ХЕРСОНСЬКИЙ НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ
(повне найменування вищого навчального закладу)
ФАКУЛЬТЕТ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ ТА ДИЗАЙНУ
(повне найменування інституту, назва факультету (відділення))
КАФЕДРА ПРОГРАМНИХ ЗАСОБІВ І ТЕХНОЛОГІЙ
(повна назва кафедри (предметної, циклової комісії))

Пояснювальна записка

до кваліфікаційної роботи
бакалавра
(рівень вищої освіти)

на тему: «Розробка програми оптимізації алгоритму шифрування RSA»

Виконав: студент 4 курсу, групи 4ПР1
спеціальності
121 «Інженерія програмного забезпечення»
(шифр і назва напряму підготовки, спеціальності)

Пішенін Володимир Олександрович
(прізвище та ініціали)

Керівник ст. викладач Боскін О.О.
(прізвище та ініціали)

Рецензент _____
(прізвище та ініціали)

Херсон – 2021

Херсонський національний технічний університет
(повне найменування вищого навчального закладу)

Інститут, факультет, відділення Факультет інформаційних технологій і дизайну
Кафедра, циклова комісія Кафедра Програмних засобів і технологій
Освітньо-кваліфікаційний рівень Бакалавр
Напрям підготовки
(шифр і назва)
Спеціальність 121 – Інженерія програмного забезпечення
(шифр і назва)

ЗАТВЕРДЖУЮ
Завідувач кафедри ПЗіТ
д.т.н. проф. В.Г. Шерстюк
"____" _____ 2021 р.

З А В Д А Н Н Я
НА КВАЛІФІКАЦІЙНУ РОБОТУ СТУДЕНТУ

Пішеніна Володимира Олекандровича
(прізвище, ім'я, по батькові)

1. Тема роботи «Розробка програми оптимізації алгоритму шифрування RSA»
керівник роботи ст. викладач Боскін О.О.,
(прізвище, ім'я, по батькові, науковий ступінь, вчене звання)
затверджена наказом вищого навчального закладу _____
2. Строк подання студентом роботи 10.06.2021
3. Вихідні дані до роботи _____

4. Зміст пояснювальної записки (перелік питань, які потрібно розробити)
Розділ 1. Опис предметної області, постановка задачі розробка програми оптимізації алгоритму шифрування rsa; Розділ 2. Аналіз та моделювання предметної області; Розділ 3. Розробка програмного забезпечення задачі; Висновки.

5. Перелік графічного матеріалу (з точним зазначенням обов'язкових креслень)
Комп'ютерна презентація

6. Консультанти розділів кваліфікаційної роботи

Розділ	Прізвище, ініціали та посада консультанта	Підпис, дата	
		завдання видав	завдання прийняв

7. Дата видачі завдання_____

КАЛЕНДАРНИЙ ПЛАН

№ з/п	Назва етапів кваліфікаційної роботи	Строк виконання етапів роботи	Примітка
1	Відбір та вивчення літературних джерел	13.02.2021 – 01.03.2021	Виконано
2	Аналіз стану вирішення завдання на сучасному етапі	02.03.2021 – 20.03.2021	Виконано
3	Побудова концептуальної моделі	21.03.2021 – 01.04.2021	Виконано
4	Розробка моделі	02.04.2021 – 20.04.2021	Виконано
5	Побудова алгоритму функціонування програмного продукту	21.04.2021 – 01.05.2021	Виконано
6	Написання вихідного коду програми	02.05.2021 – 15.05.2021	Виконано
7	Налагодження програмного коду	16.05.2021 – 22.05.2021	Виконано
8	Оформлення пояснювальної записки	23.05.2021 – 01.06.2021	Виконано

Студент _____ __Пішенін В.О._____
(підпис) (прізвище та ініціали)

Керівник роботи _____ __Боскін О. О._____
(підпис) (прізвище та ініціали)

РЕФЕРАТ

Кваліфікаційна робота бакалавра: 71 сторінок, 13 рисунків, 4 додатки, 54 джерел.

Мета роботи – розробка програми оптимізації алгоритму шифрування RSA, що включає такі функції:

1. Генерація ключів
2. Шифрування
3. Дешифрування

Об’єкт дослідження – вразливості найбільш поширеного асиметричного алгоритму шифрування RSA..

