Учреждение образования

«БЕЛОРУССКИЙ ГОСУДАРСТВЕННЫЙ ТЕХНОЛОГИЧЕСКИЙ УНИВЕРСИТЕТ»

Лабораторная работа №4

**ИССЛЕДОВАНИЕ КРИПТОГРАФИЧЕСКИХ ШИФРОВ НА ОСНОВЕ ПОСТАНОВКИ (ЗАМЕНЫ) СИМВОЛОВ**

Студент: Сосновец М.И.

ФИТ 3 курс 4 группа

Преподаватель: Нистюк О.А.

Минск 2025

**Цель:** изучение и приобретение практических навыков разработки и использования приложений для реализации подстановочных шифров

**Задачи:**

1. Закрепить теоретические знания по алгебраическому описанию, алгоритмам реализации операций зашифрования/расшифрования и оценке криптостойкости подстановочных шифров.
2. Ознакомиться с особенностями реализации и свойствами различных подстановочных шифров на основе готового программного средства (L\_LUX).
3. Разработать приложение для реализации указанных преподавателем методов подстановочного зашифрования/расшифрования.
4. Выполнить исследование криптостойкости шифров на основе статистических данных о частотах появления символов в исходном и зашифрованном сообщениях.
5. Оценить скорость зашифрования/расшифрования реализованных способов шифров.
6. Результаты выполнения лабораторной работы оформить в виде описания разработанного приложения, методики выполнения экспериментов с использованием приложения и результатов эксперимента.

**Теоретические сведения**

Сущность подстановочного шифрования состоит в том, что исходный текст (из множества М) и зашифрованный текст (из множества С) основаны на использовании одного и того же или разных алфавитов, а тайной или ключевой информацией является алгоритм подстановки.

Типов подстановочных шифров:

* моноалфавитные (шифры однозначной замены или простые подстановочные);
* полиграммные;
* омофонические (однозвучные шифры или шифры многозначной замены);
* полиалфавитные.

**Система шифрования Цезаря с ключевым словом (лозунгом).** Также является одноалфавитной системой подстановки. Особенностью этой системы является использование ключевого слова (лозунга) для смещения и изменения порядка символов в алфавите подстановки (желательно, чтобы все буквы ключевого слова были различными). Ключевое слово пишется в начале алфавита подстановки.

Применяя одновременно операции сложения и умножения по модулю n над элементами множества (индексами букв алфавита), можно получить систему подстановок, которую называют аффинной системой подстановок Цезаря. Определим процедуру зашифрования в такой системе: **y ≡ ax + b mod N**, где a и b – целые числа. При этом взаимно однозначные соответствия между открытым текстом и шифртекстом будут иметь место только при выполнении следующих условий: 0 ≤ a, b < N, наибольший общий делитель (НОД) чисел a, N равен 1, т. е. эти числа являются взаимно простыми.

**Первым известным шифром этого типа является шифр Порты**. Шифр представляется в виде таблицы. Наверху горизонтально и слева вертикально записывается стандартный алфавит. В ячейках таблицы записываются числа в определенном порядке.

**Омофонические шифры (омофоническая замена),** или однозвучные шифры подстановки, создавались с целью увеличить сложность частотного анализа шифртекстов путем маскировки реальных частот появления символов текста с помощью омофонии.

**Полиалфавитные (или многоалфавитные) шифры** состоят из нескольких шифров однозначной замены. Выбор варианта алфавита для зашифрования одного символа зависит от особенностей метода шифрования.

**Таблица Трисемуса**. В 1518 г. в развитии криптографии был сделан важный шаг благодаря появлению в Германии первой печатной книги по криптографии. Аббат Иоганнес Трисемус, настоятель монастыря в Вюрцбурге, написал книгу «Полиграфия», в которой он описал ряда шифров, один из которых развивает идею многоалфавитной подстановки. Зашифрование осуществляется так: заготавливается таблица подстановки (так называемая «таблица Трисемуса» – таблица со стороной, равной N, где N – мощность алфавита), где первая строка – это алфавит, вторая – алфавит, сдвинутый на один символ, и т. д. При зашифровании первая буква открытого текста заменяется на букву, стоящую в первой строке, вторая – на букву, стоящую во второй строке, и т. д. После использования последней строки вновь возвращаются к первой.

