## **Лабораторная работа №1. Шифры перестановки и замены**

**Цель работы:** Получить практические навыки по применению шифров перестановки и шифров простой замены.

**Теоретические сведения**

**Шифры перестановки**

Шифр, преобразования из которого изменяют только порядок следования символов исходного текста, но не изменяют их самих, называется шифром перестановки (ШП).

Шифрами перестановки называются такие шифры, преобразования из которых приводят к изменению только порядка следования символов исходного сообщения. Примером преобразования, которое может содержаться в шифре перестановки, является следующее правило. Каждая буква исходного сообщения, стоящая в тексте на позиции с четным номером, меняется местами с предшествующей ей буквой. В этом случае ясно, что и исходное, и шифрованное сообщение состоят из одних и тех же букв.

Рассмотрим преобразование из ШП, предназначенное для шифрования сообщения длиной *n* символов. Его можно представить с помощью таблицы



где *i1* - номер места шифртекста, на которое попадает первая буква исходного сообщения при выбранном преобразовании, *i2* - номер места для второй буквы и т.д. В верхней строке таблицы выписаны по порядку числа от 1 до *n*, а в нижней - те же числа, но в произвольном порядке. Такая таблица называется подстановкой степени *n*.

Зная подстановку, задающую преобразование, можно осуществить как шифрование, так и дешифрование текста. Например, если для преобразования используется подстановка



и в соответствии с ней зашифровывается слово МОСКВА, то получится КОСВМА. Попробуйте расшифровать сообщение НЧЕИУК, полученное в результате преобразования с помощью указанной выше подстановки.

В соответствии с методом математической индукции, можно легко убедиться в том, что существует  вариантов заполнения нижней строки таблицы ([1](file:///D:\Documents\OlegLaba\4%20курс\2%20семестр\Защита%20информации\МЕТОДЫ\ЛР1\78.html#genericpermut#genericpermut)). Таким образом, число различных преобразований шифра перестановки, предназначенного для шифрования сообщений длины *n*, меньше либо равно *n!* (заметим, что в это число входит и вариант преобразования, оставляющий все символы на своих местах!).

С увеличением числа *n* значение *n!* растет очень быстро. Приведем таблицу значений *n!* для первых 10 натуральных чисел:

|  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| *n* | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 |
| *n!* | 1 | 2 | 6 | 24 | 120 | 720 | 5040 | 40320 | 362880 | 3628800 |

При больших *n* для приближенного вычисления *n!* можно пользоваться известной формулой Стирлинга



где *e* = 2,718281828…

Примером ШП, предназначенного для шифрования сообщений длины *n*, является шифр, в котором в качестве множества ключей взято множество всех подстановок степени *n*, а соответствующие им преобразования шифра задаются, как было описано выше. Число ключей такого шифра равно *n!*.

Для использования на практике такой шифр не удобен, так как при больших значениях *n* приходится работать с длинными таблицами.

Широкое распространение получили шифры перестановки, использующие некоторую геометрическую фигуру. Преобразования из этого шифра состоят в том, что в фигуру исходный текст вписывается по ходу одного «маршрута», а затем по ходу другого выписывается с нее. Такой шифр называют маршрутной перестановкой. Например, можно вписывать исходное сообщение в прямоугольную таблицу, выбрав такой маршрут: по горизонтали, начиная с левого верхнего угла поочередно слева направо и справа налево. Выписывать же сообщение будем по другому маршруту: по вертикали, начиная с верхнего правого угла и двигаясь поочередно сверху вниз и снизу вверх.

Зашифруем, например, указанным способом фразу:

ПРИМЕРМАРШРУТНОЙПЕРЕСТАНОВКИ

используя прямоугольник размера 4 х 7:

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| П | Р | И | М | Е | Р | М |
| Н | Т | У | Р | Ш | Р | А |
| О | Й | П | Е | Р | Е | С |
| И | К | В | О | Н | А | Т |

Зашифрованная фраза выглядит так:

МАСТАЕРРЕШРНОЕРМИУПВКЙТРПНОИ

Теоретически маршруты могут быть значительно более изощренными, однако запутанность маршрутов усложняет использование таких шифров.

Ниже приводятся описания трех разновидностей шифров перестановки:

**Шифр «Сцитала»**. Одним из самых первых шифровальных приспособлений был жезл («Сцитала»), применявшийся еще во времена войны Спарты против Афин в V веке до н. э. Это был цилиндр, на который виток к витку наматывалась узкая папирусная лента (без просветов и нахлестов), а затем на этой ленте вдоль его оси записывался необходимый для передачи текст. Лента сматывалась с цилиндра и отправлялась адресату, который, имея цилиндр точно такого же диаметра, наматывал ленту на него и прочитывал сообщение. Ясно, что такой способ шифрования осуществляет перестановку местами букв сообщения.

