Códigos y Criptografía

Objetivo

El alumno aprenderá algoritmos de criptografía de clave secreta. Se abordarán las bases matemáticas, la seguridad demostrable, las implementaciones eficientes y seguras tanto en software como en hardware, así como los ataques y protecciones

Requisitos: Deseable conocimiento de álgebra moderna, probabilidad y variables aleatorias.

Contenido

1. Antecedentes matemáticos
    a. Conjuntos
    b. Grupos
    c. Semigrupos
    d. Anillos
    e. Campos
2. Criptosistemas clásicos
    a. Cifrado por sustitución
    b. Cifrado de César
    c. Cifrado Afín
    d. Ataques
3. Funciones y permutaciones
    a. Funciones y permutaciones aleatorias
    b. Funciones y permutaciones pseudo-aleatorias
4. Cifradores por bloque
    1.1. Seguridad
    1.2. Redes de Feistel
        1.2.1. DES
        1.2.2. Simon y Speck
    1.3. Redes de sustituciones y permutaciones
        1.3.1. AES
        1.3.2. Present y Gift
    1.4. Modos de operación clásicos (privacidad)
5. Cifradores por flujo de datos
    1.1 Seguridad
    1.2 Generadores de números aleatorios
    1.3 Registros de corrimiento con retroalimentación
        i. Trivium y Grain
    1.4 RC4
    1.5 Salsa20
6. Funciones hash
    a. Seguridad
    b. Construcción de Merkle-Damgard
    c. Estándares de hash: sha1 y sha2
    d. Permutaciones públicas (Funciones esponja)
        i. Keccak (sha3)
7. Códigos de autenticación de mensajes
    a. Seguridad
    b. Basados en funciones hash

        i. HMAC
    c. Basados en cifradores por bloque
        i. Funciones hash universales
        ii. GMAC
        iii. CBCMAC
        iv. PMAC
    d. Basados en funciones esponja
8. Cifrado autenticado
    a. Seguridad
    b. Basados en cifradores por bloque
        a. OCB
        b. GCM
        c. LOCUS y LOTUS
        d. SIV y ESTATE
        e. ElmD, COPA y COLM
    c. Basados en cifradores por flujo de datos
        a. Trivia-ck
        b. Acorn
    d. Basados en funciones esponja
        a. ASCON
        b. Oribatida

Bibliografía

1. Elena Andreeva, Andrey Bogdanov, Nilanjan Datta, Atul Luykx, Bart Mennink, Mridul Nandi, Elmar Tischhauser and Kan Yasuda. COLM v1. Final portfolio CAESAR Competition. September 15, 2016. Available online: https://competitions.cr.yp.to/round3/colmv1.pdf (Accessed 9th February 2021).
2. Mihir Bellare and Phillipe Rogaway. Introduction to Modern Cryptography. Available online:https://www.cs.ucdavis.edu/~rogaway/classes/227/fall03/book/toc.pdf (accessed February 3, 2021)
3. Guido Bertoni, Joan Daemen, Michaël Peeters and Gilles Van Asshe. The Keccak Reference. 2011. Available online: https://keccak.team/files/Keccak-reference-3.0.pdf (accessed 9th February 2021).
4. Arghya Bhattacharjee, Eik List, Cuauhtemoc Mancillas-López and Mridul Nandi. The Oribatida Family of Lightweight Authenticated Encryption Schemes. Submission to the NIST Lightweight Competition. September 27, 2019. Available online: https://csrc.nist.gov/CSRC/media/Projects/lightweight-cryptography/documents/round-2/spec-doc-rnd2/oribatida-spec-round2.pdf (Accessed February 9, 2021).
5. Avik Chakraborti, Nilanjan Datta, Ashwin Jha, Cuauhtemoc Mancillas-López, Mridul Nandi and Yu Sasaki. ESTATE: A Lightweight and Low Energy Authenticated Encryption Mode. IACR Transaction on Symetric Cryptology, Vol. 2020, Special Issue 1, pp. 350-389. 2020. doi:10.13154/tosc.v2020.iS1.350-389
6. Avik Chakraborti, Nilanjan Datta, Ashwin Jha, Cuauhtemoc Mancillas-López, Mridul Nandi and Yu Sasaki. INT-RUP Secure Lightweight Parallel AE Modes. IACR Transactions on Symmetric Cryptology, Vol. 2019, No. 4, pp. 81-118. 2019. doi:10.13154/tosc.v2019.i4.81-118

7. Avik Chakraborty and Mridul Nandi. Trivia-ck-v2. Second Round CAESAR Competition. August 28, 2015. Available online: https://competitions.cr.yp.to/round2/triviackv2.pdf (Accessed February 9, 2021).
8. Joan Daemen and Vincent Rijmen. The Design of Rijndael, The Advanced Encryption Standard (AES). Second Edition, Springer, 2020. doi: 10.1007/978-3-662-60769-5
9. Christoph Dobraunig, Maria Eichlseder, Florian Mendel, Martin Schläffer. Ascon v1.2. Final portfolio CAESAR Competition. September 15, 2016. Available online: https://competitions.cr.yp.to/round3/asconv12.pdf (Accessed February 9, 2021)
10. Christof Paar and Jan Pelzl. Understanding Cryptography: A Textbook for Students and Practitioners.
11. Springer, 2009. doi:10.1007/978-3-642-04101-3
12. Matthew Robshaw and Olivier Billet Editors. New Stream Cipher Designs, The eSTREAM Finalists. Springer, 2008. doi:10.1007/978-3-540-68351-3
13. Phillip Rogaway. Efficient Instantiations of Tweakable Blockciphers and Refinements to Modes OCB and PMAC. Advances in Cryptology - {ASIACRYPT} 2004, 10th International Conference on the Theory and Application of Cryptology and Information Security, Jeju Island, Korea, December 5-9, 2004, Proceedings. Lecture Notes in Computer Science, Vol. 3329, pp. 16-31. Springer 2004.
14. Phillip Rogaway and Thomas Shrimpton. A Provable-Security Treatment of the Key-Wrap Problem. Advances in Cryptology – EUROCRYPT 2006, 25th Annual International Conference on the Theory and Applications of Cryptographic Techniques, St. Petersburg, Russia, May 28 - June 1, 2006, Proceedings. Lecture Notes in Computer Science, Vol. 4004, pp. 373-390, Springer, 2006. doi:10.1007/11761679_23
15. Kazuo Sakiyama, Yu Sasaki and Yang Li. Security of Block Ciphers: From Algorithm Design to Hardware Implementation. John Wiley & Sons. 2015. doi: 10.1002/9781118660027
16. Victor Shoup. A Computational Introduction to Number Theory and Algebra. Cambridge University Press. 2005. doi:10.1017/CBO9781139165464
17. Douglas R. Stinson and Maura B. Paterson. Cryptography Theory and Practice (4th edition). Chapman and Hall/CRC. 2018.
18. Hongjun Wu. ACORN: A Lightweight Authenticated Cipher (v3). Final portfolio CAESAR Competition. September 15, 2016. Available online:
19. https://competitions.cr.yp.to/round3/acornv3.pdf (Accessed February 9, 2021).