Министерство образования Республики Беларусь

Учреждение образования «БЕЛОРУССКИЙ ГОСУДАРСТВЕННЫЙ ТЕХНОЛОГИЧЕСКИЙ УНИВЕРСИТЕТ»

**Отчет по выполненным лабораторным работам**

по Защите Информации

Выполнил:

студент 4 курса 1 группы

Вакуленчик В.С.

Преподаватель:

Сазонова Д.В.

Минск 2024

**Лабораторная работа №1**

ОСНОВЫ ТЕОРИИ ЧИСЕЛ И ИХ ИСПОЛЬЗОВАНИЕ В КРИПТОГРАФИИ

1 Теоретические сведения

Определение 2. Натуральные числа являются подмножеством целых чисел и образуют множество N: {1, 2, 3, ...}.

Определение 3. Делимость – одно из основных понятий тео рии чисел. Если для некоторого целого числа a и натурального числа b существует целое число q, при котором bq = a, то говорят, что число a делится на b. В этом случае b называется делителем числа a, а a называется кратным числу b.

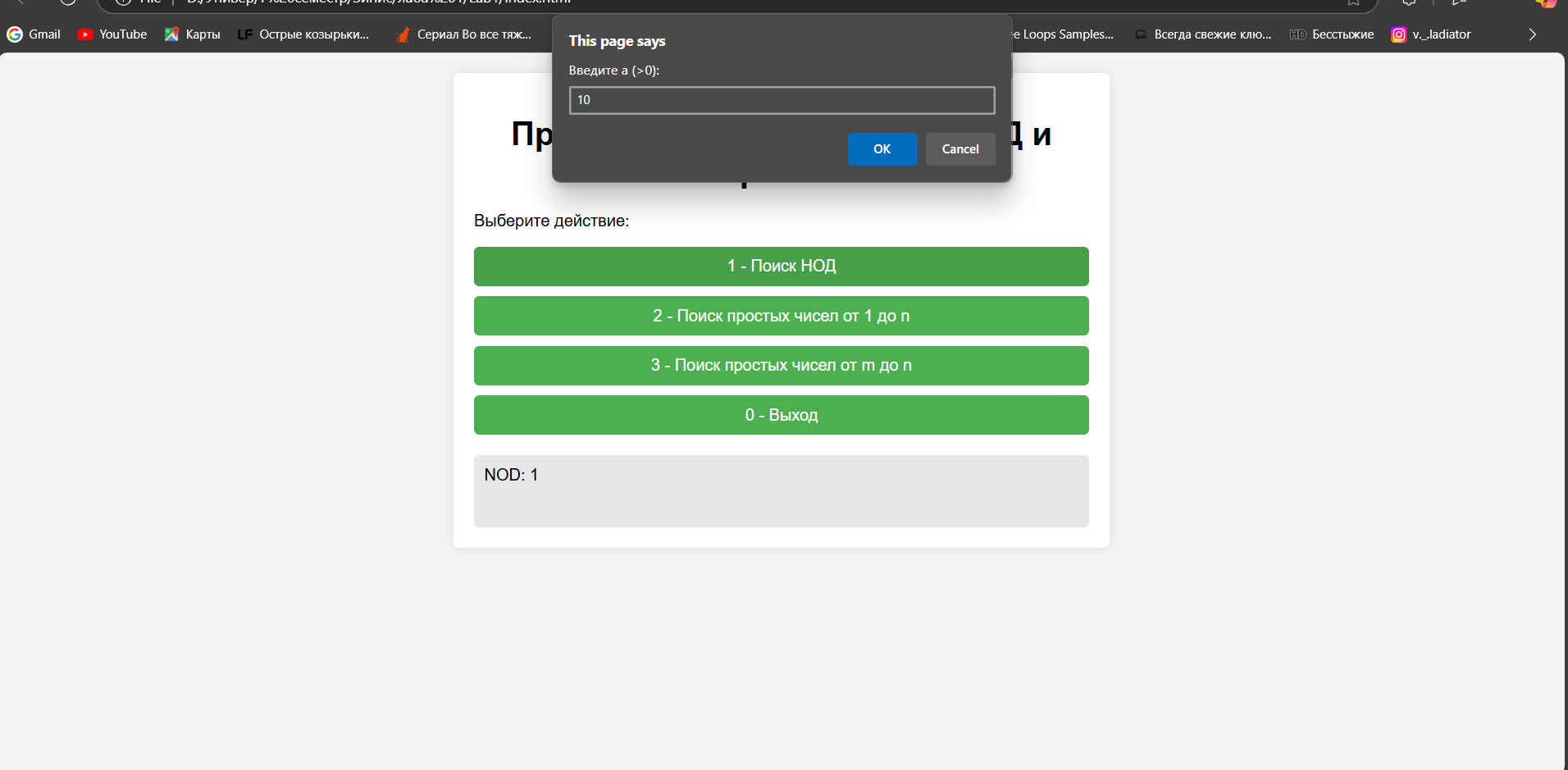
Если число не имеет делителей, кроме самого себя и еди ницы, то оно называется простым, а если у числа есть еще делители, то составным.

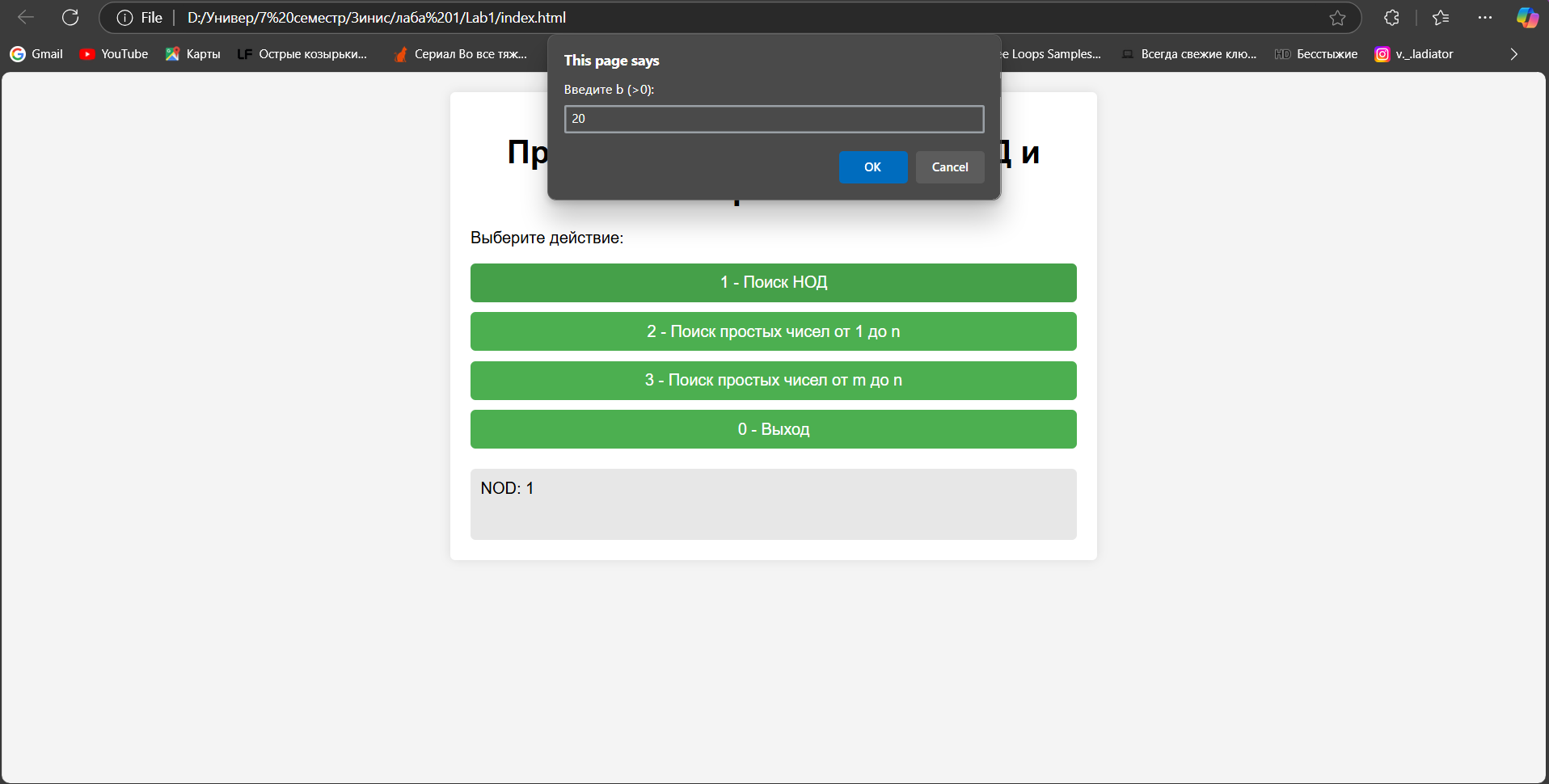
Определение 8. Если два простых числа отличаются на 2, то их называют числами-близнецами.

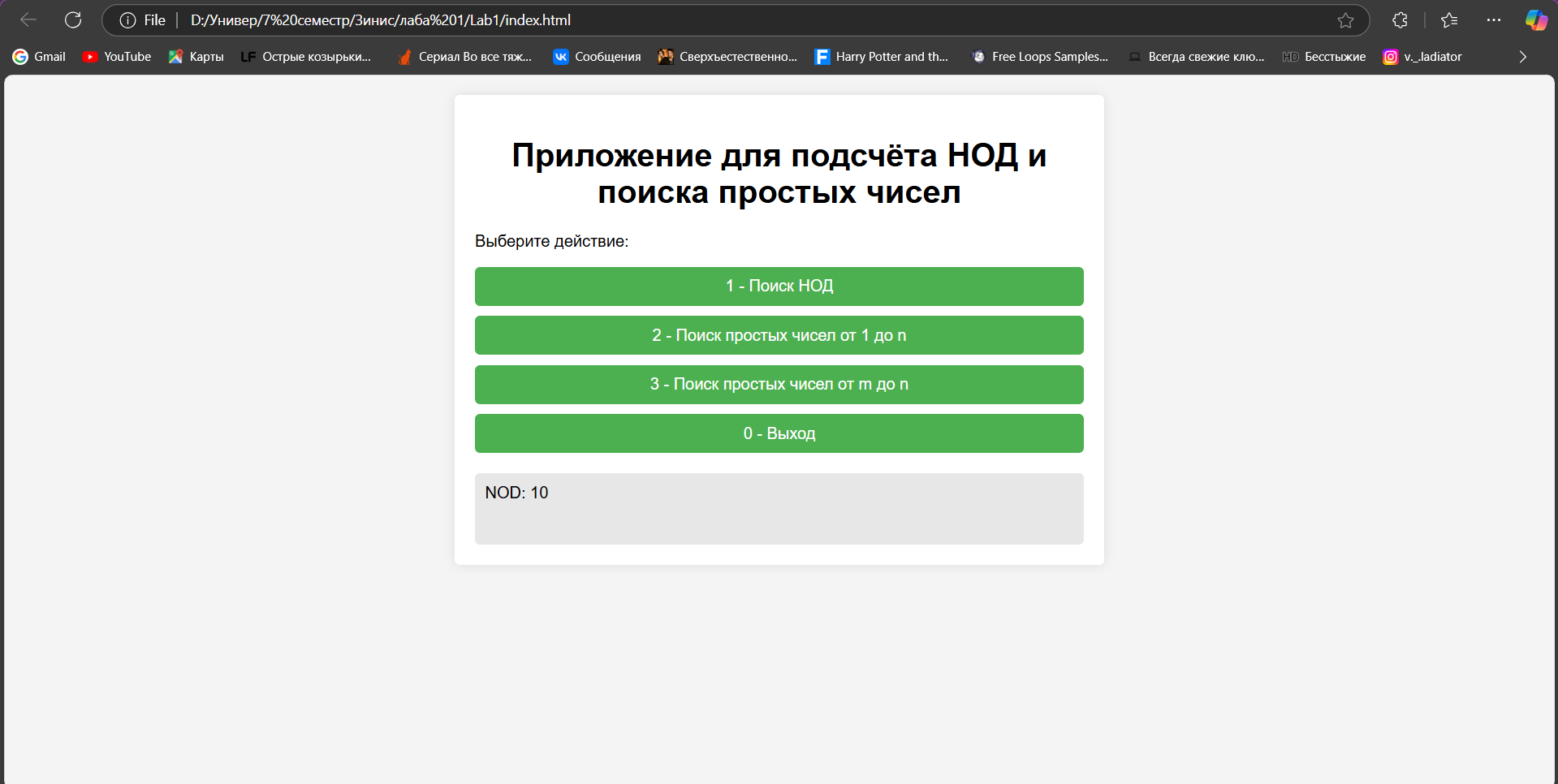
Определение 10. Взаимно простыми являются целые числа, наибольший общий делитель которых равен 1.

