Tema: Firma Digital usando clave pública con criptografía

Hugo Sepulveda - Camilo Núñez

1 Resumen

La firma digital es un proceso que garantiza que el contenido de un mensaje no haya sido alterado durante su envio. Cuando se firma digitalmente un documento, se agrega un hash unidireccional (cifrado) del contenido del mensaje utilizando un par de claves pública y privada. El cliente puede leerlo, pero el proceso crea una "firma" que solo la clave pública del firmante puede descifrar. El cliente, utilizando la clave pública del firmante, puede validar al remitente, así como la integridad del contenido del mensaje.

2 Bibliografía

- Kaijser P. (1999) On Authentication, Digital Signatures and Signature Laws. In: Preneel B. (eds) Secure Information Networks. IFIP — The International Federation for Information Processing, vol 23. Springer, Boston, MA
- F. J. Aufa, Endroyono and A. Affandi, "Security System Analysis in Combination Method: RSA Encryption and Digital Signature Algorithm," 2018 4th International Conference on Science and Technology (ICST), Yogyakarta, 2018, pp. 1-5. doi: 10.1109/ICSTC.2018.8528584
- T. Hwang, Y. Luo, P. Gope and Z. Liu, "Forward/Backward Unforgeable Digital Signature Scheme Using Symmetric-Key Crypto-System," 2016 International Computer Symposium (ICS), Chiayi, 2016, pp. 244-247. doi: 10.1109/ICS.2016.0056
- Feng Bao, Cheng-Chi Lee, Min-Shiang Hwang, Cryptanalysis and improvement on batch verifying multiple RSA digital signatures, Applied Mathematics and Computation, Volume 172, Issue 2, 2006, Pages 1195-1200, ISSN 0096-3003, https://doi.org/10.1016/j.amc.2005.03.016.
- Iuon-Chang Lin, Chin-Chen Chang, Security enhancement for digital signature schemes with fault tolerance in RSA, Information Sciences, Volume 177, Issue 19, 2007, Pages 4031-4039, ISSN 0020-0255, https://doi.org/10.1016/j.ins.2007.03.035.

- Hartini Saripan, Zaiton Hamin, The application of the digital signature law in securing internet banking: Some preliminary evidence from Malaysia, Procedia Computer Science, Volume 3, 2011, Pages 248-253, ISSN 1877-0509, https://doi.org/10.1016/j.procs.2010.12.042.
- Jae Hong Seo, Efficient digital signatures from RSA without random oracles, Information Sciences, Volume 512, 2020, Pages 471-480, ISSN 0020-0255, https://doi.org/10.1016/j.ins.2019.09.084.
- Serious Cryptography A Practical Introduction to Modern Encryption by Jean-Philippe Aumasson November 2017, 312 pp. ISBN-13: 978-1-59327-826-7
- Understanding Cryptography: A Textbook for Students and Practitioners
- Cryptography and Network Security: Principles and Practice, Sixth Edition.