БЕЛОРУССКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ

ФАКУЛЬТЕТ ПРИКЛАДНОЙ МАТЕМАТИКИ И ИНФОРМАТИКИ

Кафедра технологий программирования

Аннотация к дипломной работе

«Реализация разделения секрета в защищенной информационной системе»

Аль-юсефи Али Ганем

Научный руководитель — канд. физ.-мат. наук, доцент кафедры ТП
Горячкин В. В.

Минск, 2021

Реферат

Дипломная работа, 59 с., 39 рис., 2 таблицы, 6 приложений.

Ключевые слова: REST, HTTP, SPRING, KOTLIN

Объект исследования — объектом исследования схемы разделения секрета в защищенной информационной системе является реализация возможностей для разделения секрета и его восстановление, а также технологии разработки на языке Kotlin. Для разработки и исследования характеристик объекта исследования необходимо построить соответствующую информационную систему. В данной работе информационная система построена с использованием фреймворка Spring.

Цели работы — рассмотреть методы для разделения секрета, а также спроектировать приложение для решения задачи разделения секрета на основе схемы разделения секрета Шамира.

Методы исследования — а) теоретические: изучение литературы, посвящённой проблеме разделения секрета; б) практические: моделирование, проектирование спецификации и разработка информационной системы с помощью языка Kotlin.

Результатами являются — информационная система для решения задач разделения секрета с использованием дополненных этапов алгоритма.

Область применения — разработка новых протоколов аутентификации и хранения секретных данных в учебных, а также производственных целях.

Abstract

Bachelor Thesis, 59 pages, 39 images, 2 tables, 6 attachments.

Key words: REST, HTTP, SPRING, KOTLIN

Object of study — The object of the research is the schemes for separating secrets in a protected information system and the implementation of its capabilities for separating secrets and restoring it, as well as development technologies in the Kotlin language that will allow you to release and demonstrate the scheme. As a subject of research, we choose the development and study of the characteristics of an educational information system using the Spring framework.

Objectives of the work — consider methods for sharing a secret, and design an application to solve the problem of sharing a secret using the Shamir secret sharing scheme.

Research methods — a) theoretical: the study of literature on the issue of the division of secret; b) practical: modeling, design specification and development of an information system using the Kotlin language.

The results are — information system for solving problems of secret sharing using augmented stages of the algorithm.

Application area — development of new authentication protocol, storage of secret data, educational purposes.

الملخص

رسالة بكالوريوس 3 مرفق 6 جدول ، 2 صور ، 8صفحة ، 59

الكلمات الرئيسية REST, HTTP, SPRING, KOTLIN

موضوع الدراسة الهدف من البحث هو مخططات فصل الأسرار في نظام معلومات محمي وتنفيذ إمكانياته التي ستسمح لك Kotlin لفصل الأسرار واستعادتها ، بالإضافة إلى تقنيات التطوير بلغة بإصدار المخطط وإثباته. كموضوع بحث ، نختار تطوير ودراسة خصائص نظام المعلومات التربوي باستخدام إطار الربيع.

أهداف العمل النظر في طرق مشاركة سر ، وتصميم تطبيق لحل مشكلة مشاركة سر باستخدام نظام مشاركة سر شامير.

طرق البحث ؛ ب) عملي: النمذجة ومواصفات seret أ) النظري: دراسة الأدب حول موضوع تقسيم - Kotlin. التصميم وتطوير نظام معلومات باستخدام لغة

النتائج نظام معلومات لحل مشاكل المشاركة السرية باستخدام المراحل المعززة من الخوارزمية.

منطقة التطبيق تطوير بروتوكول المصادقة الجديد ، تخزين البيانات السرية ، الأغراض التعليمية.