ОДЕСЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ імені І.І.МЕЧНИКОВА

(повне найменування вищого навчального закладу)

Факультет математики, фізики та інформаційних технологій

(повне найменування інституту, назва факультету (відділення))

Кафедра комп'ютерної алгебри та дискретної математики

(повна назва кафедри (предметної, циклової комісії))

Дипломна робота

на здобуття освітньо-кваліфікаційного рівня «бакалавр»

(освітньо-кваліфікаційний рівень)

на тему: Проблема дискретного логарифму та цифровий підпис

The problem of discrete logarithm and digital signature .

Виконала: студентка денної форми навчання
спеціальності 6.050102 — Комп'ютерна інженерія

(шифр і назва напряму підготовки, спеціальності)

Балан Олександра Василівна

(прізвище, ім'я, по-батькові)

Керівник к.ф.-м. н., доц. Бєлозьоров Г.С.

(науковий ступінь, вчене звання, прізвище та ініціали, підпис)

Рецензент к. ф.-м. н., доц. Варбанець С.П.

(науковий ступінь, вчене звання, прізвище та ініціали)

Рекомендовано до захисту:

Протокол засідання кафедри

№_____ від «___»_____ 2019 р.

Завідувач кафедри

_____ Варбанець П.Д.

(підпис) (прізвище, ініціали)

Захищено на засіданні ЕК № ___

протокол №__ від «___» ____ 2019 р.

Оцінка_____/_____/_____

(за національною шкалою, шкалою ECTS, бали)

Голова ЕК

_____ О.О. Арсірій

(підпис) (прізвище, ініціали)

Одеса - 2019

ABSTRACT

There are many public-key cryptosystems and crypto-protocols, the robustness of which relies on the discrete logarithm problem. Finding the second one is difficult to calculate when using them as the basis of a cryptosystem.

In this thesis work, the problem of the discrete logarithm was considered and some algorithms for its solution (which are exponential in general) are given, as well as the applications of this problem to the problem of electronic digital signature. On the basis of the tasks, a program model was constructed using “long arithmetic”.

The goal of this work is to build software models for solving the discrete logarithm problem for the above algorithms, as well as software models for digital signature systems based on the discrete logarithm problem. Based on the results obtained, an analysis was performed for systems with different test conditions. As a result, the possibility of falsifying a signature for various verification conditions was revealed.

АННОТАЦИЯ

Существует множество криптосистем с открытым ключом и криптопротоколов, стойкость которых опирается на проблему дискретного логарифма. Нахождение последних является трудновычислимым при их использовании в качестве основы криптосистемы.

В данной работе была рассмотрена проблема дискретного логарифма и приведены некоторые алгоритмы ее решения (которые носят в целом экспоненциальный характер), а также приложениям указанной задачи к задаче электронной цифровой подписи. На основе поставленных задач была построена программная модель с применением «длинной арифметики».

Целью данной работы является построение программных моделей решения проблемы дискретного логарифма для указанных алгоритмов, а также программных моделей систем цифровой подписи на основе задачи о дискретном логарифме. Базируясь на полученных результатах был проведен анализ для систем с различными проверочными условиями. И как следствие — выявление возможностей фальсификации подписи для различных проверочных условий.

АНОТАЦІЯ

Існує багато криптосистем з відкритим ключем і криптопротоколів, стійкість яких опирається на проблему дискретного логарифму. Знаходження останніх є важкообчислюваним при їх використанні в якості основи криптосистеми.

У даній роботі було розглянуто проблему дискретного логарифму і наведені деякі алгоритми її вирішення (які носять в цілому експоненціальний характер), а також додаткам зазначеного завдання до завдання електронного цифрового підпису. На основі встановлених задач була побудована програмна модель із застосуванням «довгої арифметики».

Метою даної роботи є побудова програмних моделей вирішення проблеми дискретного логарифму для зазначених алгоритмів, а також програмних моделей систем цифрового підпису на основі завдання про дискретний логарифм. Базуючись на отриманих результатах було проведено аналіз для систем із різними перевірочними умовами. І як наслідок — виявлення можливостей фальсифікації підпису для різних перевірочних умов.

ЗМІСТ

стор.

ПЕРЕЛІК СКОРОЧЕНЬ, УМОВНИХ ПОЗНАЧЕНЬ І ТЕРМІНІВ

Скорочення:

ЕЦП — Електронно Цифровий Підпис.

СПХ — Сільвера-Поліга-Хеллмана(алгоритм).

RSA — Rivest Shamir Adleman(алгоритм).

MDC — Modification Detection Code.

WPF — Windows Presentation Foundation.