Предмет дослідження – оптимізація алгоритму RSA, з метою підвищення крипто стійкості та стійкості до підбору ключів з мінімальнім приростом необхідної обчислювальної потужності з боку клієнта.

Методи дослідження – аналіз та узагальнення інформації про існуючі алгоритми шифрування , їх основні переваги, недоліки та способи їх усунення, практичні методи їх реалізації.

Результат роботи:

- запропоновано математичні формули оптимізованого алгоритму шифрування на базі RSA;
- реалізовано додаток, для демонстрації роботи оновленого алгоритму

Новизна роботи:

– запропоновано оптимізацію алгоритму шифрування з підвищеною стійкістю до атак зловмисників з урахуванням поширення високопродуктивних обчислювальних систем на сьогоднішній день;
– розроблено додаток, що дозволяє оцінити реалізацію алгоритму;
– проведено ряд тестів з швидкодії та стійкості алгоритму до різноманітних атак;

Ключові слова: додаток, алгоритми шифрування, криптоаналіз, криптографія, шифрування.

АНОТАЦІЯ

Перший розділ «Опис предметної області, постановка задачі розробка програми оптимізації алгоритму шифрування RSA» складається з наступних підрозділів: «Історія розвитку криптографії», «Поняття і принципи роботи асиметричного алгоритму шифрування RSA», «Схема розробки програми оптимізації асиметричного алгоритму шифрування RSA», «Постановка задачі - розробка програми оптимізації алгоритму шифрування RSA» та «Висновки».

Другий розділ «Аналіз та моделювання предметної області» містить інформацію про життєвий цикл програмного забезпечення, аналіз та узагальнення інформації, про існуючі алгоритми шифрування, теоретичний аналіз та узагальнення інформаційних джерел з тематики криптографії, засоби для створення додатків, види комп'ютерних програм.

Третій розділ «Розробка інформаційного забезпечення задачі» складається з шести розділів: «Вибір засобів для розробки інформаційного забезпечення задачі», «Основні переваги мови C#», «Розвиток мови C #», «Порівняння з іншими мовами», «Простота», «Эффективність», «Безкоштовне поширення», «Вхідні та вихідні дані», «Алгоритм та логічна структура програми», «Вибір технічного забезпечення для виконання задачі», «Опис класів програми» та «Висновки»

ANNOTATION

The first section "Description of the subject area, problem statement development of optimization algorithm RSA encryption algorithm" consists of the following sections: "History of cryptography", "Concepts and principles of asymmetric RSA encryption algorithm", "Scheme of asymmetric optimization algorithm, RS encryption algorithm" problem statement - development of the program of optimization of the RSA encryption algorithm "and" Conclusions ".

The second section "Analysis and modeling of the subject area" contains information about the software life cycle, analysis and generalization of information, about existing encryption algorithms, theoretical analysis and generalization of information sources on cryptography, tools for creating applications, types of computer programs.

The third section "Development of information support of the problem" consists of six sections: "Selection of MEANS for the development of information support of the problem", "Main advantages of C #", "Development of C #", "Comparison with other languages", "Simplicity", " Efficiency "," Free Distribution "," Input and output data "," Algorithm and logical structure of the program "," Selection of hardware for the task "," Description of program classes "and" Conclusions "

ЗМІСТ

ПЕРЕЛІК УМОВНИХ СКОРОЧЕНЬ

Скорочення, термін, позначення	Пояснення
ІБ	Інформаційна Безпека
ПЗ	Програмне Забезпечення
IT	Information Technology
OS	Операційна Система
PC	Personal computer
SDK	Software Development Kit
ЕОМ	Електронна обчислювальна машина
RSA	аббревиатура від прізвищ Rivest, Shamir та Adleman
DES	Data Encryption Standard
ПЕОМ	Персональна електронна обчислювальна машина
MITM	Man in the middle
ЖЦ	Життєвий цикл
MSIL	Microsoft Intermediate Language
XML	eXtensible Markup Language
LINQ	Language-Integrated Query
IDE	Integrated Drive Electronics
ASCII	American standard code for information interchange
ООП	Об’єктно орієнтоване програмування

ВСТУП

Для того, щоб забезпечити захист конфіденційної інформації на сьогоднішній день будь-яка система потребує використання інноваційних методів захисту інформації. Серед таких методів – використання хмарних сховищ, надійних паролів та шифрування.

