МИНИСТЕРСТВО ОБРАЗОВАНИЯ РЕСПУБЛИКИ БЕЛАРУСЬ

БЕЛОРУССКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ

МЕХАНИКО-МАТЕМАТИЧЕСКИЙ ФАКУЛЬТЕТ

Кафедра алгебры и защиты информации

Кондратович Максим Игоревич

Алгоритмы шифрования и обеспечение безопасности веб-приложений

Дипломная работа

Научный руководитель:

доцент, кандидат физико-математических наук

Д.В. Васильев

Допущен к защите

«__ »_____ 2020 г.

Зав. кафедры алгебры и защиты информации

Доктор физико-математических наук, профессор В.В. Беняш-Кривец

Минск, 2020

Реферат

Дипломная работа содержит: 27 страниц, 7 источников

Ключевые слова: HTTP, HTTPS, SSL, TLS, RSA, ECDSA

Цель дипломной работы — изучить работу протокола HTTPS и как он обеспечивает безопасность веб-приложений.

В ходе работы было выполнено следующее:

1. Изучен алгоритм шифрования RSA
2. Изучен алгоритм цифровой подписи ECDSA
3. Проведено сравнение RSA и ECDSA
4. Изучен принцип работы протокола HTTPS

Работа имеет теоретическую ценность, с возможностью дальнейшего практического применения.

Дипломная работа выполнена автором самостоятельно.

Рэферат

Дыпломная работа змяшчае: 27 старонак, 7 выкарастанных крыніц

Ключавыя словы: HTTP, HTTPS, SSL, TLS, RSA, ECDSA

Мэта дыпломнай працы - вывучыць працу пратаколу HTTPS і як ён забяспечвае бяспеку вэб-прыкладанняў

Падчас працы было выканана наступнае:

1. Вывучаны алгарытм шыфравання RSA
2. Вывучаны алгарытм лічбавай подпісы ECDSA
3. Праведзена параўнанне RSA і ECDSA
4. Вывучаны прынцып працы пратаколу HTTPS

Праца мае тэарэтычную каштоўнасць, з магчымасцю далейшага практычнага прымянення.

Дыпломная работа выканана аўтарам самастойна.

Abstract

The diploma work contains: 27 pages, 7 sources

Keywords: HTTP, HTTPS, SSL, TLS, RSA, ECDSA

The purpose of the thesis is to learn how the HTTPS protocol works and how it provides security for web applications.

During the work the following was done:

1. The RSA encryption algorithm was studied.
2. The ECDSA digital signature algorithm has been studied
3. RSA and ECDSA were compared
4. The principle of the HTTPS protocol has been studied

The work has theoretical value, with the possibility of further practical application.

Diploma work done by the author herself.