GUI — Graphical User Interface.

ВСТУП

Народжена в середині сімдесятих років ідея асиметричного шифрування надала потужний поштовх в області прикладної математики. В цьому розділі теорії чисел можна виділити три великі проблеми: побудова великих простих чисел, завдання цілочисленої факторизації і проблема дискретного логарифму. І якщо перша досить успішно вирішується (навіть отриманий поліноміальний алгоритм вирішення задачі), то дві інші не мають на сьогоднішній день ефективного вирішення. Це завдання класу NP. Не вдаючись до подробиць чіткого визначення можна сказати, що поліноміального рішення вони не мають, але будь-яка запропонована відповідь перевіряється поліноміальним алгоритмом. Таким чином, проблема дискретного логарифму — це завдання, на основі складності якої будуються криптографічні схеми: криптосистеми і крипто протоколи.

Вже згадана проблема може бути сформульована для будь-якої кінцевої абелевої групи. У арифметиці, як правило, це група класів відрахувань по простому модулю p взаємно простих з p, тобто Z_p^*. Добре відомо, що ця група циклічна, тобто в ній є породжуючі елементи — первісні корені по модулю p. Значить, для будь-якого елемента $x \in Z_p^*$ при заданому первісному кореню g знайдеться $y \in N$, що $x = g^y (mod\ p)$. Завдання знаходження y (індексу) і є зазначеною проблемою. Вона може сформулюватися в зазначених групах (які не зобов'язані бути циклічними) і для довільних фіксованих елементів великого порядку (замість g). Так зазвичай це відбувається в групі точок еліптичної кривої над кінцевим полем.

У даній роботі розглядається проблема дискретного логарифму і наводяться деякі алгоритми її вирішення (зрозуміло, вони носять в цілому експонентний характер). Друга частина роботи присвячена додаткам зазначеного завдання до завдання електронного цифрового підпису (ЕЦП). У

третій частині даної роботи розглядається програмна реалізація, яка спирається на встановлені задачі. Зазначимо мету роботи. Отже, це:

1) Побудова програмних моделей вирішення проблеми дискретного логарифму для зазначених алгоритмів.
2) Побудова програмних моделей систем цифрового підпису на основі завдання про дискретний логарифм.
3) Аналіз отриманих результатів для систем із різними перевірочними умовами.
4) Виявлення можливостей фальсифікації підпису для різних перевірочних умов.
5) Застосування «довгої арифметики» до побудови програмних моделей.

ВИСНОВОК

В процесі виконання даної роботи були розглянуті та проаналізовані наступні алгоритми дискретного логарифмування: алгоритм Сільвера-Полліга-Хеллмана, алгоритм Шенкса, а також ρ-метод Полларда.
Було побудовано їх програмні моделі із застосуванням «довгої арифметики», як було зазначено у завданні. Наступним кроком був аналіз таких протоколів ЕЦП, як: протокол ЕЦП Ель-Гамаля і його варіанти, а також схема ЕЦП Шнорра.

Була побудована програмна модель ЕЦП Ель-Гамаля, а також користувацький ЕЦП, з власним варіантом перевірочної умови із застосуванням «довгої арифметики». На основі отриманих результатів був проведений аналіз для систем з різними перевірочними умовами, а також виявлення можливостей фальсифікації підпису.

Окрім вже перелічених задач, було побудовано графічний інтерфейс задля зручного користування з можливістю змінювати, а також доповнювати.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Молдовян Н.А., Практикум по криптосистемам с открытым ключом — СПб.: БХВ-Петербург, 2007. — 304 с.:ил.
2. Смарт Н., Криптография — М.: Техносфера, 2005. — 528 с.
3. Саломаа А., Криптография с открытым ключом. — М.: Мир, 1995. — 318 с.
4. Коблиц Н., Курс теории чисел и криптографии. — Москва: ТВПб, 2001. — 254 с.
5. Василенко О. Н., Теоретико-числовые алгоритмы в криптографии. — Москва: МЦНМО, 2003. — 328 с.
6. Джон Скит. C # для професіоналів: тонкощі програмування, 3-е видання, новий переклад = C # in Depth, 3rd ed .. — M .: «Вільямс», —2014. — C. 608
7. Метью Мак-Дональд. WPF: Windows Presentation Foundation в .NET 4.0 з прикладами на C # 2010 для професіоналів = Pro WPF in C # 2010: Windows Presentation Foundation with .NET 4.0. - M .: «Вільямс», 2011. — C. 1 024.
8. Wildermuth, Shawn. "Windows Presentation Foundation Data Binding: Part 1". Microsoft. Retrieved 24 March 2012. C. 10-25.