НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ УКРАЇНИ
“КИЇВСЬКИЙ ПОЛІТЕХНІЧНИЙ ІНСТИТУТ”
ФІЗИКО-ТЕХНІЧНИЙ ІНСТИТУТ

“**ЗАТВЕРДЖУЮ”**
Директор ФТІ
_____ Новіков О.М.

“____”_____ 2024 р.

КОМП’ЮТЕРНИЙ ПРАКТИКУМ КРЕДИТНОГО МОДУЛЯ

“МЕТОДИ РЕАЛІЗАЦІЇ КРИПТОГРАФІЧНИХ МЕХАНІЗМІВ”

для напряму підготовки:

Рекомендовано кафедрою
Математичних методів захисту інформації
(Протокол № _____ від _____ р.)

Завідувач кафедри
Математичних методів захисту інформації

_____С.В. Яковлєв

Київ – 2024/2024

Цикл лабораторних робіт (комп'ютерний практикум) дозволяє студентам придбати такі навички та уміння:

- вибір та тестування бібліотек реалізації арифметичних та алгебраїчних операцій з багато розрядними числами над полем натуральних чисел та скінченими полями чи групами;
- вибір та тестування бібліотек реалізації основних криптографічних примітивів;
- практичну реалізацію криптографічних протоколів;
- розробку програмної реалізації обраної криптосистеми.

Завдання сформовані таким чином, що кожна з бригад може обрати один з трьох типів лабораторних робіт:

перший тип спрямований на більш теоретичний характер роботи, в якому студентам доступна більша ступень свободи вибору базових алгоритмів виконання операцій в кінцевих полях,

другий тип спрямований на більш практичний характер роботи, в якому студенти обирають бібліотеки реалізації криптографічних примітивів для заданих технічних вимог щодо версій операційних систем та апаратної платформи;

третій тип спрямований на комплексне вирішення задачі побудови заданої гібридної криптосистеми з широкою можливістю вибору варіантів вирішення задачі (об'єднання в рамках однієї бригади завдань першого та другого типів).

Лабораторна робота № 1.

Тема: „Вибір та реалізація базових фреймворків та бібліотек".

Мета роботи: «Вибір базових бібліотек/сервісів для подальшої реалізації криптосистеми».

Необхідні теоретичні відомості. Необхідні теоретичні відомості містяться в роботах:

1. Задірака В.К., Олексюк О.С. Комп'ютерна арифметика багаторозряних чисел: Наукове видання. – Київ: 2003. – 264 с.

2. Д. Э. Кнут Искусство программирования, том 2. Получисленные алгоритмы, 3-е изд.: Пер. с англ.: Уч. пос.–М: Изд. дом «Вильямс», 2001.–832 с.

3. C.K.Koc High-Speed RSA Implementation TR RSA Data Security

Завдання на лабораторну роботу

Для першого типу лабораторних робіт - дослідження алгоритмів реалізації арифметичних операцій над великими (багато розрядними) числами над скінченими полями та групами з точки зору їх ефективності за часом та пам'яттю для різних програмно-апаратних середовищ.

Варіанти завдань першого типу. Дослідити бібліотеки багатослівної арифметики.

Підгрупа 1А. Бібліотеки багаторозрядної арифметики, вбудовані в програмні платформи C++/C# (BigInteger), Java (BigInt), Python або Crypto++ (обрати одну з них) для процесорів із 32-розрядною архітектурою та обсягом оперативної пам'яті до 16 ГБ (user Endpoints terminal).

Підгрупа 1В. Бібліотека багаторозрядної арифметики Pari/GP для процесорів із 64-розрядною архітектурою та обсягом оперативної пам'яті до 64 ГБ (сервери).

Підгрупа 1С. Бібліотека багаторозрядної арифметики GNU GMP для паралельної моделі обчислень – декілька процесорів (можливо багатоядерних) із 64-розрядною архітектурою та обсягом оперативної пам'яті до 128 ГБ. Приклад – сервер обробки транзакцій/обладнання провайдера хмарних послуг.

Оформлення результатів роботи. Опис функції багато розрядної арифметики обраної бібліотеки з описом алгоритму та оцінками їх складності, вхідних та вихідних даних, кодів повернення. Контрольний приклад роботи з функціями.

Для другого типу лабораторних робіт – вибір бібліотеки реалізації основних криптографічних примітивів з точки зору їх ефективності за часом та пам'яттю для різних програмних платформ.

Варіанти завдань другого типу.

Підгрупа 2А. Порівняння бібліотек OpenSSL, Crypto++, CryptoLib, PyCrypto для розробки гібрідної криптосистеми під Windows платформу.

