Федеральное агентство связи Федеральное государственное бюджетное образовательное учреждение высшего образования «Сибирский государственный университет телекоммуникаций и информатики» (СибГУТИ)

Курсовая работа по дисциплине «Программирования»

Тема: "Шифрование текста шифром Гронсфельда"

	Выполнил:
СТ	гудент гр. ИА-232
	Володин А.С
	подпись
	Проверил:
	•
Лебеденко Люд	мила Фёдоровна
	оценка полпись

Задание:

Разработать программу **KeyTable**, выполняющую шифрование в заданном тексте и **DeKeyTable** – дешифровку текста. Текст до шифрования, после шифрования и после дешифровки должен выводиться на экран.

Анализ задачи.

end function

```
1) Реализовать функции для шифровки и дешифровки русского текста в
  формате wchar t, учесть случаи некорректных данных
  (использование любого алфавита, кроме русского).
  Псевдокод функции encryptString:
  function encryptString(str: array of wchar t, key: array of int, keyLength:
  int)
         strLength = length(str)
         keyIndex = 0
        for i = 0 to strLength-1
           if str[i] != ' '
               str[i] = encryptChar(str[i], key[keyIndex % keyLength])
               keyIndex = keyIndex + 1
           end if
         next i
  end function
  Псевдокод функции encryptChar:
  function encryptChar(ch: wchar t, key: int) -> wchar t
     if ch = ' ' then
       return ch
     else if (ch \ge 0x0410 and ch \le 0x044F) or (ch \ge 0x0041 and ch \le
  0x005A) or (ch >= 0x0061 and ch <= 0x007A) then
       return ch + kev
     else
      return (ch + key) modulo ALPHABET SIZE
     end if
```

2) Реализовать функцию для сравнения текста до шифровки и после дешифровки в формате wchar t. Псевдокод функции compareStrings: function compareStrings(str1: array of wchar_t, str2: array of wchar_t) -> int len1 = length(str1)len2 = length(str2)if len1 != len2 then return 0 end if for i = 0 to len1-1 if str1[i] != str2[i] then return 0 end if next i return 1 end function 3) Реализовать смену формата argv[] из char в wchar t. wchar_t *filename1; int len1; len1 = mbstowcs(NULL, argv[1], 0) + 1; // определение дли аргументаfilename1 = (wchar t *)malloc(len1 * sizeof(wchar t)); mbstowcs(filename1, argv[1], len1); // преобразование char -> wchar t 4) Реализовать чтение файлов с выделением динамической памяти для файлов в формате txt, которые содержат текст в виде wchar t. FILE *RuFile = wfopen(filename1, L"r, ccs=UTF-8"); if (RuFile == NULL) { wprintf(L"Error: cannot open OriginalRU.txt\n"); return 1; wchar t **RuStrings = NULL; int RuStringsCount = 0: wchar t RuLine[1024]; // Буфер для считывания строки while (fgetws(RuLine, 1024, RuFile) != NULL){ RuLine[wcslen(RuLine) - 1] = $L'\n'$; RuStringsCount++; RuStrings = (wchar_t **)realloc(RuStrings, RuStringsCount * sizeof(wchar t*)); // выделение памяти для типа wchar t RuStrings[RuStringsCount - 1] = wcsdup(RuLine); fclose(RuFile);

5) Записать функции, которые используются для обработки текста, в динамическую библиотеку.

Тестовые данные

Текст файла без шифровки:

восточный экспресс

Вот и всё? Госдума окончательно приняла закон о едином реестре военнослужащих. Теперь военкомат будет получать данные о тебе от налоговой, МВД и даже от обычных больниц. А повестки будут приходить через Госуслуги. Если призывник будет скрываться от военкомата, ему запретят выезжать из страны, водить авто, открывать ИП, брать кредиты и ипотеки. Что делать прямо сейчас? Кто может помочь с решением вопросов с военкоматом и армией?

Зачем ты вообще думаешь об этом. Посмотри, там же страшно. Не говори только, что ты действительно хочешь этого. Жить страшно? Да, есть такое. Но это хуже. Ведь твоим последним чувством будет не спокойствие, а ужас. Если ты совершил какую-то ошибку, попробуй её исправить. Если не получится, берись за новое дело. Сделай себя лучше, а не хуже.

