2 ШИФРОВАНИЕ И РАСШИФРОВКА ИНФОРМАЦИИ МЕТОДОМ ДВОЙНОЙ ПЕРЕСТАНОВКИ ПО КЛЮЧУ

2.1 Описание алгоритма шифрования методом двойной перестановки по ключу

Двойной сортировкой называется метод сортировки, при котором в шифрующей таблице изменяется порядок следования столбцов и строк. Для выполнения такого шифрования обеим сторонам необходимо обменяться размерностью таблицы шифрования, а также двумя ключами для перестановки столбцов и строк.

Алгоритм шифрования методом двойной перестановки по ключу:

Шаг 1. Взять шифрующую таблицу любой размерности (в данном случае размерность может быть открытой информацией).

Шаг 2. Буквы открытого текста заносятся в таблицу по столбцам сверху вниз, слева направо.

Шаг 3. Каждый столбец нумеруется в соответствии со значением первого ключа.

Шаг 4. Каждая строка нумеруется в соответствии со значением второго ключа.

Шаг 5. Столбцы таблицы сортируются в соответствии с порядковым номером.

Шаг 6. Строки таблицы сортируются в соответствии с порядковым номером.

Шаг 7. Из таблицы считываются буквы по строкам слева направо, сверху-вниз и формируется шифртекст.

Алгоритм расшифровки сообщения, зашифрованного методом двойной перестановки по ключу:

Шаг 1. Взять шифрующую таблицу некоторой размерности (может быть открытым значением).

Шаг 2. Буквы шифртекста заносятся в таблицу по строкам слева направо, сверху-вниз.

Шаг 3. В соответствии со значением элементов ключа выполняется перестановка строк между собой по следующему правилу: i-я строка таблицы переходит на позицию, которую имеет элемент второго ключа со значением i.

Шаг 4. В соответствии со значением элементов ключа выполняется перестановка столбцов между собой по следующему правилу: i-й столбец таблицы переходит на позицию, которую имеет элемент первого ключа со значением i.

Шаг 5. Из таблицы считываются буквы по столбцам сверху вниз, слева направо и формируется открытый текст.

Число вариантов двойной перестановки быстро возрастает при увеличении размера таблицы:

- для таблицы 3x3 - 36 вариантов;
- для таблицы 4x4 - 576 вариантов;
- для таблицы 5x5 - 14400 вариантов.

2.2 Шифрование и расшифровка методом двойной перестановки по ключу

Исходное сообщение для шифрования:

ФИЛИППОВ ОЛЕГ АНАТОЛЬЕВИЧ

Пусть размерность таблицы составляет 5*5. Ключи: по высоте – 31254, по ширине – 51342.

Заполним таблицу шифрования исходным сообщением (по столбцам сверху вниз, слева направо):

Ф	П	Л	Н	Ь	**3**
И	О	Е	А	Е	**1**
Л	В	Г	Т	В	**2**
И	—	—	О	И	**5**
П	О	А	Л	Ч	**4**
5	**1**	**3**	**4**	**2**	

Отсортируем столбцы таблицы в соответствии с ключом:

П	Ь	Л	Н	Ф	**3**
О	Е	Е	А	И	**1**
В	В	Г	Т	Л	**2**
—	И	—	О	И	**5**
О	Ч	А	Л	П	**4**
1	**2**	**3**	**4**	**5**	

Отсортируем строки таблицы в соответствии с ключом:

О	Е	Е	А	И	**1**
В	В	Г	Т	Л	**2**
П	Ь	Л	Н	Ф	**3**
О	Ч	А	Л	П	**4**
—	И	—	О	И	**5**
1	**2**	**3**	**4**	**5**	

Считаем с таблицы шифртекст по строкам слева направо, сверху вниз:

ОЕЕАИВВГТЛПЬЛНФОЧАЛП—И—ОИ

Для расшифровки этого сообщения, все операции необходимо выполнить в обратном порядке в соответствии с алгоритмом, приведенным в разделе 2.1.

3 ПРОГРАММНАЯ РЕАЛИЗАЦИЯ ШИФРОВАНИЯ МЕТОДОМ ДВОЙНОЙ ПЕРЕСТАНОВКИ ПО КЛЮЧУ С ВОЗМОЖНОСТЬЮ ВНЕДРЕНИЯ ЦИФРОВОЙ ПОДПИСИ

В соответствии с алгоритмом, описанным в разделе 2.1 для шифрования сообщений методом двойной перестановки по ключу, разработано программное обеспечение DigSign, позволяющее зашифровать и расшифровать исходное сообщение в соответствии с вышеупомянутым алгоритмом. Кроме этого, программное средство предоставляет возможность внедрения электронной цифровой подписи в сообщение, а также проверку сообщения и подписи на предмет вторжения и внедрения сторонней информации.

