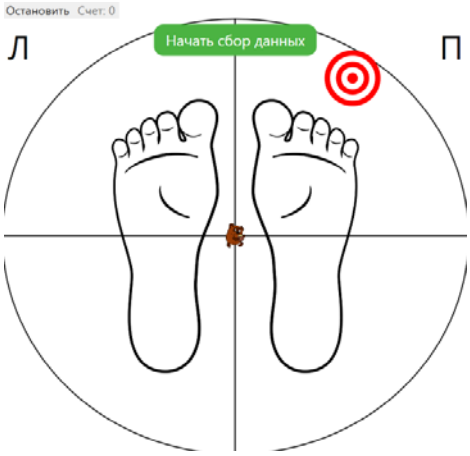

Рис. 1. Разработанная тренировка

Таким образом, в результате проведенной работы были выбраны требуемые для диагностики числовые характеристики, реализованы алгоритмы их расчета и графического представления. В дальнейшем планируется разработать несколько видов тренировок, различающихся по сложности и направленности. На основе анализа собранных данных предполагается сформировать комплекс тренировок, адаптированный под индивидуальные особенности пациента. Такой подход обеспечит персонализированную реабилитацию, направленную на восстановление функции голеностопного сустава и улучшение проприоцепции.

Литература

1. Effects of Combination of Strength and Balance Training on Postural Control and Functionality in People with Chronic Ankle Instability: A Systematic Review and Meta Analysis / A. B. S. U. Yuying [et al.], 2023.
2. Demir, A. Comparison Of Effect Of Balance Disc And Bosu Ball On Ankle Dorsiflexor And Plantarflexor Muscle Strength / A. Demir // European Journal of Physical Education and Sport Science. – 2019.

СРАВНИТЕЛЬНЫЙ АНАЛИЗ АЛГОРИТМОВ ШИФРОВАНИЯ

П. Р. Кедик, И. А. Врублевский

Белорусский государственный университет информатики и радиоэлектроники, г. Минск

Проведен комплексный сравнительный анализ двух фундаментальных классов криптографических алгоритмов – симметричных и асимметричных. Задачей ис-следования было выявление их ключевых характеристик, преимуществ и ограничений в контексте современных требований к информационной безопасности. При проведении сравнительного анализа в первую очередь учитывались такие параметры, как скорость работы и производительность, уровень криптостойкости, механизмы управления ключами, области практического применения и устойчивость к различным типам атак.

Ключевые слова: сравнительный анализ, симметричное шифрование, асимметричное шифрование, криптостойкость, производительность, управление ключами, гибридные криптосистемы, AES, RSA, ECC.

COMPARATIVE ANALYSIS OF ENCRYPTION ALGORITHMS

P. R. Kedzik, I. A. Vrublevsky

Belarusian state university of informatics and radioelectronics, Minsk

The article provides a comprehensive comparative analysis of two fundamental classes of cryptographic algorithms: symmetric and asymmetric. The research aims to identify their key characteristics, advantages, and limitations within the context of modern information security requirements. The primary focus is on comparing such parameters as operational speed and performance, the level of cryptographic strength, key management mechanisms, practical application areas, and resilience to various types of attacks.

Keywords: comparative analysis, symmetric encryption, asymmetric encryption, cryptographic strength, performance, key management, hybrid cryptosystems, AES, RSA, ECC.

Современные вызовы информационной безопасности требуют глубокого понимания криптографических методов защиты данных. Симметричные и асимметричные алгоритмы шифрования представляют собой два фундаментальных подхода к обеспечению конфиденциальности информации. Их сравнительный анализ позволяет выявить оптимальные сферы применения каждого метода. Симметричные алгоритмы характеризуются высокой скоростью работы и эффективностью при шифровании больших объемов данных. Асимметричные методы решают критически важную проблему безопасного распределения ключей. Актуальность исследования обусловлена необходимостью оптимального сочетания этих подходов в условиях их практической реализации. В статье приведен систематический анализ характеристик обоих типов шифрования с упором на сравнение производительности, криптостойкости и сложности управления ключами. На основе результатов исследований предложены рекомендации по выбору алгоритмов для эффективного решения различных прикладных задач.

Симметричные алгоритмы шифрования используют один ключ для операций шифрования и дешифрования. К наиболее распространенным алгоритмам относятся AES (Advanced Encryption Standard) с длиной ключа 128-256 бит, DES (Data Encryption Standard) и его преемник 3DES, отечественный стандарт ГОСТ 28147-89 (рис. 1).

Рис. 1. Схема симметричного алгоритма шифрования

Асимметричные алгоритмы основаны на использовании пары ключей – открытого и закрытого. Основные представители RSA (Rivest-Shamir-Adleman), эллиптические кривые ECC (Elliptic Curve Cryptography), алгоритмы Диффи-Хеллмана (рис. 2).

Рис. 2. Схема асимметричного алгоритма шифрования

Производительность: симметричные алгоритмы демонстрируют в 100–1000 раз более высокую скорость обработки данных. Например, AES показывает скорость около 1–2 Гбит/с на современном оборудовании, в то время как RSA 2048-bit – всего 5–10 Мбит/с.

Криптостойкость: асимметричные алгоритмы требуют значительно большей длины ключей для обеспечения сопоставимой стойкости. Эквивалентная стойкость достигается при AES-128 ≈ RSA-3072 и AES-256 ≈ RSA-15360.

Управление ключами: симметричные алгоритмы требуют безопасного канала для передачи ключа, что создает проблему $n(n–1)/2$ ключей для n пользователей. Асимметричные алгоритмы решают эту проблему через открытые ключи.

В реальных условиях оба типа алгоритмов используются совместно в гибридных системах: симметричное шифрование для передачи сеансового ключа и симметричное шифрование для основного обмена данными.

Такое сочетание позволяет использовать преимущества обоих подходов, таких как высокую скорость симметричного шифрования и безопасное распределение ключей асимметричных методов.

Сравнительный анализ показывает комплементарный характер двух классов алгоритмов. Оптимальный выбор зависит от конкретных требований к безопасности, производительности и масштабируемости системы. Современные реализации должны учитывать необходимость гибридного подхода для достижения максимальной эффективности защиты.

Литература

1. Тимофеев, А. М. Криптографическая защита информации : учеб.-метод. пособие / А. М. Тимофеев. – Минск : БГУИР, 2020. – 112 с.
2. Аграновский, А. В. Практическая криптография: алгоритмы и их программирование / А. В. Аграновский, Р. А. Хади. – М. : СОЛОН-Пресс, 2009. – 256 с.

ПРИНЦИПЫ ПРОЕКТИРОВАНИЯ UI-ДИЗАЙНА ДЛЯ МЕДИЦИНСКИХ ПРИЛОЖЕНИЙ НА ПРИМЕРЕ ПРОГРАММНОГО СРЕДСТВА ДИАГНОСТИКИ И КОРРЕКЦИИ ХРОНИЧЕСКОГО ПОСТИНСУЛЬТНОГО БОЛЕВОГО СИНДРОМА

А. А. Кушнер, Е. М. Косарева

Белорусский государственный университет информатики и радиоэлектроники, г. Минск

Рассмотрены принципы проектирования компонентов пользовательских интерфейсов медицинских приложений на примере диагностического приложения для врачей-неврологов.