восточный экспресс

Гордость полными вагонами, золотыми погонами С юга дуют молодые ветра Разрывая в клочья облака Не забыли, шлют издалека С дома, мама и не последняя любовь А по небу бегут, видишь, чьи-то следы Это, может быть, ты Это, может быть, я Это, может, нас ждут Это, может, нам поют свои Нашла коса на камень, идёт война на память лет

Текст файла с шифровкой:

дхтърюоѓл єлщечжщу

Ехсмршує схмхэуй квкпхвуй4 йхмцфђнр схдцпзнр У зди жъяъ охмцжђж кзщси Тзишэйбї д смцщѓе цгтбтв Фж пвиьук3 щуещ йпжзмнмз Т мруб4 озни к фж чршмнжфеї нѕвцдѓ Б чр фжйх ижлхщ- кклйею3 шєк4уц утжмэ дуц. упозщ вѓфѓ- ъэ дуц. упозщ вѓфѓ- ї Ящп4 охзнф3 оиу неыф дуц. упозщ- хву рцещ ткрп Іиътб тршб хв сбфзфэ4 клђъ дхкхв фб чвуеъю тжъ

Листинг программы

Данный код на языке С представляет собой программу для шифрования и дешифрования текста на русском языке. Программа принимает два аргумента командной строки: имя файла с исходным текстом на русском языке и имя файла с зашифрованным текстом на русском языке.

Основная логика программы заключается в чтении содержимого файлов в динамически создаваемые массивы строк в формате wchar_t, шифровке и дешифровке строк с помощью заданного ключа и сравнении их с исходным текстом. В конце программы выводится результат сравнения и освобождаются выделенные для массивов строк имена файлов.

Для работы программы используются следующие функции и библиотеки:

- Функция main() точка входа в программу.
- Библиотека kurs8.h пользовательская библиотека с объявлениями функций decryptString() и encryptString(), decryptChar() и encryptChar(), compareStrings()
- Список используемых библиотек:
 - 1) <stdio.h> библиотека ввода-вывода в стандартные потоки (например, на консоль) и файлы. Она содержит функции для работы с файловыми указателями, чтения/записи данных в файлы и консоль, форматирования вывода и ввода.
 - 2) <stdlib.h> библиотека, которая содержит функции для работы с памятью, реализации алгоритмов сортировки, функций для управления процессом выполнения программы (например, exit(), abort()), а также функции для работы со случайными числами.
 - 3) <string.h> библиотека, которая содержит функции для работы со строками, такие как копирование строк, сравнение, поиск, конкатенация и многие другие.
 - 4) <wchar.h> библиотека, которая содержит функции для работы с широкими символами (wide characters), которые могут хранить символы на разных языках, включая многобайтные символы. Она используется, например, для работы с юникодом.
 - 5) <locale.h> библиотека, которая содержит функции для установки и изменения текущей локали программы (например, языка и кодировки). Она используется для корректного отображения символов на разных языках и культурах.
- Функция setlocale() устанавливает локаль для корректной работы с русским языком.
- Функция mbstowcs() преобразует строку из многобайтового формата в широкий формат (wchar_t).
- Функция malloc() выделяет динамическую память для массивов строк.
- Функция realloc() изменяет размер выделенной памяти для массивов строк.
- Функция wcsdup() создает копию строки в формате wchar_t.

