ОБОЗРЕНИЕ
ПРИКЛАДНОЙ И ПРОМЫШЛЕННОЙ
Том 27 МАТЕМАТИКИ Выпуск 2
2020

А. В. Анашкин (Москва, Лаб. ТВП)**. О контрольном примере стандарта ГОСТ Р 34.12-2015.**

УДК 519.719.2 DOI https://doi.org/10.52513/08698325_2020_27_2_133

Резюме: Контрольный пример из ГОСТ Р 34.12-2015, в основе которого лежит алгоритм «Магма» блочного шифрования в режиме простой замены, задействует не все переходы каждой из восьми подстановок этого алгоритма. Между тем, в рамках вероятностной модели для анализа числа задействованных переходов установлено, что при том же значении ключа вероятность задействования всех переходов далеко не нулевая, и методом случайного поиска соответствующие примеры найдены.

Ключевые слова: ГОСТ 28147-89, ГОСТ Р 34.12-2015, алгоритм шифрования «Магма», блочный шифр, контрольный пример ГОСТ Р 34.12-2015, переходы в подстановках алгоритма «Магма».

СПИСОК ЛИТЕРАТУРЫ

1. *Федеральное агентство по техническому регулированию и метрологии.* Национальный стандарт Российской Федерации ГОСТ Р 34.12-2015. Информационная технология «Криптографическая защита информации». Блочные шифры. Издание официальное. М.: Стандартинформ, 2015, 25 с.// *Federal Agency on Technical Regulating and Metrology. Russian Federation,* National Standard of the Russian Federation GOST R 34.12-2015. Information Technology “Cryptographic Data Security”. Block Ciphers. Official Release. Moscow: Standardinform, 2015, 25 p. (In Russian.)
2. *Государственный комитет СССР по стандартам.* ГОСТ 28147-89. Системы обработки информации. Защита криптографическая. Алгоритм криптографического преобразования. Издание официальное. М.: ИПК Издательство стандартов, 1996, 26 с.// *USSR State Committee for Standards.* GOST 28147-89. Information Processing Systems. Cryptographic Protection. Cryptographic transformation algorithm. Official Release. Moscow: IPK Standardinform, 1996, 26 p. (In Russian.)

UDC 519.719.2 DOI https://doi.org/10.52513/08698325_2020_27_2_133

Anashkin A. V. (Moscow, TVP Laboratories)**. On the testing example in the GOST R 34.12-2015 encryption standard.**

Abstract: In the testing example from GOST R 34.12-2015, which is based on the algorithm MAGMA of block encryption in ordinary replacement mode, not all transitions are possible in each of the eight substitutions of this algorithm. Meanwhile, within the framework of a probabilistic model for analysis of the number of these transitions it is established that the probability of involving all transitions is far from zero with the same key. By means of random search relevant examples have been found then.

Keywords: GOST 28147-89, GOST R 34.12-2015, block cipher, MAGMA encryption algorithm, testing example of GOST R 34.12-2015, transitions of substitutions in MAGMA algorithm.