

***Дисциплина: Обеспечение качества функционирования компьютерных систем***

**Отчет по выполнению практической работы «Шифрование данных методами подстановки, перестановки и полиалфавитными шифрами»**

**Выполнили студенты**:

Зверев Н.Д.

Радченков В.В.

**Проверил преподаватель**:

Возвахов Д.А.

**Цель работы:** Приобретение навыков шифрования информации с использованием простейших методов шифрования.

**Алгоритм работы метода подстановки**

Шифр подстановки или замены - наиболее простой вид преобразований, заключающийся в замене символов исходного текста на другие символы того же либо другого алфавита по определенному правилу.

Историческим примером шифра подстановки является шифр Цезаря, в котором каждый символ открытого текста заменяется другой буквой, которая определяется путем смещения по алфавиту от исходной буквы влево или вправо на k букв. При достижении конца алфавита выполняется циклический переход к его началу. Цезарь использовал шифр замены при смещении вправо при k = 3.

Для произвольного ключа k шифр имеет вид:



где i – номер в алфавите символа открытого текста,

j –номер зашифрованного символа,

k –величина смещения - ключ,

n –количество букв в алфавите.

Обратная подстановка осуществляется по правилу 

Условием для успешной реализации этого метода является совпадение размера множеств открытого текста и шифротекста. Это условие в современных криптосистемах называется гомоморфизмом.

Другим вариантом метода подстановки является задание соответствия между буквами исходного алфавита и буквами подстановочного алфавита. Это позволяет заменять буквы в открытом тексте буквами из подстановочного алфавита Подстановочный алфавит может задаваться как множество символов, либо составляться по определенному правилу.

**Зашифровка и расшифровка сообщения.**

Текст в расшифрованном виде: Я, Радченков Владимир, студент Колледжа связи №54

Воспользуемся методом подстановки, а именно шифром Цезаря, чтобы зашифровать этот текст. Сместим по алфавиту от исходных букв вправо на 16 букв. Тогда мы получим такой текст.

Текст в зашифрованном виде: О, Апужфэъюс Сыпушьша, бвгуфэв Ъюыыфуцп бсочш №54

Чтобы расшифровать этот текст необходимо воспользоваться вышеупомянутым шифром Цезаря, сместив все буквы влево на 16 мы получим данный текст.

Текст в расшифрованном виде: Я, Радченков Владимир, студент Колледжа связи №54

**Вывод:** Мы приобрели навыки шифрования информации с использованием простейших методов шифрования. Мы ознакомились с теоритическим материалов в методической рекомендации. Мы описали алгоритм работы одного из методов шифрования. Мы зашифровали и расшифровали сообщение, представили его в зашифрованном и расшифрованном виде. Ответили на контрольные вопросы.

**Контрольные вопросы**

1. Метод подстановки имеет слабую надежность т.к. 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. Частотный анализ и криптоанализ – это одно и то же. Проблемой защиты информации путем ее преобразования занимается криптология. Криптология разделяется на два направления – криптографию и криптоанализ. Сфера интересов криптоанализа – исследование возможности расшифровывания информации без знания ключей.
3. Ключом в методе перестановки являются размер таблицы, маршруты вписывания и выписывания, порядки перестановки столбцов и строк.
4. Слабая криптостойкость моноалфавитных подстановок преодолевается с применением подстановок многоалфавитных. Для защиты от частотного анализа были разработаны многоалфавитные шифры, в которых для шифрования сообщения периодически используется несколько различных подстановочных алфавитов. Одним из этих подстановочных алфавитов является метод подстановки.
5. Отличие криптографии от криптоанализа заключается в том, что их цели противоположны. Криптография занимается поиском и исследованием математических методов преобразования информации. Криптоанализ исследует возможности расшифровывания информации без знания ключей.
6. По характеру используемого ключа криптографические методы делятся на симметричные и ассиметричные. Симметричные: для шифрования и дешифрования используется один и тот же секретный ключ. Асимметричные: для шифрования и дешифрования используют разные ключи, открытый – для шифрования, секретный – для дешифрования.