MA-53G Intr. a la Criptografía **Semestre Otoño, 1998**

Circular No. 1 : 11 de Marzo

Profesor: M. Kiwi Auxiliar: A. Hevia

Comentarios acerca de la bibliografía

Los textos principales del curso serán el Stinson [Sti95] y el Koblitz [Ko94]. El libro de Salomaa [Sa96] constituye una buena fuente de lectura complementaria.

El libro de Schneier [Sc94] contiene un tratamiento extenso de los aspectos más aplicados que tienen que ver con criptografía. Sin embargo este texto contiene muchos errores, omite detalles, y no contiene demostraciones.

Los libros de Stallings [Sta95] y Pfleeger [Pf89] abordan el tema de diseño de políticas de seguridad en sistemas computacionales.

La reseña histórica de la criptografía clásica puede verse en el Kahn [Ka96]. El texto de Bach y Shallit [BS96] es una excelente referencia para todo lo que concierne a la teoría de números computacional. El Ireland y Rosen [IR90] contiene un profundo tratamiento del área de teoría de números clásica. El Cormen et al. [CLR94] es un texto que puede servir de consulta para todo lo que concierne a algoritmos elementales. Dos buenos textos de consulta para todo lo que tenga que ver con teoría de la complejidad computacional son el Papadimitriou [Pa94] y el Sipser [Si97].

El *Handbook of applied cryptography* [H1-97] contiene una extensa discusión de la literatura y del estado del arte en el área. En el *Handbook of theoretical computer science, volumen A* [H2-90], se pueden encontrar dos artículos de interés. El primero, cuyo autor es Rivest, es un survey sobre criptografía. El segundo artículo, cuyors autores son A. Lenstra y H. K. Lenstra, es un survey sobre teoría de números computacional.

References

[Sti95] D.R. Stinson, "Cryptography: Theory and Practice". CRC Press, 1995.

[Ko94] N. Koblitz, "A course in number theory and cryptography", (segunda edición). Graduate Texts in Mathematics, vol. 114, Springer–Verlag, 1994

[BS96] E. Bach y J. Shallit, "Algorithmic number theory", Mit Press, vol. 1, 1996.

[Ka96] D. Kahn, "The codebreakers", Scribner, revised and updated edition, 1996.

[H1-97] A. J. Menezes, P. van Oorschot, y S. A. Vanstone, editores, "Handbook of applied cryptography", CRC Press, 1997.

[Sa96] A. Salomaa, "Public–key cryptography", Springer–Verlag, second edition, 1996.

[Sc94] B. Schneier, "Applied cryptography: protocols, algorithms, and source code in C". John Wiley & Sons, Inc., 1994.

[Sta95] W. Stallings, "Network and internetwork security: principles and practice". Prentice–Hall, 1995.

[CLR94] T. H. Cormen, C. E. Leiserson, y R. L. Rivest, "Introduction to Algorithms". MIT Press, first edition, 1990. Thirteenth printing, 1994.

[IR90] K. Ireland, y M. Rosen, "A classical introduction to modern number theory", Graduate Texts in Mathematics, vol. 84, Springer–Verlag, second edition, 1990.

[Pa94] C. H. Papadimitriou, "Computational complexity". Addison-Wesley Publishing Company, first edition, 1994.

[Pf89] C. P. Pfleeger, "Security in Computing". Prentice Hall, 1989

[Si97] M. Sipser, "Introduction to the theory of computation". PWS Publishing Company, 1997.

[H2-90] J. van Leeuwen, editor, "Algorithms and complexity". Handbook of Theoretical Computer Science, vol A, MIT Press/Elsevier, 1990.