**Шифр Виженера**. В 1586 г. французский дипломат Блез Виженер представил перед комиссией Генриха III описание простого, но довольно стойкого шифра, в основе которого лежит таблица Трисемуса. В этом шифре мы имеем дело с последовательностью сдвигов, циклически повторяющейся. Основная идея заключается в следующем. Создается таблица (таблица Виженера) размером N×N (N – число знаков в используемом алфавите). Эти знаки могут включать не только буквы, но и, например, пробел или иные знаки. В первой строке таблицы записывается весь используемый алфавит. Каждая последующая строка получается из предыдущего циклического сдвига последней на 1 символ влево. Таким образом, при мощности алфавита (английского языка), равной 26, необходимо выполнить последовательно 25 сдвигов для формирования всей таблицы.

Существует определенное сходство между подстановочными шифрами и шифрами на основе гаммирования. Последние рассматриваются как самостоятельный класс. Такие шифры схожи с подстановочными (и в определенном плане – с перестановочными) тем, что в обоих случаях можно использовать табличное представление выполняемых операций на основе ключей. В шифрах на основе гаммирования и в подстановочных шифрах при зашифровании происходит подмена одних символов другими.

**Основное задание**

1. Разработать авторское приложение в соответствии с целью лабораторной работы. Приложение должно реализовывать следующие операции:

• выполнять зашифрование/расшифрование текстовых документов (объемом не менее 5 тысяч знаков), созданных на основе алфавита языка в соответствии с нижеследующей таблицей вариантов задания; при этом следует использовать шифры подстановки из третьего столбца данной таблицы (варианты задания представлены в табл. 2.6);

• сформировать гистограммы частот появления символов для исходного и зашифрованного сообщений;

• оценить время выполнения операций зашифрования/расшифрования (напоминание: во многих языках программирования есть встроенные методы для замеров времени; при отсутствии такового в используемом языке можно воспользоваться разностью двух дат (например, в миллисекундах: время после выполнения программы – время до начала выполнения преобразования)).

При анализе полученных гистограмм можно сопоставить полученные данные с аналогичными результатами выполнения лабораторной работы № 2 из [2].

Если указанный в таблице язык исходного текста не известен разработчику программного средства, можно взять документ на требуемом языке и воспользоваться доступным электронным переводчиком (возникающие при этом отдельные семантические неточности не следует считать существенным недостатком выполняемого анализа).

2. Результаты оформить в виде отчета по установленным правилам.

**Задание 1:**

В соответствии с вариантом задания, было разработано приложение, которое выполняет зашифрование и расшифрование текста по алгоритмам Цезаря и Трисемуса. Код приложения предоставлен в листинге 1.1, 1.2 соответственно.

|  |  |  |
| --- | --- | --- |
| 12 | Русский | 1. Шифр Цезаря с ключевым словом, ключевое слово – безопасность 2. Таблица Трисемуса, ключевое слово – безопасность |

Шифр Цезаря — это один из самых простых и известных алгоритмов шифрования. Его принцип заключается в замене каждого символа текста на символ, находящийся на фиксированное число позиций (ключ) вправо или влево в алфавите. Например, при ключе 3 символ "A" заменяется на "D", а символ "B" — на "E". Для расшифрования выполняется обратная операция: символы сдвигаются влево на то же количество позиций. Шифр Цезаря прост в реализации, но уязвим к частотному анализу, так как сохраняет частоту появления символов.

|  |
| --- |
| const caesarAlphabet = 'абвгдеёжзийклмнопрстуфхцчшщъыьэюя';  function createCaesarKeyAlphabet(keyword) {      const uniqueChars = [...new Set(keyword.toLowerCase())];      const remainingChars = caesarAlphabet.split('').filter(char => !uniqueChars.includes(char));      return uniqueChars.join('') + remainingChars.join('');}  function caesarCipher(text, encrypt = true) {      const keyAlphabet = createCaesarKeyAlphabet('безопасность');      const key = 3;      let result = '';      for (let char of text.toLowerCase()) {          const index = keyAlphabet.indexOf(char);          if (index === -1) {              result += char;          } else {              const newIndex = encrypt ? (index + key) % keyAlphabet.length : (index - key + keyAlphabet.length) % keyAlphabet.length;              result += keyAlphabet[newIndex];          }}return result;} |

Листинг 1.1 – реализация алгоритма Цезаря

Зашифрование и расшифрование текста по алгоритму Цезаря представлено на рисунках 1.1, 1.2 соответственно.

