CRIPTOGRAFÍA

DANIEL MACÍAS CASTILLO

1. Objetivos para el curso

En este curso presentamos algunas de las técnicas matemáticas empleadas en criptografía de clave pública, con especial énfasis en las aplicaciones criptográficas de curvas elípticas. Clásicamente, estos incluyen el uso de curvas elípticas en la factorización y pruebas de primalidad (útil para RSA) y criptosistemas basados en el problema de logaritmo discreto para curvas elípticas (dos ejemplos: el cifrado de mensajes de Whatsapp y la seguridad de Bitcoin). Nuestro plan es cubrir también las aplicaciones más recientes, como el uso de los emparejamientos de Weil y Tate para la criptografía basada en la identidad o las propuestas para usar isogenias de curvas elípticas supersingulares en la criptografía poscuántica.

2. Contenidos del programa

1. Introducción.
   - Motivación y ejemplos.
   - Algoritmos de encriptación simples.
   - Teoría de grupos elemental y teoría de números. Cuerpos finitos.
2. El criptosistema RSA.
   - Algoritmo, ejemplos y precauciones.
   - Ataques a sistemas criptográficos, en particular RSA.
   - Pruebas de primalidad y algoritmos de factorización.
3. Problema del logaritmo discreto.
   - Enunciado y ejemplos.
   - Ataques básicos
   - Intercambio de claves de Diffie-Hellman.
   - El criptosistema de ElGamal.
   - Ataques genéricos y dependientes del grupo para el problema de logaritmo discreto.
4. Aplicaciones de curvas elípticas a la criptografía de clave pública.
   - Curvas elípticas y ley de grupo.
   - La versión elíptica del problema de logaritmo discreto.
   - Algoritmo de firma digital con curva elíptica (ECDSA).

- Aplicaciones de las curvas elípticas a la factorización y pruebas de primalidad.
- Emparejamientos y criptografía.

5. Criptografía poscuántica.
   - Algoritmo de Shor.
   - Criptografía basada en códigos.
   - Diffie-Hellman con Isogenias supersingulares (SIDH).

El tiempo dedicado a cada capítulo dependerá de los intereses y conocimientos previos de los estudiantes.

Referencias de consulta

[1] D. J. Bernstein, J. Buchmann, E. Dahmen (Eds.), Post-quantum cryptography, Springer, 2009.
[2] I. F. Blake, G. Seroussi, N. P. Smart, Elliptic curves in cryptography, LMS Lecture Note Series, 265, CUP, 2000.
[3] H. Cohen, G. Frey, Handbook of elliptic and hyperelliptic curve cryptography, Chapman & Hall/CRC, 2005.
[4] L. De Feo, Mathematics of isogeny based cryptography, Lecture notes, EMA, 2017. Available at https://arxiv.org/abs/1711.04062
[5] S. D. Galbraith, Mathematics of Public Key Cryptography, CUP 2012. Available at https://www.math.auckland.ac.nz/ sgal018/crypto-book/crypto-book.html
[6] D. Hankerson, A. J. Menezes, S. Vanstone, Guide to Elliptic Curve Cryptography, Springer, 2004.
[7] N. Koblitz, A course in number theory and cryptography, 2nd ed., Springer, 1994.
[8] H. W. Lenstra, Factoring integers with elliptic curves, Ann. of Math. (2) 126 (1987) 649-673.
[9] J. Menezes, P. C. Van Oorschot, S. A. Vanstone, Handbook of applied cryptography, CRC Press, 2001. Available at https://cacr.uwaterloo.ca/hac
[10] R. Overbeck, R. Sendrier, Code-based cryptography, in Post-quantum cryptography, D. J. Bernstein, J. Buchmann, E. Dahmen (Eds.), Springer, 2009.
[11] N. P. Smart, Cryptography: An Introduction, Available at https://www.cs.umd.edu/ waa/414-F11/IntroToCrypto.pdf
[12] D. R. Stinson, Cryptography theory and practice, 3rd Ed., Chapman & Hall/CRC, 2006.