2 Практическая часть

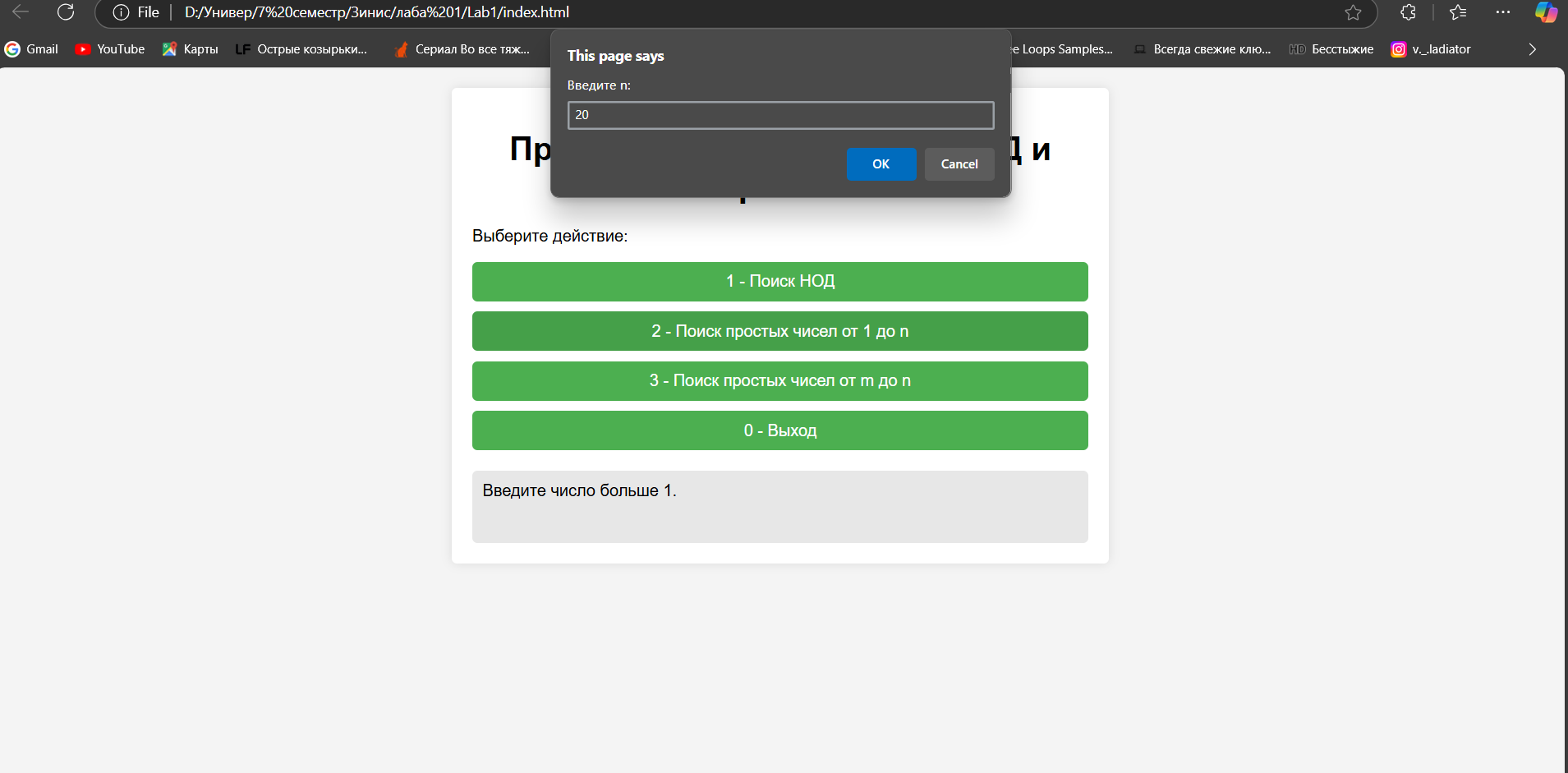
Поиск НОД:

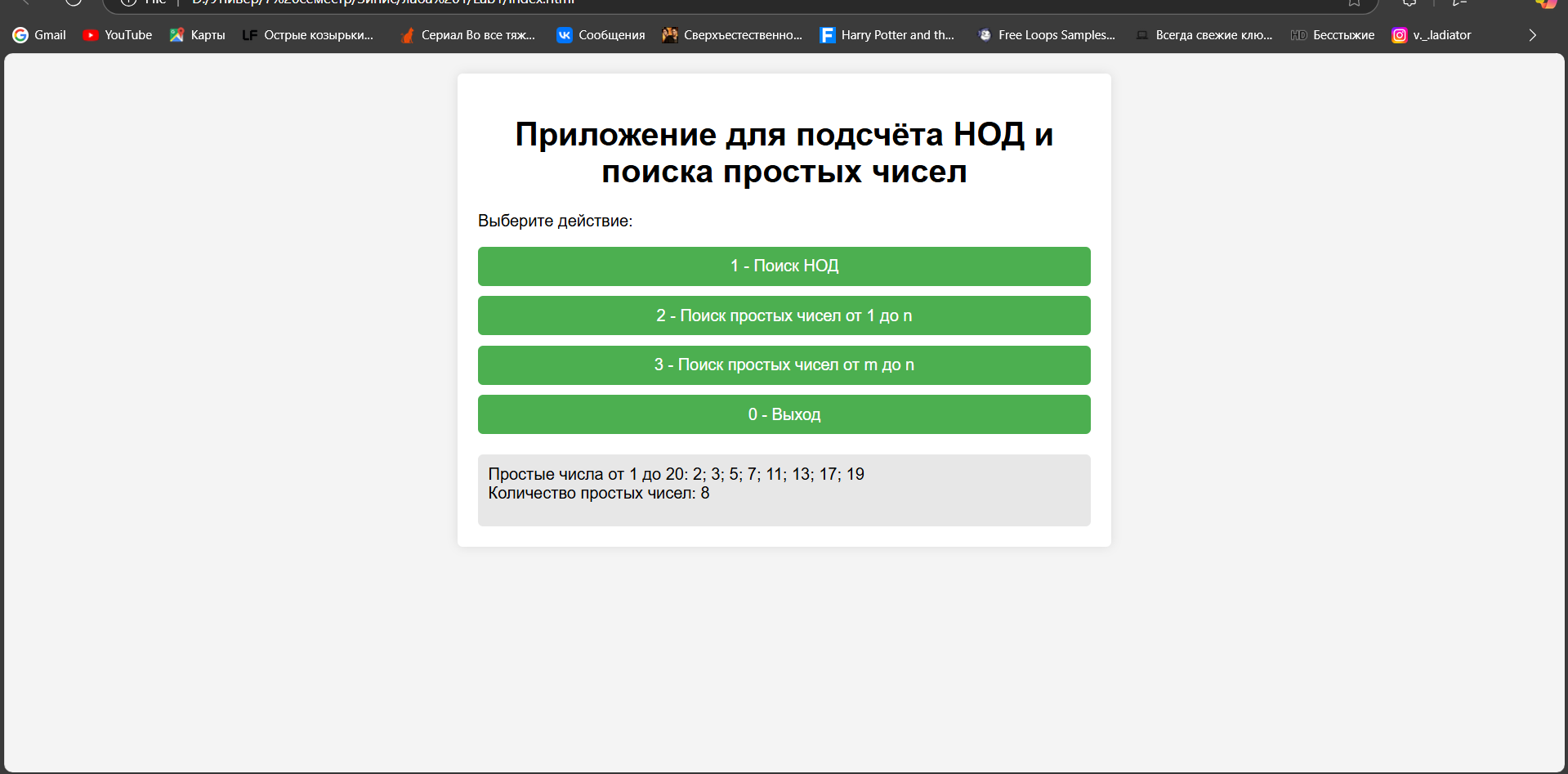




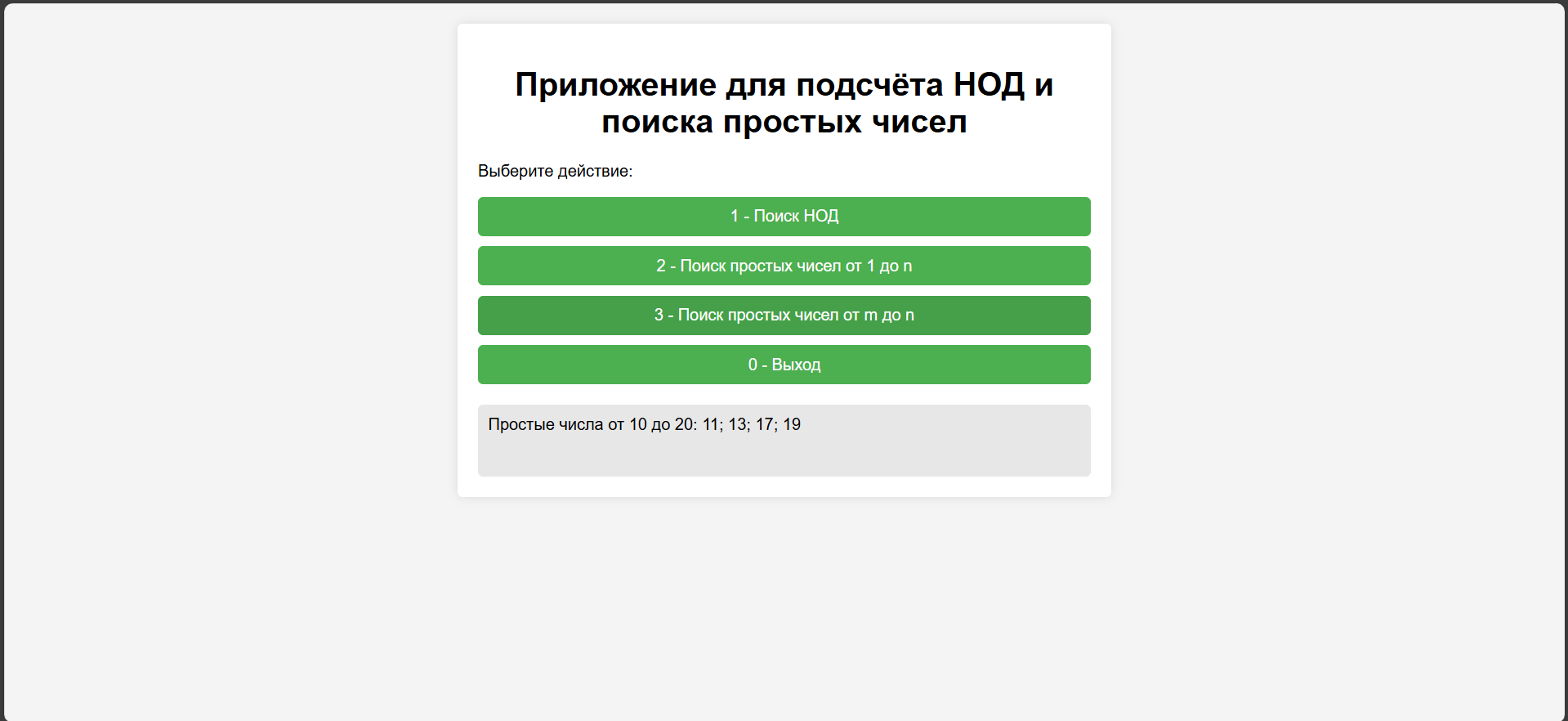


Поиск простых чисел от 1 до n:





Поиск простых чисел от m до n:



Вывод

В процессе выполнения лабораторной работы были изучены и освоены практические навыки разработки и использования приложений для работы с простыми числами.

**Лабораторная работа №2**

ИССЛЕДОВАНИЕ КРИПТОГРАФИЧЕСКИХ ШИФРОВ НА ОСНОВЕ ПОДСТАНОВКИ (ЗАМЕНЫ) СИМВОЛОВ

1 Теоретические сведения

Сущность подстановочных шифров заключается в том, что как исходный текст (М), так и зашифрованный текст (С) формируются с использованием одного или разных алфавитов, где секретной частью является алгоритм подстановки. Одним из основных недостатков моноалфавитных шифров является их низкая стойкость к взлому, поскольку криптоанализ часто основывается на частотном анализе букв в исходном тексте. Если применять одновременно операции сложения и умножения по модулю n к элементам алфавита (их индексам), можно создать систему подстановок, известную как аффинная система Цезаря.

Омофонические шифры, или шифры с однозвучной заменой, были разработаны для усложнения частотного анализа зашифрованного текста, скрывая реальную частоту символов с помощью омофонии. Существует определенное сходство между подстановочными шифрами и шифрами гаммирования, хотя последние считаются отдельным классом. Оба типа шифров используют таблицы ключей для выполнения операций, и в обоих случаях происходит замена одних символов другими.

2 Практическая часть

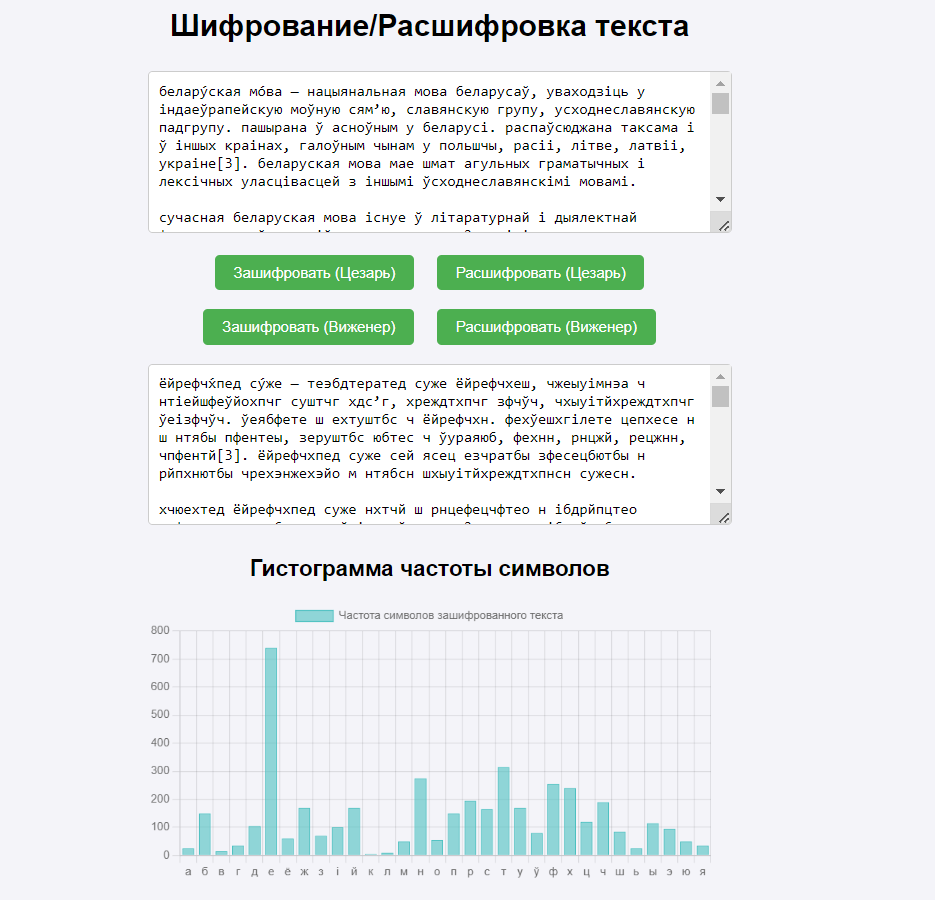


Рисунок 2.1 – Результат шифрования исходного сообщения методом аффиного преобразования;



Рисунок 2.2 – Результат дешифрования исходного сообщения методом аффиного преобразования;

На вышеуказанных рисунках отображен процесс работы веб-приложения с шифрованием и дешифрованием исходного сообщения методом аффиного преобразования.



