**Лабораторная работа № 5**

**Исследование симметричных криптоалгоритмов**

**1 Цель**: Познакомиться с различными симметричными алгоритмами шифрования.

**2 Порядок выполнения работы:**

2.1 Выбрать язык программирования.

2.2 Изучить материал.

2.3 Выполнить задания.

2.4 Ответьте на контрольные вопросы.

2.4.3 Опишите метод двойной перестановки.

2.4.4 Отличия трех методов шифрования в квадрате Полибия.

2.5 Оформить отчет.

**Теоретические сведенья**

**Шифрующие таблицы**

С начала эпохи Возрождения (конец XIV столетия) начала возрождаться и криптография. Наряду с традиционными применениями криптографии в политике, дипломатии и военном деле появляются и другие задачи - защита интеллектуальной собственности от преследований инквизиции или заимствований злоумышленников. В разработанных шифрах перестановки того времени применяются шифрующие таблицы, которые в сущности задают правила перестановки букв в сообщении.

В качестве ключа в шифрующих таблицах используются:

• размер таблицы;

• слово или фраза, задающие перестановку;

• особенности структуры таблицы.

Одним из самых примитивных табличных шифров перестановки является простая перестановка, для которой ключом служит размер таблицы. Этот метод шифрования сходен с шифром *скитала*. Например, сообщение

ТЕРМИНАТОР ПРИБЫВАЕТ СЕДЬМОГО В ПОЛНОЧЬ

записывается в таблицу поочередно по столбцам. Результат заполнения таблицы из 5 строк и 7 столбцов показан на рисунке 2.

После заполнения таблицы текстом сообщения по столбцам для формирования шифртекста считывают содержимое таблицы по строкам.

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| Т | Н | П | В | Е | Г | Л |
| Е | А | Р | А | Д | О | Н |
| Р | Т | И | Е | Ь | В | О |
| М | О | Б | Т | М | П | Ч |
| И | Р | Ы | С | О | О | Ь |

Рисунок 2 Заполнение таблицы из 5 строк и 7 столбцов

Если шифртекст записывать группами по пять букв, получается такое шифрованное сообщение:

ТНПВЕ ГЛЕАР АДОНР ТИЕЬВ ОМОБТ МПЧИР ЫСООЬ

Естественно, отправитель и получатель сообщения должны заранее условиться об общем ключе в виде размера таблицы. Следует заметить, что объединение букв шифртекста в 5-буквенные группы не входит в ключ шифра и осуществляется для удобства записи несмыслового текста. При расшифровании действия выполняют в обратном порядке.

Несколько большей стойкостью к раскрытию обладает метод шифрования, называемый одиночной перестановкой по ключу. Этот метод отличается от предыдущего тем, что столбцы таблицы переставляются по ключевому слову, фразе или набору чисел длиной в строку таблицы.

