

Elementos de Criptografía Clásica

Andrés Cortés Dávalos

Area de Computación y Sistemas, UAM-I

Sandra Díaz Santiago

UAM-I y ESCOM-IPN

Josué David Torres Covarrubias

Area de Computación y Sistemas, UAM-I

Horacio Tapia Recillas

Departamento de Matemáticas, UAM-I

htr@xanum.uam.mx

René Basurto

DACB-UJAT y Nutzer Sistemas



CIMAT

Matemática Aplicada y su Enseñanza

- Licenciatura -

Editores:

Dr. Fernando Brambila Paz
Departamento de Matemáticas,
Facultad de Ciencias. UNAM.

Dr. Alejandro J. Díaz Barriga Casales
Instituto de Matemáticas,
UNAM.

QA76 .9
C931

Elementos de Criptografía Clásica / Andrés Cortés Dávalos, Sandra Díaz
Santiago, Josué David Torres Covarrubias, Horacio Tapia Recillas y René Basurto.
Editado por Brambila Paz, Fernando y Díaz Barriga Casales, Alejandro J. - México :
Centro de Investigación en Matemáticas : Sociedad Matemática Mexicana, 2005.
VI, 59 p. ; 23 cm. il. - (Matemática Aplicada y su Enseñanza,
Nivel Licenciatura)
ISBN 968-5733-05-8

1. Criptografía.
MSC: 94Axx, 94-03

ISBN 968-5733-05-8

©D.R. Centro de Investigación en Matemáticas, A.C.
Jalisco s/n, Mineral de Valenciana,
36240 Guanajuato, Gto., México

©D.R. Sociedad Matemática Mexicana
Circuito exterior s/n, área de la investigación científica,
Ciudad Universitaria. C.P. 04510 MEXICO D.F.

Este libro no puede ser reproducido total ni parcialmente, por ningún medio electrónico o de otro tipo, sin autorización escrita del editor.

This book may not be reproduced, whole or in part, by any means, without written permission from the publisher.

Cuidado de edición: *Hernán González Aguilar*
Diseño de portada: *Odalmira Soto Alvarado*

Impreso por: *S y G Editores, S.A. de C.V.*
Cuapinol 52, Santo Domingo de los Reyes, Coyoacán
04369 - México, D.F.



Índice general

Presentación de la Serie “Matemática Aplicada y su Enseñanza”	III
Introducción	V
1. Un poco de historia	1
1.1. Motivación	1
1.2. Los Orígenes	5
1.3. Algunos conceptos de Criptografía	9
1.4. Criptografía Clásica	9
1.5. Mecanización de la confidencialidad	11
2. Sustitución Simple	19
2.1. Sustitución Aleatoria	19
2.2. Cifrado del Palomar	21
2.3. Código Sombra	23
2.4. Ejercicios	25
2.5. Cifrados de Corrimiento	28
2.6. Cifrados con Palabra Clave	29
2.7. Discos de Cifrado	30
2.8. Ejercicios	31
3. Sustitución Polialfabética	33
3.1. Aplicación del cifrado de Julio César	33
3.2. Cifrado Vigenère (Versión de Lewis Carrol)	35
3.3. Cifrado de Jefferson	37
3.4. Ejercicios	39
4. Cifrados de Permutación	42
4.1. Cifrado de la Vía del Tren	43
4.2. Cifrado Torbellino	44
4.3. Variante del cifrado Torbellino usando llave	46

4.4.	La Scytala	48
4.5.	Ejercicios	49
4.6.	Cifrado usando una retícula	50
4.7.	Ejercicios	56
	Bibliografía	59

Presentación de la Serie

“Matemática Aplicada y su Enseñanza”

Maestro ¿y esto para qué sirve?... Es la pregunta que muchas veces se oye en un salón de clase de Matemáticas. La Sociedad Matemática Mexicana a través de su Comité de Educación trata de colaborar a que la enseñanza de las matemáticas sea cada vez mejor, a que los que las estudian se convenzan de que el esfuerzo que tienen que realizar para aprenderlas no es solamente para pasar de año, sino que los procesos de pensamiento que enfrentan, las habilidades que adquieren y sobre todo la actitud que deben tener frente a los problemas es útil en su formación, en su desarrollo profesional, incluso en su vida cotidiana.