Шифр «Сцитала» реализует не более *n* перестановок (*n*, по прежнему, - длина сообщения). Действительно, этот шифр, как нетрудно видеть, эквивалентен следующему шифру маршрутной перестановки: в таблицу, состоящую из *m* столбцов, построчно записывают сообщение, после чего выписывают буквы по столбцам. Число задействованных столбцов таблицы не может превосходить длины сообщения.

Имеются еще и чисто физические ограничения, накладываемые реализацией шифра «Сцитала». Естественно предположить, что диаметр жезла не должен превосходить 10 сантиметров. При высоте строки в 1 сантиметр на одном витке такого жезла уместится не более 32 букв (). Таким образом, число перестановок, реализуемых «Сциталой», вряд ли превосходит 32.

**Шифр «Поворотная решетка».** Для использования шифра, называемого поворотной решеткой, изготавливается трафарет из прямоугольного листа клетчатой бумаги размера *2m x 2k* клеток. В трафарете вырезано *mk* клеток так, что при наложении его на чистый лист бумаги того же размера четырьмя возможными способами его вырезы полностью покрывают всю площадь листа.

Буквы сообщения последовательно вписываются в вырезы трафарета (по строкам, в каждой строке слева направо) при каждом из четырех его возможных положений в заранее установленном порядке.

Поясним процесс шифрования на примере. Пусть в качестве ключа используется решетка 6x10, приведенная на рис. 1.

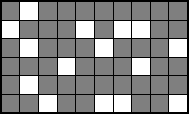


Рис. 1. Ключ шифрования для метода «Поворотной решетки».

Зашифруем с ее помощью текст

ШИФРРЕШЕТКАЯВЛЯЕТСЯЧАСТНЫМСЛУЧАЕМШИФРАМАРШРУТНОЙПЕРЕСТАНОВКИ

Наложив решетку на лист бумаги, вписываем первые 15 (по числу вырезов) букв сообщения: ШИФРРЕШЕТКАЯВЛЯ.... Сняв решетку, мы увидим текст, представленный на рис. 2. Поворачиваем решетку на 180°. В окошечках появятся новые, еще не заполненные клетки. Вписываем в них следующие 15 букв. Получится запись, приведенная на рис. 3. Затем переворачиваем решетку на другую сторону и зашифровываем остаток текста аналогичным образом (рис. [4](file:///D:\Documents\OlegLaba\4%20курс\2%20семестр\Защита%20информации\МЕТОДЫ\ЛР1\78.html#thirdlatt#thirdlatt), 5).

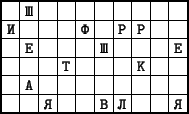


Рис. 2.



Рис. 3.

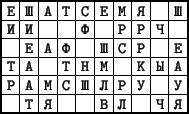


Рис. 4.

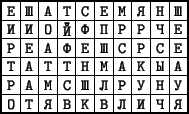


Рис. 5.

Получатель сообщения, имеющий точно такую же решетку, без труда прочтет исходный текст, наложив решетку на шифртекст по порядку четырьмя способами.

Можно доказать, что число возможных трафаретов, то есть количество ключей шифра «решетка», составляет *T = 4mk*. Этот шифр предназначен для сообщений длины *n = 4mk*. Число всех перестановок в тексте такой длины составит *(4mk)!*, что во много раз больше числа *T*. Однако, уже при размере трафарета 8x8 число возможных решеток превосходит 4 миллиарда.

Широко распространена разновидность шифра маршрутной перестановки, называемая «**шифром вертикальной перестановки» (ШВП)**. В нем снова используется прямоугольник, в который сообщение вписывается обычным способом (по строкам слева направо). Выписываются буквы по вертикали, а столбцы при этом берутся в порядке, определяемом ключом. Пусть, например, этот ключ таков: (5,4,1,7,2,6,3), и с его помощью надо зашифровать сообщение:

ВОТПРИМЕРШИФРАВЕРТИКАЛЬНОЙПЕРЕСТАНОВКИ

Впишем сообщение в прямоугольник, столбцы которого пронумерованы в соответствии с ключом:

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| 5 | 1 | 4 | 7 | 2 | 6 | 3 |
| В | О | Т | П | Р | И | М |
| Е | Р | Ш | И | Ф | Р | А |
| В | Е | Р | Т | И | К | А |
| Л | Ь | Н | О | Й | П | Е |
| Р | Е | С | Т | А | Н | О |
| В | К | И | - | - | - | - |

Теперь, выбирая столбцы в порядке, заданном ключом, и выписывая последовательно буквы каждого из них сверху вниз, получаем такую криптограмму:

ОРЕЬЕКРФИЙА-МААЕО-ТШРНСИВЕВЛРВИРКПН-ПИТОТ-

Число ключей ШВП не более *m!*, где *m* - число столбцов таблицы. Как правило, *m* гораздо меньше, чем длина текста *n* (сообщение укладывается в несколько строк по *m* букв), а, значит, и *m!* много меньше *n!*.