Применим в качестве ключа, например, слово

ПЕЛИКАН,

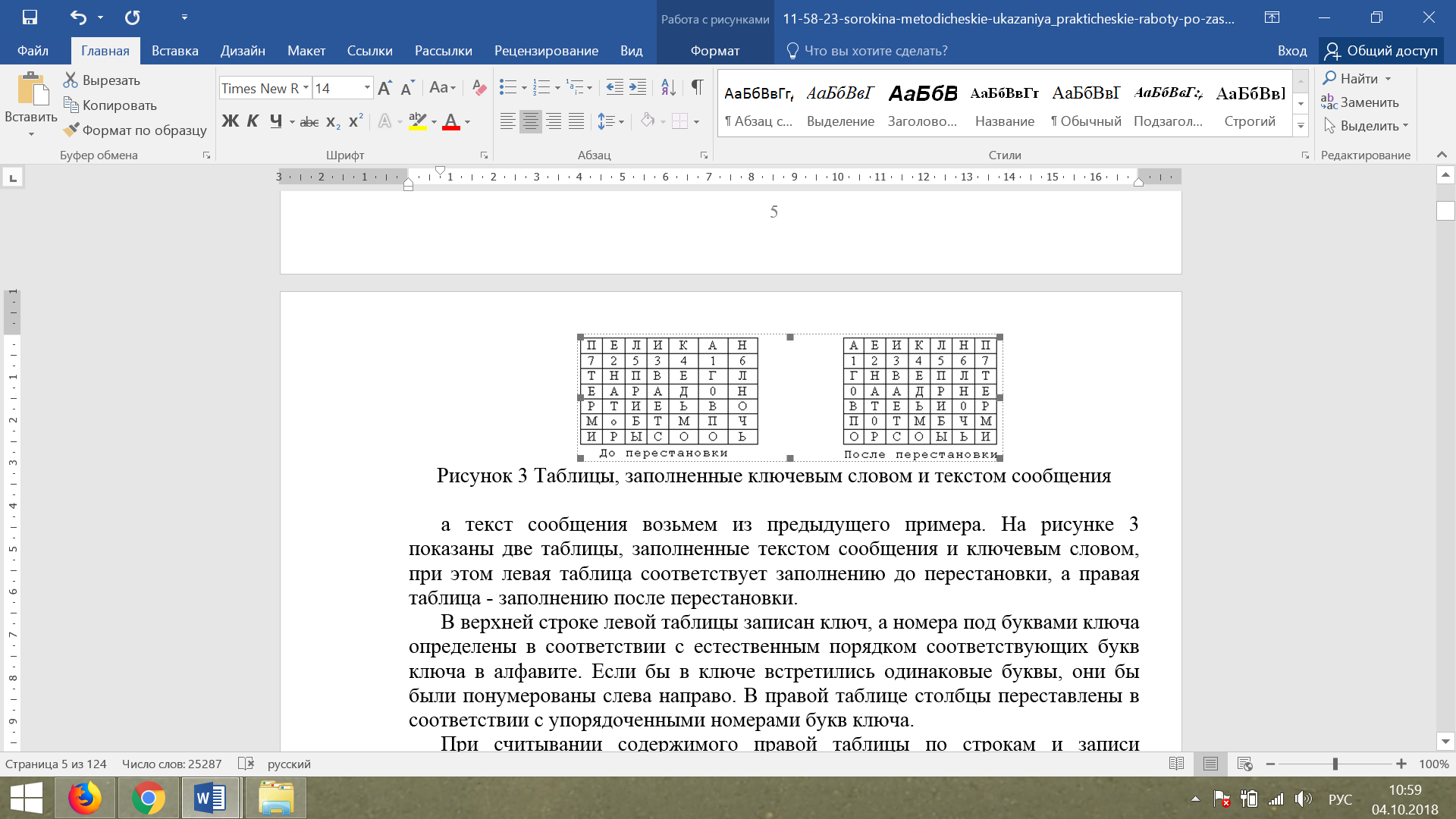


Рисунок 3 Таблицы, заполненные ключевым словом и текстом сообщения

а текст сообщения возьмем из предыдущего примера. На рисунке 3 показаны две таблицы, заполненные текстом сообщения и ключевым словом, при этом левая таблица соответствует заполнению до перестановки, а правая таблица - заполнению после перестановки.

В верхней строке левой таблицы записан ключ, а номера под буквами ключа определены в соответствии с естественным порядком соответствующих букв ключа в алфавите. Если бы в ключе встретились одинаковые буквы, они бы были понумерованы слева направо. В правой таблице столбцы переставлены в соответствии с упорядоченными номерами букв ключа.

При считывании содержимого правой таблицы по строкам и записи шифртекста группами по пять букв получим шифрованное сообщение:

ГНВЕП ЛТООА ДРНЕВ ТЕЬИО РПОТМ БЧМОР СОЫЬИ

Для обеспечения дополнительной скрытности можно повторно зашифровать сообщение, которое уже прошло шифрование. Такой метод шифрования называется *двойной перестановкой*. В случае двойной перестановки столбцов и строк таблицы перестановки определяются отдельно для столбцов и отдельно для строк. Сначала в таблицу записывается текст сообщения, а потом поочередно переставляются столбцы, а затем строки. При расшифровании порядок перестановок должен быть обратным.

Пример выполнения шифрования методом двойной перестановки показан на рисунке 4. Если считывать шифртекст из правой таблицы построчно блоками по четыре буквы, то получится следующее:

ТЮАЕ ООГМ РЛИП ОЬСВ

Ключом к шифру двойной перестановки служит последовательность номеров столбцов и номеров строк исходной таблицы (в нашем примере последовательности 4132 и 3142 соответственно).

