**Лабораторная работа №2**

**Тема:** Шифр Плейфейера.

**Задание:** При использовании шифра Плейфейера на базе русского языка из алфавита удаляются буквы Ё (заменяется буквой Е) и буква Й (заменяется буквой И). Буквы Ъ и Ь считаются одной и той же буквой. Матрица букв строится на алфавите

##### АБВГДЕЖЗИКЛМНОПРСТУФХЦЧШЩЪЫЬЭЮЯ,

состоящем из 31 буквы, и состоит из 5 строк и 6 столбцов. Например, матрица букв на базе ключевого слова ПАРУСНИК будет выглядеть следующим образом:

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

Возьмите из таблицы 2 ключевое слово и последовательность символов, соответствующие Вашему варианту. Используя ключевое слово и шифр Плейфейера, закодируйте фразу «КОД ПЛЕЙФЕЙЕРА ОСНОВАН НА ИСПОЛЬЗОВАНИИ МАТРИЦЫ БУКВ» и декодируйте указанную в задании последовательность символов.

Таблица 2

|  |  |
| --- | --- |
| № | Задание |
|  | Ключевое слово: ПОЛЕТ  Строка для декодирования:  КЛКЕПЕШОБКЕРЭЛЧСКУЛЮЕТВМВКИММЮЗОТЖША |
|  | Ключевое слово: ФИЛЬМ  Строка для декодирования:  НПВЪЗПЖИКЛБЦРПЪПЭИЯЩЛИЗПБКФАГПШУХЭЧЖРЫВЦТУНЧТЩЧНХНЩТНЯХКДНЦВЗТЧИ |
|  | Ключевое слово: КАТЕР  Строка для декодирования:  ЗЛНЖКГСЩЯЪАОЕСМЩЯСОЛКДБОУЩФРКЖФТАРТЮВИОАСЫЫРМРЕПМЩ |
|  | Ключевое слово: ПАРОЛЬ  Строка для декодирования:  ЮОГНФПЛМКЮМВРМХИНЦШБЛГЖМУПЕАЮЖЧЗПДАМАЛНЪЖЕАДПУНЕЛСЪМЧПМЪЗЧЪЭАЩЩНТЗЗУАД |
|  | Ключевое слово: КОЛЬЦА  Строка для декодирования:  МИПГПДПМЖВТЩВИЕИЛРЩЧЗОЛИНЦЩХЖПЪРВЦТУОЖАЫВХУКЖЕВИ |
|  | Ключевое слово: КАМЕНЬ  Строка для декодирования:  РСРФЪПЧСВЛНПНЪСШТОБСХЪИЪФОПГИМФАНЪУКГЩЛНВНКХЧЪДУНЛМАХКСЛИЧТБЕУ |
|  | Ключевое слово: СОЛНЦЕ  Строка для декодирования:  ЗОИЦОЫИТЗУСОШЖАЦФАВЗЗКЗЧНБЗЖУКПБЕЫТЗЪЗФЩ |
|  | Ключевое слово: ТОВАРИЩ  Строка для декодирования:  МОЩЕЯВЧЪЛТАПЯВМОМРЗФИЫПТБКВИХБЦБЩШЪЧШЩИВТЧОАДХОПАБТИВАРМЖИ |
|  | Ключевое слово: СВЯЗЬ  Строка для декодирования:  ЛМЧШЮГХТЯПХООПКПЖМКЧВЦАОБФЖГКХПНЯВЖФЪЛЯНХОФЗТЪСЦПИЛФЛЪ |
|  | Ключевое слово: МАТЕРИЯ  Строка для декодирования:  УЕНАЕЭМЧЗПФТКСЪИАРУЕПЕСЯЕХТИСЩГХМЖФЗЧБГЩКМЮАЕЪ |

**Пояснения:** *Шифр Плейфейера.*

Одним из наиболее известных шифров, базирующихся на методе многобуквенного шифрования, является шифр Плейфейера (Playfair), в котором биграммы открытого текста рассматриваются как самостоятельные единицы, преобразуемые в заданные биграммы шифрованного текста.

Алгоритм Плейфейера основан на использовании матрицы букв размерности 5×5, созданной на основе некоторого ключевого слова. Матрица создается путем размещения букв, использованных в ключевом слове, слева направо и сверху вниз. Затем оставшиеся буквы алфавита размещаются в естественном порядке в оставшихся строках и столбцах матрицы. Буквы I и J считаются одной и той же буквой. Ниже приведен пример такой матрицы для ключевого слова *monarchy* (монархия).

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

Открытый текст шифруется порциями по две буквы в соответствии со следующими правилами.

1. Если оказывается, что повторяющиеся буквы открытого текста образуют одну пару для шифрования, то между этими буквами вставляется специальная буква-заполнитель, например *X*. В частности, такое слово как *balloon* будет преобразовано к виду ba lx lo on.
2. Если буквы открытого текста попадают в одну и ту же строку матрицы, каждая из них заменяется буквой, следующей за ней в той же строке справа – с тем условием, что для замены последнего элемента строки матрицы служит первый элемент той же строки. Согласно выше построенной матрицы AR шифруется как RM.
3. Если буквы открытого текста попадают в один и тот же столбец матрицы, каждая из них заменяется буквой, состоящей в том же столбце сразу под ней, с тем условием, что для замены самого нижнего элемента столбца матрицы берется самый верхний элемент того же столбца. В примере выше MU шифруется как CM.
4. Если не выполняется ни одно из приведенных условий, каждая буква из пары букв открытого текста заменяется буквой, находящейся на пересечении содержащей эту букву строки матрицы и столбца, в котором находится вторая буква открытого текста. Например, HS шифруется как BP, а EA – как IM (или JM, по желанию шифровальщика).

Шифр Плейфейера значительно надежнее простых моноалфавитных шифров. С одной стороны, букв всего 26, а биграмм - 26×26 = 676, и поэтому идентифицировать биграммы сложнее, чем отдельные буквы. С другой стороны, относительная частота появления отдельных букв колеблется гораздо в более широком диапазоне, чем частота появления биграмм, поэтому анализ частотности употребления биграмм тоже оказывается сложнее анализа частотности употребления букв. По этим причинам очень долго считалось, что шифр Плейфейера взломать невозможно. Он служил стандартом шифрования в Британской армии во время первой мировой войны и нередко применялся в армии США и союзных войсках даже в период второй мировой войны.

Несмотря на столь высокую репутацию в прошлом, шифр Плейфейера на самом деле вскрыть относительно легко, так как шифрованный с его помощью текст все равно сохраняет многие статистические характеристики открытого текста. Для взлома этого шифра, как правило, достаточно иметь шифрованный текст, состоящий из нескольких сотен букв.

**Контрольные вопросы:**

1. Какие ограничения для ключа в этом методе?
2. Как создаётся матрица?
3. Как шифруется открытый текст?
4. Как восстанавливается сообщение при дешифрации?
5. Алгоритм шифрации.
6. Алгоритм дешифрации.
7. Анализ метода.

**Содержание отчета:**

1. Цель работы.
2. Алгоритм шифрации и дешифрации по заданному методу, который реализует разработанная программа.
3. Описание программы.
4. Анализ ограничений возможности применения разработанной программы.
5. Анализ ограничений возможности применения данного метода.