Пользуясь приведенной выше **формулой Стирлинга** при больших *m* и *n*, попытайтесь оценить, во сколько раз число возможных перестановок ШВП с *m* столбцами меньше числа всех перестановок на тексте длины *n*, кратном *m*.

В случае, когда ключ ШВП не рекомендуется записывать, его можно извлекать из какого-то легко запоминающегося слова или предложения. Для этого существует много способов. Наиболее распространенный состоит в том, чтобы приписывать буквам числа в соответствии с обычным алфавитным порядком букв. Например, пусть ключевым словом будет ПЕРЕСТАНОВКА. Присутствующая в нем буква А получает номер 1. Если какая-то буква входит несколько раз, то ее появления нумеруются последовательно слева направо. Поэтому второе вхождение буквы А получает номер 2. Поскольку буквы Б в этом слове нет, то буква В получает номер 3 и так далее. Процесс продолжается до тех пор, пока все буквы не получат номера. Таким образом, мы получаем следующий ключ:

|  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| П | Е | Р | Е | С | Т | А | Н | О | В | К | А |
| 9 | 4 | 10 | 5 | 11 | 12 | 1 | 7 | 8 | 3 | 6 | 2 |

**Шифры простой замены**

При шифровании заменой (подстановкой) символы шифруемого текста заменяются символами того же или другого алфавита с заранее установленным правилом замены. В шифре простой замены каждый символ исходного текста заменяется символами того же алфавита одинаково на всем протяжении текста. Часто шифры простой замены называют шифрами одноалфавитной подстановки.

**Полибианский квадрат**

Одним из первых шифров простой замены считается так называемый *полибианский квадрат.* За два века до нашей эры греческий писатель и историк Полибий изобрел для целей шифрования квадратную таблицу размером 5х5, заполненную буквами греческого алфавита в случайном порядке.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| q | p | w | o | e |
| i | r | u | t | y |
| z | m | x | n | c |
| b | v | a | l | s |
| k | d | j | f | h |

Полибианский квадрат, заполненный случайным образом буквами латинского алфавита и пробелом

При шифровании в этом полибианском квадрате находили очередную букву открытого текста и записывали в шифртекст букву, расположенную ниже ее в том же столбце. Если буква текста оказывалась в нижней строке таблицы, то для шифртекста брали самую верхнюю букву из того же столбца. Например, для слова

square

получается шифртекст

hixjmy

Концепция полибианского квадрата оказалась плодотворной и нашла применение в криптосистемах последующего времени.

**Система шифрования Цезаря**

Шифр Цезаря является частным случаем шифра простой замены (одноалфавитной подстановки). Свое название этот шифр получил по имени римского императора Гая Юлия Цезаря, который использовал этот шифр при переписке с Цицероном (около 50 г. до н.э.).

При шифровании исходного текста каждая буква заменялась на другую букву того же алфавита по следующему правилу. Заменяющая буква определялась путем смещения по алфавиту от исходной буквы на К букв. При достижении конца алфавита выполнялся циклический переход к его началу. Цезарь использовал шифр замены при смещении К = 3. Такой шифр замены можно задать таблицей подстановок, содержащей соответствующие пары букв открытого текста и шифртекста. Совокупность возможных подстановок для К = 3 показана в следующей таблице.

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

Например, послание Цезаря

VENI VIDI VICI

в переводе на русский означает "Пришел, Увидел, Победил"), направленное его другу Аминтию после победы над понтийским царем Фарнаком, сыном Митридата, выглядело бы в зашифрованном виде так:

YHQL YLGL YLFL

Концепция, заложенная в систему шифрования Цезаря, оказалась весьма плодотворной, о чем свидетельствуют ее многочисленные модификации. Несколько таких модификаций будут рассмотрены ниже.

**Аффинная система подстановок Цезаря**

В данном преобразовании буква, соответствующая числу *t*, заменяется на букву, соответствующую числовому значению *(at+b)* по модулю *m*.

Следует заметить, что *а* и *m* должны быть взаимно простыми числами.