Підгрупа 2В. Порівняння бібліотек OpenSSL, Crypto++, CryptoLib, PyCrypto для розробки гібрідної криптосистеми під Linux платформу.

Підгрупа 2С. Порівняння бібліотек OpenSSL, Crypto++, CryptoLib, PyCrypto для розробки гібрідної криптосистеми під Android/MacOs/IOs платформу.

Оформлення результатів роботи. Опис функції бібліотеки реалізації основних криптографічних примітивів обраної бібліотеки, з описом алгоритму, вхідних та вихідних даних, кодів повернення. Контрольний приклад роботи з функціями. Обґрунтування вибору бібліотеки.

Для третього типу лабораторних робіт – розробка технічних вимог (із вибором або бібліотеки реалізації арифметичних операцій або бібліотеки реалізації основних криптографічних примітивів) для різних варіантів реалізацій IT-систем.

Варіанти завдань третього типу.

Підгрупа 3А. Вибір бібліотеки для реалізації Web-сервісу електронного цифрового підпису.

Підгрупа 3В. Вибір бібліотеки для реалізації платіжного сервісу.

Підгрупа 3С. Вибір бібліотеки для реалізації мобільного додатку шифрування/електронного цифрового підпису.

Оформлення результатів роботи. Технічні вимоги до системи із обґрунтуванням обраних рішень.

Лабораторна робота № 2.

Тема: Реалізація алгоритмів генерації ключів гібридних криптосистем.

Мета роботи: Дослідження алгоритмів генерації псевдовипадкових послідовностей, тестування простоти чисел та генерації простих чисел з точки зору їх ефективності за часом та можливості використання для гененерації ключів асиметричних криптосистем.

Необхідні теоретичні відомості. Необхідні теоретичні відомості містяться в роботах

1. Maurer U. M. Fast generation of secure RSA-moduli with almost maximal diversity *Proceedings of Eurocrypt '89. - P. 636-647.*

2. Б. Шнайер Прикладная криптография. Протоколы, алгоритмы, исходные тексты на языке Си. – М.: Изд-во ТРИУМФ,2002. – 816 с.

Завдання на лабораторну роботу

Для першого типу лабораторних дослідити різні методи генерації випадкових послідовностей для засобів обчислювальної техніки. Дослідити ефективність за часом алгоритми тестування на простоту різних груп – імовірнісних, гипотетичних та детермінованих. Порівняти ймовірність похибки різних імовірнісних тестів (Ферма, Соловея-Штрасена та Мілера-Рабіна з різною кількістю ітерацій) з ймовірністю похибки при виконанні обчислень на ПЕОМ. Розглянути алгоритми генерації простих чисел “Чебишова” та Маурера та провести порівняльний аналіз їх складності. Розробити бібліотеку генерації псевдовипадкової послідовності, тестування простоти чисел та генерації простих чисел для Intel-сумісних ПЕОМ. Розмірність чисел – 1024/2048/4096 біт.

Підгрупа 1А. Запропонувати схему генератора ПВЧ для інтелектуальної картки, токена та смартфону. Розглянути особливості побудови генератора простих чисел в умовах обмеження пам’яті та часу генерації.

Підгрупа 1В. Запропонувати схему генератора ПВЧ для User Endpoint terminal. Розглянути особливості побудови генератора простих чисел для моделей тонкого/товстого клієнта.

Підгрупа 1С. Запропонувати схему генератора ПВЧ для хмарного провайдера. Розглянути особливості побудови генератор простих чисел для хмарного провайдера.

Оформлення результатів роботи. Опис схем із обґрунтуванням.

Для другого типу лабораторних робіт – аналіз стійкості реалізацій ПВЧ та генераторів ключів для обраної бібліотеки.

Варіанти завдань другого типу.

Підгрупа 2А. Бібліотека OpenSSL під Windows платформу.

Підгрупа 2В. Бібліотека PyCrypto під Linux платформу.

Підгрупа 2С. Бібліотека Crypto++ під Android/MacOs/Ios платформу.

Оформлення результатів роботи. Опис функції генерації ПСП та ключів бібліотеки з описом алгоритму, вхідних та вихідних даних, кодів повернення. Контрольний приклад роботи з функціями.

Для третього типу лабораторних робіт – розробка технічних вимог (із вибором схеми генерації ПСП та схеми управління ключами) для різних варіантів реалізацій ІТ-систем.

Варіанти завдань третього типу.

Підгрупа 3А. Вибір рішень для реалізації Web-сервісу електронного цифрового підпису.

Підгрупа 3В. Вибір рішень для реалізації платіжного сервісу.

Підгрупа 3С. Вибір рішень для реалізації мобільного додатку шифрування/електронного цифрового підпису.

Оформлення результатів роботи. Технічні вимоги до системи із обґрунтуванням обраних рішень.