Por saber matemáticas entendemos participar del quehacer matemático; es decir, tener habilidad para resolver problemas, conjeturar, hacer demostraciones.

Gracias al apoyo del CONACYT, la Sociedad Matemática Mexicana (SMM) ha podido sostener el proyecto “Matemática Aplicada y su Enseñanza”, que ha colaborado y estamos seguros colaborará a que los profesores nos podamos enfrentar a ofrecer a nuestros estudiantes un producto, las matemáticas, más interesante, más lúdico, de más calidad. A que los alumnos puedan tener a la mano respuestas a la pregunta que hacemos al inicio de esta presentación.

Desde su inicio el proyecto se dividió en dos niveles: el nivel de Bachillerato y el nivel de Licenciatura.

Algunos de los trabajos que presentamos en estos volúmenes fueron hechos a petición expresa y con muchas horas de discusión sobre lo que debía de ser el resultado del proyecto, luego éstos pasaron a arbitraje. Posteriormente hicimos un primer concurso para convocar a la comunidad matemática del País a que colaborara con este proyecto, poniendo en la página de la Sociedad ejemplos de qué es lo que estábamos esperando. La respuesta de la comunidad ha sido excepcionalmente buena y para iniciar la serie ya contamos con material para seis volúmenes de Bachillerato y seis de Licenciatura.

Cada volumen de Bachillerato cuenta con algunos fascículos que tratan temas de matemáticas con aplicaciones, a veces a la matemática misma, y en ocasiones la forma de cómo se puede desarrollar este contenido en clase a manera de una propuesta didáctica.

Para el nivel Licenciatura se tiene la idea de mostrar aplicaciones que sean susceptibles de enseñar en los primeros semestres de una Licenciatura como Biología, alguna Ingeniería, Economía, Química, desde luego Matemáticas, etc.

Para su presentación hay dos tipos de clasificaciones, una por áreas de las matemáticas, así hay volúmenes para Cálculo, para Álgebra Lineal, para Geometría, otra por la aplicación; Matemáticas Aplicadas a la Ciencias de la Vida y Matemáticas Aplicadas a la Negociación.

Sinceramente esperamos colaborar con maestros y alumnos en lograr un mejor y más profundo aprendizaje de las matemáticas.

“Provocar aprendizajes, es nuestra tarea en la enseñanza”.

Agradecemos a todos los que en algún momento han colaborado con este proyecto: escritores, árbitros, concursantes. Todo aquel que se ha enfrentado a la tarea de editar sabe que ésta es ardua. Ha sido importante la colaboración de María Teresa V. Martínez Palacios, Gricelda Cedillo Ramírez, Martha Cerrilla y Aranda, Alejandro Bravo Mojica, Graciela González Hita y Hernán González a ellos les damos las gracias. Por último queremos agradecer al CIMAT y a su director José Carlos Gómez Larrañaga por esta coedición con la SMM.

Afectuosamente,

Coordinadores del Proyecto “Matemática Aplicada y su Enseñanza” de la SMM.

Dr. Fernando Brambila Paz
Departamento de Matemáticas,
Facultad de Ciencias, UNAM.

Dr. Alejandro J. Díaz Barriga Casales
Instituto de Matemáticas
UNAM.

Octubre de 2005.

Introducción

En la actualidad es cada vez más común que instituciones bancarias, comerciales, gubernamentales, educativas, etc. se comuniquen y realicen transacciones a través de la Internet o medios de transmisión inseguros. La información que viaja por éstos medios es en muchas ocasiones de carácter confidencial, y por lo tanto necesita ser protegida contra el acceso de personas o entidades no autorizadas. Para ello, se tienen un conjunto de herramientas y mecanismos que conforman la *seguridad computacional* o *seguridad informática*. La *criptografía* es de los más importantes mecanismos para este propósito.

