МИНИСТЕРСТВО ОБРАЗОВАНИЯ РЕСПУБЛИКИ БЕЛАРУСЬ

Учреждение образования   
«БЕЛОРУССКИЙ ГОСУДАРСТВЕННЫЙ ТЕХНОЛОГИЧЕСКИЙ УНИВЕРСИТЕТ»

Кафедра Информационных систем и технологий

Специальность 1-98 01 03 Программное обеспечение информационной безопасности мобильных систем

**ПОЯСНИТЕЛЬНАЯ ЗАПИСКА**

**КУРСОВОГО ПРОЕКТА:**

по дисциплине «Защита информации и надежность информационных систем»

Тема: «Сравнительный анализ производительности и безопасности симметричных алгоритмов шифрования XXTEA и CAST»

Исполнитель

Студент 4 курса группы 7 Голубицкая Ю. В.

(Ф.И.О.)

Руководитель работы Сазонова Д. В. (учен. степень, звание, должность, подпись, Ф.И.О.)

Курсовой проект защищен с оценкой

Минск 2024

Оглавление

[Введение 3](#_Toc180429623)

[1. Постановка задачи 4](#_Toc180429624)

[2. Аналитический обзор литературы 5](#_Toc180429625)

# Введение

С развитием цифровых технологий и увеличением объема передаваемой информации, вопросы безопасности данных становятся все более актуальными. Шифрование информации – один из ключевых методов защиты, позволяющий предотвратить несанкционированный доступ к конфиденциальным данным. Среди множества алгоритмов шифрования особое внимание уделяется симметричным алгоритмам, которые используют один и тот же ключ как для шифрования, так и для расшифрования данных.

В данной работе будет проведен сравнительный анализ производительности и безопасности двух симметричных алгоритмов шифрования – XXTEA и CAST. Выбор этих алгоритмов обусловлен их распространенностью и различиями в подходах к шифрованию. XXTEA, являющийся усовершенствованной версией алгоритма TEA, отличается высокой скоростью работы и простотой реализации. В то же время, алгоритм CAST, разработанный с акцентом на безопасность, обеспечивает надежную защиту данных благодаря использованию различных режимов шифрования и длины ключа.

Результатом данной курсовой работы является проект, содержащий в себе реализацию двух алгоритмов, и позволяющий сравнить их по некоторым признакам.

# Постановка задачи

В рамках данного курсового проекта необходимо провести сравнительный анализ производительности и безопасности симметричных алгоритмов шифрования XXTEA и CAST. Для достижения этой цели следует рассмотреть ряд задач:

Требование к средствам разработки:

* Язык программирования JavaScript.
* Средство разработки MS Visual Studio Code.

Приложение должно:

* Приложение должно шифровать и расшифровывать текстовые сообщения.
* Выводить время, затраченное на шифрование и расшифрование, что позволит оценить производительность каждого из алгоритмов.
* Реализовать удобный интерфейс для ввода данных и отображения результатов, включая возможность выбора алгоритма шифрования.

Кроме того, необходимо сравнить результаты тестирования по производительности и безопасности, а также сформулировать выводы о том, какой из алгоритмов лучше подходит для определенных условий и задач.

# Аналитический обзор литературы