Рисунок 2.3 – результат шифрования исходного сообщения шифром Виженера;



Рисунок 2.4 – результат дешифрования исходного сообщения шифром Виженера;

На вышеуказанных рисунках отображен процесс работы веб-приложения с шифрованием и дешифрованием исходного сообщения шифром Виженера с использованием ключа Вакуленчик.

Основные функции программы представлены ниже.

|  |
| --- |
| // Шифр Цезаря  function caesarEncrypt() {      const text = document.getElementById("inputText").value.toLowerCase();      const encryptedText = text.split('').map(char => {          const index = alphabet.indexOf(char);          if (index === -1) return char;          return alphabet[(index + 5) % n];      }).join('');      document.getElementById("outputText").value = encryptedText;      // Подсчет частоты символов для исходного текста      const originalFrequency = countFrequency(text);      drawFrequencyChart(originalFrequency, 'Частота символов исходного текста');      // Подсчет частоты символов для зашифрованного текста      const encryptedFrequency = countFrequency(encryptedText);      setTimeout(() => drawFrequencyChart(encryptedFrequency, 'Частота символов зашифрованного текста'), 2000); // Ожидание 2 секунды перед перерисовкой  }  // Шифр Виженера  function vigenereEncrypt() {      const text = document.getElementById("inputText").value.toLowerCase();      let encryptedText = '';      let keyIndex = 0;      for (let i = 0; i < text.length; i++) {          const char = text[i];          const index = alphabet.indexOf(char);          if (index === -1) {              encryptedText += char;          } else {              const keyChar = keyWord[keyIndex % keyWord.length];              const keyCharIndex = alphabet.indexOf(keyChar);              const newIndex = (index + keyCharIndex) % n;              encryptedText += alphabet[newIndex];              keyIndex++;          }      }      document.getElementById("outputText").value = encryptedText;      // Подсчет частоты символов для исходного текста      const originalFrequency = countFrequency(text);      drawFrequencyChart(originalFrequency, 'Частота символов исходного текста');      // Подсчет частоты символов для зашифрованного текста      const encryptedFrequency = countFrequency(encryptedText);      setTimeout(() => drawFrequencyChart(encryptedFrequency, 'Частота символов зашифрованного текста'), 2000); // Ожидание 2 секунды перед перерисовкой  } |

Вывод

В процессе выполнения лабораторной работы были изучены и освоены практические навыки разработки и использования приложений для реализации подстановочных шифров.

**Лабораторная работа №3**

ИССЛЕДОВАНИЕ КРИПТОГРАФИЧЕСКИХ ШИФРОВ НА ОСНОВЕ ПЕРЕСТАНОВКИ СИМВОЛОВ

Цель: изучение и приобретение практических навыков разра ботки и использования приложений для реализации перестановоч ных шифров (работа рассчитана на 4 часа аудиторных занятий).

Задачи:

1. Закрепить теоретические знания по алгебраическому описа нию, алгоритмам реализации операций зашифрования/расшифро вания и оценке криптостойкости перестановочных шифров.

2. Ознакомиться с особенностями реализации и свойствами различных перестановочных шифров на основе готового программ ного средства (L\_LUX).

3. Разработать приложение для реализации указанных препода вателем методов перестановочного зашифрования/расшифрования.

4. Выполнить исследование криптостойкости шифров на ос нове статистических данных о частотах появления символов в ис ходном и зашифрованном сообщениях.

5. Оценить скорость зашифрования/расшифрования реализо ванных способов шифров.

6. Результаты выполнения лабораторной работы оформить в виде описания разработанного приложения, методики выполне ния экспериментов с использованием приложения и результатов эксперимента.

1 Теоретические сведения

Шифры на основе перестановки символов (транспозиционные шифры) — это криптографические методы, где шифрование происходит путём изменения порядка символов в сообщении без их замены. Основная цель таких шифров — усложнить текст для несанкционированного доступа, сохраняя при этом исходный набор символов.

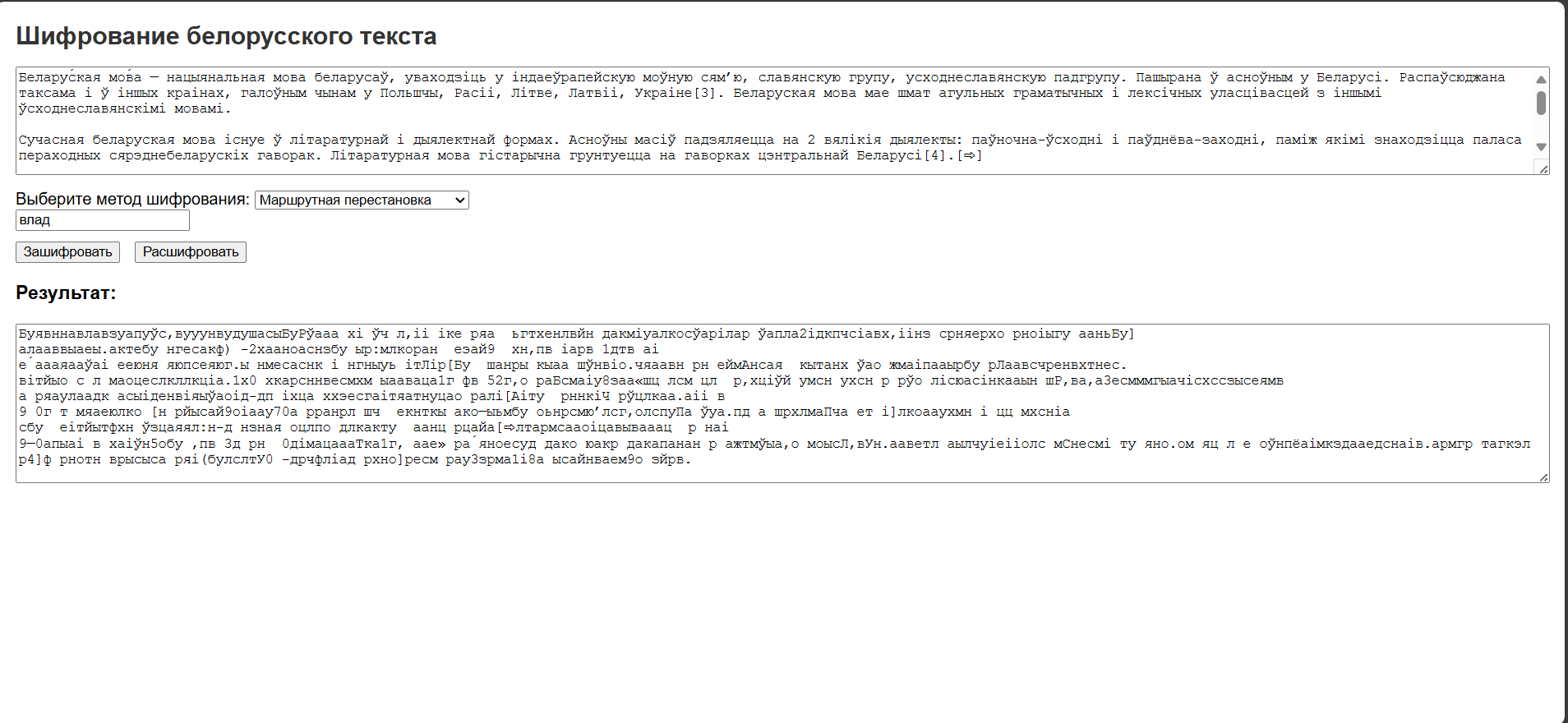
**Основные аспекты исследования:**

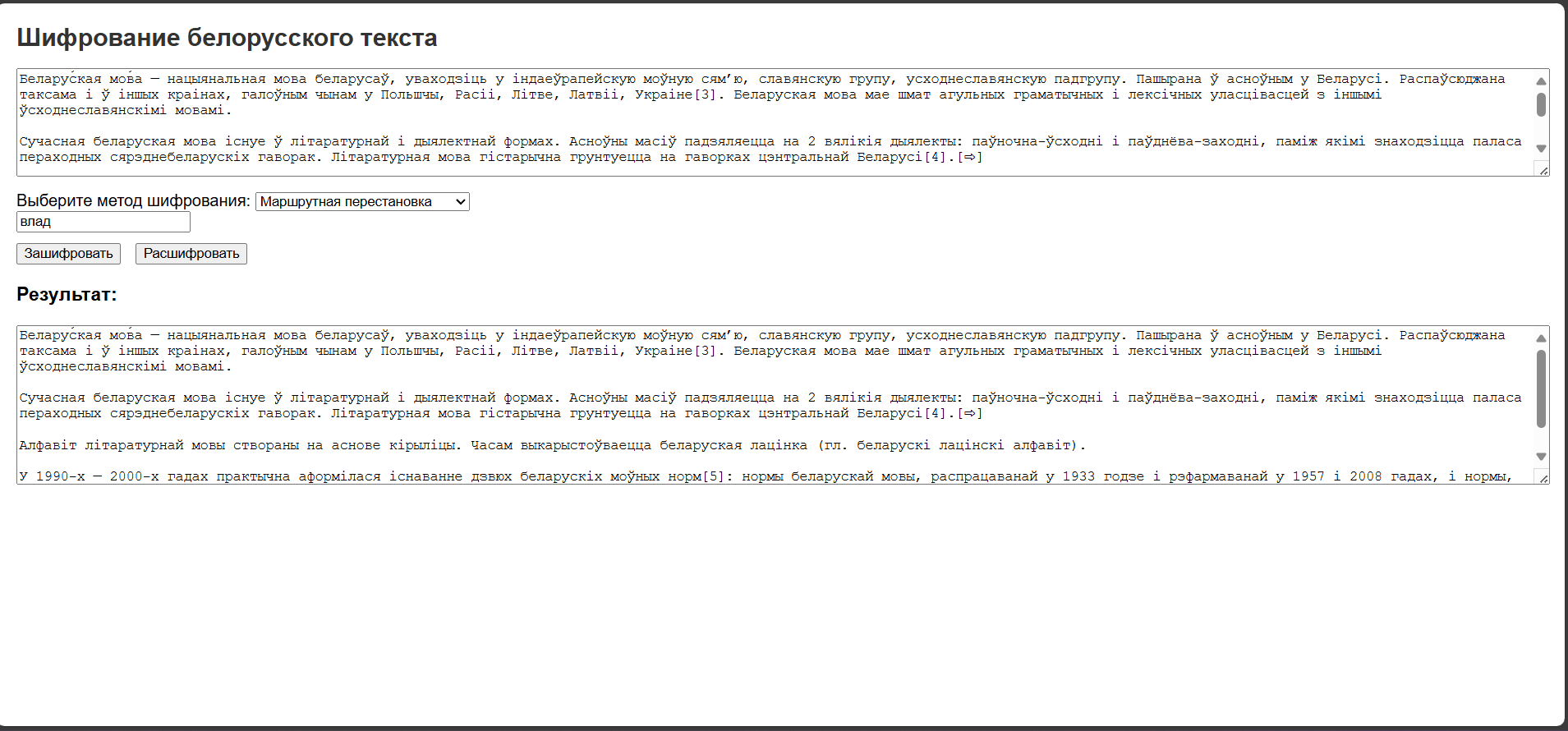
1. **Принципы работы:**
   * Символы исходного текста перемещаются в определённом порядке согласно ключу шифрования.
   * Шифрование и расшифрование зависят от алгоритма перестановки.
2. **Примеры алгоритмов:**
   * **Столбцовый шифр:** текст записывается по строкам в таблицу, а чтение происходит по столбцам в порядке, заданном ключом.
   * **Шифр "решётка":** используются специальные матрицы или схемы для упорядочивания символов.
3. **Исследуемые характеристики:**
   * Устойчивость шифра к криптоанализу (например, частотному анализу).
   * Эффективность восстановления текста при перехвате части данных.
   * Влияние длины ключа на безопасность.
4. **Преимущества:**
   * Простота реализации.
   * Подходящи для комбинирования с другими методами (например, заменой символов).
5. **Недостатки:**
   * Без использования сложных ключей такие шифры легко поддаются анализу.
   * Устойчивость сильно зависит от длины и секретности ключа.

2 Практическая часть



Вводим ключ и производим шифрование:



Производим расшифрование и получаем исходный текст:

Вывод

В процессе выполнения лабораторной работы были изучены и освоены практические навыки разработки и использования приложений для реализации перестановочных шифров.

**Лабораторная работа №4**

ИЗУЧЕНИЕ УСТРОЙСТВА И ФУНКЦИОНАЛЬНЫХ ОСОБЕННОСТЕЙ ШИФРОВАЛЬНОЙ МАШИНЫ «ЭНИГМА»

1 Теоретические сведения

Шифровальная машина «Энигма» — это электромеханическое устройство, использовавшееся для шифрования и расшифрования сообщений, широко применявшееся немецкими военными в XX веке.

**Устройство:**

1. **Клавиатура и лампы:** для ввода и отображения букв.
2. **Роторы:** ключевой элемент, отвечающий за шифрование. Каждый ротор создавал уникальную перестановку символов и вращался после каждой буквы.
3. **Рефлектор:** обеспечивал симметричность шифрования, возвращая сигнал обратно через роторы.
4. **Переключательная панель:** дополнительно изменяла соответствие символов, повышая сложность.

**Функциональные особенности:**

1. **Динамичность шифрования:** после ввода каждой буквы роторы вращались, создавая новый шифр.
2. **Большое количество ключей:** благодаря комбинациям роторов, их начальных положений и панели, общее число настроек достигало триллионов.
3. **Симметричность:** один и тот же ключ использовался для шифрования и расшифрования.