Например, пусть m=26, а=3, b=5. Тогда, очевидно, НОД (3,26)=1, и мы получаем следующее соответствие между числовыми кодами букв:

|  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| t | 0 | 1 | 2 | 3 | 4 | … | 23 | 24 | 25 |
| 3t+5 | 5 | 8 | 11 | 14 | 17 | … | 22 | 25 | 2 |

Преобразуя числа в буквы английского языка, получаем следующее соответствие для букв открытого текста и шифртекста:

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| А | B | C | D | Е | F | G | Н | I | J | К | L | М | N | O | Р | Q | R | S | T | U | V | W | Х | Y | Z |
| F | I | L | O | R | U | Х | А | D | G | J | М | Р | S | V | Y | В | Е | Н | K | N | Q | Т | W | Z | C |

Исходное сообщение HOPE преобразуется в шифртекст AVYR

Достоинством аффинной системы является удобное управление ключами - ключи шифрования и дешифрования представляются в компактной форме в виде пары чисел (а, b). Недостатки аффинной системы аналогичны недостаткам системы шифрования Цезаря.

Аффинная система использовалась на практике несколько веков назад, а сегодня ее применение ограничивается большей частью иллюстрациями основных криптологических положений.

**Система Цезаря с ключевым словом**

Система шифрования Цезаря с ключевым словом является одноалфавитной системой подстановки. Особенностью этой системы является использование ключевого слова для смещения и изменения порядка символов в алфавите подстановки.

Выберем некоторое число *k*, , и слово или короткую фразу в качестве *ключевого слова.* Желательно, чтобы все буквы ключевого слова были различными. Пусть выбраны слово DIPLOMAT в качестве ключевого слова и число k = 5.

Ключевое слово записывается под буквами алфавита, начиная с буквы, числовой код которой совпадает с выбранным числом k:

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 0 | 1 | 2 | 3 | 4 | 5 |  |  |  |  | 10 |  |  |  |  | 15 |  |  |  |  | 20 |  |  |  |  | 25 |
| А | B | C | D | Е | F | G | Н | I | J | К | L | М | N | O | Р | Q | R | S | T | U | V | W | Х | Y | Z |
|  |  |  |  |  | D | I | P | L | O | M | A | T |  |  |  |  |  |  |  |  |  |  |  |  |  |

Оставшиеся буквы алфавита подстановки записываются после ключевого слова в алфавитном порядке:

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  |  |  |  |  | 5 |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| А | B | C | D | Е | F | G | Н | I | J | К | L | М | N | O | Р | Q | R | S | T | U | V | W | Х | Y | Z |
| V | W | Х | Y | Z | D | I | P | L | O | M | A | T | B | C | E | F | G | H | J | K | N | Q | R | S | U |

Теперь мы имеем подстановку для каждой буквы произвольного сообщения.

Исходное сообщение HELLO шифруется как PZAAC

Несомненным достоинством системы Цезаря с ключевым словом является то, что количество возможных ключевых слов практически неисчерпаемо. Недостатком этой системы является возможность взлома шифртекста на основе анализа частот появления букв.

**Шифрующие таблицы Трисемуса**

В 1508 г. аббат из Германии Иоганн Трисемус написал печатную работу по криптологии под названием «Полиграфия». В этой книге он впервые систематически описал применение шифрующих таблиц, заполненных алфавитом в случайном порядке. Для получения такого шифра замены обычно использовались таблица для записи букв алфавита и ключевое слово (или фраза). В таблицу сначала вписывалось по строкам ключевое слово, причем повторяющиеся буквы отбрасывались. Затем эта таблица дополнялась не вошедшими в нее буквами алфавита по порядку.

Поскольку ключевое слово или фразу легко хранить в памяти, то такой подход упрощал процессы шифрования и дешифрования. Поясним этот метод шифрования на примере. Для русского алфавита шифрующая таблица может иметь размер 4х8. Выберем в качестве ключа слово БАНДЕРОЛЬ.

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| Б | А | Н | Д | Е | Р | О | Л |
| Ь | В | Г | Ж | 3 | И | Й | К |
| М | П | С | Т | У | Ф | Х | Ц |
| Ч | Ш | Щ | Ы | Ъ | Э | Ю | Я |

Как и в случае полибианского квадрата, при шифровании находят в этой таблице очередную букву открытого текста и записывают в шифртекст букву, расположенную ниже ее в том же столбце. Если буква текста оказывается в нижней строке таблицы, тогда для шифртекста берут самую верхнюю букву из того же столбца.

Например, при шифровании с помощью этой таблицы сообщения

ВЫЛЕТАЕМПЯТОГО

получаем шифртекст

ПДКЗЫВЗЧШЛЫЙСЙ

Такие табличные шифры называются монограммными, так как шифрование выполняется по одной букве. Трисемус первым заметил, что шифрующие таблицы позволяют шифровать сразу по две буквы. Такие шифры называются биграммными.

**Биграммный шифр Плейфейра**

Шифр Плейфейра, изобретенный в 1854 г., является наиболее известным биграммным шифром замены. Он применялся Великобританией во время первой мировой войны. Основой шифра Плейфейра является шифрующая таблица со случайно расположенными буквами алфавита исходных сообщений.

