УДК 003.26:004.056.5

Анализ и построение криптосистем с открытым ключом

Макиенков В.В. (СПБ ГЛТУ им. Кирова), Ярцева Н.А. (Университет ИТМО), Ярцев М.Д. (СПБ ГЛТУ им. Кирова)

Научный руководитель - кандидат технических наук, доцент Карманов А.Г. (Университет ИТМО)

Введение. Исследованы принципы работы и криптостойкость асимметричных криптосистем. Цель – анализ современных алгоритмов и разработка рекомендаций по их практическому применению для обеспечения конфиденциальности и аутентификации данных.

Основная часть. Проведен сравнительный анализ алгоритмов RSA, Эль-Гамаля, ECC (Elliptic Curve Cryptography) и алгоритмов на основе задачи о рюкзаке. Рассмотрены математические основы, оценена вычислительная сложность и стойкость к известным атакам. Разработана модель для оценки времени генерации ключей, шифрования и расшифрования.

Выводы. Установлено, что алгоритмы на основе эллиптических кривых (ECC) обеспечивают сопоставимую с RSA криптостойкость при значительно меньшей длине ключа, что делает их предпочтительными для систем с ограниченными ресурсами. Для большинства прикладных задач рекомендовано использование гибридных схем, сочетающих скорость симметричного шифрования и удобство асимметричного обмена ключами.

Список использованных источников

1. ГОСТ Р 34.10-2012 "Информационная технология. Криптографическая защита информации"
2. Menezes A., van Oorschot P., Vanstone S. Handbook of Applied Cryptography. – CRC Press, 1996
3. Schneier B. Applied Cryptography. – John Wiley & Sons, 2015
4. National Institute of Standards and Technology (NIST). FIPS 186-5 Digital Signature Standard (DSS). – 2023