**Исследования:**

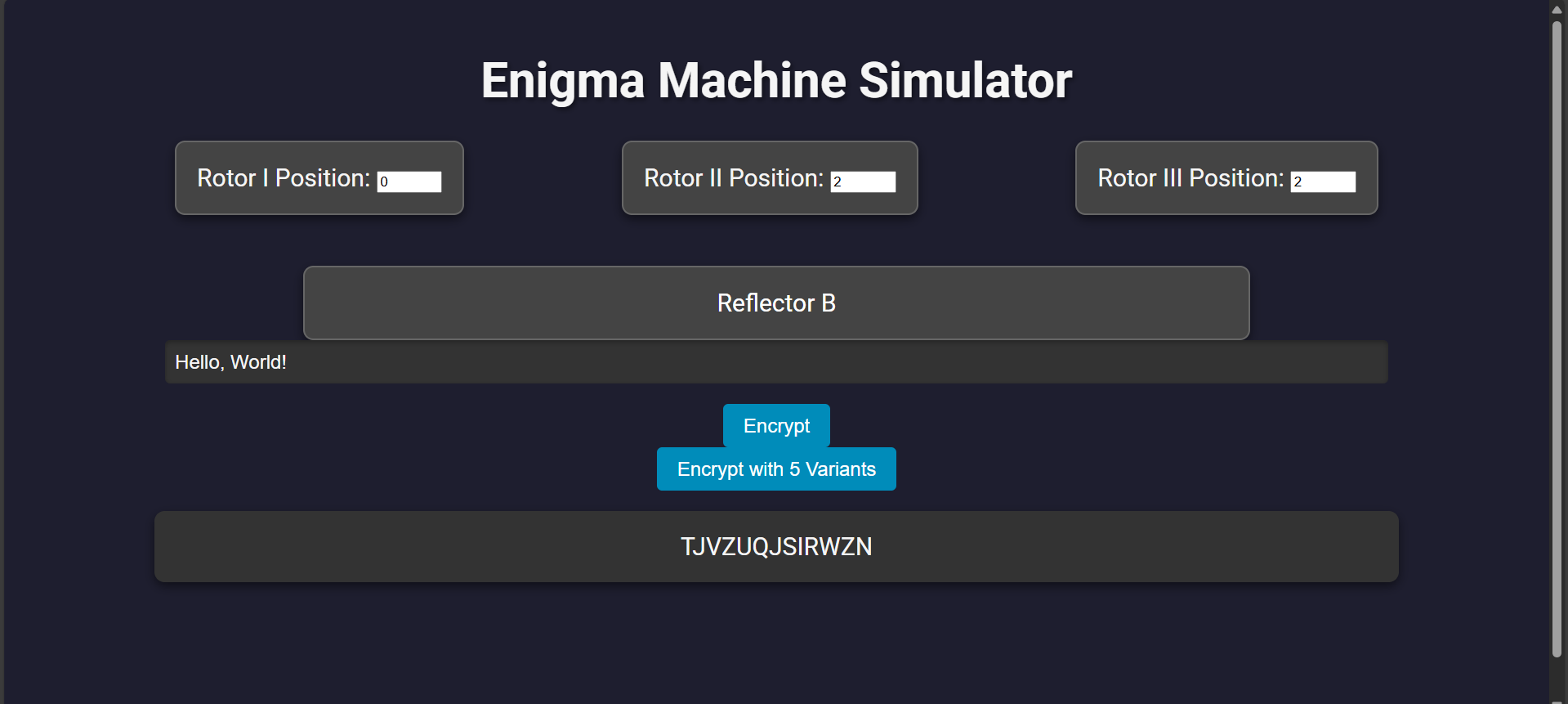
Изучение устройства «Энигмы» показало, что её стойкость кроется в сложности механизма, но регулярные ошибки операторов и утечка информации позволили криптоаналитикам (например, в Блетчли-Парк под руководством Алана Тьюринга) взломать шифры, что сыграло ключевую роль во Второй мировой войне.

**Значение:**

«Энигма» стала важным этапом в истории криптографии и стимулировала развитие современных методов шифрования и вычислительных технологий.

2 Практическая часть

Можно зашифровать одиночную запись:



Также можно произвести шифрование пятью вариантами:



Вывод

В процессе выполнения лабораторной работы были изучены и освоены практические навыки разработки и использования приложений для реализации механизма работы машины «Энигма».

**Лабораторная работа №5**

ИССЛЕДОВАНИЕ БЛОЧНЫХ ШИФРОВ

1 Теоретические сведения

Блочные шифры — это криптографические алгоритмы, которые разбивают входные данные на блоки фиксированной длины и шифруют каждый блок с использованием ключа. Они являются основой современной симметричной криптографии.

### Основные аспекты исследования:

1. **Принцип работы:**
   * Данные разбиваются на блоки одинакового размера (например, 64 или 128 бит).
   * Каждый блок шифруется отдельно или в зависимости от предыдущего блока, что зависит от режима работы.
2. **Режимы работы блочных шифров:**
   * **ECB (Electronic Codebook):** Каждый блок шифруется независимо. Уязвим для атак, если данные повторяются.
   * **CBC (Cipher Block Chaining):** Каждый блок шифруется с использованием результата предыдущего блока, повышая безопасность.
   * **CTR (Counter):** Преобразует блочный шифр в потоковый, шифруя последовательности счётчика.
3. **Характеристики:**
   * Сложность алгоритма и устойчивость к атакам.
   * Эффективность при шифровании больших объёмов данных.
   * Возможность использования в различных приложениях (хранилище данных, сетевые протоколы и т. д.).
4. **Примеры блочных шифров:**
   * **DES (Data Encryption Standard):** Устаревший шифр с длиной ключа 56 бит.
   * **AES (Advanced Encryption Standard):** Современный стандарт с длиной ключа 128, 192, или 256 бит, обладающий высокой стойкостью.

### Преимущества:

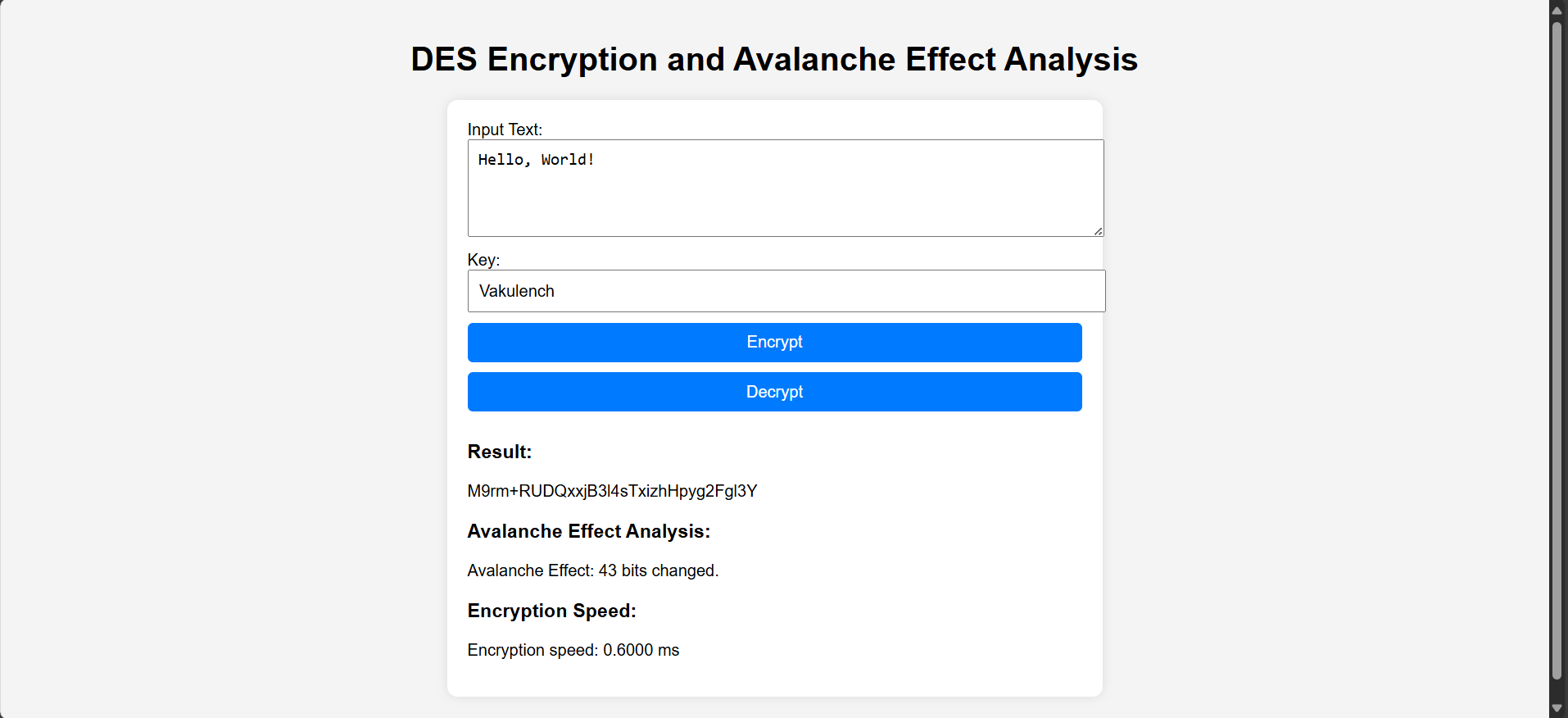
* Высокая скорость шифрования.
* Гибкость при использовании различных режимов работы.
* Простота аппаратной и программной реализации.

### Недостатки:

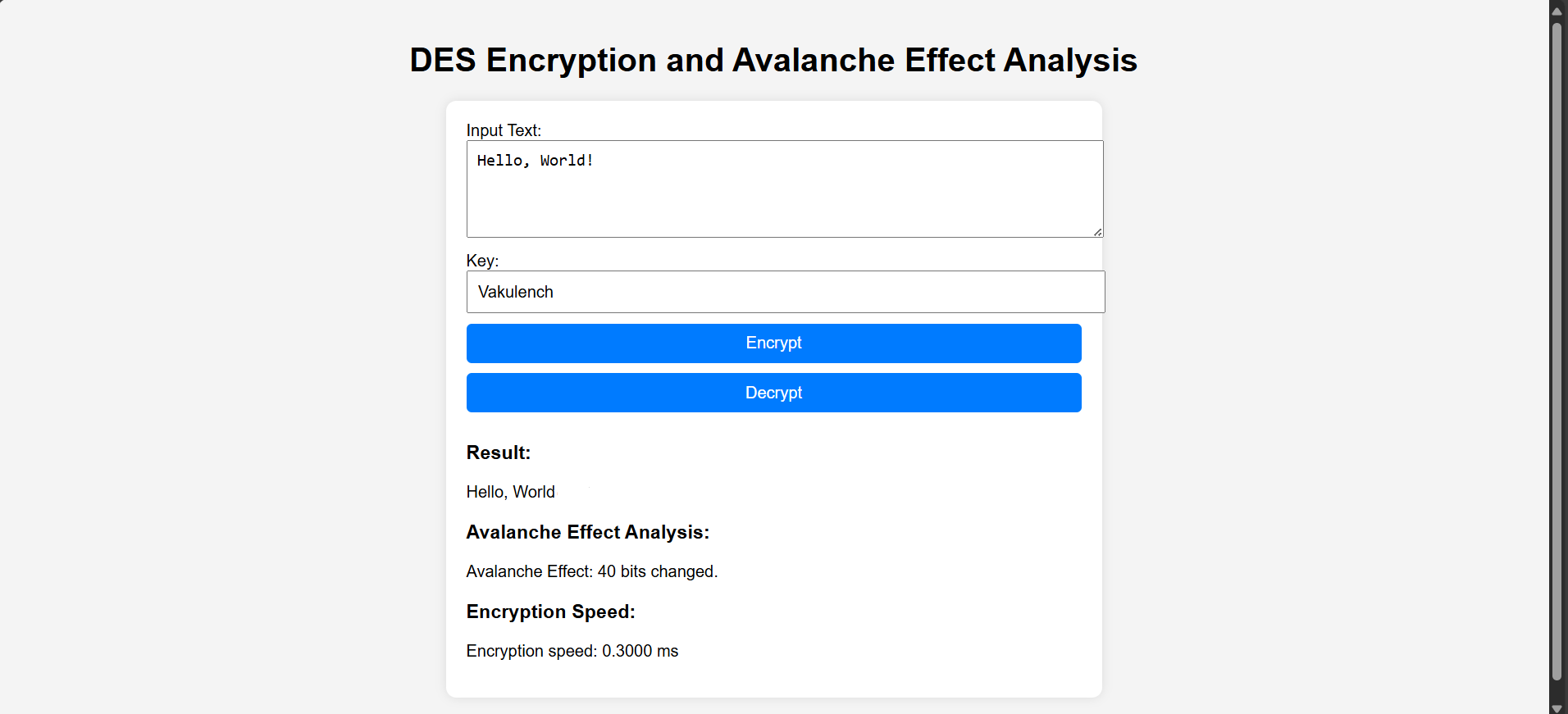
* Размер блока фиксирован, что может потребовать дополнения данных.
* Уязвимости зависят от выбранного режима работы (например, ECB).

2 Практическая часть

Шифрование через DES посредствам ввода исходного текста и ключа:



Расшифрование при нажатии на кнопку Decrypt:



Вывод

В процессе выполнения лабораторной работы были изучены и освоены практические навыки разработки и использования приложений для реализации блочных шифров.

**Лабораторная работа №6**

ИССЛЕДОВАНИЕ ПОТОКОВЫХ ШИФРОВ

1 Теоретические сведения

Потоковые шифры — это криптографические алгоритмы, которые шифруют данные по одному символу или биту за раз, в отличие от блочных шифров, работающих с фиксированными блоками данных. Они широко применяются для шифрования потоков данных в реальном времени, таких как голосовые или видеосообщения.

### Основные аспекты исследования:

1. **Принцип работы:**
   * Генерируется длинная последовательность (поток) псевдослучайных ключей (кея).
   * Каждый бит (или символ) исходного текста комбинируется с соответствующим битом потока с использованием операции XOR (или другой операции).
2. **Типы потоковых шифров:**
   * **Синхронные:** Зависимость только от текущего состояния генератора ключей. Если данные теряются, требуется синхронизация.
   * **Самосинхронизирующиеся:** Используют предыдущие зашифрованные биты для генерации ключей, что позволяет восстановить синхронизацию.
3. **Генераторы псевдослучайных последовательностей:**
   * Основой потокового шифра является генератор, который создаёт поток ключей.
   * Примеры: линейные сдвиговые регистры (LFSR), нелинейные генераторы, алгоритмы на основе хаоса.
4. **Примеры потоковых шифров:**
   * **RC4:** Один из наиболее известных, но устаревший из-за выявленных уязвимостей.
   * **Salsa20/ChaCha20:** Современные и безопасные шифры, широко применяемые в системах реального времени.

