Journal of Systems Science and Complexity 1994 7 (2): 128-132 ISSN: 1000-0577 CN: 11-2019/O1

论文

DIFFERENTIAL CRYPTANALYSIS OF A SIMPLE BLOCK CIPHER

YANG Junhui

Computing Center, Academia Sinica, Beijing 100080, China

收稿日期 修回日期 网络版发布日期 接受日期

摘要 The method of differential cryptanalysis is applied to solve a DES type block cipher with a particularly simple confusion function.

关键词 DES, differential cryptanalysis

分类号

DIFFERENTIAL CRYPTANALYSIS OF A SIMPLE BLOCK CIPHER

YANG Junhui

Computing Center, Academia Sinica, Beijing 100080, China

Abstract The method of differential cryptanalysis is applied to solve a DES type block cipher with a particularly simple confusion function.

Key words DES differential cryptanalysis

DOI:

通讯作者