- Функция fgetws() считывает строку из файла в формате wchar t.
- Функция wfopen() открывает файл в формате wchar t.
- Функция wprintf() выводит строку в формате wchar_t на экран.

```
Для файла kurs8.c:
#include "kurs8.h"
int main(int argc, char **argv)
  if (argc < 3)
     printf("Usage: %s <filename>\n", argv[0]);
     return 1;
  setlocale(LC ALL, "");
  int key[] = \{2, 7, 1, 8\};
  wchar t*filename1;
  // Определяем размер буфера для хранения имени файла в формате wchar t
  int len1 = mbstowcs(NULL, argv[1], 0) + 1;
  filename1 = (wchar t*)malloc(len1 * sizeof(wchar t));
  // Преобразуем строку argv[1] в формат wchar t
  mbstowcs(filename1, argv[1], len1);
  wchar t *filename2;
  // Определяем размер буфера для хранения имени файла в формате wchar t
  int len2 = mbstowcs(NULL, argv[2], 0) + 1;
  filename2 = (wchar t*)malloc(len2 * sizeof(wchar t));
  // Преобразуем строку argv[1] в формат wchar t
  mbstowcs(filename2, argv[2], len2);
  // Открываем файл для чтения
  FILE *RuFile = _wfopen(filename1, L"r, ccs=UTF-8");
  if (RuFile == NULL)
     wprintf(L"Error: cannot open OriginalRU.txt\n");
     return 1;
  }
  // Создаем динамический массив для хранения строк из файла OriginalRU.txt
```

```
wchar t **RuStrings = NULL;
  int RuStringsCount = 0;
  wchar t RuLine[1024]; // Буфер для считывания строки
  while (fgetws(RuLine, 1024, RuFile) != NULL)
    RuLine[wcslen(RuLine) - 1] = L'\n';
    // Увеличиваем размер массива RuStrings на 1
    RuStringsCount++;
    RuStrings = (wchar t **)realloc(RuStrings, RuStringsCount * sizeof(wchar t *));
    // Создаем копию строки RuLine и добавляем ее в массив RuStrings
    RuStrings[RuStringsCount - 1] = wcsdup(RuLine);
  }
  // Освобождаем память, используемую для чтения строк
  fclose(RuFile);
  FILE *ENFile = wfopen(filename2, L"r, ccs=UTF-8");
  if (ENFile == NULL)
    wprintf(L"Error: cannot open OriginalRU.txt\n");
    return 1;
  }
  // Создаем динамический массив для хранения строк из файла EncryptRU.txt
  wchar t **ENStrings = NULL;
  wchar t **DEStrings = NULL;
  int ENStringsCount = 0;
  wchar t ENLine[1024]; // Буфер для считывания строки
  while (fgetws(ENLine, 1024, ENFile) != NULL)
  {
    ENLine[wcslen(ENLine) - 1] = L'\n'; // добавляем элемент конца строки
    // Увеличиваем размер массива RuStrings на 1
    ENStringsCount++;
    DEStrings = (wchar t **)realloc(DEStrings, ENStringsCount * sizeof(wchar t *));
    ENStrings = (wchar t **)realloc(ENStrings, ENStringsCount * sizeof(wchar t *));
    // Создаем копию строки ENLine и добавляем ее в массив ENStrings
    ENStrings[ENStringsCount - 1] = wcsdup(ENLine);
    // Создаем копию строки ENLine, но уже после дешифровки и добавляем
ее в массив DEStrings
```

```
wchar t *DELine = wcsdup(ENLine);
  decryptString(DELine, key, 4);
  DELine[wcslen(DELine) - 1] = L'\n'; // добавляем элемент конца строки
  DEStrings[ENStringsCount - 1] = DELine;
}
// Освобождаем память, используемую для чтения строк
fclose(ENFile);
// Выводим содержимое массива RuStrings
wprintf(L"\n=====ORIGINAL TEXT=====\n");
for (int i = 0; i < RuStringsCount; i++)
{
  wprintf(L"%ls", RuStrings[i]);
}
wprintf(L"\n=====ENCRYPT TEXT=====\n");
// Выводим содержимое массива ENStrings
for (int i = 0; i < ENStringsCount; i++)
  // decryptString(ENStrings[i], key, 4);
  wprintf(L"%ls", ENStrings[i]);
}
wprintf(L"\n");
wprintf(L"\n=====DECRYPT TEXT=====\n");
// Выводим содержимое массива ENStrings
for (int i = 0; i < ENStringsCount; i++)
{
  // decryptString(ENStrings[i], key, 4);
  wprintf(L"%ls", DEStrings[i]);
}
wprintf(L"\n");
int count = 0;
for (int i = 0; i < RuStringsCount; i++)
{
  if (compareStrings(RuStrings[i], DEStrings[i]))
  {
     count++;
}
```

```
if (count == RuStringsCount)
