НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ УКРАЇНИ
«КИЇВСЬКИЙ ПОЛІТЕХНІЧНИЙ ІНСТИТУТ
імені ІГОРЯ СІКОРСЬКОГО»

Факультет прикладної математики

Кафедра програмного забезпечення комп'ютерних систем

«До захисту допущено»
Науковий керівник кафедри
_____ І.А. Дичка
(підпис)
"___" _____ 2017 р.

Дипломна робота

на здобуття ступеня бакалавра

з напряму підготовки 6.050103 "Програмна інженерія"

на тему «МЕТОД ВИКОНАННЯ ОПЕРАЦІЙ НАД ЕЛЕМЕНТАМИ ПОЛЯ $GF(P^m)$»

Виконав: студент 4 курсу, групи КП-32
Агарков Дмитро Олександрович _____
(підпис)

Керівник старший викладач Онай М.В. _____
(підпис)

Рецензент доц. кафедри СПіСКС, доц., к.т.н. Романкевич В.О. _____
(підпис)

Засвідчую, що у цьому дипломному проекті немає запозичень з праць інших авторів без відповідних посилань.
Студент _____
(підпис)

Київ – 2017

АНОТАЦІЯ

Дана дипломна робота присвячена дослідженню методів знаходження мультиплікативно-оберненого елемента, піднесеня до степеня та множення елементів поля $GF(p^m)$.

Її мета полягає у дослідженні і модифікації існуючих та побудові нових методів знаходження мультиплікативно-оберненого елемента, піднесення до степеня та множення елементів поля $GF(p^m)$, що забезпечують приріст швидкодії.

Результатом виконання даної роботи є програмний комплекс для дослідження методів знаходження мультиплікативно-обереного елемента, піднесеня до степеня та множення елементів у полі $GF(p^m)$, комплексне дослідження швидкодії методів піднесення до степеня, запропоновані модифікації, які дають приріст швидкодії на 10%.

ABSTRACT

This thesis is devoted to the investigation of multiplicative-inverse search, exponentiation and multiplication methods of elements in the field $GF(p^m)$.

Its goal is to investigate and modify existing ones and to construct new methods of multiplicative-inverse search, exponentiation and multiplication of elements in the field $GF(p^m)$, which will ensure an increase in speed.

The result of the implementation of this work is a software package for the investigation methods of multiplicative-inverse search, exponentiation and multiplication of elements in the field $GF(p^m)$, a complex investigation of the speed of exponentiation methods, proposed new modifications that give the increase in speed.

Список використаної літератури

1. C# - Вікіпедія [Електронний ресурс]. — Режим доступу: https://uk.wikipedia.org/wiki/C#
2. Hankerson, Menezes, Vanstone. Guide to elliptic curve cryptography [Електронний ресурс] — https://vk.com/doc6159151_437219225?hash=16f6d20702c875270f&dl=ea399e15010498c796
3. Abdulah Abdulah Zadeh, Division and Inversion Over Finite Fields [Електронний ресурс]. — http://cdn.intechopen.com/pdfs/29704.pdf
4. Cetin K. Koc, Third Annual Workshop on Selected Areas in Cryptography [Електронний ресурс]. — http://research.microsoft.com/pubs/103203/j47mmugf.pdf
5. Kobayashi E.A., Algorithm Inversion Using Polynomial MultiplyI nstruction [Електронний ресурс]. — https://vk.com/doc6159151_437204293?hash=f37885d319c6ee99f2&dl=1110c18dbfff6a6edf
6. Швидке перетворення Фур'є – Вікіпедія [Електронний ресурс]. — Режим доступу: https://uk.wikipedia.org/wiki/Швидке_перетворення_Фур%27є
7. Ключ (криптографія) – Вікіпедія [Електронний ресурс]. — Режим доступу: https://uk.wikipedia.org/wiki/Ключ_(криптографія)
8. Асиметричні алгоритми шифрування – Вікіпедія [Електронний ресурс]. — Режим доступу: https://uk.wikipedia.org/wiki/Асиметричні_алгоритми_шифрування
9. Шифрування з симетричними ключами – Вікіпедія [Електронний ресурс]. — Режим доступу: https://uk.wikipedia.org/wiki/Шифрування_з_симетричними_ключами

10. RSA – Вікіпедія [Електронний ресурс]. — Режим доступу: https://uk.wikipedia.org/wiki/RSA
11. Криптографія – Вікіпедія [Електронний ресурс]. — Режим доступу: https://uk.wikipedia.org/wiki/Криптографія
12. Digital Signature Algorithm – Вікіпедія [Електронний ресурс]. — Режим доступу: https://en.wikipedia.org/wiki/Digital_Signature_Algorithm
13. Схема Ель-Гамаля – Вікіпедія [Електронний ресурс]. — Режим доступу: https://uk.wikipedia.org/wiki/Схема_Ель-Гамаля
14. Elliptic Curve Digital Signature Algorithm – Вікіпедія [Електронний ресурс]. — Режим доступу: https://en.wikipedia.org/wiki/Elliptic_Curve_Digital_Signature_Algorithm
15. Протокол Діффі-Геллмана – Вікіпедія [Електронний ресурс]. — Режим доступу: https://uk.wikipedia.org/wiki/Протокол_Діффі-Геллмана
16. Запобігання витоків інформації – Вікіпедія [Електронний ресурс]. — Режим доступу: https://uk.wikipedia.org/wiki/Протокол_Діффі-Геллмана
17. Криптография: Базовые знания о науке шифрования – [Електронний ресурс]. — Режим доступу: http://www.furfur.me/furfur/culture/culture/166567-kriptografiya
18. Введение в криптографию – Вікіпедія [Електронний ресурс]. — Режим доступу: http://algolist.manual.ru/defence/intro.php
19. Модифікований віконний метод однократного множення точки еліптичної кривої на скаляр поля $GF(P)$ – Вікіпедія [Електронний ресурс]. — Режим доступу: https://cyberleninka.ru/article/v/modifikovaniy-vikonniy-metod-odnokratnogo-mnozhennya-tochki-eliptichnoyi-krivoyi-na-skalyar-u-poli-gf-p