МИНИСТЕРСТВО ОБРАЗОВАНИЯ РЕСПУБЛИКИ БЕЛАРУСЬ

Учреждения образования «БЕЛОРУССКИЙ ГОСУДАРСТВЕННЫЙ

ТЕХНОЛОГИЧЕСКИЙ УНИВЕРСИТЕТ»

Факультет информационных технологий

Кафедра программной инженерии

Специальность 1-40 01 01 Программное обеспечение информационных технологий

Направление специальности 1-40 01 01 10 Программное обеспечение информационных технологий (программирование интернет-приложений)

ОТЧЁТ ПО ЛАБОРАТОРНОЙ РАБОТЕ:

по дисциплине «Информационная безопасность»

Исполнитель

студент (ка) 3 курса группы 6 Розель Станислав Александрович

(Ф.И.О.)

Минск 2024

1. **Шифр Цезаря**

В лабораторной работе нужно было реализовать шифр Цезаря с ключевым словом и сдвигом этого слова. Алфавитом, на котором проводилось зашифрование и расшифрование был белорусский, а слово інфарматыка было ключевым. На листинге 1.1 представлен код шифра.

|  |
| --- |
| function removeLettersArray(array1, array2) {  const lettersToRemove = new Set(array1);  return array2.filter(letter => !lettersToRemove.has(letter));  }  function createNewAlphabet(keyword, number) {  const belAlphabet = [...belarusianAlphabet];  const arrKeyword = removeDuplicateLetters(keyword).split('');  const chunk1 = belAlphabet.splice(number, belAlphabet.length);  const chunk2 = belAlphabet.splice(0, number);  return [  ...removeLettersArray(arrKeyword, chunk1),  ...arrKeyword,  ...removeLettersArray(arrKeyword, chunk2)  ]  }  function createMapAlphabet(newAlphabet) {  for (let i = 0; i < newAlphabet.length; i++) {  alphabets[belarusianAlphabet[i]] = newAlphabet[i];  }  }  function \_encode(text, replacements) {  let result = '';  for (const char of text.toUpperCase()) {  result += replacements[char] || char;  }  return result;  }  function \_decode(text, replacements) {  const reversedReplacements = Object.fromEntries(  Object.entries(replacements).map(([key, value]) => [value, key])  );  let result = '';  for (const char of text) {  result += reversedReplacements[char] || char;  }  return result;  } |

Листинг 1.1 – Код реализации шифра Цезаря

Так же нужно было сравнить количество символов в исходном и зашифрованном сообщении. Сравнение представлено в таблице 1.1

Таблица 1.1 – Сравнение количества символов.

|  |  |
| --- | --- |
| Исходный текст | Зашифрованный текст |
|  |  |

Было измерено время для шифрования и расшифрования сообщения:

* Шифрование текста шифрем Цезаря: 32.438ms
* Расшифровка текста шифрем Цезаря: 29.635ms

1. **Шифр Трисемуса**

Ещё один шифр, который разбирался в ходе лабораторной работы это был шифр Тресимуса. Так же использовался белорусский язык, в роли ключа использовалось собственное имя: Станіслаў. На листинге 2.1 представлен код реализующий шифрование и расшифрование с помощью шифра Трисемуса.

|  |
| --- |
| function createTableWithKeyword(keyword) {  const uniqueChars = Array.from(new Set(keyword.toUpperCase().split('')));  const validKeyChars = uniqueChars.filter(char => ALPHABET.includes(char));  const remainingChars = ALPHABET.filter(char => !validKeyChars.includes(char));  const newAlphabet = [...validKeyChars, ...remainingChars];  const rows = 8;  const cols = 4;  const table = [];  let charIndex = 0;  for (let i = 0; i < rows; i++) {  const row = [];  for (let j = 0; j < cols; j++) {  if (charIndex < newAlphabet.length) {  row.push(newAlphabet[charIndex]);  charIndex++;  } else {  row.push('');  }  }  table.push(row);  }  return table;  }  function encrypt(text, keyword) {  const table = createTableWithKeyword(keyword);  return text.toUpperCase().split('').map(char => {  if (!ALPHABET.includes(char)) {  return char;  }  for (let i = 0; i < table.length; i++) {  for (let j = 0; j < table[i].length; j++) {  if (table[i][j] === char) {  return table[i][0];  }  }  }  return char;  }).join('');  }  function decrypt(encryptedText, keyword) {  const table = createTableWithKeyword(keyword);  return encryptedText.toLowerCase().split('').map(char => {  if (!ALPHABET.includes(char)) {  return char;  }  for (let i = 0; i < table.length; i++) {  if (table[i][0] === char) {  return char;  }  }  return char;  }).join('');  } |

Листинг 2.1 – Шифр Трисемуса

Так же как и с шифром Цезаря, нужно проверить как изменилось количество символов. Сравнение приведено в таблице 2.1.

Таблица 2.1 – Сравнение количества символов.

|  |  |
| --- | --- |
| Исходный текст | Зашифрованный текст |
|  |  |

Было измерено время для шифрования и расшифрования сообщения:

* Шифрование текста таблицей Трисемуса: 37.184ms
* Расшифровка текста таблицей Трисемуса: 30.662ms