    wprintf(L"SUCCES!\n");
  }
  else
    wprintf(L"FAIL!\n");
  }
  // Освобождаем память, используемую для хранения строк
  for (int i = 0; i < RuStringsCount; i++)
  {
    free(RuStrings[i]);
  free(RuStrings);
  // Освобождаем память, используемую для хранения строк
  for (int i = 0; i < ENStringsCount; i++)
    free(ENStrings[i]);
    free(DEStrings[i]);
  free(ENStrings);
  free(DEStrings);
  free(filename1);
  free(filename2);
}
```

```
#include "kurs8.h"
// Функция для шифрования символа с использованием ключа
wchar_t encryptChar(wchar_t ch, int key)
  if (ch == L' ')
  {
    return ch;
  else if ((ch \geq 0x0410 && ch \leq 0x044F) || (ch \geq 0x0041 && ch \leq 0x005A) || (ch
>= 0x0061 \&\& ch <= 0x007A))
  {
    return ch + key;
  else
    return (ch + key) % ALPHABET_SIZE;
}
// Функция для дешифрования символа с использованием ключа
wchar_t decryptChar(wchar_t ch, int key)
{
  if (ch == L' ')
  {
    return ch;
  else if ((ch \geq 0x0410 && ch \leq 0x044F) || (ch \geq 0x0041 && ch \leq 0x005A) || (ch
= 0x0061 \&\& ch <= 0x007A)
  {
    return ch - key;
  else
    return (ch - key + ALPHABET_SIZE) % ALPHABET_SIZE;
}
// Функция для шифрования строки с использованием ключа
void encryptString(wchar t *str, int *key, int keyLength)
{
```

```
int strLength = wcslen(str);
  int keyIndex = 0;
  for (int i = 0; i < strLength; i++)
     if (str[i] != L' ')
     {
       str[i] = encryptChar(str[i], key[keyIndex % keyLength]);
       keyIndex++;
     }
  }
}
// Функция для дешифрования строки с использованием ключа
void decryptString(wchar_t *str, int *key, int keyLength)
  int strLength = wcslen(str);
  int keyIndex = 0;
  for (int i = 0; i < strLength; i++)
     if (str[i] != L' ')
       str[i] = decryptChar(str[i], key[keyIndex % keyLength]);
       keyIndex++;
     }
  }
}
// Функция для сравнения оригинального текста и дешифрованного текста
int compareStrings(wchar_t *str1, wchar_t *str2)
{
  // Сравниваем длины строк
  size_t len1 = wcslen(str1);
  size t len2 = wcslen(str2);
  if (len1 != len2)
  {
     return 0;
  }
  // Сравниваем символы строк
  for (size_t i = 0; i < len1; i++)
     if (str1[i] != str2[i])
     {
       return 0;
```

```
}
  return 1;
}
Для файла kurs8.h:
#include <stdio.h>
#include <stdlib.h>
#include <string.h>
#include <wchar.h>
#include <locale.h>
#define ALPHABET SIZE 1114112 // Максимальное значение кода Unicode 13.0
wchar_t encryptChar(wchar_t ch, int key);
wchar t decryptChar(wchar t ch, int key);
void encryptString(wchar t *str, int *key, int keyLength);
void decryptString(wchar t *str, int *key, int keyLength);
int compareStrings(wchar_t *str1, wchar_t *str2);
Для файла text.c: // файл для добавления текста в txt
#include "kurs8.h"
int main(int argc, char **argv)
  setlocale(LC_ALL, "");
  int key[] = \{2, 7, 1, 8\};
  // Ввод и вывод текста для файлов
  wchar t text[1000];
  if (argc < 2)
  {
     printf("Usage: %s <filename>\n", argv[0]);
     return 1;
  }
  else
     mbstowcs(text, argv[1], 1000);
  int len = wcslen(text);
  text[len] = L' ';
                   // добавляем пробел в конец массива
  text[len + 1] = L'\0'; // добавляем нулевой символ в конец массива
```

```
FILE *file1 = _wfopen(L"originalru.txt", L"a, ccs=UTF-8");
  if (!file1)
  {
     wprintf(L"Error opening file1\n");
     return 1:
  }
  fwprintf(file1, L"\n%ls", text);
  fclose(file1);
  encryptString(text, key, 4);
  wprintf(L"Encoded text: %ls\n", text);
  FILE *file2 = wfopen(L"encryptru.txt", L"a, ccs=UTF-8");
  if (!file2)
  {
     wprintf(L"Error opening file2\n");
     return 1;
  }
  fwprintf(file2, L"\n%ls", text);
  fclose(file2);
  decryptString(text, key, 4);
  wprintf(L"Decoded text: %ls\n", text);
  return 0;
}
```

