МИНИСТЕРСТВО ОБРАЗОВАНИЯ РЕСПУБЛИКИ БЕЛАРУСЬ
БЕЛОРУССКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ
ФАКУЛЬТЕТ РАДИОФИЗИКИ И КОМПЬЮТЕРНЫХ ТЕХНОЛОГИЙ
Кафедра информатики и компьютерных систем

Аннотация к дипломной работе

«Разработка системы обмена текстовыми сообщениями в локальной сети с шифрованием информации»

Синявский Сергей Владимирович

Научный руководитель — ст. преподаватель Барсуков Е. А.

Минск, 2020

РЕФЕРАТ

Дипломная работа: 44 страницы, 11 рисунков, 6 таблиц, 8 источников.

СИСТЕМА ОБМЕНА ТЕКСТОВЫМИ СООБЩЕНИЯМИ, АНАЛИЗ ПРОБЛЕМ ПРИ РАЗРАБОТКЕ ПРИЛОЖЕНИЙ ДЛЯ КОММУНИКАЦИИ В ЛОКАЛЬНОЙ СЕТИ, TCP-, UDP- ПРОТОКОЛЫ, WPF, СИММЕТРИЧНОЕ И АССИМЕТРИЧНОЕ ШИФРОВАНИЕ ИНФОРМАЦИИ, AES ШИФРОВАНИЕ, RSA ШИФРОВАНИЕ.

Объект исследования — система обмена текстовыми сообщениями в локальной децентрализованной сети с шифрованием информации.

Цель работы — анализ готовых решений для осуществления обмена сообщениями в децентрализованной сети, реализация программной модели мессенджера и шифрования информации.

В результате выполнения работы была реализована система обмена текстовыми сообщениями в локальной сети с помощью использования протоколов транспортного уровня TCP для отправки сообщений и UDP для поиска новых узлов сети используя широковещательный канал, а также было реализовано шифрование информации с помощью симметричного алгоритма шифрования RSA и асимметричного алгоритма шифрования AES.

РЭФЕРАТ

Дыпломная праца: 44 старонкі, 11 малюнкаў, 6 табліц, 8 крыніц.

СІСТЭМА АБМЕНУ ТЭКСТАВЫМІ ПАВЕДАМЛЕННЯМІ, АНАЛІЗ ПРАБЛЕМ ПРЫ РАСПРАЦОЎЦЫ СІСТЭМЫ ДЛЯ КАМУНІКАЦЫІ У ЛАКАЛЬНЫХ СЕТКАХ, TCP-, UDP- ПРАТАКОЛЫ, WPF, СІМЕТРЫЧНЫЯ І АСІМЕТРЫЧНЫЯ ШЫФРАВАННЯ ІНФАРМАЦЫІ, AES ШЫФРАВАННЯ, RSA ШЫФРАВАННЯ.

Аб'ект даследавання — сістэма абмену тэкставымі паведамленнямі ў лакальнай дэцэнтралізаванай сеткі з шыфраваннем інфармацыі.

Мэта работы — аналіз гатовых рашэнняў для ажыццяўлення абмену паведамленнямі ў дэцэнтралізаванай сеткі, рэалізацыя праграмнай мадэлі мессенджера і шыфравання інфармацыі.

У выніку выканання работы была рэалізавана сістэма абмену тэкставымі паведамленнямі ў лакальнай сеткі з дапамогай выкарыстання пратаколаў транспартнага ўзроўню TCP для адпраўкі паведамленняў і UDP для пошуку новых вузлоў сеткі выкарыстоўваючы шырокавяшчальны канал, а таксама было рэалізавана шыфраванне інфармацыі з дапамогай сіметрычнага алгарытму шыфравання RSA і асіметрычнага алгарытму шыфравання AES.

ABSTRACT

The diploma consists of 44 pages. It contains 11 figures, 6 tables, 8 sources.

TEXT MESSAGE EXCHANGE SYSTEM, APPLICATIONS FOR COMMUNICATION IN LOCAL NETWORK, TCP, UDP, WPF, SYMMETRIC-KEY AND PUBLIC-KEY CRYPTOGRAPHY, AES ENCRYPTION, RSA ENCRYPTION

Object of research — text messaging system in a local decentralized network with information encryption.

Objective — analysis of ready solutions for the implementation of messaging in a decentralized network, the implementation of the program model of the messenger and encryption of information.

As a result of the work, a text messaging system was implemented in the local network using the TCP transport layer protocols to send messages and UDP to search for new network nodes using the broadcast channel, and information was encrypted using the symmetric RSA encryption algorithm and the asymmetric encryption algorithm AES.