### Преимущества:

* Высокая скорость шифрования, особенно для потоковых данных.
* Нет необходимости в дополнении данных (паддинге), как в блочных шифрах.
* Эффективность при работе с длинными непрерывными потоками информации.

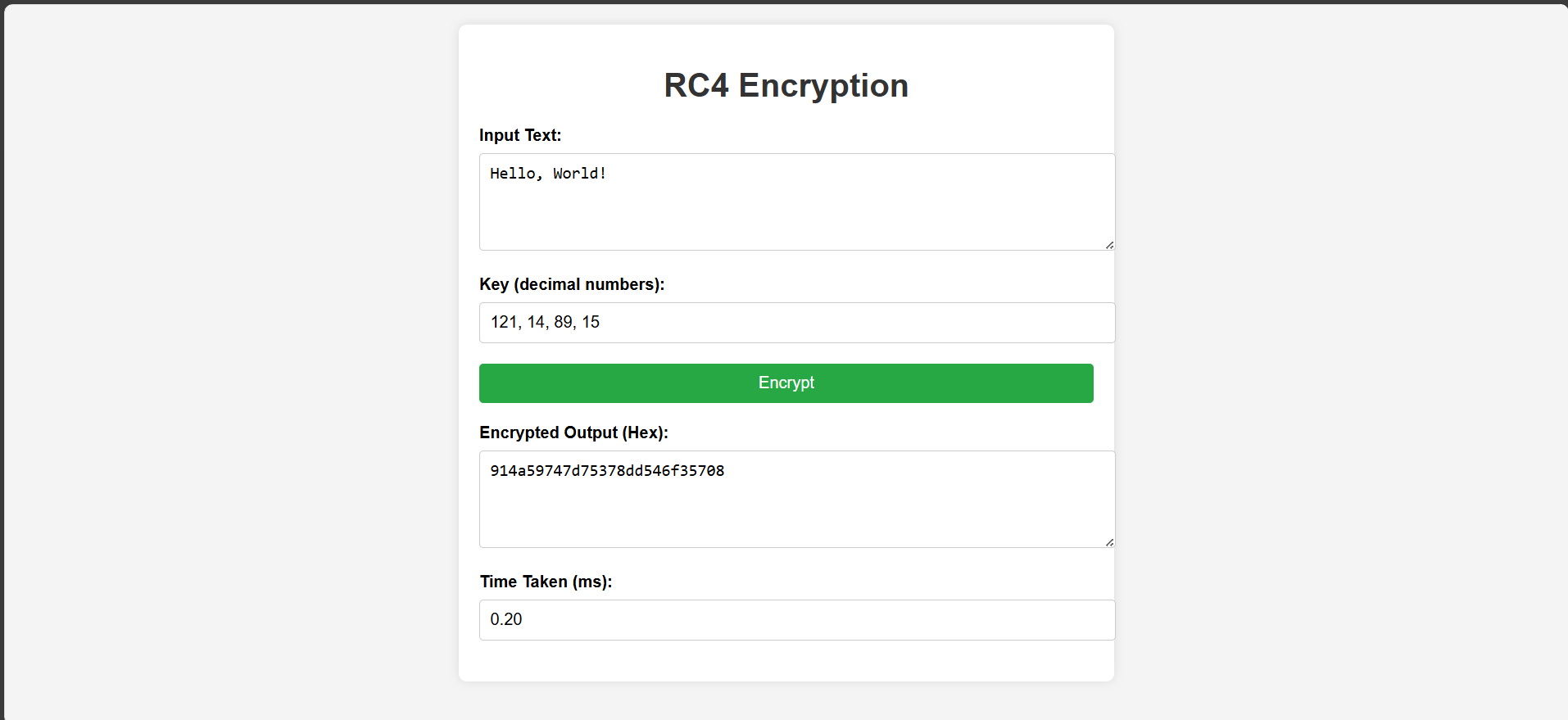
### Недостатки:

* Чувствительность к утечке или повторному использованию ключа.
* Уязвимость к атаке на основе предсказуемости генератора ключей.

### Области применения:

* Защита беспроводных сетей (например, WEP, WPA).
* Шифрование мультимедийных потоков (видеоконференции, VoIP).
* Использование в мобильных и встроенных устройствах.

2 Практическая часть



Вывод

В процессе выполнения лабораторной работы были изучены и освоены практические навыки разработки и использования приложений для реализации потоковых шифров.

**Лабораторная работа №7**

ИССЛЕДОВАНИЕ АСИММЕТРИЧНЫХ ШИФРОВ

1 Теоретические сведения

Асимметричные шифры — это криптографические алгоритмы, использующие пару ключей: открытый (public key) и закрытый (private key). Такие шифры являются основой современной криптографии, обеспечивая шифрование, цифровую подпись и обмен ключами.

### Основные аспекты исследования:

1. **Принцип работы:**
   * **Шифрование:** Сообщение шифруется с использованием открытого ключа, и его можно расшифровать только с помощью соответствующего закрытого ключа.
   * **Цифровая подпись:** Сообщение подписывается закрытым ключом отправителя, а проверяется с использованием открытого ключа.
2. **Основные алгоритмы:**
   * **RSA:** Основан на сложности разложения больших чисел на простые множители.
   * **DSA (цифровая подпись):** Основан на сложности вычисления дискретного логарифма.
   * **Эллиптические кривые (ECC):** Основаны на математике эллиптических кривых, обеспечивают высокую безопасность при меньших размерах ключей.
3. **Характеристики:**
   * Обеспечивает конфиденциальность (шифрование).
   * Поддерживает подлинность и целостность (цифровые подписи).
   * Используется для обмена ключами в симметричных шифрах.

### Преимущества:

* **Безопасность:** Открытый ключ может быть широко доступен, но это не позволяет восстановить закрытый ключ.
* **Гибкость:** Подходит как для шифрования, так и для цифровых подписей.
* **Масштабируемость:** Упрощает управление ключами в больших системах.

### Недостатки:

* **Скорость:** Асимметричные шифры работают медленнее, чем симметричные.
* **Ресурсоёмкость:** Требуют значительных вычислительных мощностей для шифрования и расшифрования.

### Применение:

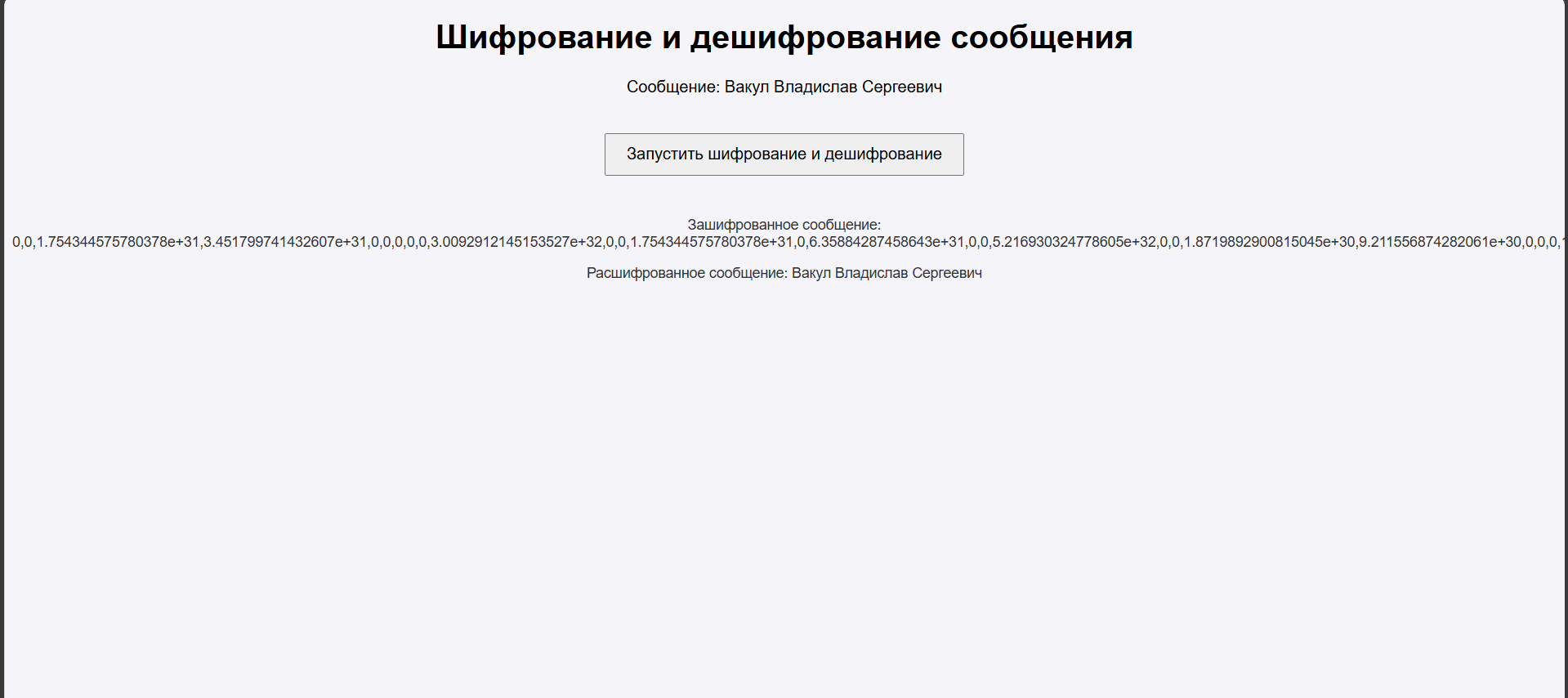
* **Обмен ключами:** Генерация и передача ключей для симметричного шифрования (например, в TLS).
* **Цифровые подписи:** Проверка подлинности данных и отправителей.
* **Электронная коммерция:** Защита транзакций и данных кредитных карт.
* **Электронная почта:** Протоколы PGP и S/MIME.

### Современные исследования:

* Оптимизация алгоритмов для повышения скорости и снижения затрат на вычисления.
* Применение криптографии эллиптических кривых для использования на мобильных устройствах и в IoT.
* Изучение стойкости к атакам, включая атаки квантовых компьютеров, что привело к развитию постквантовой криптографии.

обоих подходов для создания максимально безопасных решений.

2 Практическая часть



Вывод

В процессе выполнения лабораторной работы были изучены и освоены практические навыки разработки и использования приложений для реализации ассиметричных шифров.

**Лабораторная работа №8**

Исследование асимметричных шифров RSA и Эль-Гамаля

1 Теоретические сведения

Асимметричные шифры RSA и Эль-Гамаля являются фундаментальными алгоритмами в криптографии, основанной на открытых ключах. Они обеспечивают шифрование, цифровую подпись и защищённый обмен ключами, основываясь на сложных математических задачах.

### ****Алгоритм RSA****

**Основа RSA** — сложность разложения больших чисел на простые множители.

1. **Ключевая идея:**
   * Используются два ключа: открытый (для шифрования) и закрытый (для расшифрования).
   * Секретность основана на невозможности быстро разложить произведение двух больших простых чисел.
2. **Шаги генерации ключей:**
   * Выбираются два больших простых числа pp и qq.
   * Вычисляется n=p×qn = p \times q.
   * Рассчитывается функция Эйлера ϕ(n)=(p−1)(q−1)\phi(n) = (p-1)(q-1).
   * Выбирается открытая экспонента ee, взаимно простая с ϕ(n)\phi(n).
   * Вычисляется закрытая экспонента dd, такая, что e×d≡1 (mod ϕ(n))e \times d \equiv 1 \ (\text{mod } \phi(n)).
3. **Шифрование и расшифрование:**
   * **Шифрование:** C=Me (mod n)C = M^e \ (\text{mod } n), где MM — исходное сообщение.
   * **Расшифрование:** M=Cd (mod n)M = C^d \ (\text{mod } n).
4. **Преимущества RSA:**
   * Простота реализации.
   * Возможность использовать как для шифрования, так и для цифровых подписей.
5. **Недостатки RSA:**
   * Высокие вычислительные затраты.
   * Необходимость работы с длинными ключами для обеспечения стойкости.