Хмарні сховища можуть використовуватись як для створення резервніх копій так і в якості основного сховища даних. У будь-якому випадку конфіденційність може бути порушена за умови ненадійності сховища, та/або використання ненадійного каналу зв’язку для передачі інформації в хмару. Саме для створення захищеного каналу передачі будь-якої інформації і необхідне шифрування.

Наразі виділяють три основних типи алгоритмів шифрування:

- Симетричне
- Асиметричне
- Хеш-функції

Кожен з них має певні переваги та недоліки і відповідно сферу використання. Варто пам’ятати що жоден з сучасних методів шифрування не є абсолютно безпечним. Незважаючи на це існує математично виведена абсолютно стійка система – основними критеріями якої є:

Статистична надійність ключа(всі символи мають однакову ймовірність потрапити до ключа)

Довжина ключа більша або дорівнює довжині повідомлення

Кожен ключ використовується лише один раз

Такий шифр стійкий до частотного аналізу, та достатньо стійкий до перебору ключа(у переважній більшості випадків затрати часу на підбір ключа перевищують вартість інформації в кожному окремому повідомленні), але на практиці такі системи повинні мати велику обчислювальну здатність, що робить їх використання не рентабельним.

При виборі алгоритму шифрування варто розглянути всі переваги та недоліки окремо для кожної системи. Необхідно враховувати такі показники як крипто-стійкість, стійкість до підбору ключа та можливість використання з урахуванням обчислювальної потужності

Актуальність теми**.** алгоритм шифрування RSA був першим алгоритмом який міг застосовуватися одночасно і для захисту повідомлень, і для цифрового підпису та наразі залишається одним з передових алгоритмів з моменту його опублікування в 1977 році. Але з зростанням обчислювальної потужності персональних комп'ютерів зростають і його основні вразливості, через що його використання все частіше обмежується створенням каналу для передачі секретного ключа.

Об'єкт дослідження – вразливості найбільш поширеного асиметричного алгоритму шифрування RSA.

Предмет дослідження – оптимізація алгоритму RSA, з метою підвищення крипто стійкості та стійкості до підбору ключів з мінімальнім приростом необхідної обчислювальної потужності з боку клієнта.

Методи дослідження – аналіз та узагальнення інформації про існуючі алгоритми шифрування , їх основні переваги, недоліки та способи їх усунення, практичні методи їх реалізації.

Мета і задачі дослідження - мета дослідження полягає в розробці методів усунення основних недоліків алгоритму шифрування RSA, та його оптимізації, що включає в себе збільшення швидкодії з використанням мінімального приросту обчислювальної потужності.

Основним завданням дипломного проекту з теми «Оптимізація алгоритму шифрування RSA» є дослідження методу, його оптимізація та створення додатку, який виконуватиме функції шифрування та розшифровування на основі отриманих формул та методів.

Досягнення поставленої мети передбачає реалізацію таких завдань:

1) розглянути поняття шифрування, вразливості сучасних алгоритмів, зокрема алгоритму RSA;

2) визначити тренди розвитку криптографії та їхній вплив на сучасні алгоритми;

3) здійснити порівняльний аналіз систем та платформ для створення додатків під управлінням популярних операційних систем;

4) розробити систему для шифрування-дешифрування тексту за алгоритмом з урахуванням всіх модифікацій.

Наукова новизна одержаних результатів:

- запропоновано оптимізацію алгоритму шифрування з підвищеною стійкістю до атак зловмисників з урахуванням поширення високопродуктивних обчислювальних систем на сьогоднішній день;
- розроблено додаток, що дозволяє оцінити реалізацію алгоритму;
- проведено ряд тестів з швидкодії та стійкості алгоритму до різноманітних атак;

Практичне значення одержаних результатів. Оновлений алгоритм має не тільки теоретичне, а і практичне значення і може сприяти підвищенню безпеки як персонального так і комерційного листування, реалізований додаток, що виконує функції шифрування та дешифрування під керуванням операційної системи MS Windows 10, який відображає якість кінцевих алгоритмів.

Апробація результатів бакалаврської кваліфікаційної роботи. Одержані результати можна використовувати для забезпечення таємниці листування, цілісності даних та захисту в разі витоків інформації; запропоновану систему використовувати для подальшого удосконалення стійкості алгоритму з підвищенням мінімальної обчислювальної потужності клієнта.