

## **Лабораторная работа № 1. Шифрование данных методами подстановки, перестановки и полиалфавитными шифрами**

### **Цель работы:**

Приобретение навыков шифрования информации с использованием простейших методов шифрования.

### **Постановка задачи:**

Разработать алгоритм и составить программу, позволяющую закодировать любой текст одним из методов (метод подстановки, метод перестановки, многоалфавитный шифр) и выполнить обратное преобразование. Метод, которым необходимо зашифровать исходную информацию, выбирается в соответствии с вариантом из таблиц 1.1, 1.2, 1.3. Язык программирования выбирается произвольно.

### **Описание исходных данных:**

В данной лабораторной я реализую все 3 метода шифрования. В качестве вариантов я выбираю варианты 1 (метод подстановки; подстановочный алфавит № 3; английский алфавит), 2 (метод перестановки; группа перестановки № 1; ASCII-код) и 3 (многоалфавитный шифр; подстановочные алфавиты № 1, 2 и 5; русский алфавит).

#### **Метод подстановки:**

Исходный текст: "EVERY COMPLEX PROBLEM HAS A SOLUTION THAT IS CLEAR, SIMPLE, AND WRONG."

Английский алфавит: "ABCDEFGHIJKLMNOPQRSTUVWXYZ ,!;:;?-"

#### **Метод перестановки:**

Исходный текст: "<<({{EVERY COMPLEX PROBLEM HAS A SOLUTION THAT IS CLEAR, SIMPLE, AND WRONG.}})>>"

Подстановочный алфавит № 3: "Z .XY;!ST;:QR?-NOPLMUVWABCDEFGHIJK"

Группа перестановки № 1: исходные индексы = [1, 2, 3, 4, 5, 6], индексы после перестановки [3, 5, 2, 6, 1, 4]

#### **Метод многоалфавитного шифра:**

Исходный текст: "ШИФРОВАНИЕ ПРОСТОЙ ПОДСТАНОВКОЙ НА КОРОТКИХ АЛФАВИТАХ ОБЕСПЕЧИВАЕТ СЛАБУЮ ЗАЩИТУ ОТКРЫТОГО ТЕКСТА"

Русский алфавит: "АБВГДЕЁЖЗИЙКЛМНОПРСТУФХЦЧШЩЪЫЬЭЮЯ "

Подстановочный алфавит № 1: "БЮГЫЕЪЗШЙЦЛФНТПРСОУМХКЧИЩЖЪДЭВЯ АЁ"

Подстановочный алфавит № 2: "СОУМКХЧИЩЖЪДЭВЯАБЮГ ЕЪЗШЙЦЁФНТПРЫЛ"

Подстановочный алфавит № 5: "МНОПРСТУФХЦЧШЩЪЫЬЭЮЯ АБВГДЕЁЖЗИЙКЛ"

### **Алгоритм работы программы:**

#### **Метод подстановки:**

1. Создаем ассоциативный массив (Map) между символами исходного алфавита и символами подстановочного алфавита; ключом являются символы исходного алфавита.
2. Для всех символов исходного текста (из исходного алфавита), заменяем их на соответствующие символы из подстановочного алфавита с помощью ассоциативного массива из п.1.

3. Получаем закодированный текст.
4. Создаем ассоциативный массив (Map) между символами исходного алфавита и символами подстановочного алфавита; ключом являются символы подстановочного алфавита.
5. Для всех символов закодированного текста (из подстановочного алфавита), заменяем их на соответствующие символы из исходного алфавита с помощью ассоциативного массива из п.4.
6. Получаем раскодированный текст.
7. Сравниваем исходный текст с закодированным текстом - они должны не совпадать.
8. Сравниваем исходный текст с раскодированным текстом - они должны совпадать.

