# Практическая работа №5. Тема: Шифрование данных.

**Цель работы:** знакомство с простейшими приемами шифрования текстовой информации.

# Теоретические сведения

Дипломатические, военные и промышленные секреты обычно передаются или хранятся не в исходном виде, а после шифрования. В отличие от тайнописи, которая прячет сам факт наличия сообщения, шифровки передаются открыто, а прячется сам смысл. Итак, криптография обеспечивает сокрытие смысла сообщения с помощью шифрования и открытие его расшифровкой, которые выполняются по специальным криптографическим алгоритмам с помощью ключей у отправителя и получателя.

# Шифр Цезаря

Шифр Цезаря — один из древнейших шифров. При шифровании каждый символ заменяется другим, отстоящим от него в алфавите на фиксированное число позиций. Шифр Цезаря можно классифицировать как шифр подстановки, при более узкой классификации — шифр простой замены.

Шифр назван в честь римского императора Гая Юлия Цезаря, использовавшего его для секретной переписки. Естественным развитием шифра Цезаря стал шифр Виженера. С точки зрения современного криптоанализа, шифр Цезаря не имеет приемлемой стойкости.

Суть шифра состоит в замене каждой буквы на букву, отстоящую от нее в алфавите на 3 позиции вправо (возможен выбор любого ключа). Подобные шифры, основанные на замене одних букв другими, называются подстановочными. Моноалфавитные шифры (к которым относится и шифр Цезаря) – это разновидность подстановочных шифров, в которой каждой букве нешифрованного текста всегда соответствует одна и та же буква в шифрованном тексте.

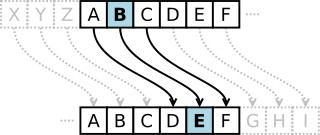


Рисунок 1 Шифр Цезаря

Алфавит:

|  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **Буква** | **А** | **Б** | **В** | **Г** | **Д** | **Е** | **Ё** | **Ж** | **З** | **И** | **Й** |
| Номер | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 |
| **Буква** | **К** | **Л** | **М** | **Н** | **О** | **П** | **Р** | **С** | **Т** | **У** | **Ф** |
| Номер | 12 | 13 | 14 | 15 | 16 | 17 | 18 | 19 | 20 | 21 | 22 |
| **Буква** | **Х** | **Ц** | **Ч** | **Ш** | **Щ** | **Ь** | **Ы** | **Ъ** | **Э** | **Ю** | **Я** |
| Номер | 23 | 24 | 25 | 26 | 27 | 28 | 29 | 30 | 31 | 32 | 33 |

# Пример:

Необходимо зашифровать сообщение по методу Цезаря.

Исходное сообщение: «Криптография» Ключ: 3

Решение:

|  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Сообщение | **К** | **Р** | **И** | **П** | **Т** | **О** | **Г** | **Р** | **А** | **Ф** | **И** | **Я** |
| Номер 1 | 12 | 18 | 10 | 17 | 20 | 16 | 4 | 18 | 1 | 22 | 10 | 33 |
| Номер 1 + 3 | 15 | 21 | 13 | 20 | 23 | 19 | 7 | 21 | 4 | 25 | 13 | 3 |
| Шифр | **Н** | **У** | **Л** | **Т** | **Х** | **С** | **Ё** | **У** | **Г** | **Ч** | **Л** | **В** |

***Номер 1*** – номер буквы согласно табл.

***Номер 1+3*** – номер буквы согласно табл. + ключ (перемещаем букву на 3 позиции вперед) Ответ: «Нултхсёугчлв»

Достоинством системы шифрования Цезаря является простота шифрования и расшифрования. К недостаткам системы Цезаря следует отнести следующие:

* подстановки, выполняемые в соответствии с системой Цезаря, не маскируют частот появления различных букв исходного открытого текста;
* сохраняется алфавитный порядок в последовательности заменяющих букв;
* шифр Цезаря легко вскрывается на основе анализа частот появления букв в шифртексте. Однако, концепция, заложенная в систему шифрования Цезаря, оказалась весьма плодотворной, о чем свидетельствуют ее многочисленные модификации.

## *Шифр Гронсфельда*

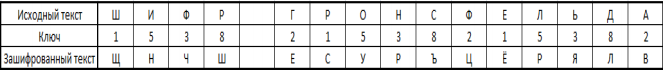
Для шифрования здесь используется числовой ключ. Но каждая буква смещается не на постоянное число позиций, а на то число, которое соответствует ключу. Ключ соответственно состоит не из одной цифры, а из группы цифр.

Ключ не обязательно должен быть таким же длинным как шифруемое сообщение. Если ключ короче сообщения, то его просто повторяют по циклу. Так, например, если в тексте 10 символов, а длина ключа 5 символов, то для шифрования ключ будет использоваться 2 раза.

Пример:

Исходный текст: «шифр гронсфельда» Ключ 15382

Зашифрованный текст: «щнчш есуръцёрялв»



# Шифр Атбаш

Еще один шифр простой (моноалфавитной) замены.

Шифрование осуществляется путем замены первой буквы алфавита на последнюю, второй на предпоследнюю и так далее.

Этот шифр использовался для еврейского алфавита и отсюда получил свое название. Первая буква – алеф, заменяется на тау (последнюю), вторая буква – бет, заменяется на шин (предпоследнюю). Из этих букв и сформировалось название.

Шифр Атбаш для русского алфавита.

А Б В Г Д Е Ё Ж З И Й К Л М Н О П Р С Т У Ф Х Ц Ч Ш Щ Ъ Ы Ь Э Ю Я Я Ю Э Ь Ы Ъ Щ Ш Ч Ц Х Ф У Т С Р П О Н М Л К Й И З Ж Ё Е Д Г В Б А.

Пример:

Исходное слово: замена

Зашифрованное слово: чятъся

# Цифровые шифры

Алфавит разбивается на группы с равным числом букв, затем каждой группе присваивается свой номер. Так формируется первая цифра для шифровки символа. Вторая цифра – это порядковый номер буквы в группе.



Таблица не обязательно должна выглядеть таким образом. Количество групп может быть другим. Также буквы из алфавита могут идти в таблице не по порядку.

Пример:

Зашифруем таким способом слово «цифра» Зашифрованный текст: 63 31 61 51 11

## *Задание:*

1. Изучить самостоятельно [Шифр Виженера](http://shifr-online.ru/shifr-vigenera.htm) и зашифровать любое выбранное вами слово.
2. Зашифровать слово, связанное с ИБ 2-мя способами: шифром Цезаря и цифровым шифром.
3. Зашифровать словосочетание, связанное с ИБ шифром Гронсфельда и шифром Атбаш.

Примечание: при шифровании использовать слова с количеством букв не менее 7 и сложные словосочетания.

***Сделать выводы.***

# Вопросы для проверки знаний и умений:

1. Дайте определение понятию «Шифрование»
2. Опишите принцип Шифра Цезаря.
3. Опишите принцип Шифра Гронсфельда.
4. Сравните шифр Атбаш и шифр Гронсфельда.
5. В чем заключается сущность цифрового шифра.