Для удобства запоминания шифрующей таблицы отправителем и получателем сообщений можно использовать ключевое слово (или фразу) при заполнении начальных строк таблицы. В целом структура шифрующей таблицы системы Плейфейра полностью аналогична структуре шифрующей таблицы Трисемуса. Поэтому для пояснения процедур шифрования и расшифрования в системе Плейфейра воспользуемся шифрующей таблицей Трисемуса из предыдущего раздела.

Процедура шифрования включает следующие шаги:

1. Открытый текст исходного сообщения разбивается на пары букв (биграммы). Текст должен иметь четное количество букв и в нем не должно быть биграмм, содержащих две одинаковые буквы. Если эти требования не выполнены, то текст модифицируется даже из-за незначительных орфографических ошибок.

2. Последовательность биграмм открытого текста преобразуется с помощью шифрующей таблицы в последовательность биграмм шифртекста по следующим правилам:

2а. Если обе буквы биграммы открытого текста не попадают на одну строку или столбец (как, например, буквы А и Й), тогда находят буквы в углах прямоугольника, определяемого данной парой букв. (В нашем примере это буквы АЙОВ. Пара букв АЙ отображается в пару ОВ. Последовательность букв в биграмме шифртекста должна быть зеркально расположенной по отношению к последовательности букв в биграмме открытого текста).

2б. Если обе буквы биграммы открытого текста принадлежат одному столбцу таблицы, то буквами шифртекста считаются буквы, которые лежат под ними. (Например, биграмма НС дает биграмму шифртекста ГЩ.) Если при этом буква открытого текста находится в нижней строке, то для шифртекста берется соответствующая буква из верхней строки того же столбца. (Например, биграмма ВШ дает биграмму шифртекста ПА.)

2в. Если обе буквы биграммы открытого текста принадлежат одной строке таблицы, то буквами шифртекста считаются буквы, которые лежат справа от них. (Например, биграмма НО дает биграмму шифртекста ДЛ.) Если при этом буква открытого текста находится в крайнем правом столбце, то для шифра берут соответствующую букву из левого столбца в той же строке. (Например, биграмма ФЦ дает биграмму шифртекста ХМ.).

Зашифруем текст

ВСЕ ТАЙНОЕ СТАНЕТ ЯВНЫМ

Разбиение этого текста на биграммы дает

ВС ЕТ АЙ НО ЕС ТА НЕ ТЯ ВН ЫМ

Данная последовательность биграмм открытого текста преобразуется с помощью шифрующей таблицы в следующую последовательность биграмм шифртекста

ГП ДУ ОВ ДЛ НУ ПД ДР ЦЫ ГА ЧТ

При дешифровании применяется обратный порядок действий.

Следует отметить, что шифрование биграммами резко повышает стойкость шифров к вскрытию. Хотя книга И.Трисемуса «Полиграфия» была относительно доступной, описанные в ней идеи получили признание лишь спустя три столетия. По всей вероятности, это было обусловлено плохой осведомленностью криптографов о работах богослова и библиофила Трисемуса в области криптографии.

**Система омофонов**

Система омофонов обеспечивает простейшую защиту от криптоаналитических атак, основанных на подсчете частот появления букв в шифртексте. Система омофонов является одноалфавитной, хотя при этом буквы исходного сообщения имеют несколько замен. Число замен берется пропорциональным вероятности появления буквы в открытом тексте.

Данные о распределениях вероятностей букв в русском и английском текстах приведены в таблицах. Буквы в таблицах указаны в порядке убывания вероятности их появления в тексте. Например, русская буква Е встречается в 36 раз чаще, чем буква Ф, а английская буква Е встречается в 123 раза чаще, чем буква Z.

Шифруя букву исходного сообщения, выбирают случайным образом одну из ее замен. Замены (часто называемые омофонами) могут быть представлены трехразрядными числами от 000 до 999. Например, в английском алфавите букве Е присваиваются 123 случайных номера, буквам В и G - по 16 номеров, а буквам J и Z - по 1 номеру. Если омофоны (замены) присваиваются случайным образом различным появлениям одной и той же буквы, тогда каждый омофон появляется в шифртексте равновероятно.

