IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.301
Volume 3, Issue 1, June 2023

Cryptography Machine for Encryption and Decryption

Om Gautam, Aditya Sabale, Harshal Sawant, Prof. A.Y. Kadam
Department of Information Technology
Smt. Kashibai Navale College of Engineering, Pune, India

Abstract: *Computers are most valuable when they are used to solve problems that humans cannot easily solve for themselves. Charles Babbage, for example, wanted to automate the production of mathematical tables, partly because it was a tedious task, but mostly because the people who undertook the necessary calculations made so many mistakes. Computers, however, are also useful when they solve problems faster than human beings. If you face a situation in which timeliness is essential, you may not be able to wait for results generated at human speeds. In such cases, it may be necessary to develop a technological solution to get the answers you need when you need them. In World War II, the Allies faced precisely this situation. The shipping lanes of the North Atlantic were under such threat from German U-boats that Britain was in danger of being starved into submission. Breaking the U-boat code was a critical turning point in the war and may have changed its outcome. Faced with a code that changed every day, the British had to develop mechanical tools that would allow them to read German military dispatches quickly enough to act on that information. Breaking the German military codes was an early application of cryptography, which is the science of creating and decoding messages whose meaning cannot be understood by those who intercept the message. In the language of cryptography, the message you are trying to send is called the plaintext; the message you actually send is called the ciphertext. Unless your adversaries know the secret of the encoding system, which is usually embodied in some privileged piece of information called a key, intercepting the ciphertext should not make it possible for them to discover the original plaintext version of the message. On the other hand, the recipient, who is presumably in possession of the key, can easily translate the ciphertext back into its plaintext counterpart. Cryptographic Hash functions are used to achieve a number of security objectives. In this paper, we bring out the importance of hash functions, its various structures, design techniques, attacks and the progressive recent development in this field.*

Keywords: Cryptography, Hash function, compression function

REFERENCES

[1]. D. Kahn,TheCodebreakers: The Comprehensive History of Secret Communication from Ancient Times to the Internet, Scribner, 1996.
[2]. W. Diffie, and M. Hellman, “New Directions in Cryptography”,IEEE Transactions on Information Theory, vol. 22, No. 6, 1976, pp. 644-654.
[3]. B. V. Rompay, “Analysis and Design of Cryptographic Hash functions, MAC algorithms and Block Ciphers”, Ph.D. thesis, Electrical Engineering Department, KatholiekeUniversiteit, Leuven, Belgium, 2004.
[4]. FIPS 180, Secure Hash Standard (SHS), National Institute of Standardsand Technology, US Department of Commerce, WashingtonD. C., 1993.
[5]. FIPS 180-1, Secure Hash Standard (SHS), National Institute of Standards and Technology, US Department of Commerce, WashingtonD. C.,1995.
[6]. FIPS 180-2, Secure Hash Standard (SHS), National Institute of Standards and Technology, US Department of Commerce, WashingtonD. C.,2002.
[7]. FIPS 197, Advanced Encryption Standard, National Institute of Standards and Technology, US Department of Commerce, WashingtonD. C.,2001.

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.301
Volume 3, Issue 1, June 2023

[8]. FIPS180-3, Secure Hash Standard (SHS), National Institute of Standards and Technology, US Department of Commerce, Washington D. C., 2008.
[9]. R. Rivest, "The MD4 Message Digest Algorithm", IETF RFC 1320, 1992.
[10]. R. Rivest, "The MD5 Message Digest Algorithm", IETF RFC 1321, 1992.
[11]. S. Lucks, "Design Principled for Iterated Hash Functions", in IACR Cryptology ePrint Archive, 2004, pp. 253.
[12]. G. Bertoni, J.Daemen, M. Peeters, and G. Van Assche, "Cryptographic Sponges", [online] http://sponge.noekeon.org/.
[13]. National Institute of Standard and Technology (NIST): Cryptographic Hash Algorithm Competition. [online] http://csrc.nist.gov/groups/ST/hash/sha-3/
[14]. [46]G. Bertoni, J. Daemen, M. Peeters, and G. V. Assche, "The Keccak Reference", Submission to NIST (Round 3),2011.[online] http://csrc.nist.gov/groups/ST/hash/sha-3/Round3/submissions_rnd3.html.
[15]. B.den Boer, and A. Bosselaers, "Collisions for the compression function of MD5", in EUROCRYPT, 1993, pp. 293-304.
[16]. L. Knudsen. "Block Ciphers: Analysis, Design and Applications", Ph.D.thesis, Aarhus University, Aarhus,
[17]. Denmark, 1994
[18]. O. Mikle, "Practical Attacks on Digital Signatures Using MD5 Message Digest", IACR Cryptology ePrint Archive, 2004, pp.356.
[19]. H. Dobbertin, "Cryptanalysis of MD5 compress", inEUROCRYPT, 1996
[20]. KUL15-RMC- 1.0, private communications, 2006.
[21]. E. Andreeva, G. Neven, B. Preneel, and T. Shrimpton, "Seven-Property-Preserving Iterated Hashing: ROX", IACR Cryptology ePrint Archive, 2007, pp.176.
[22]. M. Bellare, and T. Ristenpart, "Multi-Property- Preserving Hash Domain Extension and the EMD Transform", in ASIACRYPT, 2006, pp.299-314 .
[23]. T. Duong, and J. Rizzo, "Flickr's API Signature Forgery Vulnerability", 2009 [online] http://netifera.com/research/flickr_api_signature_forgery.pdf
[24]. B. Kaliski, and M. Robshaw. "Message Authentication with MD5". RSA Labs' CryptoBytes, Vol. 1, No. 1, Spring 1991.