On Security Properties of RC5 Cipher's Non Standard Modifications

Tytuł
On Security Properties of RC5 Cipher's Non Standard Modifications

Typ publikacji
Artykuł

Rok
2017

Data dokładna

Autorzy słownie
Kurkowski Mirosław

Autorzy
Kozakiewicz Adam

ISBN/ISSN
ISSN: 2450–9302

Informacje dodatkowe
Mathematics XXI Scientific Issues of Jan Długosz University, Cz. 21; str. 115-122.

DOI:10.16926/m.2016.21.10

Abstract: The RC5 algorithm is the cipher from the family of symmetric ciphers created by Ronald Rivest. Unlike other encryption algorithms, RC5 is designed this way, that a user or a security system architect can change some of its parameters. RC5 is a block cipher processing cipher-text blocks in the sequential rounds, where input of each round is the output of the previous one. In each round data is processed with usage of the key. The parameters of the cipher that can be changed are following:

length of the key, length of the processed block and number of rounds. These parameters should be chosen based on the required level of security of communication. However there are such structures in RC5 that use of them is not entirely clear from the point of view for algorithm’s security. The aim of this paper is to examine how a cryptographic power of the cipher is affected by modifications to these structures.For this purpose will be used the well-known NIST tests.

Powiązane publikacje

-

Adres url strony

http://dlibra.bg.ajd.czest.pl:8080/dlibra/docmetadata?id=4016&from=publication

Plik