Лабораторна роботи № 3.

Тема: Реалізація основних асиметричних криптосистем.

Мета роботи: Дослідження можливостей побудови загальних та спеціальних криптографічних протоколів за допомогою асиметричних криптосистем.

Необхідні теоретичні відомості. Необхідні теоретичні відомості містяться в роботах

1. Б. Шнайер Прикладная криптография. Протоколы, алгоритмы, исходные тексты на языке Си. – М.:Изд-во ТРИУМФ, 2002. -816 с.

Завдання на лабораторну роботу

Для першого типу лабораторних робіт – дослідити можливість реалізації одного з чотирьох криптографічних протоколів: розділення секрету, сліпого цифрового підпису, несуперечливого цифрового підпису та розподілу ключів для симетричної криптосистеми за допомогою різних асиметричних алгоритмів (не менше як двох) та порівняти їх ефективність за обраним критерієм.

Підгрупа 1А. Розподіл секрету.

Підгрупа 1В. Розподіл ключів.

Підгрупа 1С. Сліпий цифровий підпис.

Для другого типу лабораторних робіт – розробити реалізацію асиметричної криптосистеми.

Варіанти завдань другого типу.

Підгрупа 2А. Бібліотека OpenSSL під Windows платформу. Кр/с Ель Гамаля. [1] с. 535.

Підгрупа 2В. Бібліотека PyCrypto під Linux платформу. Стандарт ECDSA.

Підгрупа 2С. Бібліотека Crypto++ під Android/MacOs/Ios платформу. Реалізація несуперечного цифрового підпису.

Оформлення результатів Контрольний приклад роботи з асиметричною криптосистемою.

Для третього типу лабораторних робіт – розробка реалізацій ІТ-систем.

Варіанти завдань третього типу.

Підгрупа 3А. Реалізація Web-сервісу електронного цифрового підпису.

Підгрупа 3В. Реалізація платіжного сервісу.

Підгрупа 3С. Реалізація мобільного додатку шифрування/електронного цифрового підпису.

Лабораторна робота № 4.

Тема: Дослідження особливостей реалізації існуючих програмних систем, які використовують криптографічні механізми захисту інформації.

Мета роботи: Отримання практичних навичок побудови гібридних криптосистем.

Необхідні теоретичні відомості. Необхідні теоретичні відомості містяться в роботах.

1. Б. Шнайер Прикладная криптография. Протоколы, алгоритмы, исходные тексты на языке Си. – М.:Изд-во ТРИУМФ, 2002. -816 с.

Завдання на лабораторну роботу

Для першого типу лабораторних робіт – дослідити основні задачі, що виникають при програмній реалізації криптосистем. Запропонувати методи вирішення задачі контролю доступу до ключової інформації, що зберігається в оперативній пам'яті ЕОМ для різних (обраних) операційних систем. Запропонувати методи вирішення задачі контролю правильності функціонування програми криптографічної обробки інформації. Порівняти з точки зору вирішення цих задач інтерфейси Crypto API, PKCS 11.

Підгрупа 1A. Реалізація для інтелектуальної картки, токена.

Підгрупа 1B. Реалізація для User Endpoint terminal.

Підгрупа 1C. Реалізація для провайдера хмарних послуг.

Оформлення результатів роботи: звіт з методами вирішення поставлених задач.

Для другого типу лабораторних робіт – розробити реалізацію асиметричної криптосистеми у відповідності до стандартних вимог Crypto API або стандартів PKCS та дослідити стійкість стандартних криптопровайдерів до атак, що використовують недосконаліть механізмів захисту операційної системи.

Варіанти завдань другого типу.

Підгрупа 2A. Бібліотека OpenSSL під Windows платформу. Кр/с Ель Гамаля. [1] с. 535.

Підгрупа 2B. Бібліотека PyCrypto під Linux платформу. Стандарт ECDSA.

Підгрупа 2C. Бібліотека PyCrypto під Crypto++ під Android/MacOs/Ios платформу. Реалізація несуперечного цифрового підпису.

Оформлення результатів: контрольний приклад роботи з асиметричною криптосистемою. Приклад атаки або демонстрація їх неможливості.

Для третього типу лабораторних робіт – розробка реалізацій IT-систем у відповідності до стандартних вимог Crypto API або стандартів PKCS.

Варіанти завдань третього типу.

Підгрупа 3А. Реалізація Web-сервісу електронного цифрового підпису.

Підгрупа 3В. Реалізація платіжного сервісу.

Підгрупа 3С. Реалізація мобільного додатку шифрування/електронного цифрового підпису.

Оформлення результатів: контрольний приклад роботи з асиметричною криптосистемою. Приклад атаки за побічним каналом або демонстрація їх неможливості.