БЕЛОРУССКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ

ФАКУЛЬТЕТ ПРИКЛАДНОЙ МАТЕМАТИКИ И ИНФОРМАТИКИ

Кафедра технологий программирования

Аннотация к дипломной работе

«Разработка web-приложения для безопасного хранения учётных данных пользователя»

Касакович Михаил Сергеевич

Научный руководитель – технических наук, доцент кафедры технологий программирования Войтешенко И. С.

Минск, 2021

Реферат

Дипломная работа, 55 с., 11 рис., 2 таблицы, 9 приложений.

ЗАЩИТА ИНФОРМАЦИИ, КРИПТОГРАФИЯ, AES, RSA, SPRING, WEB-ПРИЛОЖЕНИЕ

Объект исследования – объектом исследования является защита пользовательских данных при помощи криптосистем, интегрирование их в web-приложения. Предмет исследования – исследование криптосистем и разработка собственного приложения для обеспечения безопасности пользовательских данных.

Цель работы – изучить построение различных криптосистем, разработать собственную криптосистему, ознакомиться с Spring Framework, разработать web-приложение для хранения пользовательских данных.

За время работы были реализованы следующие задачи: изучены базовые понятия и механизмы хеш-функций, изучены теоретические сведения о симметричных и асимметричных криптосистемах, рассмотрены существующие экземпляры вышеупомянутых криптосистем, разработана собственная криптосистема, основывающаяся на существующих примерах и расширяющая их, разработана объектная модель приложения, изучены особенности работы с платформой для разработки приложений Spring Framework, реализовано web-приложение, удовлетворяющее современным требованиям, создан понятный для пользователя и простой для кастомизации и расширения функционал.

Работа имеет широкое практическое применение в сфере защиты пользовательских данных, так как предоставляет достаточный функционал по шифрованию, хранению и предоставлению доступа к данным, которые пользователь желает безопасно хранить.

Реализация даёт возможность надёжно хранить необходимые данные, делегировать сложные математические операции мощному серверу и иметь доступ как к локальному, так и к облачному хранению данных.

Рэферат

Дыпломная работа, 55 ст., 11 мал., 2 табліцы, 19 дадаткаў.

АБАРОНА ІНФАРМАЦЫІ, крыптаграфія, AES, RSA, SPRING, WEB-ПРЫКЛАДАННЕ

Аб’ект даследавання –аб’ектам даследавання з'яўляецца абарона карыстацкіх дадзеных пры дапамозе крыптасістэм, інтэграванне іх у web-прыкладання. Прадмет даследавання - даследаванне крыптасістэм і распрацоўка ўласнага прыкладання для забеспячэння бяспекі карыстацкіх дадзеных.

Мэта працы – вывучыць пабудова розных крыптасістэм, распрацаваць уласную крыптасістэму, азнаёміцца з Spring Framework, распрацаваць web-дадатак для захоўвання карыстацкіх дадзеных.

За час працы былі рэалізаваны наступныя задачы: вывучаны базавыя паняцці і механізмы хэш-функцый, вывучаны тэарэтычныя звесткі аб сіметрычных і асіметрычных крыптасістэмы, разгледжаны існуючыя асобнікі вышэйзгаданых криптосистем, распрацавана ўласная крыптасістэмы, якая засноўваецца на існуючых прыкладах і якая пашырае іх, распрацавана аб'ектная мадэль прыкладання, вывучаны асаблівасці працы з платформай для распрацоўкі прыкладанняў Spring Framework, рэалізавана web-дадатак, якое задавальняе сучасным патрабаванням, створаны зразумелы для карыстальніка і просты для кастомизации і пашырэння функцыянал.

Праца мае шырокае практычнае прымяненне ў сферы абароны карыстацкіх дадзеных, таму што прадастаўляе дастатковы функцыянал па шыфраванні, захоўванню і прадастаўленню доступу да дадзеных, якія карыстальнік жадае бяспечна захоўваць.

Рэалізацыя дае магчымасць надзейна захоўваць неабходныя дадзеныя, дэлегаваць складаныя матэматычныя аперацыі магутнаму сервера і мець доступ як да лакальнага, так і да хмарнаму захоўванні дадзеных.

Abstract

Graduate Work, 55 p., 11 illustrations, 2 tables, 9 appendixes.

PROTECTION OF INFORMATION, CRYPTOGRAPHY, AES, RSA, SPRING, WEB-APP

The object of research is the protection of user data using cryptosystems, their integration into web applications. The subject of the research is the study of cryptosystems and the development of its own application to ensure the security of user data.

The purpose is to study the construction of various cryptosystems, develop your own cryptosystem, familiarize yourself with the Spring Framework, develop a web application for storing user data.

During the work, the following tasks were implemented: the basic concepts and mechanisms of hash functions were studied, theoretical information about symmetric and asymmetric cryptosystems were studied, the existing instances of the aforementioned cryptosystems were considered, their own cryptosystem was developed, based on existing examples and expanding them, an object model of the application was developed, features of working with the platform for developing applications Spring Framework, implemented a web application that meets modern requirements, created a user-friendly and easy to customize and extend functionality.

The work has wide practical application in the field of protecting user data, as it provides sufficient functionality for encryption, storage and provision of access to data that the user wishes to securely store.

The implementation makes it possible to securely store the necessary data, delegate complex mathematical operations to a powerful server and have access to both local and cloud data storage.