#### **Метод перестановки:**

1. Проверяем длину исходного текста; если она не кратна длине группы перестановки, то дополняем исходный текст пробелами, пока его длина не станет кратна длине группы перестановки
2. Разбиваем исходный текст на порции, длина которых равна длине группы перестановки
3. Для каждой порции проводим замену символов согласно группе перестановки: для каждой перестановки символ, расположенный по исходному индексу переставляется на индекс после перестановки. Например, пусть группа перестановки имеет следующий вид: исходные индексы = [1, 2], индексы после перестановки [2, 1]; пусть данная порция содержит подстроку "XY", тогда эта порция будет преобразована в подстроку "YX" согласно группе перестановки.
4. Получаем закодированный текст.
5. Разбиваем закодированный текст на порции, длина которых равна длине группы перестановки.
6. Для каждой порции проводим замену символов согласно группе перестановки: для каждой перестановки символ, расположенный по индексу после перестановки переставляется на исходный индекс. Например, пусть группа перестановки имеет следующий вид: исходные индексы = [1, 2], индексы после перестановки [2, 1]; пусть данная порция содержит подстроку "YX", тогда эта порция будет преобразована в подстроку "XY" согласно группе перестановки.
7. Получаем раскодированный текст.
8. Сравниваем исходный текст с закодированным текстом - они должны не совпадать.
9. Сравниваем исходный текст с раскодированным текстом - они должны совпадать.

#### **Метод многоалфавитного шифра:**

1. Создаем массив ассоциативных массивов; каждым элементом этого массива является ассоциативный массив между символами исходного алфавита и символами соответствующего подстановочного алфавита; ключом являются символы исходного алфавита. Например, если у нас 2 подстановочных алфавита в многоалфавитном шифре, то у нас получится массив из 2 элементов: 1-м элементом (с индексом 0) будет ассоциативный массив между символами исходного алфавита и символами 1-го подстановочного алфавита, 2-м элементом (с индексом 1) будет ассоциативный массив между символами исходного алфавита и символами 2-го подстановочного алфавита.
2. Для всех символов исходного текста (из исходного алфавита), заменяем их на соответствующие символы из соответствующего подстановочного алфавита. Для

каждого символа выбирается свой подстановочный алфавит следующим образом: если у нас **N** подстановочных алфавитов и индекс символа в строке - **i**, то будет выбран подстановочный алфавит с индексом  $i \% N$ . В нашем случае это означает, что для символа с индексом **i** в исходной строке, мы из массива ассоциативных массивов (из п.1) возьмем ассоциативный массив с индексом  $i \% N$  и с его помощью уже получим результирующий символ.

3. Получаем закодированный текст.

4. Создаем массив ассоциативных массивов; каждым элементом этого массива является ассоциативный массив между символами соответствующего подстановочного алфавита и символами исходного алфавита; ключом являются символы соответствующего подстановочного алфавита. Например, если у нас 2 подстановочных алфавита в многоалфавитном шифре, то у нас получится массив из 2 элементов: 1-м элементом (с индексом 0) будет ассоциативный массив между символами 1-го подстановочного алфавита и символами исходного алфавита, 2-м элементом (с индексом 1) будет ассоциативный массив между символами 2-го подстановочного алфавита и символами исходного алфавита.

5. Для всех символов закодированного текста, заменяем их на соответствующие символы из исходного алфавита. Для каждого символа выбирается свой подстановочный алфавит следующим образом: если у нас **N** подстановочных алфавитов и индекс символа в строке - **i**, то будет выбран подстановочный алфавит с индексом  $i \% N$ . В нашем случае это означает, что для символа с индексом **i** в исходной строке, мы из массива ассоциативных массивов (из п.4) возьмем ассоциативный массив с индексом  $i \% N$  и с его помощью уже получим исходный символ.

6. Получаем раскодированный текст.

7. Сравниваем исходный текст с закодированным текстом - они должны не совпадать.

8. Сравниваем исходный текст с раскодированным текстом - они должны совпадать.

## Тексты программы:

В качестве языка программирования я использую C#. Исходный текст программы приведен в отдельном файле Program.cs (без дополнительных файлов проекта - \*.csproj и решения - \*.sln).

## Результаты работы программы:

### Метод подстановки:

Исходный текст:

EVERY COMPLEX PROBLEM HAS A SOLUTION THAT IS CLEAR, SIMPLE, AND WRONG.

