MA-53G INTRODUCCION A LA CRIPTOGRAFIA

(10 UD)

Requisitos

Algebra (MA 11A), Probabilidad y Procesos Estocásticos (MA 34A), Modelos Matemáticos Discretos (MA 30A) o Fundamentos de Ciencias de la Computación (CC 30B), o autorización del profesor.

Es recomendable cierta familiaridad con técnicas de análisis de algoritmos, teoría de la complejidad computacional, y madurez matemática.

Objetivos

Estudiar y discutir las nociones fundamentales de la criptografía moderna, los principios matemáticos en que se sustenta y sus aplicaciones.

Programa

El énfasis de la criptografía ha sido, clasicamente, el estudio de las formas de establecer comunicaciones privadas entre individuos bajo la presencia de adversarios maliciosos. Los avances tecnológicos relacionados con computación han expandido los requisitos de privacidad, los requerimientos de seguridad y el ámbito de las aplicaciones que las técnicas criptográficas deben satisfacer.

Este curso es un estudio riguroso de las técnicas de la criptografía moderna, sus fundamentos y sus aplicaciones. En particular, el programa del curso es el siguiente:

1. Introducción

   Terminología básica, elementos de teoría de la información y preliminares matemáticos.

2. Criptografía Clásica (de clave Secreta)

   - Códigos de substitución y transposición.
   - Introducción a la teoría de la información.
   - One-time pad, data encryption standard (DES), criptoanálisis diferenciable.

3. Fundamentos Teóricos de la Criptografía Moderna

   - Nociones elementales de teoría de números.
   - Teoría de cuerpos finitos.
   - Nociones básicas de la teoría de la complejidad computacional.

4. Criptografía Moderna (de clave Pública)

   - Algoritmos de clave pública: Diffie–Hellman, RSA, ElGamal, Schnorr, Rabin, Feige-Fiat-Shamir, McEliece, knapsacks, cifrado probabilista, etc.
   - Firmas Digitales.
   - Funciones Hash.
   - Protocolos para la distribución de claves, de identificación, de autentificación.

5. Tópicos

Posibles tópicos (énfasis dependerá de los intereses de los participantes en el curso):

- Primalidad y factorización.
- Generación de números pseudo-aleatorios.
- Protocolos para la compartición de secretos.
- Nula divulgación.
- Aplicaciones: Skipjack, Kerberos, secure hash algorithm (SHA), message digest algorithm (MD5), international data encryption algorithm (IDEA), pretty good privacy (PGP), privacy enhanced mail (PEM), etc.

Bibliografía

- D.R. Stinson, "Cryptography: Theory and Practice". CRC Press, 1995.
- N. Koblitz, "A course in number theory and cryptography", (segunda edición). Graduate Texts in Mathematics, vol. 114, Springer–Verlag, 1994
- C. P. Pfleeger, "Security in Computing". Prentice Hall, 1989
- B. Schneier, "Applied cryptography: protocols, algorithms, and source code in C". John Wiley & Sons, Inc., 1994.
- W. Stallings, "Network and internetwork security: principles and practice". Prentice–Hall, 1995.
- J. van Leeuwen, editor, "Algorithms and complexity". Handbook of Theoretical Computer Science, vol A, MIT Press/Elsevier, 1990.