Министерство образования Республики Беларусь
Учреждение образования «Белорусский государственный университет информатики и радиоэлектроники»

Факультет компьютерных систем и сетей

Кафедра информатики

Дисциплина: Методы защиты информации

ОТЧЁТ
к лабораторной работе №7
на тему

КРИПТОГРАФИЯ С ИСПОЛЬЗОВАНИЕМ ЭЛЛИПТИЧЕСКИХ КРИВЫХ

Выполнил: студент гр.253505
Снежко М.А.

Проверил: ассистент кафедры информатики
Герчик А.В.

Минск 2025

СОДЕРЖАНИЕ

1 Цель работы 3
2 Ход работы 4
Заключение 5
Приложение А (обязательное) Листинг программного кода 6

1 ЦЕЛЬ РАБОТЫ

Современный этап развития информационных технологий характеризуется повсеместным использованием криптографических методов для защиты данных. Одним из наиболее перспективных направлений в этой области является криптография на эллиптических кривых (*Elliptic Curve Cryptography, ECC*), которая предлагает высокий уровень безопасности при относительно небольших вычислительных затратах. Это особенно важно в условиях растущих требований к производительности и энергоэффективности вычислительных систем.

Математический аппарат эллиптических кривых основан на использовании алгебраических структур специального типа. Криптосистемы на эллиптических кривых опираются на сложность решения задачи дискретного логарифмирования в группе точек кривой. Важным преимуществом *ECC* является возможность использования ключей значительно меньшей длины по сравнению с традиционными криптосистемами при обеспечении сопоставимого уровня безопасности. Это делает данную технологию особенно привлекательным для применений в мобильных устройствах и системах с ограниченными ресурсами.

Изучение криптографии на эллиптических кривых представляет значительный теоретический и практический интерес. Понимание математических основ *ECC* позволяет специалистам в области информационной безопасности более эффективно проектировать и реализовывать защищенные системы. Практическое освоение алгоритмов работы с эллиптическими кривыми способствует глубокому пониманию современных криптографических методов и принципов их применения.

2 ХОД РАБОТЫ

Программное средство реализовано при помощи языка программирования *Javascript*.

На первом этапе проведено изучение математических основ и принципов работы с эллиптическими кривыми. Особое внимание уделено изучению теории групп точек эллиптической кривой, операций сложения и удвоения точек, а также алгоритма умножения точки на скаляр. Исследованы механизмы генерации ключевых пар и принципы использования открытого и закрытого ключей для шифрования и дешифрования данных.

После освоения теоретического материала приступили к практической реализации. Были написаны функции для задания параметров эллиптической кривой, генерации базовой точки и создания ключевой пары. Реализованы алгоритмы шифрования данных с использованием открытого ключа получателя и дешифрования с применением закрытого ключа.

На рисунке 3.1 изображен результат работы программы.