Закодированный текст:

YVYPBD.-RNQYADNP-  
QYRDSZLDZDL-QUMT-?DMSZMDTLD.QYZPFDLTRNQYFDZ?XDWP-?IE

Раскодированный текст:

EVERY COMPLEX PROBLEM HAS A SOLUTION THAT IS CLEAR, SIMPLE, AND WRONG.

### Метод перестановки:

Исходный текст:

<<(((EVERY COMPLEX PROBLEM HAS A SOLUTION THAT IS CLEAR, SIMPLE, AND WRONG.)))))>>

Закодированный текст:

{{<{(EYV ERMLOECPPPO BXRMHEAL AS OS TOUNLIHTT A LSEIC,SRIA L,P MEDWNRA G}N}O.> ) }>

Раскодированный текст:

<<(((EVERY COMPLEX PROBLEM HAS A SOLUTION THAT IS CLEAR, SIMPLE, AND WRONG.)))))>>

### Метод многоалфавитного шифра:

Исходный текст:

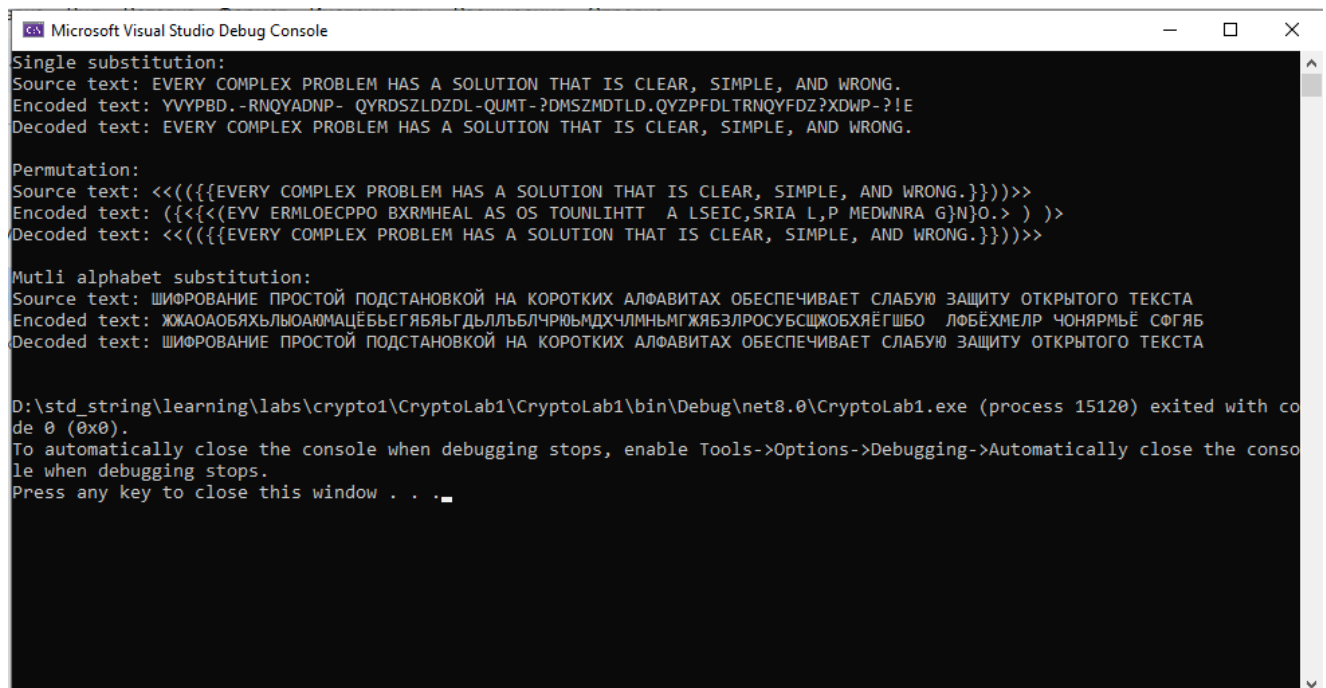
ШИФРОВАНИЕ ПРОСТОЙ ПОДСТАНОВКОЙ НА КОРОТКИХ АЛФАВИТАХ ОБЕСПЕЧИВАЕТ СЛАБУЮ ЗАЩИТУ ОТКРЫТОГО ТЕКСТА

