conjuntos]** Dados dos conjuntos A y B se definen su *intersección*, su *unión* y la *diferencia* de A menos B como:

- $A \cap B = \{x : x \in A \text{ y } x \in B\}$.
- $A \cup B = \{x : x \in A \text{ o } x \in B\}$.
- $A \setminus B = \{x : x \in A \text{ y } x \notin B\}$.

Definición. **[Función]** Vamos a explorar ahora el concepto de *función*, fundamental en todo el desarrollo de las Matemáticas contemporáneas. Es posible dar una definición rigurosa de función, pero no lo necesitamos para nuestros objetivos, así que adoptaremos una informal. La idea que subyace en el concepto de función es la de un mecanismo que permite asignar a cada elemento de un conjunto "inicial" (llamado *dominio* de la función) un único elemento de otro conjunto "final" (llamado *codominio* de la función). Si f es el nombre de una función, se suele escribir $f : A \to B$ para indicar que A es el dominio de f y B es su codominio. Si un elemento a del dominio se transforma en otro b del codominio, decimos que b es la *imagen* de a por f y escribimos $b = f(a)$. Decimos también que a es una *preimagen* de b para f

Definición. **[Funciones inyectivas y suprayectivas]** Una función $f : A \to B$ es *inyectiva* si nunca transforma dos elementos distintos de A en el mismo elemento de B. Dicho de otra forma, si dados $r, s \in A$ cualesquiera con $r \neq s$ se cumple que $f(r) \neq f(s)$. La función será *suprayectiva* o *sobreyectiva* si cumple que todo elemento de B es imagen de algún elemento de A. Por último diremos que una función f es *biyectiva* (o una *biyección*) si es simultáneamente inyectiva y supreyectiva. Las funciones biyectivas son importantes ya que están caracterizadas por poseer una *función inversa*, que se suele denotar como $f^{-1} : B \to A$. Dos funciones que sean inversas la una de la otra tienen la propiedad de que si aplicamos primero una y luego la otra volvemos al mismo elemento de partida.

Es importante darse cuenta de que una función $f : A \to B$ entre conjuntos finitos que cumpla que $|A| > |B|$ nunca podrá ser inyectiva. Análogamente, si $|A| < |B|$, la función no podrá ser suprayectiva.

Una función biyectiva establece una correspondencia biunívoca entre los elementos de dos conjuntos: cada elemento del conjunto inicial (dominio) está vinculado con un único elemento del conjunto final (codominio) y viceversa. Es por esto que está caracterizada por tener una función inversa que la "revierte". Una función biyectiva de un conjunto en sí mismo se denomina una permutación de ese conjunto.

Llamamos *estructura algebraica* a una abstracción matemática que modela un conjunto dotado de una o varias operaciones que cumplen ciertas propiedades. Por ejemplo, en el conjunto de los números enteros $\mathbb{Z}$ podemos considerar las *operaciones internas* de *suma* y *producto*. Estas operaciones verifican varias propiedades, como la *conmutativa*, la *asociativa*, la *distributiva* de la segunda respecto de la primera, la *existencia de elementos neutros* para ambas y de *opuestos* para la primera. La abstracción de todo ello conduce al concepto de *anillo* (en este caso *conmutativo* y *con unidad*). Otro ejemplo es la estructura de *cuerpo*, en la que, adicionalmente, cada elemento distinto del neutro de la suma tiene *inverso* para la segunda operación. En este texto estamos especialmente interesados en la estructura de *grupo*, en la que se considera únicamente una operación. La definimos formalmente a continuación.

Definición. **[Grupo]** Un *grupo* es una pareja $(G,\cdot)$, donde G es un conjunto no vacío y $\cdot$ es una *operación interna* en G. Esto quiere decir que al operar dos elementos a y b de G se obtiene un tercer elemento c que vuelve a estar en G. Se denota $a \cdot b = c$. A esta operación se le pide que cumpla las siguientes propiedades:

- *Asociativa*: dados $a,b,c \in G$, siempre se cumple que $a \cdot (b \cdot c) = (a \cdot b) \cdot c$.
- *Existencia de elemento neutro*: existe un elemento $e \in G$ con la propiedad de que para cualquier $a \in G$ se cumple $a \cdot e = e \cdot a = a$.
- *Existencia de inversos*: dado cualquier $a \in G$ existe un elemento $a^{-1} \in G$ que cumple $a \cdot a^{-1} = a^{-1} \cdot a = e$.

