УДК 519.72

КРИПТОАНАЛИЗ ШИФРОВ С КЛЮЧАМИ НА ОСНОВЕ ЛИНЕЙНОГО КОНГРУЭНТНОГО ГЕНЕРАТОРА

Д. С. Кондрашова[1]

Самарский национальный исследовательский университет имени академика С.П. Королева, г. Самара, Российская Федерация

Научный руководитель: В. В. Севостьянова, к ф.-м.н., доцент

Самарский национальный исследовательский университет имени академика С.П. Королева, г. Самара, Российская Федерация

Ключевые слова: Линейный конгруэнтный генератор, обратный линейный конгруэнтный генератор

Цель работы – провести анализ криптосистемы с ключом на основе линейного конгруэнтного генератора и обратного линейного конгруэнтного генератора.

Задача – проверить возможность вскрытия линейного конгруэнтного генератора и обратного линейного конгруэнтного генератор с помощью нескольких пар открытого текста и шифротекста.

В работе даны основные понятия теории информации, описана общая модель криптосистем, рассмотрены математические модели элементарных шифров, изучены линейный конгруэнтный генератор и обратный линейный конгруэнтный генератор.

В ходе работы был рассмотрен шифр, ключ которого получается из линейной конгруэнтной последовательности и обратной линейной конгруэнтной последовательности. Было выявлено, что при большой длине открытого текста, криптоаналитик может узнать практически все об открытом тексте, на основе информации об открытом тексте и информации, которую можно получить анализом шифротекста. Такой способ построения ключа делает криптосистему крайне нестойкой, поэтому его использование не рекомендуется. А использование обратного линейного конгруэнтного генератора в качестве источника ключа значительно усложняет взлом криптосистемы, но при этом есть намеки на принцип получения ключа.

[1] Кондрашова Дарья Сергеевна, студент группы 6542-100501D, email: kondrashova_dasha@mail.ru