**Лабораторная работа №4**

**Тема:** Метод вертикальной перестановки.

**Задание:** 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. табл. 4). Требуется по имеющемуся шифртексту закончить восстановление ключа и получить открытый текст, соответствующий шифрованному сообщению.

Таблица 4. Варианты условий к лабораторной работе №4

|  |  |
| --- | --- |
|  | Зашифрованный текст:  ФТБЕОЗРЬЩМАОСЕОИАОИНШВОНЖ  Частично восстановленный ключ: XX5X1 |
|  | Зашифрованный текст:  ПНОСОЕЕНМРЗОЮЯАЬЬАПТКТБС  Частично восстановленный ключ: 6XX1X4 |
|  | Зашифрованный текст:  ОННАНЦОНДЛЬХФИСНИАТЫКЕЬД  Частично восстановленный ключ: XX24X3 |
|  | Зашифрованный текст:  СИВОСЕНЕЗОПЕОПТОЧЕБСЕСЙАИБЕТЕН  Частично восстановленный ключ: 4XX13X |
|  | Зашифрованный текст:  СНСКЫЕЕОАНОЕЕУАБЧДПНПИТДМ  Частично восстановленный ключ: 3XXX5 |
|  | Зашифрованный текст:  АКДВСЕШНЛСООСИЫАЧЕФЯКЕТРИМИИ  Частично восстановленный ключ: 63XX27X |
|  | Зашифрованный текст:  ИАОТЮОЕРКМФНТЫЧРИКМОШВСЫЛ  Частично восстановленный ключ: XX3X2 |
|  | Зашифрованный текст:  ЛЩЕОЬИЙМААТЛНТОАОЯСВКЗЕЗЛААТ  Частично восстановленный ключ: 7XX3X24 |
|  | Зашифрованный текст:  СУХЫЫМИЗЕМТРОТНАНЦПЙАЗИАЛЕИЩФИЬМЗИОИ  Частично восстановленный ключ: 2XX3X6 |
|  | Зашифрованный текст:  БСЕАГНМЗЛАЕООЯНПЛТБНАЕЕСЬЬЕА  Частично восстановленный ключ: 2X41XX7 |

**Пояснения:**

*Шифр вертикальной перестановки.*

Пример шифрования фразы «ПЕРЕСТАНОВКА ТЕКСТА ПО СТОЛБЦАМ» с ключом 4312567.

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Ключ: | 4 | 3 | 1 | 2 | 5 | 6 | 7 |  |
| Открытый текст: | П | Е | Р | Е | С | Т | А |  |
|  | Н | О | В | К | А | Т | Е |  |
|  | К | С | Т | А | П | О | С |  |
|  | Т | О | Л | Б | Ц | А | М |  |
| Шифрованный текст: | РВТЛЕКАБЕОСОПНКТСАПЦТТОААЕСМ | | | | | | | | |

Простой перестановочный шифр очень легко распознать, так как буквы в нем встречаются с той же частотой, что и в открытом тексте. Например, для только что рассмотренного способа шифрования с перестановкой столбцов анализ шифра выполнить достаточно просто – необходимо записать шифрованный текст в виде матрицы и перебрать возможные варианты перестановок для столбцов.

Перестановочный шифр можно сделать существенно более защищенным, выполнив шифрование с использованием перестановок несколько раз. Оказывается, что в этом случае примененную для шифрования перестановку воссоздать уже не так просто. Например, если предыдущее сообщение шифровать еще раз с помощью того же самого алгоритма, то результат будет следующим:

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Ключ: | 4 | 3 | 1 | 2 | 5 | 6 | 7 |  |
| Открытый текст: | Р | В | Т | Л | Е | К | А |  |
|  | Б | Е | О | С | О | П | Н |  |
|  | К | Т | С | А | П | Ц | Т |  |
|  | Т | О | А | А | Е | С | М |  |
| Шифрованный текст: | ТОСАЛСААВЕТОРБКТЕОПЕКПЦСАНТМ | | | | | | | | |

**Контрольные вопросы:**

1. Что представляет собой ключ в этом методе?
2. Как сообщение записывается при шифрации?
3. Как закодированное сообщение считывается при шифрации?
4. Как закодированное сообщение записывается при дешифрации?
5. Как восстановленное сообщение считывается при дешифрации?
6. Можно ли организовать дешифрацию с неизвестным ключом?
7. Алгоритм шифрации.
8. Алгоритм дешифрации.
9. Анализ метода.

**Содержание отчета:**

1. Цель работы.
2. Алгоритм шифрации и дешифрации по заданному методу, который реализует разработанная программа.
3. Описание программы (исходный код с комментариями).
4. Анализ ограничений возможности применения разработанной программы.
5. Анализ ограничений возможности применения данного метода.
6. Заключение.