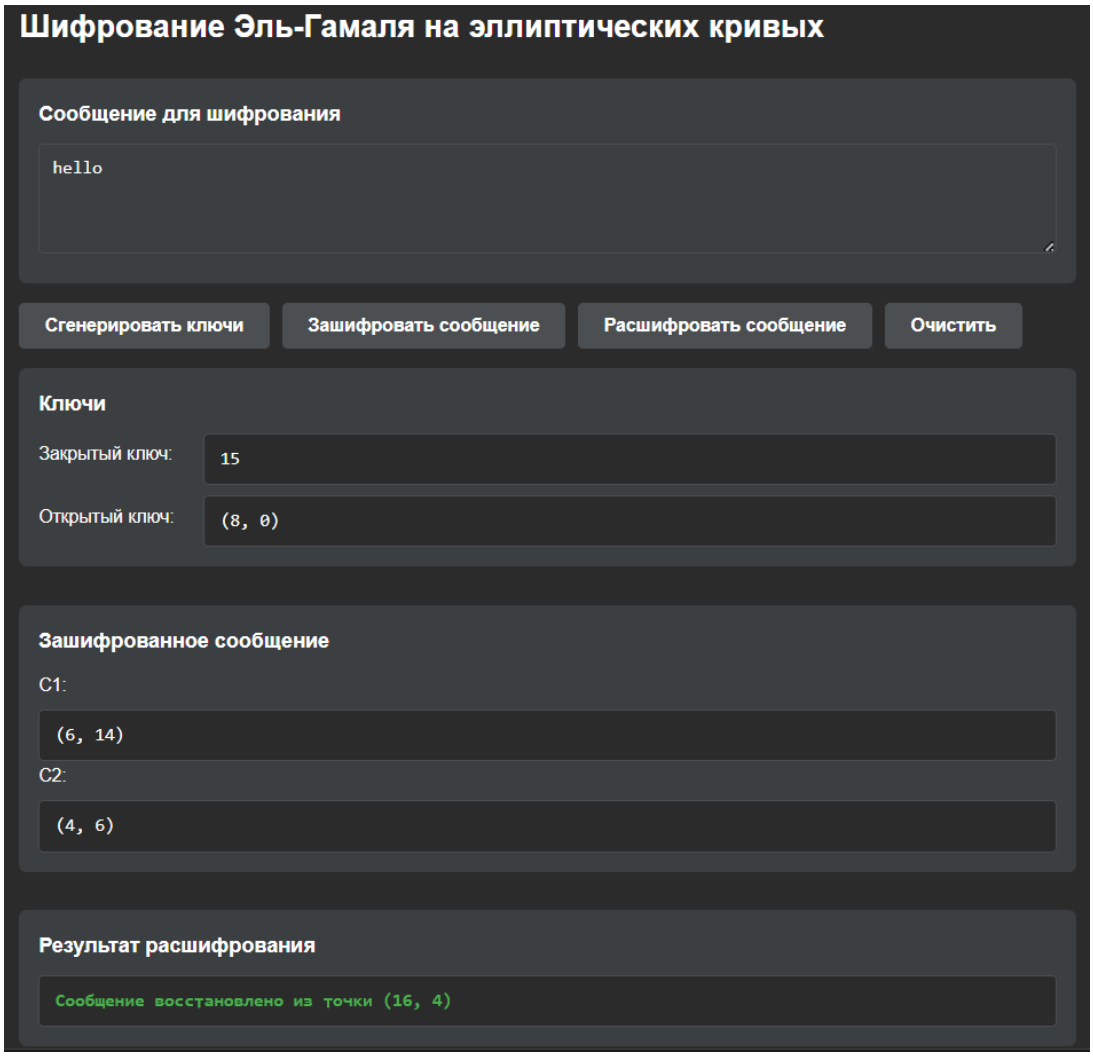

Рисунок 3.1 – Результат работы программы

ЗАКЛЮЧЕНИЕ

В результате выполнения лабораторной работы была успешно реализована система шифрования на основе методов эллиптической криптографии. Практическая реализация охватила все ключевые аспекты работы с эллиптическими кривыми: генерацию параметров кривой, создание ключевой пары, алгоритмы шифрования данных с использованием открытого ключа и процедуру дешифрования с применением закрытого ключа. Основным достижением работы стало создание работоспособного программного средства, наглядно демонстрирующего принципы построения криптографических систем на эллиптических кривых.

Реализация подтвердила теоретические положения эллиптической криптографии, в частности, важность корректного выполнения математических операций над точками кривой и строгого соблюдения протоколов шифрования. Особое значение имела точная реализация алгоритма умножения точки на скаляр и операций сложения точек эллиптической кривой. Разработанная система продемонстрировала способность надежно шифровать данные и обеспечивать их конфиденциальность при передаче.

Таким образом, реализованная система шифрования на эллиптических кривых представляет собой законченное решение, которое демонстрирует принципы построения современных криптографических средств защиты информации и служит основой для дальнейшего изучения методов обеспечения конфиденциальности данных.

ПРИЛОЖЕНИЕ А
(обязательное)
Листинг программного кода

```
class EncryptionApp {
    constructor() {
        this.privateKey = null;
        this.publicKey = null;
        this.encryptedMessage = null;
        this.currentMessage = '';

        this.initializeElements();
        this.attachEventListeners();
    }

    initializeElements() {
        this.messageInput = document.getElementById('message-input');

        this.generateKeysBtn = document.getElementById('generate-keys-btn');
        this.encryptBtn = document.getElementById('encrypt-btn');
        this.decryptBtn = document.getElementById('decrypt-btn');
        this.clearBtn = document.getElementById('clear-btn');

        this.privateKeyDisplay = document.getElementById('private-key');
        this.publicKeyDisplay = document.getElementById('public-key');
        this.c1Display = document.getElementById('c1-display');
        this.c2Display = document.getElementById('c2-display');
        this.decryptionResult = document.getElementById('decryption-result');

        this.tabButtons = document.querySelectorAll('.tab-button');
        this.tabContents = document.querySelectorAll('.tab-content');
    }

    attachEventListeners() {
        this.generateKeysBtn.addEventListener('click',          ()          =>
this.generateKeys());
        this.encryptBtn.addEventListener('click',             ()             =>
this.encryptMessage());
        this.decryptBtn.addEventListener('click',             ()             =>
this.decryptMessage());
        this.clearBtn.addEventListener('click', () => this.clearAll());

        this.tabButtons.forEach(button => {
            button.addEventListener('click', () => this.switchTab(button));
        });
    }

    switchTab(clickedButton) {
        const tabId = clickedButton.getAttribute('data-tab');

        this.tabButtons.forEach(button => button.classList.remove('active'));
        clickedButton.classList.add('active');

        this.tabContents.forEach(content                                    =>
content.classList.remove('active'));
        document.getElementById(tabId).classList.add('active');
    }
```