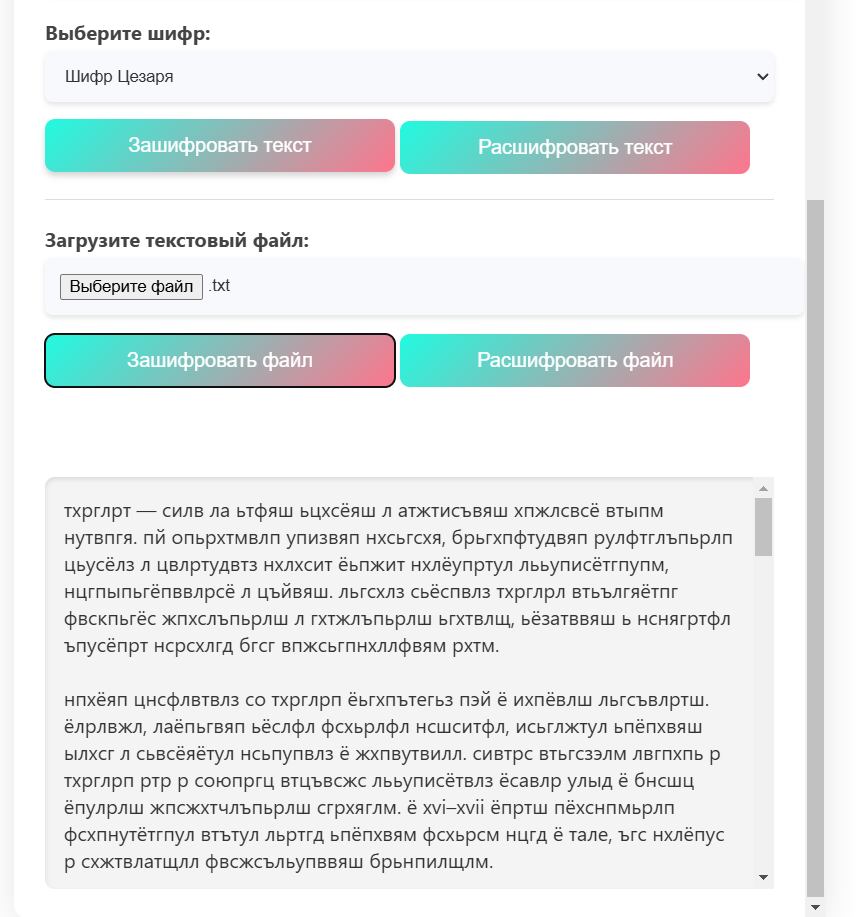


Рисунок 1.1 – Результат зашифрования текста

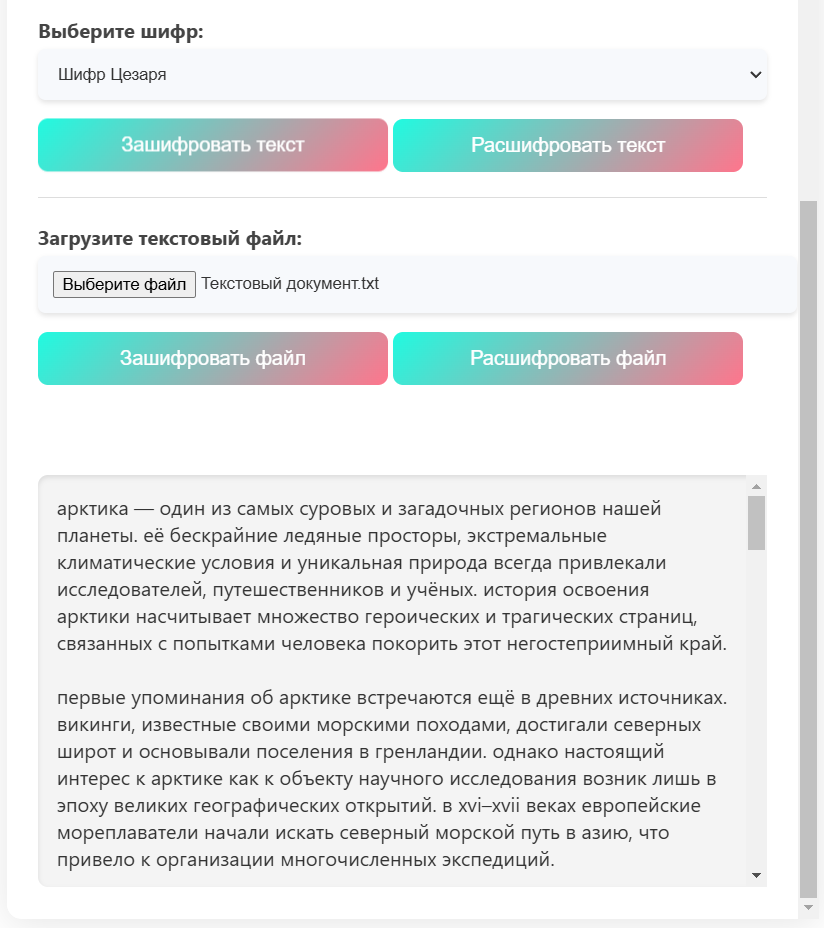


Рисунок 1.2 – Результат расшифрования текста

Шифрование с использованием **таблиц Трисемуса** проводится следующим образом: формируется таблица определенного размера, в которую вписывается по строкам ключевое слово, причем повторяющиеся буквы отбрасываются. Затем эта таблица дополняется не вошедшими в нее буквами алфавита по порядку. Было использовано слово – безопасность – в качестве ключа и сформирована таблица 8×4.

|  |  |  |  |
| --- | --- | --- | --- |
| б | е | з | о |
| п | а | с | н |
| т | ь | в | г |
| д | ж | и | й |
| к | л | м | р |
| у | ф | х | ц |
| ч | ш | щ | ъ |
| ы | э | ю | я |

При шифровании находят в этой таблице букву открытого текста и записывают в шифротекст букву, расположенную ниже нее в том же столбце. Если буква текста оказывает в нижней строке таблицы, тогда для шифротекста берут самую верхнюю букву из того же столбца.

|  |
| --- |
| const alphabet = 'абвгдежзийклмнопрстуфхцчшщъыьэюя'.split('');  function removeDuplicates(keyword) {      const keywordList = [];      const remainingAlphabet = [...alphabet];      for (const char of keyword) {          if (!keywordList.includes(char)) {              keywordList.push(char);}          const index = remainingAlphabet.indexOf(char);          if (index !