**Лабораторная работа № 7**

**Тема:** «Перестановочные шифры».

**Цель:** изучить перестановочные шифры. Шифр «Лесенка». Шифр вертикальнойиперестановки. Шифр «Поворотная решетка».

Задание 1. К открытому тексту был применен шифр «Лесенка». Восстановите сообщение по шифрованному тексту из таблицы 1.

Таблица 1.1 – Условие задания

|  |  |
| --- | --- |
| № варианта | Задание |
| 4 | ВРОСМЕННАЗАРТМНММММИМНИАКНФЦЯСОВУЕАДЕНАНСХТАОИЛЕЛОЮЕЖОНФЦЫТЭРЯРЯАБЬДРБНКТОИХЕЛОИМВНЯОИАУЫУА |

Для расшифровки сообщение нам необходимо узнать ключ шифрования (количество «Ступенек»). Для этого будем делить сообщение на N равных частей (количество символов зашифрованного сообщения – 91).

Таблица 1.2 – Расшифровка сообщения перебором ключа

|  |  |
| --- | --- |
| Ключ | Расшифровка сообщения по ключу |
| 2 | ВЛРЕОЛС… |
| 3 | ВВЯРУРО… |
| 4 | ВАЛБРКЕ… |
| 5 | ВИНФОРМАЦИОННЫХСИСТЕМАХЭЛЕКТРОННАЯИНФОРМАЦИЯВЗЯЛАНАСЕБЯРОЛЬОТВОДИМУЮРАНЕЕБУМАЖНЫМДОКУМЕНТАМ |

Расшифровка с ключом 5 имело начало слова «ИНФОРМация», поэтому расшифровывали сообщение по ключу 5 до конца и получаили расшифрованное сообщение: «ВИНФОРМАЦИОННЫХСИСТЕМАХЭЛЕКТРОННАЯИНФОРМАЦИЯВЗЯЛАНАСЕБЯРОЛЬОТВОДИМУЮРАНЕЕБУМАЖНЫМДОКУМЕНТАМ».

Задание 2. В ходе анализа ряда перехваченных сообщений, шифруемых методом вертикальной перестановки, криптоаналитиками был частично восстановлен используемый при этом ключ. В частности, они определили количество символов в ключе, а также числовые значения некоторых позиций. Результат работы криптоаналитиков представлен в виде строки, длина которой совпадает с длиной ключа, а символом X отмечены позиции ключа, значения которых на текущий момент неизвестны (см. задание в таблице 2). От Вас требуется по имеющемуся шифртексту закончить восстановление ключа и получить открытый текст, соответствующий шифрованному сообщению.

Таблица 2.1 – Условие задания

|  |  |
| --- | --- |
| № варианта | Задание |
| 4 | Зашифрованный текст:  СИВОСЕНЕЗОПЕОПТОЧЕБСЕСЙАИБЕТЕН  Частично восстановленный ключ: 4XX13X |

1) Запишем зашифрованный текст по столбцам:

Таблица 2.2 – Шифр в таблице

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| 1 | 2 | 3 | 4 | 5 | 6 |
| С | Е | П | О | Е | Б |
| И | Н | Е | Ч | С | Е |
| В | Е | О | Е | Й | Т |
| О | З | П | Б | А | Е |
| С | О | Т | С | И | Н |

2) Произведём перестановку столбцов по известным цифрам ключа (4XX13X):

Таблица 2.3 – Переставленные столбцы

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| 4 | 5 | 2 | 1 | 3 | 6 |
| О | Е | Е | С | П | Б |
| Ч | С | Н | И | Е | Е |
| Е | Й | Е | В | О | Т |
| Б | А | З | О | П | Е |
| С | И | О | С | Т | Н |

3) Осталось поставить в правильное место столбцы 2, 5 и 6. Перебором понимаем, что первая строка имеет все буквы, чтобы составить начало слова «ОБЕСПЕЧЕНИЕ». В соответствии с этим расставим столбцы по первой строке:

Таблица 2.4 – Перестановка по первой строке

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| 4 | 6 | 5 | 1 | 3 | 2 |
| О | Б | Е | С | П | Е |
| Ч | Е | С | И | Е | Н |
| Е | Т | Й | В | О | Е |
| Б | Е | А | О | П | З |
| С | Н | И | С | Т | О |

4) После перстановки 6 столбец однозначно встал на свое место (обновленный ключ – 46X13X). Осталось переставить столбцы 2 и 5. Продолжение слова «ОБЕСПЕЧЕНИЕ» находится во второй строке, поэтому строка 2 должна начинаться с «ЧЕНИЕ…». Производим ещё одну перестановку столбцов 2 и 5:

Таблица 2.4 – Перестановка по второй строке

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| 4 | 6 | 2 | 1 | 3 | 5 |
| О | Б | Е | С | П | Е |
| Ч | Е | Н | И | Е | С |
| Е | Т | Е | В | О | Й |
| Б | Е | З | О | П | А |
| С | Н | О | С | Т | И |

5) После последней перестановки получаем расшифрованное сообщение: «ОБЕСПЕЧЕНИЕСЕТЕВОЙБЕЗОПАСНОСТИ».

Контрольные вопросы.

1. На чем основывается метод перестановок?

Метод перестановок основывается на изменении порядка следования символов в открытом тексте с использованием какого-либо ключа или правила. Это может включать в себя перестановку символов, блоков текста или другие подобные манипуляции для создания зашифрованного сообщения. Примером является шифр перестановок, где символы открытого текста переставляются согласно определенному правилу, управляемому ключом.

2. Оцените надежность шифра «Лесенка».

Шифр "Лесенка" не является шифром в традиционном смысле, а представляет собой метод построения ключа для шифрования данных. Он применяется в криптографии для генерации подключей и предотвращения атак посредством использования многоступенчатых подстановок и перестановок. Оценка надежности зависит от конкретной реализации, используемых алгоритмов и длины ключа. В целом, если правильно реализован, он может обеспечивать достаточный уровень безопасности, но важно учитывать современные стандарты безопасности.

3. Дайте определение абсолютной защищенности.

Понятие абсолютной защищенности относится к теоретически идеальной системе шифрования, которая была бы абсолютно невозможной для взлома, даже при наличии неограниченных ресурсов. Концепция абсолютной защищенности была введена Клодом Шенноном. В практической реальности абсолютная защищенность трудно достижима из-за факторов, таких как ограниченные ресурсы, развитие криптоанализа и т.д. Многие системы шифрования стремятся к высокому уровню безопасности, но абсолютной защищенности, вероятно, никогда не будет достигнуто.