Распределение вероятностей букв в русских текстах

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| Буква | Вероятность | Буква | Вероятность | Буква | Вероятность | Буква | Вероятность |
| Пробел | 0,175 | Р | 0,040 | Я | 0,018 | X | 0,009 |
| О | 0,090 | В | 0,038 | Ы | 0.016 | Ж | 0,007 |
| Е | 0,072 | Л | 0,035 | 3 | 0,016 | Ю | 0,006 |
| А | 0,062 | K | 0,028 | Ъ | 0,014 | Ш | 0,006 |
| И | 0,062 | M | 0,026 | Б | 0,014 | Ц | 0,004 |
| Н | 0,053 | Д | 0,025 | Г | 0,013 | Щ | 0,003 |
| Т | 0,053 | П | 0,023 | Ч | 0,012 | Э | 0,003 |
| C | 0,045 | У | 0,021 | Й | 0,010 | Ф | 0,002 |

Распределение вероятностей букв в английских текстах

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Буква | Вероятность | Буква | Вероятность | Буква | Вероятность |
| Е | 0,123 | L | 0,040 | В | 0,016 |
| Т | 0,096 | D | 0,036 | G | 0,016 |
| А | 0,081 | С | 0,032 | V | 0,009 |
| O | 0,079 | U | 0,031 | К | 0,005 |
| N | 0,072 | Р | 0,023 | Q | 0,002 |
| I | 0,071 | F | 0,023 | X | 0,002 |
| S | 0,066 | М | 0,022 | J | 0,001 |
| R | 0,060 | W | 0,020 | Z | 0,001 |
| Н | 0,051 | Y | 0,019 |  |  |

При таком подходе к формированию шифртекста простой подсчет частот уже ничего не дает криптоаналитику. Однако в принципе полезна также информация о распределении пар и троек букв в различных естественных языках. Если эту информацию использовать при криптоанализе, он будет проведен более успешно.

**Шифры сложной замены**

Шифры сложной замены называют многоалфавитными, так как для шифрования каждого символа исходного сообщения применяют свой шифр простой замены. Многоалфавитная подстановка последовательно и циклически меняет используемые алфавиты.

При r-алфавитной подстановке символ x0 исходного сообщения заменяется символом y0 из алфавита В0, символ x1 -символом y1 из алфавита B1, и так далее, символ xr-1 заменяется символом yr-1 из алфавита Br-1, символ xr заменяется символом yr снова из алфавита Во, и т.д.

Общая схема многоалфавитной подстановки для случая г = 4 приведена ниже.

|  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Входной символ: | X0 | X1 | X2 | X3 | X4 | X5 | X6 | X7 | X8 | X9 |
| Алфавит подстановки: | В0 | B1 | B2 | В3 | В0 | B1 | B2 | В3 | В0 | B1 |

Эффект использования многоалфавитной подстановки заключается в том, что обеспечивается маскировка естественной статистики исходного языка, так как конкретный символ из исходного алфавита А может быть преобразован в несколько различных символов шифровальных алфавитов Вj. Степень обеспечиваемой защиты теоретически пропорциональна длине периода г в последовательности используемых алфавитов Вj.

Многоалфавитные шифры замены предложил и ввел в практику криптографии Леон Батист Альберти, который также был известным архитектором и теоретиком искусства. Его книга «Трактат о шифре», написанная в 1566 г., представляла собой первый в Европе научный труд по криптологии. Кроме шифра многоалфавитной замены, Альберти также подробно описал устройства из вращающихся колес для его реализации. Криптологи всего мира почитают Л.Альберти основоположником криптологии.

**Шифр Гронсфельда**

Этот шифр сложной замены, называемый шифром Гронсфельда, представляет собой модификацию шифра Цезаря числовым ключом. Для этого под буквами исходного сообщения записывают цифры числового ключа. Если ключ короче сообщения, то его запись циклически повторяют. Шифртекст получают примерно, как в шифре Цезаря, но отсчитывают по алфавиту не третью букву (как это делается в шифре Цезаря), а выбирают ту букву, которая смещена по алфавиту на соответствующую цифру ключа. Например, применяя в качестве ключа группу из четырех начальных цифр числа e (основания натуральных логарифмов), а именно 2718, получаем для исходного сообщения ВОСТОЧНЫЙ ЭКСПРЕСС следующий шифртекст:

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Сообщение |  | В | О | С | Т | О | Ч | Н | Ы | Й |  | Э | К | С | П | Р | Е | С | С |
| Ключ |  | 2 | 7 | 1 | 8 | 2 | 7 | 1 | 8 | 2 |  | 7 | 1 | 8 | 2 | 7 | 1 | 8 | 2 |
| Шифртекст |  | Д | Х | Т | Ь | Р | Ю | О | Г | Л |  | Д | Л | Щ | С | Ч | Ж | Щ | У |

Чтобы зашифровать первую букву сообщения В, используя первую цифру ключа 2 , нужно отсчитать вторую по порядку букву от В в алфавите

|  |  |  |
| --- | --- | --- |
| В | Г | Д |
|  | 1 | 2 |

получается первая буква шифр-текста Д.

Следует отметить, что шифр Гронсфельда вскрывается относительно легко, если учесть, что в числовом ключе каждая цифра имеет только десять значений, а значит, имеется лишь десять вариантов прочтения каждой буквы шифртекста. С другой стороны, шифр Гронсфельда допускает дальнейшие модификации, улучшающие его стойкость, в частности двойное шифрование разными числовыми ключами.