Оценка Криптостойкости шифра:

Данный шифр можно легко подвергнуть криптоанализу, так как он использует простую замену символов с использованием ключа, который повторяется каждые keyLength символов. Это означает, что зная длину ключа и имея достаточно зашифрованного текста, можно провести атаку перебора ключа и восстановить исходный текст. Кроме того, данный шифр не учитывает частоту встречаемости символов в языке и не делает никаких преобразований над блоками текста. Это означает, что статистический криптоанализ может легко выявить закономерности в зашифрованном тексте и позволит восстановить исходный текст.

Таким образом, данный шифр не обладает достаточной криптостойкостью и не рекомендуется использовать для защиты конфиденциальной информации

Скрины с результатами:

PS C:\Users\volod\.vscode\Homework\kursach> ./kurs originalru.txt encryptru.txt

====ORIGINAL TEXT====

восточный экспресс

Вот и всё? Госдума окончательно приняла закон о едином реестре военнослужащих. Теперь военкомат буде т получать данные о тебе от налоговой, МВД и даже от обычных больниц. А повестки будут приходить чер ез Госуслуги. Если призывник будет скрываться от военкомата, ему запретят выезжать из страны, водить авто, открывать ИП, брать кредиты и ипотеки. Что делать прямо сейчас? Кто может помочь с решением в опросов с военкоматом и армией?

Зачем ты вообще думаешь об этом. Посмотри, там же страшно. Не говори только, что ты действительно хо чешь этого. Жить страшно? Да, есть такое. Но это хуже. Ведь твоим последним чувством будет не спокой ствие, а ужас. Если ты совершил какую-то ошибку, попробуй её исправить. Если не получится, берись за новое дело. Сделай себя лучше, а не хуже.

восточный экспресс

Гордость полными вагонами, золотыми погонами С юга дуют молодые ветра Разрывая в клочья облака Не за были, шлют издалека С дома, мама и не последняя любовь А по небу бегут, видишь, чьи-то следы Это, мо жет быть, ты Это, может быть, я Это, может, нас ждут Это, может, нам поют свои Нашла коса на камень, идёт война на память ле

====ENCRYPT TEXT=====

дхтърно?л єлщсчжщу

Дху р дш?G Ехтмхуб цмхоявшжуюфп чтпоїнз иимхо ц злйхру снэшушз йпнпфпщнъзиыпц6 Фмрнт? гцэфлцозу йхлж ъ схмыщзує жзохэм п ъзиж цф фбуркпкрр- ФДЛ й мвнж цф хв?щфьэ гхмєппч6 В цпкзшутк ифмхщ ршкьпмкщэ язч жп Ехтыутфлк5 Жщнп ршкоькппл йхлжь усс?дзуєу? пъ дхжхмхнифз- ноъ иисчжъёщ г?зозиф? йп ущсип?- крлйью згър3 пъмчьквщэ РСЗ вшвщэ ттмерф? й рсхунмп/ Яфх еннзує счфр шжсщзтG Мщп фрнжъ схнцщ? т шзяжхкмн кр цсцухг щ дхжхмхнифхн р вчнрэр@

Йзшно щь крхвёз лффвище ри юъру/ Чршнцфчй4 фзн оз шушвяоц0 Фж лрйпшк щпуюсп4 щщп ъэ лжсущгрфимепх цц шище ящплр5 Зрф? тътэщхрF Еи. мтъю щбтрм/ Хр еуц чъзн0 Йжию щгцку рцутжиппн яхйтъдхн йхлжъ пм тчрспс ущгрз3 б ыизт6 Зшир ф? тидискт лимъя5фх пкилы. цпчтхвыл м? руцсидпуе0 Мтук фж чртфякщтї. ижшкшэ пв ф пкрм еннх/ Шужимил шжйё тфяъм- и пм цыим/

