Tópicos Selectos en Criptografía

Objetivo

Presentar descubrimientos recientes en criptografía. Aprender a leer, analizar y estudiar artículos científicos recientes y relevantes en el área de criptografía de curvas elípticas y de emparejamientos bilineales.

Descripción

El curso inicia con un análisis y recuento de las primitivas usadas en criptografía, seguido por una discusión de los esquemas que han sido propuestos recientemente para realizar criptografía simétrica y de clave pública.
El curso está dirigido a estudiantes de Maestría y de Doctorado con interés especial en criptografía.

Contenido

1. Marco Teórico
a. Funciones de un solo sentido
b. Funciones y permutaciones seudo-aleatorias
c. Generadores seudo-aleatorios.

2. Criptografía de clave simétrica
a. Nociones y definiciones de seguridad
b. Modos de operación en cifradores por bloque
c. Códigos de autenticación de mensajes

3. Criptografía de la clave pública
a. RSA-OAEP
b. El problema del logaritmo discreto e hipótesis de Diffie Hellman

4. Criptografía de curvas elípticas
a. Preliminares matemáticos
b. Introducción a curvas elípticas
c. Aritmética de curvas elípticas
d. Curvas con endomorfismo que pueden calcularse eficientemente.

5. Criptografía basada en emparejamientos
a. Conceptos básicos
b. Protocolos
c. Emparejamiento de Tate.
d. Cómputo eficiente de emparejamiento de Tate

Bibliografía

a. Roberto M. Avanzi, Henri Cohen, Christophe Doche, Gerhard Frey, Tanja Lange, Kim Nguyen, Goldreich: Foundations of Cryptography. Cambridge University Press, 2004

b. Darrel Hankerson, Alfred Menezes, and Scott Vanstone. Guide to Elliptic Cryptography. Springer-Verlag, New York, 2004.
c. Michael George Luby: Pseudorandomness and Cryptographic Applications. Princeton University Press, 1996.
d. Menezes, P. van Oorschot, S. Vanstone: Handbook of Applied Cryptography, CRC Press, Boca Raton, 1996
e. D. Stinson: Cryptography-Theory and Practice, CRC Press, 2006
f. Frederik Vercauteren. Handbook of Elliptic and Hyperelliptic Curve Cryptography Champan & Hall/CRC, 2005.
g. Lawrence C. Washington Elliptic Curves: Number Theory and Cryptography, Second Edition (Discrete Mathematics and Its Applications). Chapman & Hall/CRC; 2 edition (April 3, 2008).