Шифр Гронсфельда представляет собой по существу частный случай системы шифрования Вижинера.

**Система шифрования Вижинера**

Система Вижинера впервые была опубликована в 1586 г. и является одной из старейших и наиболее известных многоалфавитных систем. Свое название она получила по имени французского дипломата XVI века Блеза Вижинера, который развивал и совершенствовал криптографические системы.

Система Вижинера подобна такой системе шифрования Цезаря, у которой ключ подстановки меняется от буквы к букве. Этот шифр многоалфавитной замены можно описать таблицей шифрования, называемой таблицей (квадратом) Вижинера. Ниже показаны таблицы Вижинера для русского и английского алфавитов соответственно.

Таблица Вижинера используется для шифрования и дешифрования. Таблица имеет два входа:

* верхнюю строку подчеркнутых символов, используемую для считывания очередной буквы исходного открытого текста;
* крайний левый столбец ключа.

Последовательность ключей обычно получают из числовых значений букв ключевого слова.

При шифровании исходного сообщения его выписывают в строку, а под ним записывают ключевое слово (или фразу). Если ключ оказался короче сообщения, то его циклически повторяют. В процессе шифрования находят в верхней строке таблицы очередную букву исходного текста и в левом столбце очередное значение ключа. Очередная буква шифртекста находится на пересечении столбца, определяемого шифруемой буквой, и строки, определяемой числовым значением ключа.

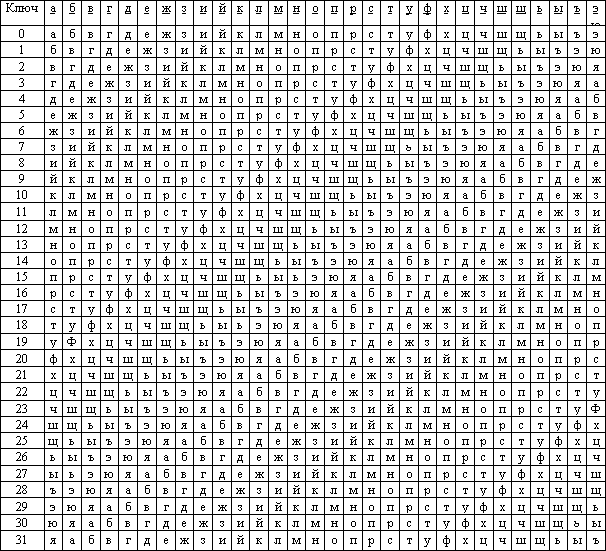


Таблица Вижинера для русского алфавита

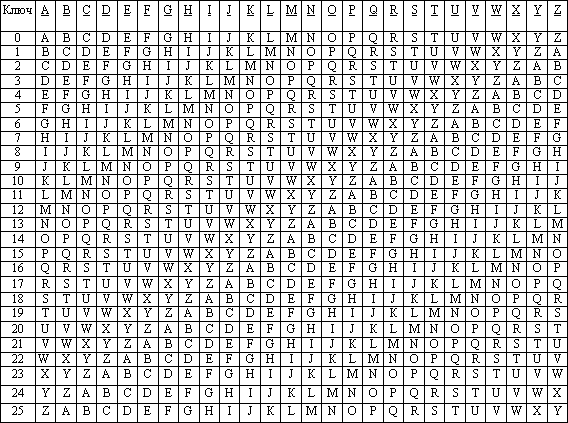


Таблица Вижинера для английского алфавита

Рассмотрим пример получения шифртекста с помощью таблицы Вижинера. Пусть выбрано ключевое слово АМБРОЗИЯ. Необходимо зашифровать сообщение ПРИЛЕТАЮ СЕДЬМОГО.

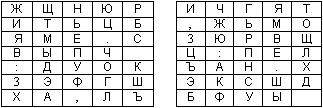
Выпишем исходное сообщение в строку и запишем под ним ключевое слово с повторением. В третью строку будем выписывать буквы шифртекста, определяемые из таблицы Вижинера.

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Сообщение | П | Р | И | Л | Е | Т | А | Ю |  | С | Е | Д | Ь | М | О | Г | О |
| Ключ | А | М | Б | Р | О | З | И | Я |  | А | М | Б | Р | О | З | И | Я |
| Шифртекст | П | Ъ | Й | Ы | У | Щ | И | Э |  | С | С | Е | К | Ь | Х | Л | Н |

**Шифр «двойной квадрат» Уитстона**

  В 1854 г. англичанин Чарльз Уитстон разработал новый метод шифрования биграммами, который называют «двойным квадратом». Свое название этот шифр получил по аналогии с по-либианским квадратом. Шифр Уитстона открыл новый этап в истории развития криптографии. В отличие от полибианского шифр «двойной квадрат» использует сразу две таблицы, размещенные по одной горизонтали, а шифрование идет биграммами, как в шифре Плейфейра. Эти не столь сложные модификации привели к появлению на свет качественно новой криптографической системы ручного шифрования. Шифр «двойной квадрат» оказался очень надежным и удобным и применялся Германией даже в годы второй мировой войны.

