Abstract

SHA-1 is a widely used cryptographic hashing algorithm for validating the integrity of data. Until recently, SHA-1 was considered to be the most secure hashing algorithm and also remains the most widely used hashing function till date. In this paper, we review various collision search attacks on the original full 80-step SHA-1 algorithm and present a new optimized version of the algorithm that reduces the chance of collision and increases the theoretical lower bound of the time complexity required to detect such a collision by an exponential factor of 2.

References

5. Mieliestronk's list of more than 58 000 English words: http://www.mieliestronk.com/wordlist.html.

Index Terms

Computer Science Security

Keywords

SHA-1, SHA-0, Hash Functions, Collision Search Attacks, Improvements in SHA-1