Закодированный текст:

ЖЖАОАОБЯХЬЛЫОАЮМАЦЁБЬЕГЯБЯЬГДЬЛЛЬБЛЧРЮЬМДХЧЛМНЬМГЖЯБЗЛПРОСУ БСЩЖОБХЯЁГШБО ЛФБЁХМЕЛР ЧОНЯРМЬЁ СФГЯБ

Раскодированный текст:

ШИФРОВАНИЕ ПРОСТОЙ ПОДСТАНОВКОЙ НА КОРОТКИХ АЛФАВИТАХ ОБЕСПЕЧИВАЕТ СЛАБУЮ ЗАЩИТУ ОТКРЫТОГО ТЕКСТА



```
Microsoft Visual Studio Debug Console

Single substitution:
Source text: EVERY COMPLEX PROBLEM HAS A SOLUTION THAT IS CLEAR, SIMPLE, AND WRONG.
Encoded text: YVYPBD.-RNQYADNP- QYRDSZLDZDL-QUMT-?DMSZMDTLD.QYZPFDLTRNQYFDZ?XOWP-?!E
Decoded text: EVERY COMPLEX PROBLEM HAS A SOLUTION THAT IS CLEAR, SIMPLE, AND WRONG.

Permutation:
Source text: <<(((EVERY COMPLEX PROBLEM HAS A SOLUTION THAT IS CLEAR, SIMPLE, AND WRONG.)))))>>
Encoded text: {{<{(EYV ERMLOECPPPO BXRMHEAL AS OS TOUNLIHTT A LSEIC,SRIA L,P MEDWNRA G}N}O.> ) }>
Decoded text: <<(((EVERY COMPLEX PROBLEM HAS A SOLUTION THAT IS CLEAR, SIMPLE, AND WRONG.)))))>>

Multi alphabet substitution:
Source text: ШИФРОВАНИЕ ПРОСТОЙ ПОДСТАНОВКОЙ НА КОРОТКИХ АЛФАВИТАХ ОБЕСПЕЧИВАЕТ СЛАБУЮ ЗАЩИТУ ОТКРЫТОГО ТЕКСТА
Encoded text: ЖЖАОАОБЯХЬЛЫОАЮМАЦЁБЬЕГЯБЯЬГДЬЛЛЬБЛЧРЮЬМДХЧЛМНЬМГЖЯБЗЛПРОСУБСЩЖОБХЯЁГШБО ЛФБЁХМЕЛР ЧОНЯРМЬЁ СФГЯБ
Decoded text: ШИФРОВАНИЕ ПРОСТОЙ ПОДСТАНОВКОЙ НА КОРОТКИХ АЛФАВИТАХ ОБЕСПЕЧИВАЕТ СЛАБУЮ ЗАЩИТУ ОТКРЫТОГО ТЕКСТА

D:\std_string\learning\labs\crypto1\CryptoLab1\CryptoLab1\bin\Debug\net8.0\CryptoLab1.exe (process 15120) exited with code 0 (0x0).
To automatically close the console when debugging stops, enable Tools->Options->Debugging->Automatically close the console when debugging stops.
Press any key to close this window . . .
```

### Анализ результатов:

1. Все три метода позволяют быстро и просто (см. исходный текст программы) зашифровать текст и расшифровать его. При этом (при правильной реализации), если мы зашифруем некоторый текст, а потом расшифруем его, то мы получим исходный текст; т.е. при шифровании и последующей расшифровке информация не теряется.

