Analyzing Digital Signature Robustness with Message Digest Algorithms

Abstract

A hash function is a deterministic procedure that takes an arbitrary block of data and returns a fixed-size bit string, called the message digest, such that any change to the data will change the digest value. The message digest are being extensively used for digital signature for online transactions. In this paper we have analyzed the robustness of various message digest with respect to digital signature. The repetitive sequences in the digest will decrease the robustness of the message digest as it can lead to same message digest for differing message blocks. In this paper the robustness of message digest is analyzed with respect to sequence repetitions as digest with more repetitive sequence are more likely or have increased probability of generating the same digest for differing message blocks. We have analyzed the robustness of various popular message digest algorithms such as MD5, SHA1, RIEMD160, PANAMA, and TIGER.
References

- Curry, Ian March 2001 An Introduction to Cryptography and Digital Signatures. Version 2.0
- Rompay, Bart Van, June 2004. Analysis and Design of Cryptographic Hash functions, Mac algorithms and Block ciphers”
- http://www.quadibloc.com/crypto/co4821.htm
- Ross, Anderson and Eli, Biham, Tiger: A Fast new hash function” by

Index Terms

Computer Science

Keywords

Message Digest  Hash function  Digital Signature  Secure communication  Information security