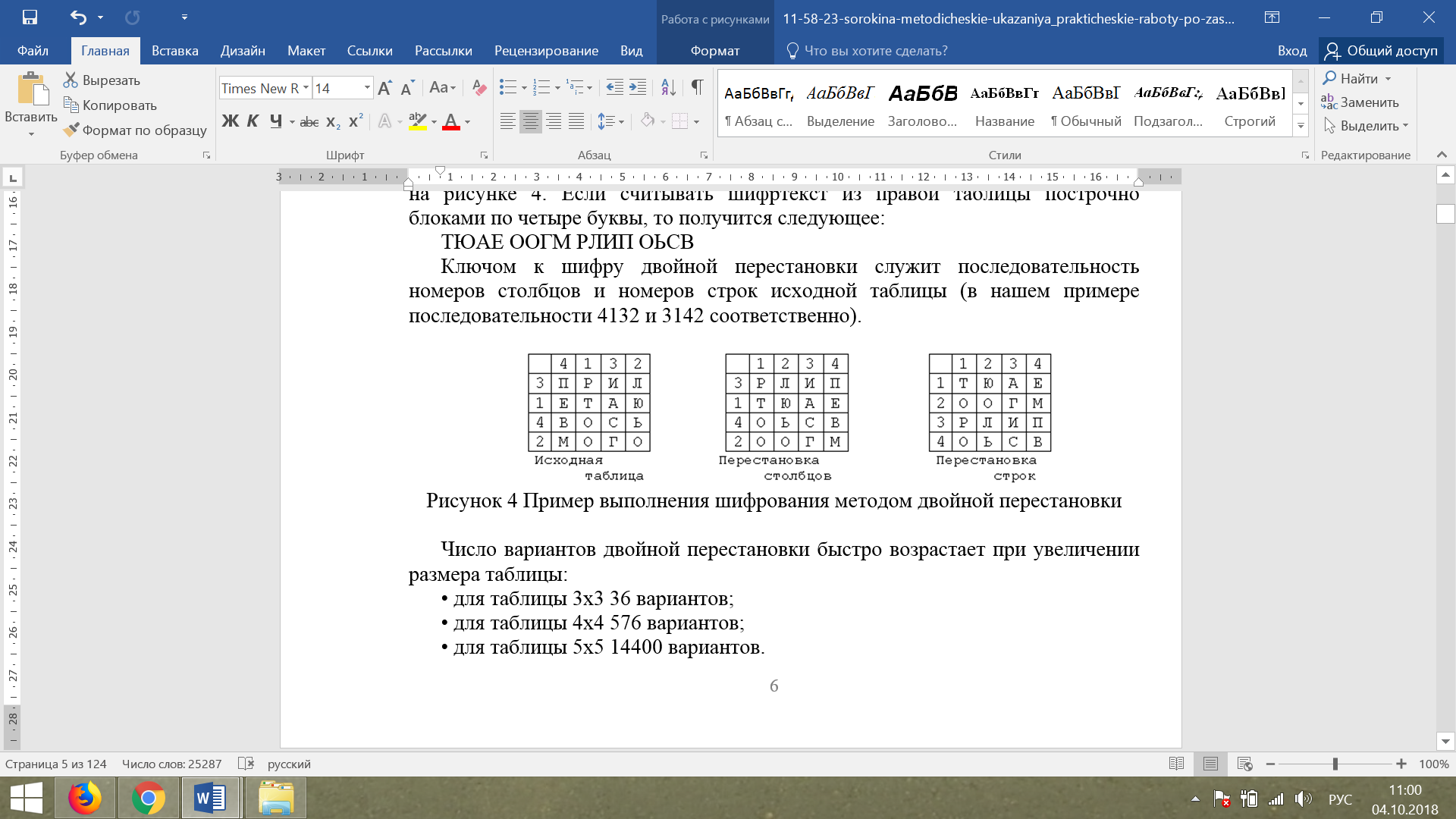


Рисунок 4 Пример выполнения шифрования методом двойной перестановки

Число вариантов двойной перестановки быстро возрастает при увеличении размера таблицы:

• для таблицы 3х3 36 вариантов;

• для таблицы 4х4 576 вариантов;

• для таблицы 5х5 14400 вариантов.

Однако двойная перестановка не отличается высокой стойкостью и сравнительно просто «взламывается» при любом размере таблицы шифрования.

# **Квадрат Полибия**

### ***Шаг 1: Формирование таблицы шифрования***

К каждому языку отдельно составляется таблица шифрования с одинаковым (не обязательно) количеством пронумерованных строк и столбцов, параметры которой зависят от его мощности (количества букв в алфавите). Берутся два целых числа, произведение которых ближе всего к количеству букв в языке — получаем нужное число строк и столбцов. Затем вписываем в таблицу все буквы алфавита подряд — по одной на каждую клетку. При нехватке клеток можно вписать в одну две буквы (редко употребляющиеся или схожие по употреблению).

