Departamento de Ingeniería Matemática
Universidad de Chile, Facultad de Ciencias Físicas y Matemáticas

Introducción a la Criptografía

(MA-53G)

Semestre Primavera 1996

Profesor Marcos Kiwi

Prefacio

Estos apuntes fueron generados durante el desarrollo del curso *Introducción a la Criptografía* (MA-53G) que se dictó en la Facultad de Ciencias Físicas y Matemáticas de la Universidad de Chile durante el semestre primavera de 1996. La idea de hacer un curso que abordara temas de criptografía fue mostrar una bonita interacción entre matemáticas puras, las ciencias de la computación, y un tema de importancia para la ingeniería — la seguridad de nuestros sistemas y redes computacionales. La constatación de las casi nulas instancias que hay en el país de discusión y estudio de los problemas de seguridad y las futuras predecibles demandas que impondremos sobre nuestros sistemas computacionales también motivaron la decisión de crear el curso *Introducción a la Criptografía.*

Estos apuntes corresponden a la transcripción de aproximadamente 2/3 de las cátedras dictadas.[1] La confección de estos apuntes se hicieron en forma conjunta entre el profesor y los alumnos participantes en el curso. La transcripción de cada cátedra corresponde a una versión detallada del material discutido en clase, la incorporación de citas bibliográficas y material relacionado con los temas cubiertos en cada clase.

El objetivo de estos apuntes es crear material que apoye la labor docente y que quede disponible a aquellos interesados en temas relacionados con criptografía y seguridad.[2]

Estos apuntes son una primera versión que se irá completando y mejorando las proximas veces que se dicte el curso MA-53G. Ciertamente el material que sigue contiene algunos errores, requieren de una mejor organización, y falta uniformizar mejor la notación. Sin embargo confío que, inclusive en su forma actual, el lector encontrará en estos apuntes material de interés y actualidad para las matemáticas, la computación y la ingeniería, además de una fuente de asombro y desafiantes problemas en que pensar.

Quisiera muy especialmente agradecer a aquellos que contribuyeron en el desarrollo de estos apuntes, ellos son: Juan Pablo Alamo, Julio Aracena, Gregorio Gonzalez, Rodrigo Gonzalez, Jens Hardings, Alejandro Hevia, Mladen Nadinic, y Ricardo Valenzuela.

Para el desarrollo de este curso fue importante el apoyo brindado por FONDECYT Proyecto No. 1960849 y Fundación Andes a través del Programa de Becas de Reinserción de Científicos Chilenos.

Marcos Kiwi
28 de Noviembre, 1996

[1] Durante el curso se realizaron 26 cátedras. No se transcribieron las cátedras 11, 12, 20–26.

[2] Estos apuntes, así como demás material relacionado con el curso MA-53G esta disponibles en la WWW en `http://www.dim.uchile.cl/~mkiwi/cripto_96.html`