дхтърюо?л єлщсчжщу

Ехсмршує схмхэуй квкпхвуй4 йхмцф?нр схдцпзнр У ?ди жьяъ охмцж?ж кзщси Тзишэйбї д смцщ? цгтбтв Фж пви ьук3 щущ йпжэмнмз Т мруб4 озни к фж чршмнжфї н?вид? Б чр фжйх ижлхщ- кклйю3 шєк4уц утжмэ дуц. упозщ в?ф?- ъэ дуц. упозщ в?ф?- ї Ящп4 охзнф3 оиу неыф дуц. упозщ- хву рцщ ткрп Іиьтб тршб хв сбфзфэ4 кл?ъ дхкхв фб чвуъю тж

====DECRYPT TEXT====

восточный экспресс

Вот и всё? Госдума окончательно приняла закон о едином реестре военнослужащих. Теперь военкомат буде т получать данные о тебе от налоговой, МВД и даже от обычных больниц. А повестки будут приходить чер ез Госуслуги. Если призывник будет скрываться от военкомата, ему запретят выезжать из страны, водить авто, открывать ИП, брать кредиты и ипотеки. Что делать прямо сейчас? Кто может помочь с решением в опросов с военкоматом и армией?

Зачем ты вообще думаешь об этом. Посмотри, там же страшно. Не говори только, что ты действительно хо чешь этого. Жить страшно? Да, есть такое. Но это хуже. Ведь твоим последним чувством будет не спокой ствие, а ужас. Если ты совершил какую-то ошибку, попробуй её исправить. Если не получится, берись за новое дело. Сделай себя лучше, а не хуже.

восточный экспресс

Гордость полными вагонами, золотыми погонами С юга дуют молодые ветра Разрывая в клочья облака Не за были, шлют издалека С дома, мама и не последняя любовь А по небу бегут, видишь, чьи-то следы Это, мо жет быть, ты Это, может быть, я Это, может, нас ждут Это, может, нам поют свои Нашла коса на камень, идёт война на память ле

SUCCES!

Заключение

Работа с типом данных wchar_t на языке программирования С оказалась для меня очень интересной. Этот тип данных предоставляет множество преимуществ в работе с символами и строками на разных языках.

Одним из основных преимуществ типа данных wchar_t является его поддержка многобайтных символов и кодировок, таких как UTF-8, UTF-16 и UTF-32. Это позволяет работать с символами из разных языков и поддерживать многоязычные приложения. Кроме того, тип данных wchar_t также может использоваться для работы с символами, которые не могут быть представлены в ASCII-кодировке, таких как символы кириллицы и других алфавитов.

В процессе работы я узнал много нового о работе с типом данных wchar_t на языке программирования С. Я познакомился с функциями для работы с широкими символами, такими как wcsdup(), fgetws(), _wfopen() wcscpy(), wcslen() и wprintf(). Я также научился использовать специальные символы, такие как L для обозначения широких символов.

Кроме преимуществ, связанных с работой с многобайтными символами и различными кодировками, тип данных wchar_t также имеет недостатки. Одним из главных недостатков является расход памяти по сравнению с элементами типа char. Так как широкие символы занимают больше места в памяти, чем обычные символы типа char, использование типа данных wchar_t может привести к значительному увеличению объема памяти, необходимой для хранения строк и символов. Это может быть особенно проблематично в случае больших текстовых файлов или при работе с большими объемами данных.

Кроме того, использование типа данных wchar_t может также привести к проблемам совместимости с другими типами данных и библиотеками, которые не поддерживают широкие символы. Это может ограничить возможности использования этого типа данных в некоторых проектах.

В целом, при работе с типом данных wchar_t необходимо учитывать как его преимущества, так и недостатки, и выбирать его использование в зависимости от конкретных задач и требований проекта.

Список литературы

- 1. Microsoft. (2021). Char, wchar_t, char16_t, char32_t. Retrieved from https://learn.microsoft.com/ru-ru/cpp/cpp/char-wchar-t-char16-t-char32-t?view=msvc-160
- 2. Лопатин, A. (2012). Программирование на языке C++. Работа со строками. Habr. Retrieved from https://habr.com/ru/articles/164193/
- 3. GeeksforGeeks. (2021). Wide char and Library functions in C/C++. Retrieved from https://www.geeksforgeeks.org/wide-char-and-library-functions-in-c/
- 4. Microsoft. (2021). How to: Convert Between Various String Types. Retrieved from https://learn.microsoft.com/ru-ru/cpp/text/how-to-convert-between-various-string-types?view=msvc-160