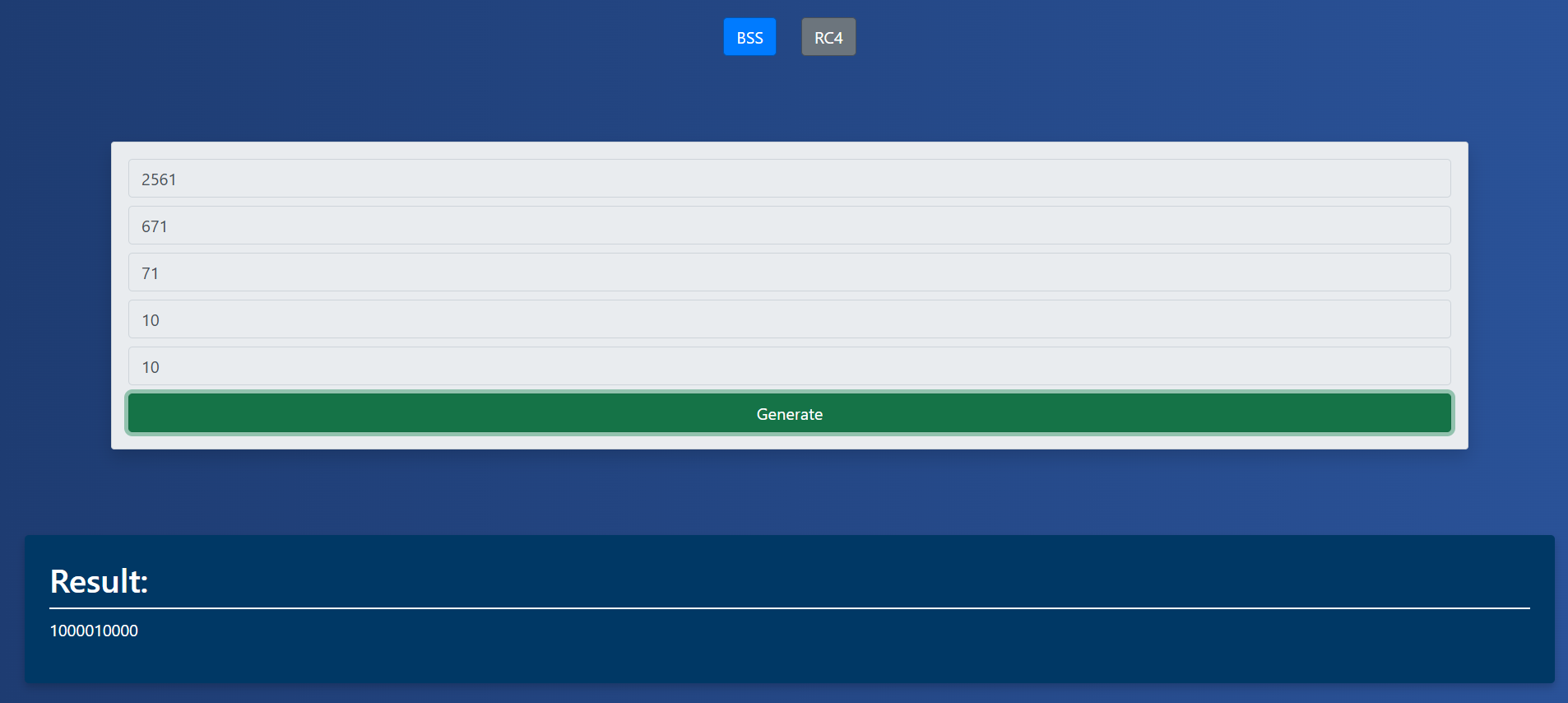
### ****Алгоритм Эль-Гамаля****

**Основа Эль-Гамаля** — сложность вычисления дискретного логарифма в конечном поле.

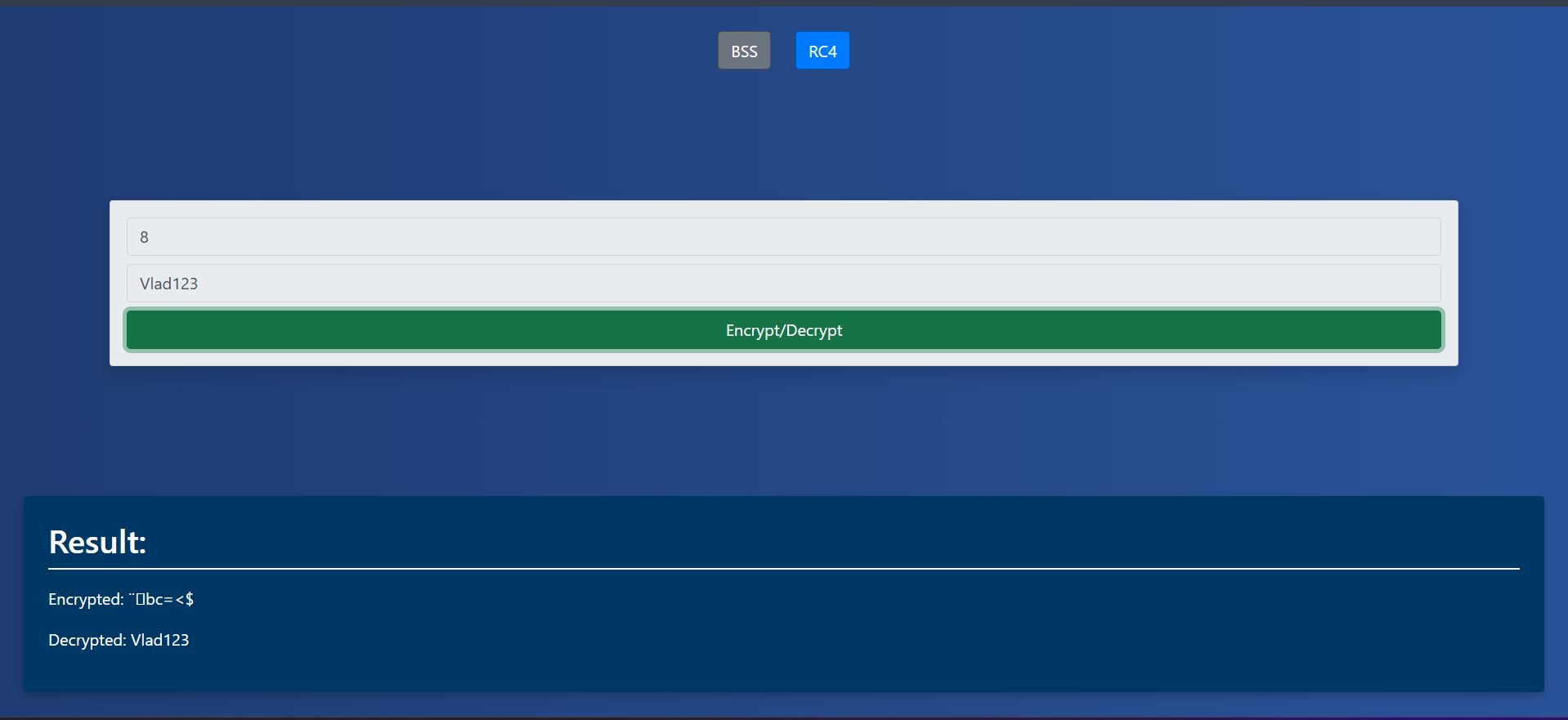
1. **Ключевая идея:**
   * Используются два ключа: открытый и закрытый.
   * Защищённость алгоритма основана на трудности восстановления закрытого ключа из открытого.
2. **Шаги генерации ключей:**
   * Выбирается большое простое число pp и примитивный корень gg.
   * Случайным образом выбирается закрытый ключ xx, где x∈[1,p−1]x \in [1, p-1].
   * Вычисляется открытый ключ y=gx (mod p)y = g^x \ (\text{mod } p).
3. **Шифрование и расшифрование:**
   * **Шифрование:**
     + Выбирается случайное число kk, где k∈[1,p−1]k \in [1, p-1].
     + Вычисляются два параметра:  
       c1=gk (mod p)c\_1 = g^k \ (\text{mod } p)  
       c2=M⋅yk (mod p)c\_2 = M \cdot y^k \ (\text{mod } p), где MM — сообщение.
   * **Расшифрование:**
     + M=c2⋅(c1x)−1 (mod p)M = c\_2 \cdot (c\_1^x)^{-1} \ (\text{mod } p).
4. **Преимущества Эль-Гамаля:**
   * Высокая стойкость благодаря использованию дискретного логарифма.
   * Адаптация для использования в других криптографических схемах (например, DSA).
5. **Недостатки Эль-Гамаля:**
   * Необходимость случайного числа kk, которое нельзя использовать повторно.
   * Увеличение размера зашифрованного сообщения (в два раза).

2 Практическая часть

Тестирование BSS:



Тестирование RC4:



Вывод

В процессе выполнения лабораторной работы были изучены и освоены практические навыки разработки и использования приложений для реализации ассиметричных шифров.

**Лабораторная работа №9**

Исследование криптографических хеш-функций

1 Теоретические сведения

Криптографические хеш-функции являются фундаментальной частью современной криптографии и широко используются для обеспечения безопасности данных. Их основные задачи — создание уникальных цифровых отпечатков данных, проверка целостности информации и обеспечение надежности криптографических протоколов. В этом исследовании рассмотрим ключевые аспекты криптографических хеш-функций: их свойства, области применения, примеры, атаки и перспективы развития.

### ****1. Что такое криптографические хеш-функции?****

Криптографическая хеш-функция — это математический алгоритм, который преобразует входные данные произвольной длины в фиксированный размер строки (хеш). При этом хеш должен удовлетворять следующим свойствам:

* **Определенность:** один и тот же вход всегда дает один и тот же хеш.
* **Необратимость:** невозможно восстановить исходные данные из хеша.
* **Стойкость к коллизиям:** крайне сложно найти два разных входных значения, имеющих одинаковый хеш.
* **Чувствительность к изменениям:** малейшее изменение исходных данных приводит к полностью другому хешу.
* **Эффективность:** вычисление хеша должно быть быстрым для любого входа.

### ****2. Примеры криптографических хеш-функций****

* **MD5 (Message Digest 5):** устаревшая хеш-функция с фиксированным размером хеша 128 бит. Уязвима к коллизиям, используется только в некритичных приложениях.
* **SHA-1 (Secure Hash Algorithm 1):** имеет размер хеша 160 бит. Также считается устаревшей из-за уязвимости к атакам на коллизии.
* **SHA-2 (SHA-224, SHA-256, SHA-384, SHA-512):** современный стандарт с различными длинами хешей. Обеспечивает высокий уровень безопасности.
* **SHA-3 (Keccak):** новый стандарт хеширования с повышенной устойчивостью к атакам.
* **BLAKE2, Argon2:** примеры более современных алгоритмов, которые фокусируются на скорости и безопасности.

### ****3. Применение криптографических хеш-функций****

1. **Целостность данных:**
   * Проверка того, что данные не были изменены во время передачи или хранения.
   * Например, контрольные суммы (checksum) файлов.
2. **Аутентификация:**
   * Используются в системах хранения паролей. Вместо хранения пароля в базе данных сохраняется его хеш.
   * Аутентификация основана на сравнении хеша введенного пароля с сохраненным.
3. **Электронная подпись:**
   * Хеш-функции обеспечивают компактное представление данных для подписи.
4. **Криптографические протоколы:**
   * Используются в SSL/TLS, IPsec, цифровых сертификатах и других безопасных соединениях.
5. **Блокчейн:**
   * В системах, таких как Bitcoin и Ethereum, хеш-функции применяются для формирования блоков, проверки транзакций и поддержания безопасности цепи блоков

### ****4. Угрозы и атаки на хеш-функции****

Несмотря на их надежность, криптографические хеш-функции подвержены атакам:

* **Атака на коллизии:** поиск двух различных входных данных, дающих одинаковый хеш.
* **Атака "день рождения":** ускоренный способ нахождения коллизий, основанный на теории вероятностей.
* **Атака на предварительное изображение:** попытка найти входные данные, соответствующие заданному хешу.
* **Атака на второе изображение:** поиск альтернативного входного значения для определенного хеша.

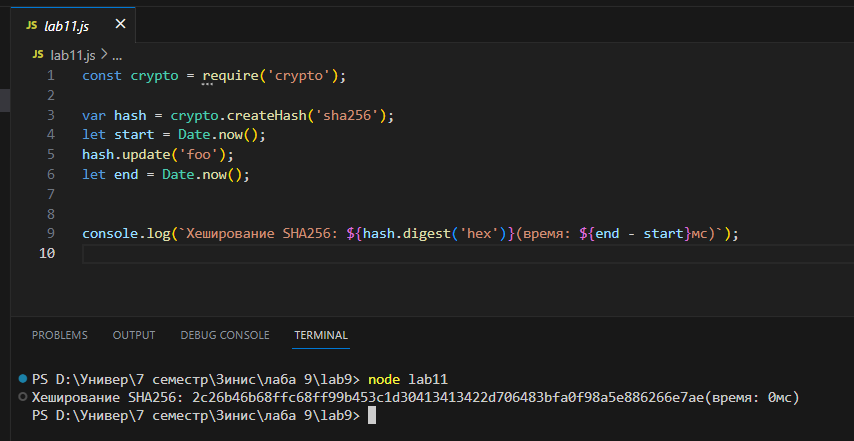
Эти атаки привели к устареванию алгоритмов, таких как MD5 и SHA-1, и переходу на более современные, такие как SHA-2 и SHA-3.

### ****5. Перспективы развития****

С ростом вычислительных мощностей и появлением квантовых компьютеров разработка новых хеш-функций становится особенно актуальной. Перспективные направления:

1. **Квантовая криптография:**
   * Разработка алгоритмов, устойчивых к атакам квантовых компьютеров.
2. **Улучшение производительности:**
   * Современные алгоритмы, такие как BLAKE3, направлены на увеличение скорости вычислений без потери безопасности.
3. **Адаптация к новым задачам:**
   * Оптимизация алгоритмов для систем с ограниченными ресурсами, таких как IoT.

2 Практическая часть



Вывод

В процессе выполнения лабораторной работы были изучены и освоены практические навыки разработки и использования приложений для реализации хеш-функций.

**Лабораторная работа №10**

ИССЛЕДОВАНИЕ АЛГОРИТМОВ ГЕНЕРАЦИИ И ВЕРИФИКАЦИИ ЭЛЕКТРОННОЙ ЦИФРОВОЙ ПОДПИСИ

1 Теоретические сведения

Электронная цифровая подпись (ЭЦП) — это один из ключевых инструментов обеспечения безопасности и подлинности данных в цифровом пространстве. Алгоритмы генерации и верификации ЭЦП основаны на криптографических методах и играют важную роль в защите информации, обеспечивая аутентификацию, целостность и невозможность отказа от авторства. В этом исследовании рассмотрим основы, алгоритмы, свойства, методы генерации и верификации ЭЦП, а также их применение и перспективы развития.

### ****1. Что такое электронная цифровая подпись?****

Электронная цифровая подпись (ЭЦП) — это криптографический механизм, который подтверждает подлинность отправителя (подписанта) и целостность данных. ЭЦП используется для:

* **Аутентификации:** подтверждение личности подписанта.
* **Целостности данных:** защита от изменений в передаваемых данных.
* **Невозможности отказа от авторства:** юридическое подтверждение факта подписания.

ЭЦП базируется на асимметричном шифровании, которое использует пару ключей: **закрытый (приватный) ключ** для создания подписи и **открытый ключ** для проверки подписи.

### ****2. Алгоритмы генерации и верификации ЭЦП****

ЭЦП формируется на основе криптографических алгоритмов, обеспечивающих высокую степень безопасности. Наиболее распространенные алгоритмы:

#### **2.1. RSA (Rivest–Shamir–Adleman):**

* **Генерация подписи:**
  + Исходные данные хэшируются с использованием криптографической хеш-функции (например, SHA-256).
  + Хеш зашифровывается приватным ключом.
* **Верификация:**
  + Подпись расшифровывается с использованием открытого ключа.
  + Сравнивается расшифрованный хеш с хешем исходных данных.
* **Особенности:** высокая надежность, но относительно низкая скорость работы.

#### **2.2. DSA (Digital Signature Algorithm):**

* Основан на алгоритме Диффи-Хеллмана и использует модульное арифметическое шифрование.
* **Генерация подписи:**
  + Исходные данные хэшируются.
  + Подпись вычисляется с использованием приватного ключа и случайного значения.
* **Верификация:**
  + Проверка подписи выполняется с помощью открытого ключа.
* **Особенности:** быстрее, чем RSA, но сложнее в реализации.