== -1) {              remainingAlphabet.splice(index, 1);  }}return [...keywordList, ...remainingAlphabet];}  function formTable(keyword) {      const combinedAlphabet = removeDuplicates(keyword);      const table = [];      while (combinedAlphabet.length) {          table.push(combinedAlphabet.splice(0, 4));      }return table;}  function trithemiusEncrypt(keyword, text) {      let result = '';      const table = formTable(keyword);      for (const char of text) {          let encodedChar = char;          for (let i = 0; i < table.length; i++) {              const row = table[i];              const colIndex = row.indexOf(char);              if (colIndex !== -1) {                  encodedChar = table[(i + 1) % table.length][colIndex];                  break;}result += encodedChar;      }return result;}  function trithemiusDecrypt(keyword, text) {      let result = '';      const table = formTable(keyword);      for (const char of text) {          let decodedChar = char;          for (let i = 0; i < table.length; i++) {              const row = table[i];              const colIndex = row.indexOf(char);              if (colIndex !== -1) {                  decodedChar = table[(i - 1 + table.length) % table.length][colIndex];                  break;}}          result += decodedChar;}      return result;} |

Листинг 1.2 – реализация Трисемуса

Зашифрование и расшифрование текста по Трисемусу представлено на рисунках 1.3, 1.4 соответственно.