La palabra criptografía viene del griego *kriptos* (*ocultar*) y *graphos* (*escritura*), es decir, significa ocultar la escritura. En un principio era considerada como un arte, sin embargo al evolucionar y basar sus conceptos en diversas ramas de las matemáticas como la teoría de números, el álgebra, la probabilidad y la estadística entre otras, y posteriormente en las ciencias de la computación, se ha constituido como una ciencia. Actualmente, ésta ciencia juega un papel de suma importancia en la protección de la información garantizando su privacidad, integridad, autenticidad y no repudio, refiriéndose esto último a que una entidad no puede negar la autoría de sus mensajes.

En nuestro país es cada vez mayor la demanda de expertos con conocimientos en seguridad en cómputo y criptografía. En consecuencia varias instituciones educativas han tratado de satisfacer ésta demanda, incluyendo en los planes de estudio de las carreras de Matemáticas y Computación, cursos relacionados con la criptografía. Una de tales instituciones es la Universidad Autónoma Metropolitana, la cuál a través del Departamento de Matemáticas de la Unidad Iztapalapa, ofrece desde hace varios años un *Seminario de Criptografía* que se imparte cada trimestre con la finalidad de divulgar y promover el interés en esta área (además de organizar otra serie de actividades). Dicho seminario está dirigido al público en general y en su organización participan docentes y alumnos del Departamento de Matemáticas y del Área de Computación y Sistemas.

Este libro surgió con la necesidad de ofrecer material escrito en español a los participantes del Seminario de Criptografía y se han adaptado para un público más general, incluyendo estudiantes desde nivel medio superior. Los requisitos para leer este libro son mínimos y no se requiere prácticamente conceptos avanzados de matemáticas.

La intención es proveer un punto de partida accesible al estudio de la criptografía para el público en general. Los autores de este libro decidimos empezar describiendo algunos de los cifrados clásicos puesto que sientan las bases para comprender los conceptos de la criptografía. Así mismo es importante señalar que éste trabajo es una introducción al tema y que en un futuro esperamos ofrecer una segunda parte, donde se traten los aspectos de la criptografía moderna.

El trabajo está organizado en cuatro capítulos, el primero de ellos ofrece una introducción histórica; con la finalidad de resaltar la importancia que la criptografía ha tenido a lo largo de la historia y también para tener una idea de la evolución que ésta ciencia ha tenido. El segundo capítulo abarca los métodos de sustitución simple, métodos que en su momento fueron muy importantes. En el tercer capítulo se tratan algunos métodos de sustitución polialfabética. Y por último, en el cuarto capítulo se tratan los cifrados basados en permutaciones. Al final de cada capítulo se incluyen una serie de ejercicios con el propósito de que el amable lector al realizarlos pueda verificar si ha comprendido cada uno de los temas. Cabe mencionar que este libro está basado principalmente en las referencias [GAR72], [KAH67] y [SIN99], donde el lector interesado puede profundizar en algunos temas.

Deseamos agradecer a las autoridades de la UAM-Iztapalapa y al Departamento de Matemáticas por facilitarnos las instalaciones para el desarrollo de este libro. A los participantes del Seminario de Criptografía por sus valiosos comentarios y a la Srita. Corina Sánchez Santiago, por apoyarnos en la redacción de este libro. Todas las sugerencias y comentarios constructivos serán bien recibidos para mejorar el contenido y presentación de este material.

Agradecemos a la Sociedad Matemática Mexicana por darnos la oportunidad de hacer llegar a diversos públicos, a través de sus publicaciones, algunas ideas relacionadas con el apasionante tema de la Criptografía.

México, D.F., Octubre de 2005.