#### **2.3. ECDSA (Elliptic Curve Digital Signature Algorithm):**

* Использует эллиптические кривые для повышения производительности.
* **Генерация подписи:**
  + Хэш данных преобразуется в координаты на эллиптической кривой.
  + Подпись создается с использованием приватного ключа.
* **Верификация:**
  + Проверка подписи выполняется с использованием открытого ключа и точек на эллиптической кривой.
* **Особенности:** высокая безопасность при меньшей длине ключа.

#### **2.4. ГОСТ Р 34.10-2012 (ЭЦП на эллиптических кривых):**

* Российский стандарт, аналогичный ECDSA, с учетом национальных криптографических особенностей.
* **Особенности:** активно используется в российских системах электронной подписи.

### ****3. Процесс работы ЭЦП****

#### **3.1. Генерация ЭЦП**

1. Исходные данные обрабатываются с использованием криптографической хеш-функции (например, SHA-256).
2. Полученный хеш шифруется с помощью приватного ключа подписанта.
3. Итоговая подпись вместе с открытым ключом передается получателю.

#### **3.2. Верификация ЭЦП**

1. Полученные данные снова хэшируются с использованием той же хеш-функции.
2. Подпись расшифровывается с помощью открытого ключа.
3. Хеши сравниваются: если они совпадают, подпись действительна.

### ****4. Применение ЭЦП****

1. **Документооборот:**
   * Юридически значимые документы подписываются ЭЦП (договоры, акты, счета).
2. **Электронная коммерция:**
   * Использование ЭЦП для безопасного проведения финансовых транзакций.
3. **Электронное правительство:**
   * Госуслуги и взаимодействие с гражданами через цифровые платформы.
4. **Кибербезопасность:**
   * Обеспечение аутентификации в криптографических протоколах (SSL/TLS, VPN).

### ****5. Угрозы и меры защиты****

#### **5.1. Возможные угрозы**

* Кража приватного ключа.
* Уязвимость алгоритмов хеширования.
* Атаки на недостаточно защищенные системы хранения ключей.

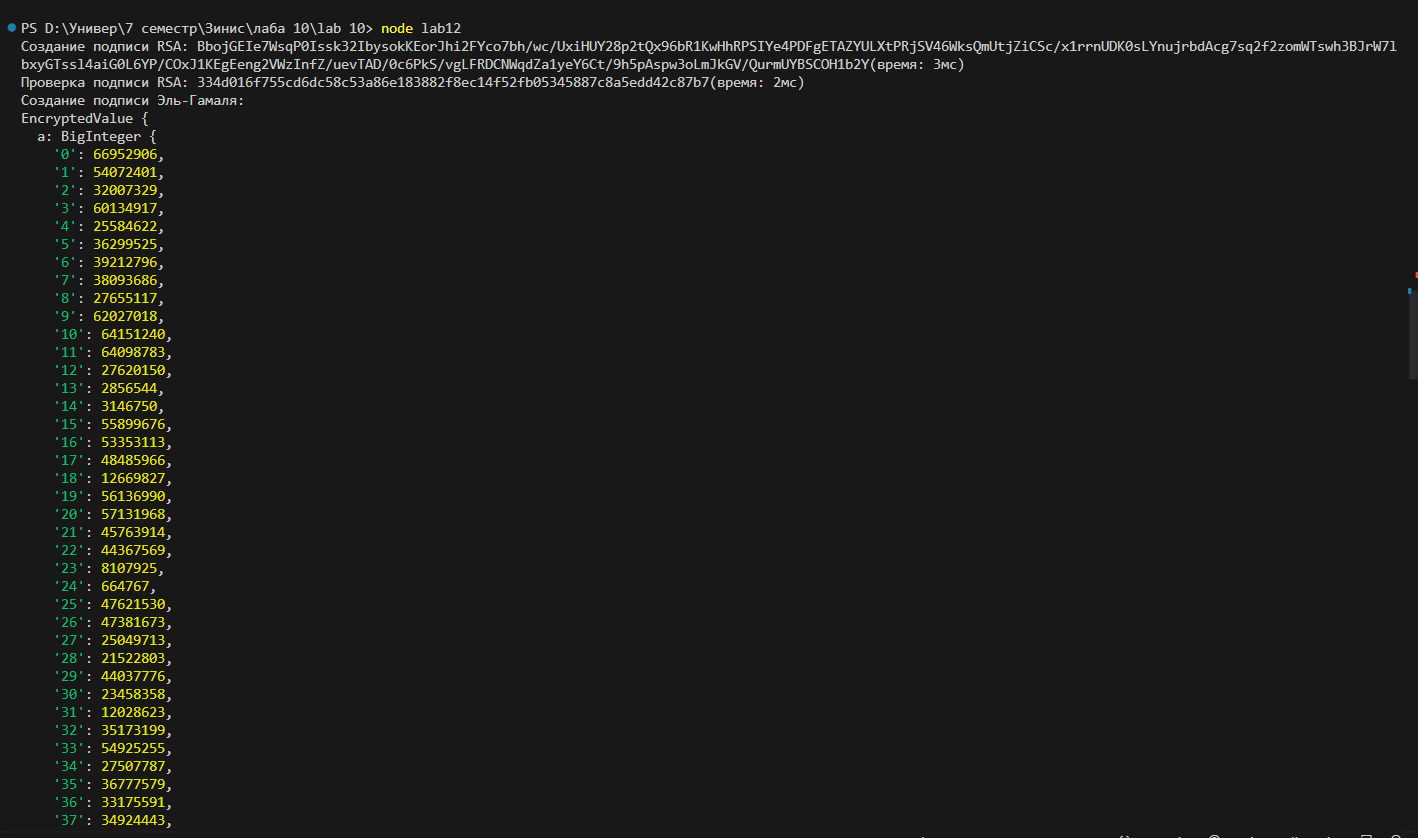
#### **5.2. Меры защиты**

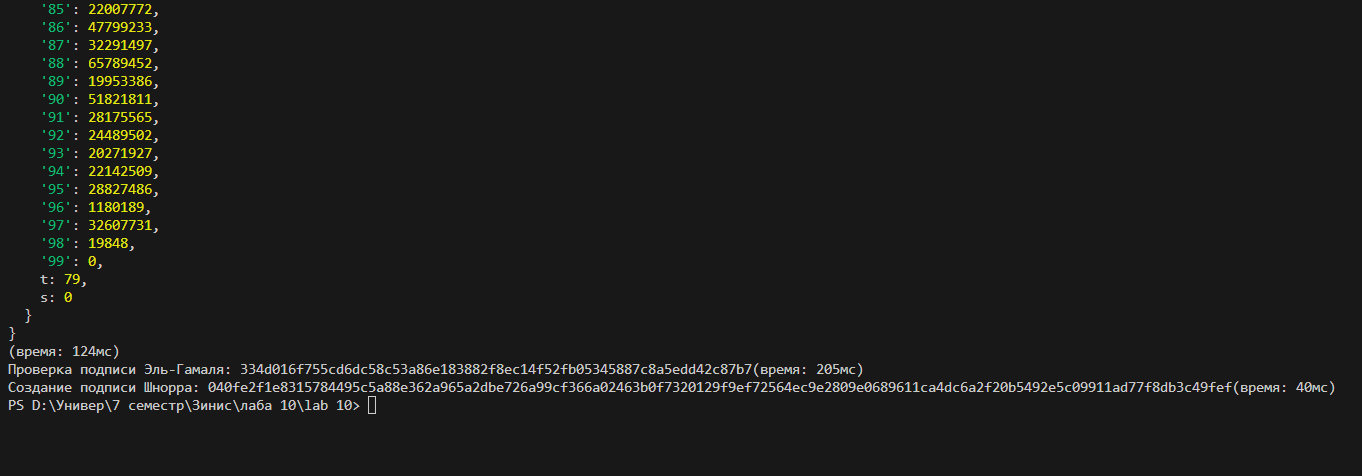
* Использование надежных хеш-функций (SHA-256, SHA-3).
* Защита ключей с помощью аппаратных решений (HSM, токены).
* Регулярное обновление криптографических стандартов.

### ****6. Перспективы развития****

1. **Квантовая криптография:**
   * Разработка алгоритмов, устойчивых к квантовым атакам.
   * Пример: алгоритм CRYSTALS-Dilithium, победитель конкурса NIST по постквантовой криптографии.
2. **Интеграция с блокчейном:**
   * Использование ЭЦП для обеспечения неизменности записей в распределенных реестрах.
3. **Автоматизация процессов:**
   * Внедрение смарт-контрактов с поддержкой ЭЦП.

2 Практическая часть





Вывод

В процессе выполнения лабораторной работы были изучены и освоены практические навыки разработки и использования приложений для реализации ЭЦП.

**Лабораторная работа №11**

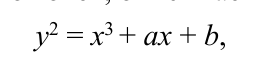
ИССЛЕДОВАНИЕ КРИПТОГРАФИЧЕСКИХ АЛГОРИТМОВ НА ОСНОВЕ ЭЛЛИПТИЧЕСКИХ КРИВЫХ

1 Теоретические сведения

Криптографические алгоритмы на основе эллиптических кривых (ECC, Elliptic Curve Cryptography) представляют собой один из самых современных и эффективных подходов к шифрованию и обеспечению безопасности данных. Они основаны на математических свойствах эллиптических кривых и отличаются высокой степенью надежности при меньшей длине ключа по сравнению с традиционными алгоритмами, такими как RSA или DSA. В этом исследовании рассмотрим основы ECC, их преимущества, алгоритмы, область применения и перспективы развития.

### ****1. Основы эллиптических кривых в криптографии****

Эллиптическая кривая — это множество точек, удовлетворяющих уравнению:

 где:

* a и b — коэффициенты, определяющие форму кривой.
* p — простое число, задающее конечное поле.

Эллиптические кривые обладают рядом математических свойств, таких как групповая операция сложения точек, которые и используются в криптографии.

### ****2. Преимущества ECC****

1. **Высокая надежность при меньшей длине ключа:**
   * ECC обеспечивает уровень безопасности, эквивалентный RSA, но с меньшими размерами ключей. Например:
     + Ключ ECC длиной 256 бит соответствует RSA-ключу длиной 3072 бита.
2. **Более высокая производительность:**
   * Меньший объем вычислений позволяет быстрее генерировать ключи и выполнять операции шифрования/подписи.
3. **Экономия ресурсов:**
   * Подходит для устройств с ограниченными вычислительными возможностями (IoT, мобильные устройства).
4. **Устойчивость к современным атакам:**
   * Высокая сложность задачи дискретного логарифмирования на эллиптических кривых делает алгоритмы ECC надежными.

### ****3. Основные алгоритмы на основе ECC****

#### **3.1. ECDSA (Elliptic Curve Digital Signature Algorithm):**

* Используется для создания и проверки цифровых подписей.
* **Процесс:**
  + Генерация подписи: создается случайное число и вычисляются координаты точки на кривой.
  + Верификация подписи: проверяется совпадение вычисленных и переданных данных.
* **Применение:** криптографические протоколы (TLS, SSL), системы ЭЦП.

#### **3.2. ECDH (Elliptic Curve Diffie-Hellman):**

* Протокол обмена ключами на основе эллиптических кривых.
* **Процесс:**
  + Каждая сторона генерирует приватный ключ и вычисляет публичный ключ.
  + Общий секретный ключ получается путем комбинации приватного ключа одной стороны и публичного ключа другой.
* **Применение:** безопасная передача данных в сетях, VPN, мессенджеры.

#### **3.3. Алгоритмы ГОСТ на эллиптических кривых:**

* Российские стандарты криптографии:
  + ГОСТ Р 34.10-2012 — аналог ECDSA.
  + ГОСТ Р 34.11-2012 — хеширование с использованием эллиптических кривых.
* **Применение:** защита информации в российских системах.

### ****4. Применение ECC****

1. **Сетевые протоколы:**
   * TLS/SSL: защита соединений в Интернете.
   * HTTPS: шифрование данных на веб-сайтах.
2. **Электронная подпись:**
   * Используется для подтверждения подлинности документов и данных.
3. **Мобильные устройства и IoT:**
   * Эффективность ECC делает его идеальным для устройств с ограниченными ресурсами.
4. **Криптовалюты и блокчейн:**
   * ECC используется для создания кошельков и цифровых подписей в блокчейне (например, в Bitcoin и Ethereum).
5. **VPN и мессенджеры:**
   * Безопасный обмен ключами с использованием ECDH.

### ****5. Угрозы и методы защиты****

#### **5.1. Угрозы:**

* **Квантовые вычисления:**
  + Алгоритмы ECC уязвимы для атак на основе квантовых компьютеров (алгоритм Шора).
* **Ошибки реализации:**
  + Неправильная реализация криптографических операций может привести к утечке данных.

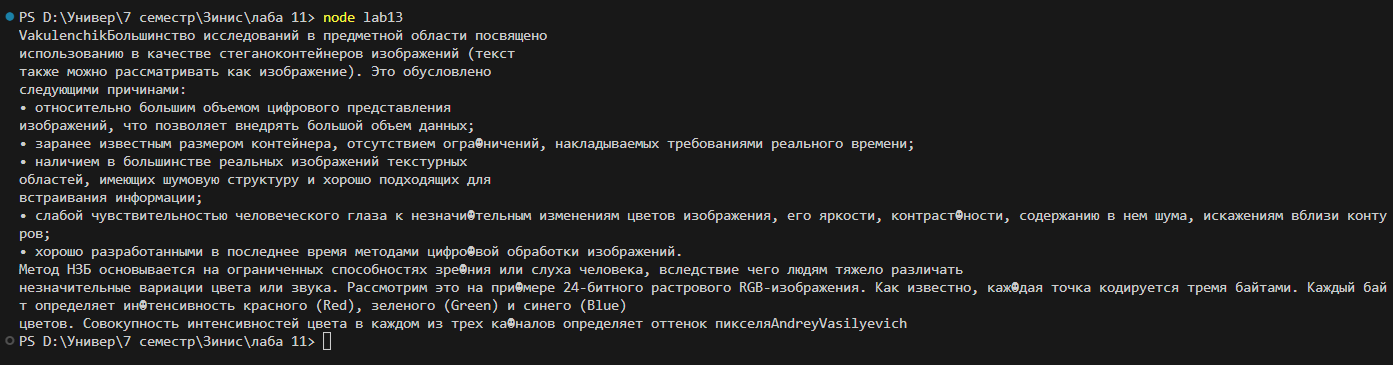
#### **5.2. Методы защиты:**

* **Использование современных стандартов:**
  + Выбор параметров кривых, рекомендованных NIST (P-256, P-384) или российскими стандартами.
* **Подготовка к квантовой криптографии:**
  + Разработка постквантовых алгоритмов, таких как CRYSTALS-Dilithium.