#### Латинский алфавит

В современном латинском алфавите 26 букв, следовательно таблица должна состоять из 5 строк и 5 столбцов, так как 25=5\*5 наиболее близкое к 26 число. При этом буквы I, J не различаются (J отождествляется с буквой I), так как не хватает 1 ячейки:

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
|  | **1** | **2** | **3** | **4** | **5** |
| 1 | A | B | C | D | E |
| 2 | F | G | H | I/J | K |
| 3 | L | M | N | O | P |
| 4 | Q | R | S | T | U |
| 5 | V | W | X | Y | Z |

#### Русский алфавит

Идею формирования таблицы шифрования проиллюстрируем для русского языка. Число букв в русском алфавите отличается от числа букв в греческом алфавите, поэтому размер таблицы выбран другой (квадрат 6\*6=36, поскольку 36 наиболее близкое число к 33):

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
|  | **1** | **2** | **3** | **4** | **5** | **6** |
| 1 | А | Б | В | Г | Д | Е |
| 2 | Ё | Ж | З | И | Й | К |
| 3 | Л | М | Н | О | П | Р |
| 4 | С | Т | У | Ф | Х | Ц |
| 5 | Ч | Ш | Щ | Ъ | Ы | Ь |
| 6 | Э | Ю | Я | — | — | — |

Возможен также другой вариант составления, предусматривающий объединение букв Е и Ё, И и Й, Ъ и Ь. В данном случае получаем следующий результат:

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
|  | **1** | **2** | **3** | **4** | **5** | **6** |
| 1 | А | Б | В | Г | Д | Е/Ё |
| 2 | Ж | З | И/Й | К | Л | М |
| 3 | Н | О | П | Р | С | Т |
| 4 | У | Ф | Х | Ц | Ч | Ш |
| 5 | Щ | Ы | Ь/Ъ | Э | Ю | Я |

Используя подобный алгоритм, таблицу шифрования можно задать для любого языка. Чтобы расшифровать закрытый текст необходимо знать, таблицей шифрования какого алфавита он зашифрован.

Или есть такой вариант: Шифр «Квадрат Полибия».

«Квадрат Полибия» представляет собой квадрат 5×5, столбцы и строки которого нумеруются цифрами от 1 до 5. В каждую клетку этого квадрата записывается одна буква (в нашем алфавите 31 буква, Ъ и Ё исключены, кроме того в одну клетку поместите буквы е-э, и-й, ж-з, р-с, ф-х, ш-щ). Буквы расположены в алфавитном порядке. В результате каждой букве соответствует пара чисел, и шифрованное сообщение превращается в последовательность пар чисел. Расшифровывается путем нахождения буквы, стоящей на пересечении строки и столбца.

1 2 3 4 5

1 А Б В Г Д

2 Е/Э Ж З И/Й К

3 Л М Н О П

4 Р/С Т У Ф/Х Ц

5 Ч Ш/Щ Ы Ю Я

### ***Шаг 2: Принцип шифрования***

Существует несколько методов шифрования с помощью квадрата Полибия. Ниже приведены три из них.

#### Метод 1

Сообщение преобразуется в координаты по квадрату Полибия, координаты записываются вертикально:

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Таблица координат | | | | | | | | |
| **Буква:** | **S** | **O** | **M** | **E** | **T** | **E** | **X** | **T** |
| **Координата горизонтальная:** | **3** | **4** | **2** | **5** | **4** | **5** | **3** | **4** |
| **Координата вертикальная:** | **4** | **3** | **3** | **1** | **4** | **1** | **5** | **4** |

Затем координаты считывают по строкам:

34 25 45 34 43 31 41 54 (\*)

Далее координаты преобразуются в буквы по этому же квадрату:

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Таблица координат | | | | | | | | |
| **Координата горизонтальная:** | **3** | **2** | **4** | **3** | **4** | **3** | **4** | **5** |
| **Координата вертикальная:** | **4** | **5** | **5** | **4** | **3** | **1** | **1** | **4** |
| **Буква:** | **S** | **W** | **Y** | **S** | **O** | **C** | **D** | **U** |