2. Наиболее удобен с точки зрения реализации метод перестановки, т.к. при его реализации не нужно знание алфавита исходного текста - достаточно знать индексы до перестановки и после в группе. Для остальных методов (метода подстановки и метода многоалфавитного шифра) необходимо знать исходный алфавит и подстановочный алфавит/алфавиты; при этом, если в исходном тексте попадет символ, которого нет в исходном алфавите, то поведение метода шифрования/расшифровки не определено (т.е. зависит от реализации). Т.е. метод подстановки, в отличие от других методов, не чувствителен к используемому алфавиту.

3. Все три метода позволяют расшифровать исходный текст по шифрограмме с помощью метода частотного анализа. Наиболее просто это можно продемонстрировать для метода подстановок: так, например, буква Е появляется в исходном тексте 6 раз, она заменяется на букву У, которая появляется в зашифрованном тексте тоже 6 раз и т.д.

### **Выводы:**

Мы изучили простые методы для шифрования и расшифровки текста: метод подстановки, метод перестановки и метод многоалфавитного шифра и реализовали все эти три метода. С помощью нашей реализации мы показали, что эти методы позволяют зашифровать некоторый текст, после чего его расшифровать и получить в итоге тот же самый исходный текст (при соблюдении некоторых условий, например, правильного задания алфавитов).

### **Контрольные вопросы:**

1. Почему метод подстановки имеет слабую надежность? Шифрование простой подстановкой на коротких алфавитах обеспечивает слабую защиту открытого текста. Подстановочные криптограммы можно раскрыть, составляя частотные таблицы для букв, пар букв (биграмм) и троек букв (триграмм). Большие частоты появления одних букв и малые других, а также частые ассоциации гласных с согласными позволяют найти буквы открытого текста. С увеличением размера алфавита применение частотного анализа становится все более дорогим, однако, принцип подстановки теряет свою практическую значимость.

2. Что такое частотный анализ? Частотный анализ — один из методов криптоанализа, основывающийся на предположении о существовании нетривиального статистического распределения отдельных символов и их последовательностей, как в открытом тексте, так и в шифротексте, которое, с точностью до замены символов, будет сохраняться в процессе шифрования и дешифрования. Проще говоря, частотный анализ предполагает, что частотность появления заданной буквы алфавита в достаточно длинных текстах одна и та же для разных текстов одного языка. При этом, в случае моноалфавитного шифрования, если в шифротексте будет символ с аналогичной вероятностью появления, то можно предположить, что он и является указанной зашифрованной буквой. Аналогичные рассуждения применяются к биграммам (двубуквенным последовательностям), триграммам и т. д. в случае полиалфавитных шифров. Хорошим примером применения частотного анализа является рассказ Артура Конана Дойля “Пляшущие человечки”.

3. Что является криптографическим ключом в методе перестановки? Криптографическим криптографическим ключом в методе перестановки является группа перестановки - т.е. пары исходный индекс символа в группе - индекс символа в группе после перестановки (индексы в группе перестановки начинаются с 1).
4. Как связаны метод подстановки и многоалфавитные шифры? Метод подстановки является предельным случаем метода многоалфавитного шифра, когда количество используемых алфавитов в многоалфавитном шифре равно 1.
5. В чем отличие криптографии от криптоанализа? Криптография — наука о методах обеспечения конфиденциальности, целостности данных, аутентификации, шифрования. Криптоанализ — наука о методах дешифровки зашифрованной информации без предназначенного для этого ключа, а также сам процесс такой дешифровки. Получается, что криптография - это наука о использовании криптосредств штатными способами, а криптоанализ - это попытка обойти штатные способы обработки информации (например, за счет использования частотного анализа).
6. По какому признаку шифры делят на симметричные и асимметричные? Симметричные шифры — это способ шифрования, в котором для шифрования и расшифрования применяется один и тот же криптографический ключ. Асимметричный шифр — это система шифрования и/или электронной подписи (ЭП), при которой открытый ключ передаётся по открытому (то есть незащищенному, доступному для наблюдения) каналу и используется для проверки ЭП и для шифрования сообщения. Для генерации ЭП и для расшифровки сообщения используется закрытый ключ.