Abstract

In this paper, we describe non invertible matrix in GF(2) which can be used as multiplication matrix in Hill Cipher technique for one way hash algorithm. The matrices proposed are permutation matrices with exactly one entry 1 in each row and each column and 0 elsewhere. Such matrices represent a permutation of m elements. Since the invention, Hill cipher algorithm was used for symmetric encryption, where the multiplication matrix is the key. The Hill cipher requires the inverse of the matrix to recover the plaintext from cipher text. We propose a class of matrices in GF(2) which are non invertible and easy to generate.

References

- Zhang, Fuzhen. Matrix Theory. s. l. : Springer, 2011.
- Thoma H. Cormen, Charles E. Leiserson, Ronald L. Rivest, Clifford Stein. Introduction To Algorithms. s. l. : MIT Press, 2001.
- Knuth, Donald. The Art Of Computer Programming. Boston : Addison-Wesley, 1998.
Index Terms

Computer Science | Algorithms

Keywords

Hill cipher technique  Non-invertible matrix  Galois field GF(2)  hash algorithm
One-way hash function
plaintext
integrity