ИССЛЕДОВАНИЕ КРИПТОСТОЙКОСТИ АЛГОРИТМОВ СИММЕТРИЧНОГО ТИПА

А.М. Тимофеев[1], А.Н. Шишпаренок[2], В.Е. Юруть[2]

[1]*Учреждение образования «Белорусский государственный университет информатики и радиоэлектроники», Минск, Беларусь*
[2]*Учреждение образования «Национальный детский технопарк», Минск, Беларусь*

При разработке криптографических систем связи симметричного типа, обеспечивающих конфиденциальность передаваемой информации, одной из наиболее важных задач является оценка криптостойкости таких систем [1]. В этой связи целесообразно создавать программное обеспечение для оценки криптостойкости криптографических систем связи симметричного типа, что являлось целью данной работы. Создана компьютерная программа, которая реализует криптографические алгоритмы симметричного типа и процедуры их криптоанализа. Компьютерная программа написана на языке программирования Rust с использованием библиотек bitvec, itertools, tokio, tracing, thiserror и rayon [2, 3]. Пользовательская часть программы выполнена в виде набора подпрограмм, предусматривающих возможность выбора исследуемого алгоритма, режима его функционирования и экстраполяции полученных результатов для оценки достаточно высокой криптостойкости (10 и более лет). Выполнены исследования по оценке криптостойкости алгоритмов симметричного типа.

Список литературы

1. Бабенко, Л. К. Криптографическая защита информации: симметричное шифрование / Л. К. Бабенко. – М., Издательство Юрайт, 2020.

2. Blandy, J. Programming Rust / J. Blandy. – Sebastopol, Ca: O'Reilly Media, 2021.

3. Klabnik, S. The Rust Programming Language / S. Klabnik. – San Francisco, Starch Press, 2021.