Министерство науки и высшего образования Российской Федерации
ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ АВТОНОМНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ
НАЦИОНАЛЬНЫЙ ИССЛЕДОВАТЕЛЬСКИЙ УНИВЕРСИТЕТ ИТМО
ITMO University

ЗАДАНИЕ НА ВЫПУСКНУЮ КВАЛИФИКАЦИОННУЮ РАБОТУ / OBJECTIVES FOR A GRADUATION THESIS

Обучающийся / Student Гутник Дмитрий Вячеславович
Факультет/институт/кластер/ Faculty/Institute/Cluster факультет безопасности информационных технологий
Группа/Group N34491
Направление подготовки/ Subject area 10.03.01 Информационная безопасность
Образовательная программа / Educational program Технологии защиты информации 2019
Язык реализации ОП / Language of the educational program Русский
Статус ОП / Status of educational program
Квалификация/ Degree level Бакалавр
Тема ВКР/ Thesis topic Разработка интерактивной методики оценки эффективности систем цифровой подписи на основе библиотеки PyCryptodome
Руководитель ВКР/ Thesis supervisor Таранов Сергей Владимирович, кандидат технических наук, Университет ИТМО, факультет безопасности информационных технологий, доцент (квалификационная категория "ординарный доцент")

Основные вопросы, подлежащие разработке / Key issues to be analyzed
Цель работы:
Повышение эффективности применения алгоритмов цифровой подписи путём рекомендации подходящего алгоритма в зависимости от условий применения

Задачи работы:
1. Анализ и разделение на виды актуальных алгоритмов цифровой подписи.
2. Разработка критериев к методике оценки цифровых подписей.
3. Создание методики оценки эффективности цифровых подписей.
4. Разработка программной реализации методики.
5. Разработка рекомендаций к практическому применению методики.

Исходные данные:
1. Алгоритм ECDSA
2. Алгоритм DSA
3. Алгоритм RSA (PKCS#1 v1.5 и PKCS#1 PSS)
4. Алгоритм EdDSA
5. Алгоритм SHA 256
6. Алгоритм SHA 384
7. Алгоритм SHA 512

Содержание выпускной квалификационной работы:

1. Анализ и разделение на виды актуальных алгоритмов цифровой подписи
2. Общая информация о разработанной методике
3. Описание структуры методики оценки эффективности подписей
4. Описание программной реализации методики
5. Оценка скорости работы алгоритмов

Исходные материалы и пособия:
1. RFC 8017 // Datatracker [Электронный ресурс]. – 2016. – URL: https://datatracker.ietf.org/doc/html/rfc8017 (дата обращения: 10.03.2023).
2. 1363-2000 - IEEE Standard Specifications for Public-Key Cryptography // IEEE Xplore [Электронный ресурс]. – 2000. – URL: https://ieeexplore.ieee.org/document/891000 (дата обращения: 10.03.2023).
3. Digital Signature Standard (DSS) // NIST Technical Series Publications [Электронный ресурс]. – 2013. – URL: https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.186-4.pdf (дата обращения: 20.03.2023).
4. RFC 8032 // Datatracker [Электронный ресурс]. – 2017. – URL: https://datatracker.ietf.org/doc/html/rfc8032 (дата обращения: 20.03.2023).
5. Desmedt, Y., A. Odlyzko A Chosen Text Attack on the RSA Cryptosystem and Some Discrete Logarithm Schemes // Lecture Notes in Computer Science. - Heverlee: 1985. - С. 516-522.

Форма представления материалов ВКР / Format(s) of thesis materials:
Текст ВКР, презентация, программный код, графический материал в виде блок-схемы

Дата выдачи задания / Assignment issued on: 01.12.2022

Срок представления готовой ВКР / Deadline for final edition of the thesis 26.05.2023

Характеристика темы ВКР / Description of thesis subject (topic)

Название организации-партнера / Name of partner organization: нет / not
Тема в области фундаментальных исследований / Subject of fundamental research: нет / not
Тема в области прикладных исследований / Subject of applied research: да / yes

СОГЛАСОВАНО / AGREED:

Руководитель ВКР/ Thesis supervisor

Документ подписан
Таранов Сергей Владимирович
14.05.2023

(эл. подпись)

Таранов Сергей Владимирович

Задание принял к исполнению/ Objectives assumed BY

Документ подписан
Гутник Дмитрий Вячеславович
14.05.2023

(эл. подпись)

Гутник Дмитрий Вячеславович

Руководитель ОП/ Head of educational program

(эл. подпись)