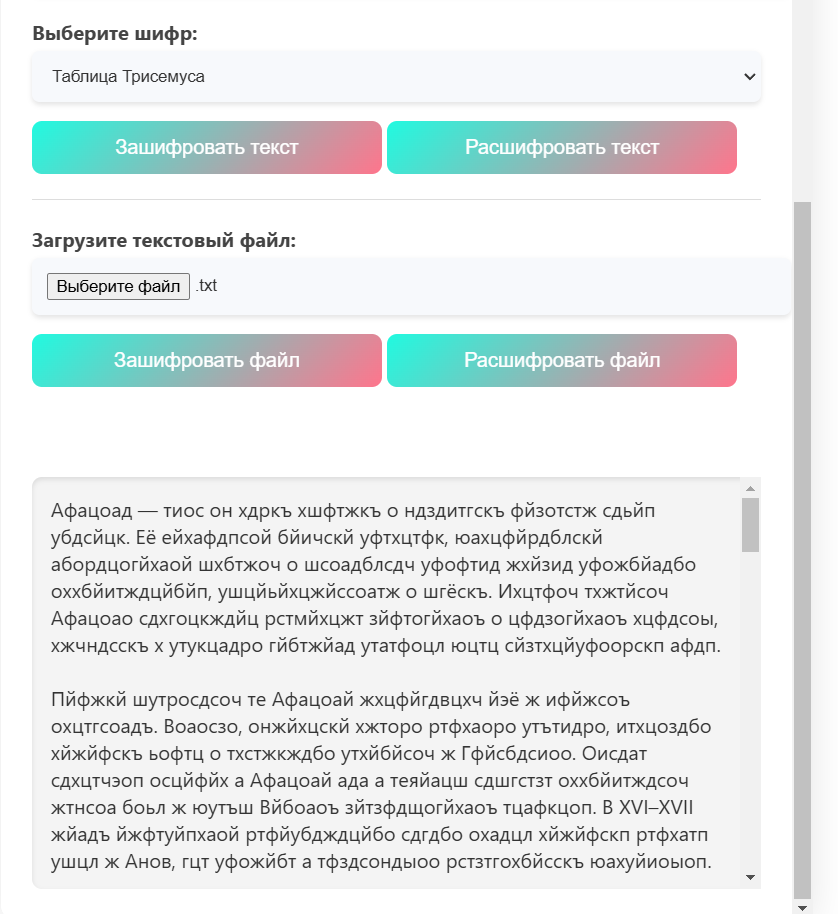


Рисунок 1.3 – Результат зашифрования текста

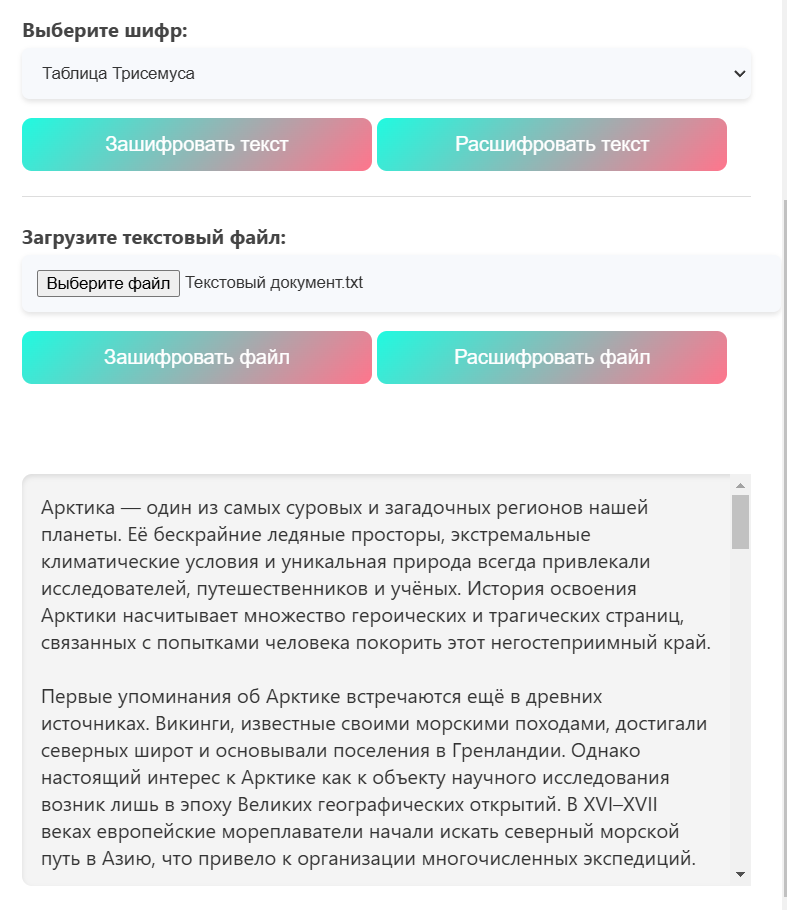


Рисунок 1.4 – Результат расшифрования текста

На рисунке 1.5 представлены гистограммы частот появления символов для исходного и зашифрованного сообщений;