Запуск приложения осуществляется из консоли.

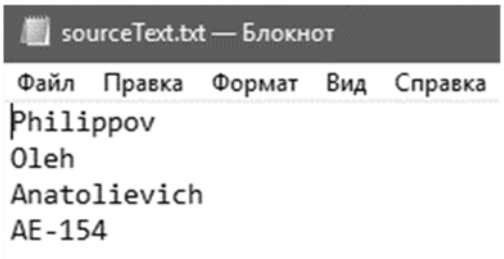
Список доступных параметров программного средства при запуске из командной строки:

1. Полный путь к исходному файлу (E:\crypto\source_file.txt)
2. Операция, которую необходимо выполнить:
   - -enc — шифрование исходного файла;
   - -dec — расшифровка зашифрованного файла;
   - -sign — создание цифровой для файла;
   - -verify — проверка цифровой подписи файла.
3. Полный путь к приватному ключу (или модификатор –n, позволяющий создать новую пару публичный/приватный ключ, а затем зашифровать сообщение полученным приватный ключом) (для операции –sign), публичный ключ (для операции –verify), ключ по высоте (для операций –enc/-dec в формате 1,2,3,4,5).

4. Полный путь к файлу с цифровой подписью (для операции –verify), ключ по высоте (для операций –enc/-dec в формате 1,2,3,4,5).

Пример использования приложения DigSign:

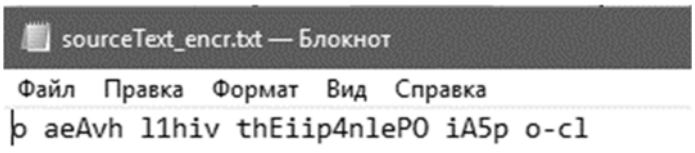
Данные для шифрования:



Зашифруем исходное сообщение:

```
C:\Users\club->E:\DigSign.exe E:\crypto\sourceFile.txt -enc 3,0,2,5,1,4 6,0,3,2,5,4,1
The file is successfully encrypted at path: E:\crypto\sourceFile_encr.txt
```

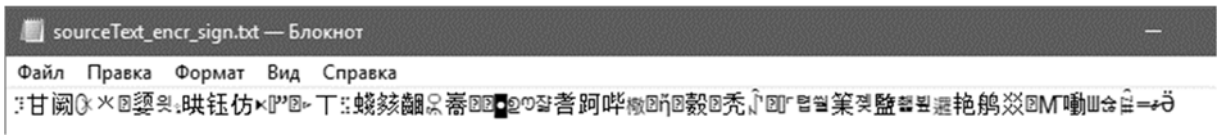
Содержимое файла после выполнения шифрования:



Подпишем зашифрованный файл с помощью нового сгенерированного приватного ключа:

```
C:\Users\club->E:\DigSign.exe E:\crypto\sourceText_encr.txt -sign -n
The e-Signature is successfully created at the path: E:\crypto\sourceText_encr_sign.txt
```

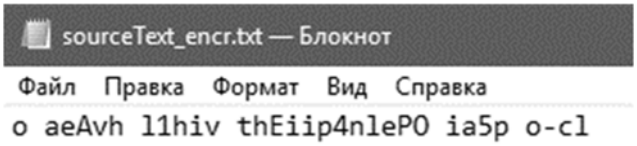
Содержимое файла с подписью:



Проверим эту цифровую подпись:

```
C:\Users\club->E:\DigSign.exe E:\crypto\sourceText_encr.txt -verify E:\crypto\publicKey.xml
E:\crypto\sourceText_encr_sign.txt
The e-Signature is valid
```

Внесем правки в зашифрованный файл:



Проверим цифровую подпись повторно:

```
C:\Users\club->E:\DigSign.exe E:\crypto\sourceText_encr.txt -verify E:\crypto\publicKey.xml
E:\crypto\sourceText_encr_sign.txt
The e-Signature is invailid!
```

Расшифруем зашифрованный файл:

```
C:\Users\club->E:\DigSign.exe E:\crypto\sourceText_encr.txt -dec 3,0,2,5,1,4 6,0,3,2,5,4,1
The file is successfully decrypted at path: E:\crypto\sourceText_encr_decr.txt
```

Содержимое файла после расшифровки: