УДК 004.421.5

ГЕНЕРАЦИЯ КРИПТОГРАФИЧЕСКИХ КЛЮЧЕЙ НА ОСНОВЕ МОДИФИЦИРОВАННОГО АЛГОРИТМА БЛОЧНОГО ШИФРОВАНИЯ

Синюта А.А. (ИТМО)
Научный руководитель – Грозов В.А.
(ИТМО)

Введение. Современные криптографические системы играют важную роль в обеспечении информационной безопасности, защищая данные от несанкционированного доступа и обеспечивая конфиденциальность и целостность информации. Одной из важнейших задач криптографии является генерация криптографических ключей, которые должны демонстрировать высокую степень случайности и устойчивости к атакам. Существующие методы генерации ключей на основе блочных шифров имеют недостатки, такие как: предсказуемость генерируемых ключей, недостаточная производительность и уязвимость к новым формам атак. Зарубежные исследования в области криптографии активно развиваются, в частности, работы в области постквантовой криптографии (NIST PQC) демонстрируют значительный прогресс, стандартизируя алгоритмы, устойчивые к квантовым атакам [1]. В то же время отечественные разработки также активно применяются, но их модификация для задач генерации ключей требует дополнительных исследований.

Основная часть. В данной работе предлагается метод генерации криптографических ключей на основе алгоритма блочного шифрования «Кузнечик» (ГОСТ Р 34.12–2015) [2] с использованием режима гаммирования и модификацией стандартного счетчика. Основная цель предлагаемого подхода – увеличение случайности и непредсказуемости генерируемых последовательностей для повышения их устойчивости к атакам. Стандартный счетчик в режиме гаммирования представляет собой последовательные номера, что может создавать определенные уязвимости. Предлагаемое решение использует операции в поле Галуа для вычисления значений счетчика [3]. Это позволяет повысить случайность генерируемых последовательностей, поскольку использование операций в поле Галуа увеличивает сложность процесса генерации ключей, делая их менее предсказуемыми. Кроме того, повышается безопасность за счет снижения вероятности успешного криптоанализа. Для проверки эффективности разработанного алгоритма используются тесты NIST, целью которых является определение меры случайности двоичных последовательностей.

Выводы. Предложен метод генерации криптографических ключей, основанный на применении блочного шифра в режиме гаммирования с модифицированным счетчиком. Представленный способ может быть использован для модернизации существующих решений на базе отечественных стандартов шифрования.

Список использованных источников:

1. Post-Quantum Cryptography [Электронный ресурс] / NIST. — Режим доступа: https://csrc.nist.gov/projects/post-quantum-cryptography (дата обращения: 16.02.202).
2. ГОСТ Р 34.12–2015. Информационная технология. Криптографическая защита информации. Блочные шифры. – Москва: Стандартинформ, 2015. – 21 с.
3. David Johnston. Random Number Generators—Principles and Practices: A Guide for Engineers and Programmers. - Walter de Gruyter GmbH & Co KG, 2018. - 439 с.