### ****6. Перспективы развития ECC****

1. **Интеграция с постквантовыми технологиями:**
   * Сочетание ECC с квантово-устойчивыми алгоритмами.
2. **Улучшение стандартизации:**
   * Разработка новых стандартов для глобальной интеграции ECC в различные отрасли.
3. **Расширение применения в IoT:**
   * Обеспечение безопасности большого числа подключенных устройств.
4. **Внедрение в блокчейн:**
   * Усиление безопасности транзакций и контрактов.

2 Практическая часть



Вывод

В процессе выполнения лабораторной работы были изучены и освоены практические навыки разработки и использования приложений для реализации эллиптических кривых.

**Лабораторная работа №12**

ИССЛЕДОВАНИЕ СТЕГАНОГРАФИЧЕСКОГО МЕТОДА НА ОСНОВЕ ПРЕОБРАЗОВАНИЯ НАИМЕНЕЕ ЗНАЧАЩИХ БИТОВ

1 Теоретические сведения

**Метод изменения наименее значащих битов (LSB)** применяется для скрытия информации в носителях, таких как изображения, аудио и видео. Он заключается в замене младших битов данных носителя на биты скрываемой информации, что минимально влияет на качество носителя.

### ****Преимущества:****

1. **Простота реализации**: метод легок в освоении и использовании.
2. **Незаметность изменений**: визуально или на слух изменения практически не заметны.
3. **Высокая емкость**: позволяет скрывать значительные объемы данных в больших файлах.
4. **Скорость работы**: обеспечивает быстрое кодирование и извлечение.

### ****Недостатки:****

1. **Уязвимость к стегоанализу**: метод легко выявляется с помощью статистического анализа.
2. **Чувствительность к изменениям носителя**: обработка, например сжатие JPEG, может уничтожить скрытые данные.
3. **Ограниченный объем информации**: зависит от размера и качества носителя.
4. **Отсутствие встроенной защиты**: данные можно извлечь без шифрования.

### ****Применение:****

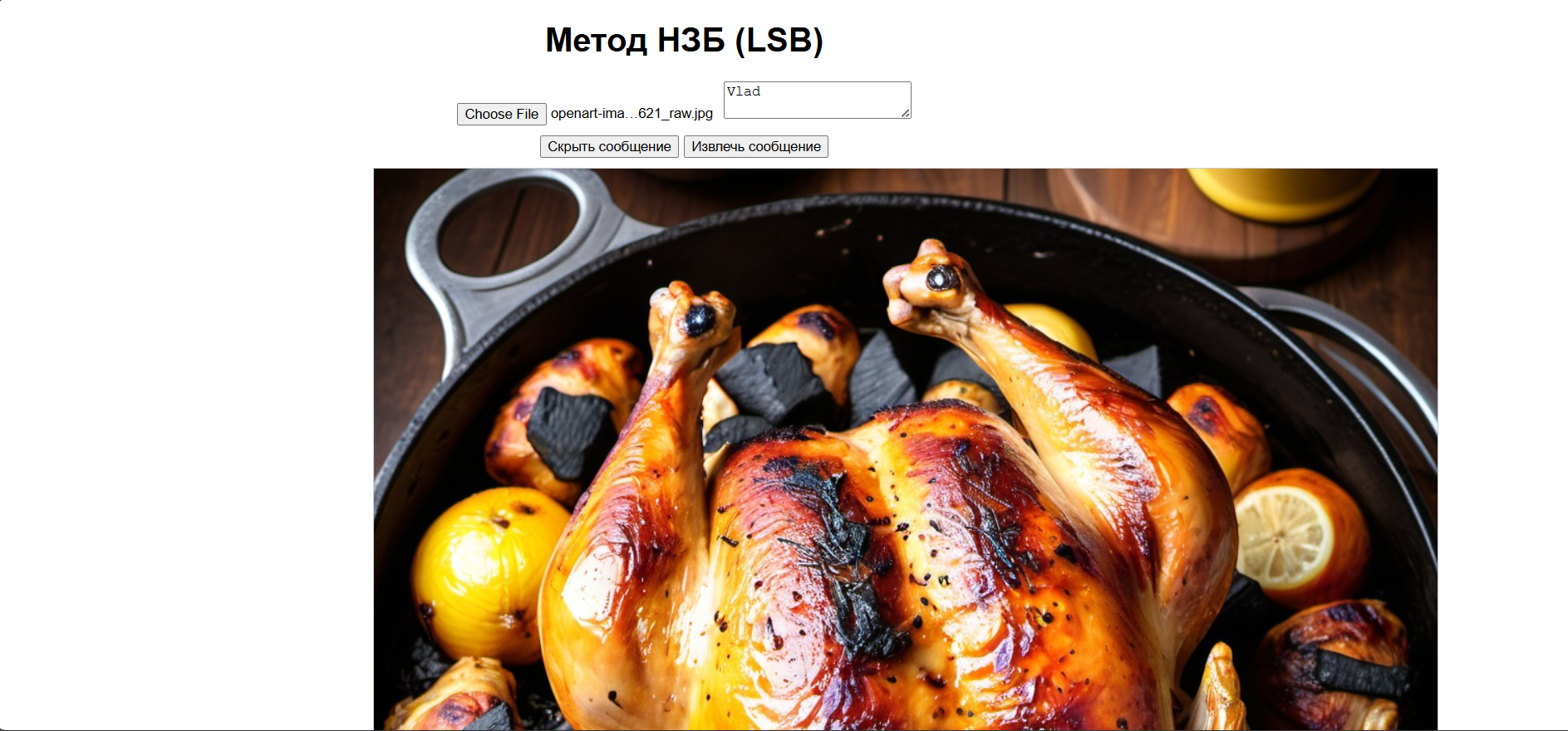
* Передача скрытых сообщений.
* Защита авторских прав через цифровые водяные знаки.
* Добавление метаданных в медиафайлы.
* Использование в конфиденциальных голосованиях.

### ****Улучшения и перспективы:****

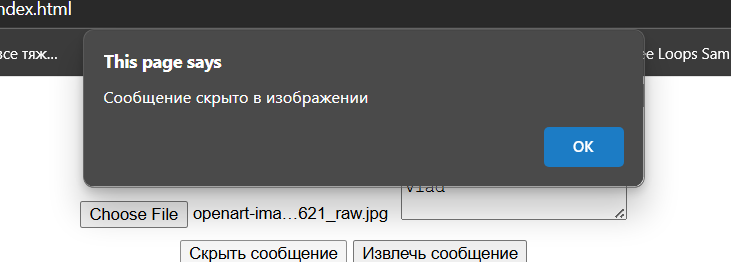
Для повышения безопасности и устойчивости метод можно сочетать с криптографией, случайным выбором пикселей или адаптивными алгоритмами, что делает его более надежным в условиях современных угроз.

2 Практическая часть

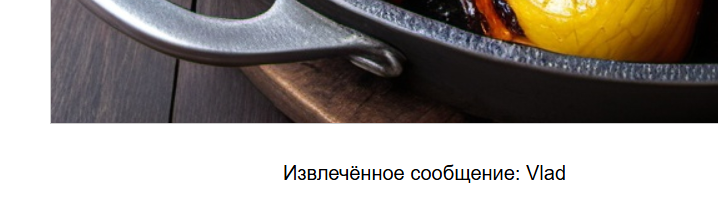
Загрузим изображение:



При нажатии на кнопку Скрыть сообщение получаем сообщение что скрытие прошло успешно:



При нажатии на кнопку Извлечь сообщение, получаем следующую запись:



Вывод

В процессе выполнения лабораторной работы были изучены и освоены практические навыки разработки и использования приложений для реализации стеганографических методов.

**Лабораторная работа №13**

ИССЛЕДОВАНИЕ МЕТОДОВ ТЕКСТОВОЙ СТЕГАНОГРАФИИ

1 Теоретические сведения

**Текстовая стеганография** — это метод скрытия информации в текстах путем изменения их структуры или содержания. Она используется для скрытой передачи данных, когда визуально текст кажется обычным.

### ****Основные методы текстовой стеганографии:****

1. **Методы на основе изменения структуры текста:**
   * **Добавление пробелов**: Использование дополнительных пробелов или табуляций для кодирования данных.
   * **Изменение формата текста**: Незаметное изменение шрифта, размера букв или их положения.
2. **Методы на основе изменения содержания текста:**
   * **Замена слов**: Подбор синонимов для определенных слов, которые кодируют скрытые данные.
   * **Адаптация текста**: Включение специальных слов или фраз, соответствующих закодированному сообщению.
3. **Использование скрытых символов:**
   * Внедрение невидимых символов, таких как нулевой ширины пробел или невидимые Unicode-символы.

### ****Преимущества:****

1. Высокая степень скрытности, так как текст выглядит естественно.
2. Возможность передачи данных через обычные текстовые документы, письма или соцсети.
3. Не требует сложного оборудования или программного обеспечения.

### ****Недостатки:****

1. Ограниченный объем данных, который можно скрыть.
2. Уязвимость к редактированию текста, что может повредить скрытую информацию.
3. Легкость выявления при использовании неестественных слов или изменений.

### ****Применение:****

* Скрытая коммуникация в условиях цензуры.
* Встраивание метаданных для защиты авторских прав.
* Добавление скрытых инструкций в автоматизированных системах.

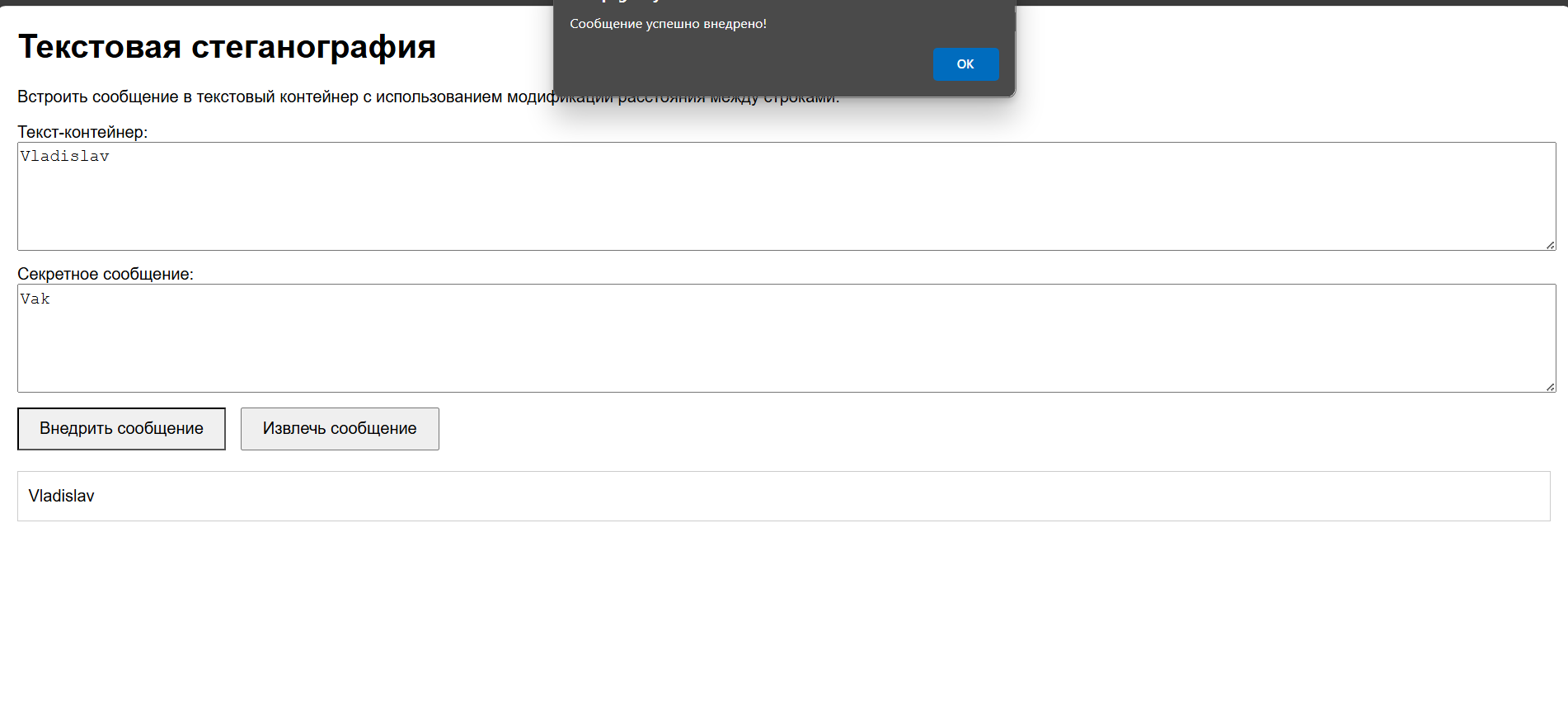
### ****Улучшения и перспективы:****

Для повышения устойчивости текстовой стеганографии возможно использование:

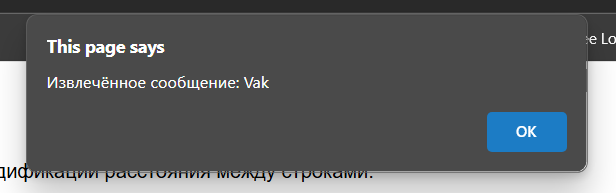
* Машинного обучения для создания естественных текстов с скрытыми данными.
* Комбинирования с криптографией для шифрования передаваемой информации.
* Использования редких символов Unicode и методов, незаметных для человеческого восприятия.

2 Практическая часть

Внедряем сообщение Vak в текст Vladislav:



Извлекаем сообщение Vak из контейнера Vladislav:



Вывод

В процессе выполнения лабораторной работы были изучены и освоены практические навыки разработки и использования приложений для реализации стеганографических методов.