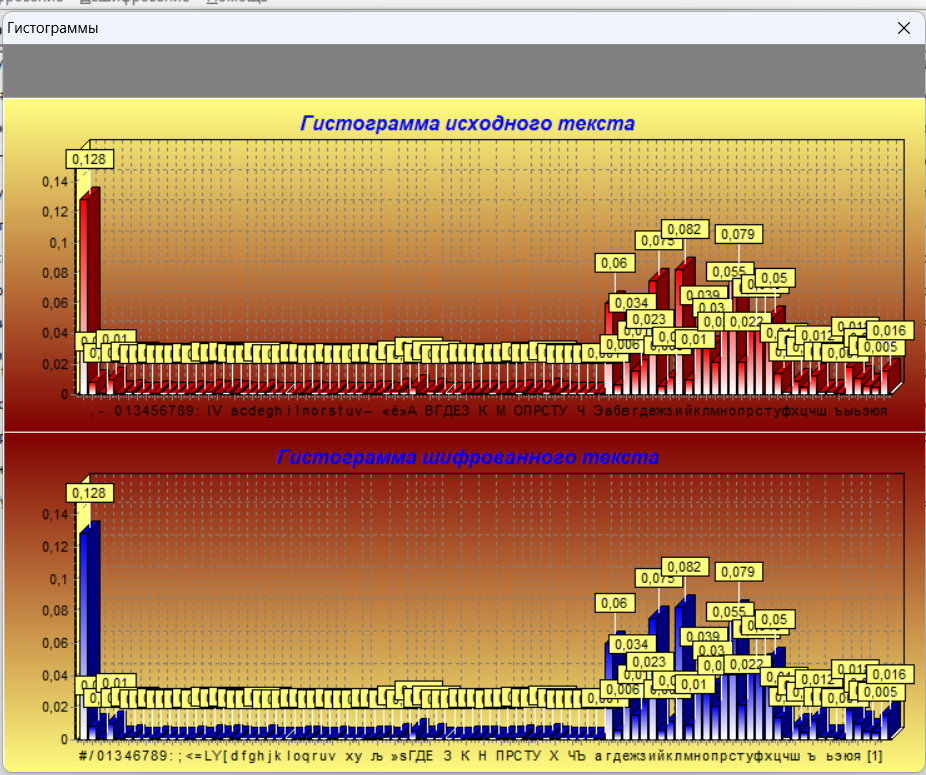


Рисунок 1.5 – Гистограммы частот появления символов для исходного и зашифрованного сообщений

Оценка времени выполнения операций зашифрования/расшифрования представлена на рисунке 1.6.

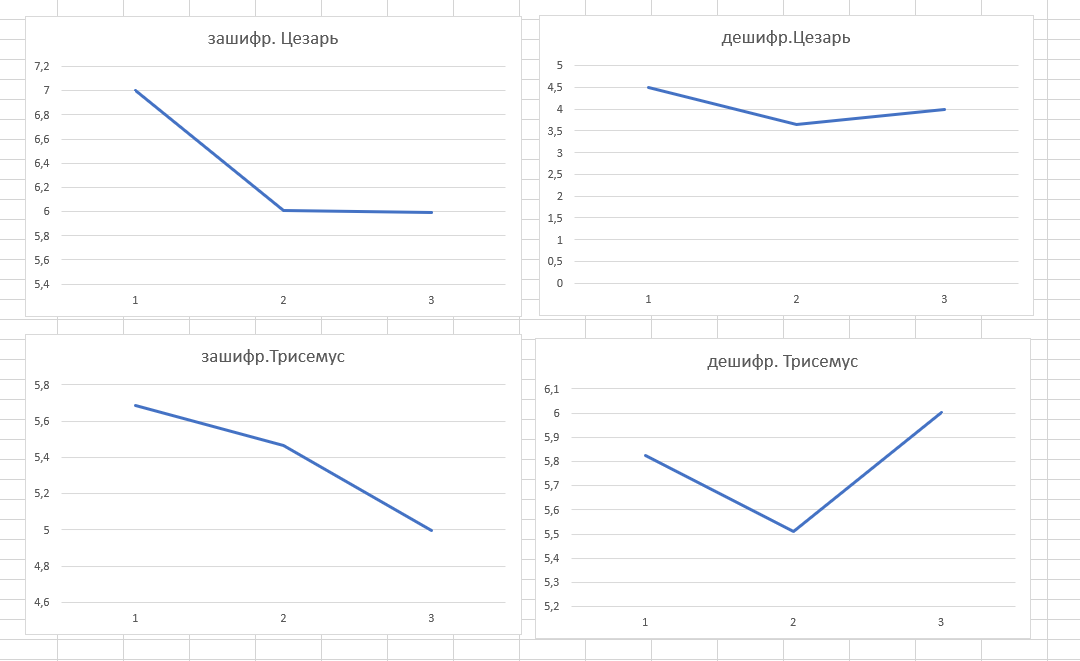


Рисунок 1.6 – Оценка времени выполнения операций зашифрования/расшифрования

**Вывод:**

В данной лабораторной работе мной были изучены и приобретены практических навыков разработки и использования приложений для реализации подстановочных шифров. Были изучены алгоритмы шифрования Цезаря и таблица Трисемуса.