Таким образом после шифрования получаем:

|  |  |
| --- | --- |
| Результат | |
| **До шифрования:** | **SOMETEXT** |
| **После шифрования:** | **SWYSOCDU** |

#### Метод 2

Усложненный вариант, который заключается в следующем: полученный первичный шифротекст (\*) шифруется вторично. При этом он выписывается без разбиения на пары:

3425453443314154

Полученная последовательность цифр сдвигается циклически влево на один шаг(нечетное количество шагов):

4254534433141543

Эта последовательность вновь разбивается в группы по два:

42 54 53 44 33 14 15 43

и по таблице заменяется на окончательный шифротекст:

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Таблица координат | | | | | | | | |
| **Координата горизонтальная:** | **4** | **5** | **5** | **4** | **3** | **1** | **1** | **4** |
| **Координата вертикальная:** | **2** | **4** | **3** | **4** | **3** | **4** | **5** | **3** |
| **Буква:** | **I** | **U** | **P** | **T** | **N** | **Q** | **V** | **O** |

Таким образом после шифрования получаем:

|  |  |
| --- | --- |
| Результат | |
| **До шифрования:** | **SOMETEXT** |
| **После шифрования:** | **IUPTNQVO** |

## *Метод 3*

## Добавление ключа

На первый взгляд шифр кажется очень нестойким, но для его реальной оценки следует учитывать два фактора:

1. *возможность заполнить квадрат Полибия буквами произвольно, а не только строго по алфавиту;*
2. *возможность периодически заменять квадраты.*

Тогда анализ предыдущих сообщений ничего не дает, так как к моменту раскрытия шифра он может быть заменен.

Буквы могут вписываться в таблицу в произвольном порядке — заполнение таблицы в этом случае и является ключом. Для латинского алфавита в первую клетку можно вписать одну из 25 букв, во вторую — одну из 24, в третью — одну из 23 и т. д. Получаем максимальное количество ключей для шифра на таблице латинского алфавита:

N = 25*24*23*...*2*1 = 25!

Соответственно для дешифрования сообщения потребуется не только знание алфавита, но и ключа, с помощью которого составлялась таблица шифрования. Но произвольный порядок букв тяжело запомнить, поэтому пользователю шифра необходимо постоянно иметь при себе ключ — квадрат. Появляется опасность тайного ознакомления с ключом посторонних лиц. В качестве компромиссного решения был предложен ключ — пароль. Пароль выписывается без повторов букв в квадрат; в оставшиеся клетки в алфавитном порядке выписываются буквы алфавита, отсутствующие в пароле.

### Пример

Зашифруем слово «SOMETEXT», используя ключ «DRAFT». Составим предварительно таблицу шифрования с данным ключом, записывая символы ключа по порядку в таблицу, после них остальной алфавит:

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
|  | **1** | **2** | **3** | **4** | **5** |
| 1 | D | R | A | F | T |
| 2 | B | C | E | G | H |
| 3 | I | K | L | M | N |
| 4 | O | P | Q | S | U |
| 5 | V | W | X | Y | Z |

Преобразуем сообщение в координаты по квадрату Полибия:

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Таблица координат | | | | | | | | |
| **Буква:** | **S** | **O** | **M** | **E** | **T** | **E** | **X** | **T** |
| **Координата горизонтальная:** | **4** | **1** | **4** | **3** | **5** | **3** | **3** | **5** |
| **Координата вертикальная:** | **4** | **4** | **3** | **2** | **1** | **2** | **5** | **1** |

Считаем координаты по строкам:

41 43 53 35 44 32 12 51

Преобразуем координаты в буквы по этому же квадрату

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Таблица координат | | | | | | | | |
| **Координата горизонтальная:** | **4** | **4** | **5** | **3** | **4** | **3** | **1** | **5** |
| **Координата вертикальная:** | **1** | **3** | **3** | **5** | **4** | **2** | **2** | **1** |
| **Буква:** | **F** | **M** | **N** | **X** | **S** | **E** | **B** | **T** |

Таким образом после шифрования получаем:

|  |  |
| --- | --- |
| Результат | |
| **До шифрования:** | **SOMETEXT** |
| **После шифрования:** | **FMNXSEBT** |

**Задание №1**

Зашифровать методом двойной перестановки индивидуальную фразу. Попытаться выбрать максимально криптостойкую таблицу.

**Задание №2**

Зашифровать квадратом Полибия индивидуальную фразу **тремя** способами.