Si además la operación es *conmutativa*, esto es, siempre se cumple que $a \cdot b = b \cdot a$, se dice que el grupo es *conmutativo* o *abeliano*.

Es importante puntualizar que la operación de grupo puede tener formas muy distintas. Por ejemplo, $(\mathbb{Z},+)$ es un grupo abeliano. Cuando la operación es "parecida" a la suma se suele decir que estamos ante un *grupo aditivo*. Las propiedades son las mismas formalmente, pero en lugar de hablar del inverso de un elemento, se habla de su *opuesto*. Así pues, el neutro para esta operación es $e = 0$ y el opuesto de, por ejemplo, 5 es -5, ya que $5 + (-5) = 0 = e$.

Otras veces la operación es "más parecida" al concepto que tenemos de una multiplicación. En estos casos hablamos de *grupos multiplicativos* y mantenemos la denominación de inversos. Así, $\mathbb{R}^+$, el conjunto de los números reales positivos, con la operación de multiplicar es un grupo abeliano, el elemento neutro es $e=1$ y el inverso de, por ejemplo, 2 es $0,5$, ya que $2\cdot(0,5)=1$; escribiremos $2^{-1}=0,5$. Un ejemplo de grupo multiplicativo no abeliano son las matrices 2 por 2 con determinante distinto de cero, dotadas de la multiplicación habitual de matrices. En este caso el elemento neutro es la matriz identidad y el inverso de una matriz es, como no podía ser de otra forma, lo que habitualmente llamamos inversa de esa matriz.

También es habitual dotar de estructura de grupo a algunos conjuntos de funciones biyectivas de un conjunto en sí mismo. La operación en este caso es la *composición* de funciones, que consiste en aplicar primero una función y al resultado aplicarle la siguiente. Por ejemplo, el conjunto de las biyecciones de un conjunto finito en sí mismo junto con la operación de componer es un grupo no abeliano que recibe el nombre de *grupo simétrico*.

Un concepto importante en la Teoría de Grupos es el de *orden de un elemento* $a\in G$. Para definirlo necesitamos primero introducir notación de potencias: dado k un entero positivo, se define a^k como el resultado de operar el elemento a consigo mismo k veces; a^{-k} se define como $(a^{-1})^k$; por último se considera que $a^0=e$. Esta notación es compatible con las propiedades de las potencias a las que estamos acostumbrados: para multiplicar potencias de las misma base se suman los exponentes, una potencia elevada a otra se calcula usando como exponente el producto de los exponentes, etc.

Definición. **[Orden de un elemento]** Dado $a\in G$, se define el *orden* de a como el mínimo entero positivo m que cumple que $a^m=e$, en caso de que dicho entero exista, y escribiremos $ord(a)=m$. Si no es así, se dice que a tiene *orden infinito*. Si nos fijamos en esta definición observaremos que el elemento neutro e siempre tiene orden 1.

Definición. **[Grupo cíclico]** Decimos que un grupo G es *cíclico* si puede obtenerse calculando todas las potencias de uno de sus elementos. En el caso de que $a\in G$ sea uno de esos elementos, decimos que a es un *generador* de G y escribimos $G=\langle a\rangle$. La situación en la que estamos más interesados es aquella en la que G es finito. En ese caso, el orden de todos sus elementos también tiene que ser finito. Si además G es cíclico, $|G|=m$ y a es uno de sus generadores, se puede demostrar que $ord(a)=m$ y que $G=\langle a\rangle=\{e,a,a^2,\ldots,a^{m-1}\}$. Cabe puntualizar que hablamos de uno de sus generadores y no *del* generador ya que habitualmente un grupo cíclico tendrá más de un generador.