Iniciació a la Criptografia

Artur Travesa

(versió 2024-07)

Referències

[Co-93] Cohen, H.: *A Course in Computational Algebraic Number Theory*. Springer-Verlag, GTM 138. Berlin, Heidelberg, 1993. ISBN: 3-540-55640-0.

[D-H] Diffie, W.; Hellman, M.E.: New directions in cryptography. *IEEE Transactions on Information Theory*, **22** (1976), p. 644- 654.

[DS-S] FIPS PUB 186-4: Digital Signature Standard (DSS). *Federal Information Processing Standards Publication.* National Institute of Standards and Technology, 2013.

[ElGamal] ElGamal, T.: A Public-Key Cryptosystem and a Signature Scheme Based on Discrete Logarithms. *IEEE Transactions on Information Theory*, **31** (1985), p. 469-472.

[RSA] Rivest, R.L.; Shamir, A.; Adleman, L.: A method for obtaining digital signatures and public-key cryptosystems. *Communications of the ACM* **21** (1978), p. 120-126. (Received April 4, 1977; revised, September 1, 1977.)

[RSA-S] Jonsson, J.; Kaliski, B.: RFC 3447. *Public-Key Cryptography Standards (PKCS) #1: RSA Cryptography Specifications*, Version 2.1. RSA Laboratories, February 2003.

[Tr-Ar] Travesa, A.: *Aritmètica.* Edicions de la Universitat de Barelona, col·lecció UB, n. 25. Barcelona, 1998. ISBN:84-8338-031-5.

[Tr-Cr]: Travesa, A.: *Iniciació a la Criptografia*. Accessible en format de llibreta de *SageMath* i en fromat pdf des de https://travesa.cat/notes.html (https://travesa.cat/notes.html)

[Tr-PrF] Travesa, A.: *Primeritat i Factorització. Accessible en format de llibreta de SageMath i en format pdf des de https://travesa.cat/notes.html (https://travesa.cat/notes.html)*

Fi de les Referències