Abstract

It is well known that Hash algorithm works in one way, and it cannot be reversed. We can build a new algorithm by using Hill cipher technique. Since its invention in 1929, Hill cipher algorithm which is one of the most famous symmetric cryptosystems. Hill cipher requires the inverse of the key matrix for decryption. This inverse not always exists, so we can use non-invertible matrices to propose a model for our new hash algorithm, and we proof the four requirements
that needed to design a practical one way hash algorithm.

Reference

- DaniloGligoroski†, Smile Markovski†† and Svein J. Knapskog†(2006):"A Secure Hash Algorithm with only 8 Folded SHA-1 Steps", IJCSNS International Journal of 194 Computer Science and Network Security, VOL:6 No.10
- Johannes Mittmann, (may ,2005): “One-Way Encryption and Message Authentication“.
- Murray Eisenber ( 1999): “Hill Ciphers and Modular Linear Algebra”.
Index Terms

Computer Science  Security

Key words

Hill cipher technique  Non-invertible matrix  hash
algorithm

One-way hash function

plaintext

integrity