Поясним процедуру шифрования этим шифром на примере. Пусть имеются две таблицы со случайно расположенными в них русскими алфавитами. Перед шифрованием исходное сообщение разбивают на биграммы. Каждая биграмма шифруется отдельно. Первую букву биграммы находят в левой таблице, а вторую букву - в правой таблице. Затем мысленно строят прямоугольник так, чтобы буквы биграммы лежали в его противоположных вершинах. Другие две вершины этого прямоугольника дают буквы биграммы шифртекста.



Две таблицы со случайно расположенными символами русского алфавита  
для шифра «двойной квадрат»

Предположим, что шифруется биграмма исходного текста ИЛ. Буква И находится в столбце 1 и строке 2 левой таблицы. Буква Л находится в столбце 5 и строке 4 правой таблицы. Это означает, что прямоугольник образован строками 2 и 4, а также столбцами 1 левой таблицы и 5 правой таблицы. Следовательно, в биграмму шифртекста входят буква О, расположенная в столбце 5 и строке 2 правой таблицы, и буква В, расположенная в столбце 1 и строке 4 левой таблицы, т.е. получаем биграмму шифртекста ОВ.

Если обе буквы биграммы сообщения лежат в одной строке, то и буквы шифртекста берут из этой же строки. Первую букву биграммы шифртекста берут из левой таблицы в столбце, соответствующем второй букве биграммы сообщения. Вторая же буква биграммы шифртекста берется из правой таблицы в столбце, соответствующем первой букве биграммы сообщения. Поэтому биграмма сообщения ТО превращается в биграмму шифртекста ЖБ. Аналогичным образом шифруются все биграммы сообщения:

Сообщение ПР ИЛ ЕТ АЮ \_Ш ЕС ТО ГО

Шифртекст ПЕ ОВ ЩН ФМ ЕШ РФ БЖ ДЦ

Шифрование методом «двойного квадрата» дает весьма устойчивый к вскрытию и простой в применении шифр. Взламывание шифртекста «двойного квадрата» требует больших усилий, при этом длина сообщения должна быть не менее тридцати строк.

**Одноразовая система шифрования**

  Почти все применяемые на практике шифры характеризуются как условно надежные, поскольку они могут быть в принципе раскрыты при наличии неограниченных вычислительных возможностей. Абсолютно надежные шифры нельзя разрушить даже при использовании неограниченных вычислительных возможностей. Существует единственный такой шифр, применяемый на практике, - одноразовая система шифрования. Характерной особенностью одноразовой системы шифрования является одноразовое использование ключевой последовательности.

Одноразовая система изобретена в 1917 г. американцами Дж.Моборном и Г.Вернамом. Для реализации этой системы подстановки иногда используют одноразовый блокнот. Этот блокнот составлен из отрывных страниц, на каждой из которых напечатана таблица со случайными числами (ключами) Кi. Блокнот выполняется в двух экземплярах: один используется отправителем, а другой - получателем. Для каждого символа Xi сообщения используется свой ключ Кi из таблицы только один раз. После того как таблица использована, она должна быть удалена из блокнота и уничтожена. Шифрование нового сообщения начинается с новой страницы.

Этот шифр абсолютно надежен, если набор ключей Кi действительно случаен и непредсказуем. Если криптоаналитик попытается использовать для заданного шифртекста все возможные наборы ключей и восстановить все возможные варианты исходного текста, то они все окажутся равновероятными. Не существует способа выбрать исходный текст, который был действительно послан. Теоретически доказано, что одноразовые системы являются нераскрываемыми системами, поскольку их шифртекст не содержит достаточной информации для восстановления открытого текста.

Казалось бы, что благодаря данному достоинству одноразовые системы следует применять во всех случаях, требующих абсолютной информационной безопасности. Однако возможности применения одноразовой системы ограничены чисто практическими аспектами. Существенным моментом является требование одноразового использования случайной ключевой последовательности. Ключевая последовательность с длиной, не меньшей длины сообщения, должна передаваться получателю сообщения заранее или отдельно по некоторому секретному каналу. Это требование не будет слишком обременительным для передачи действительно важных одноразовых сообщений, например, по горячей линии Вашингтон - Москва. Однако такое требование практически неосуществимо для современных систем обработки информации, где требуется шифровать многие миллионы символов.

В некоторых вариантах одноразового блокнота прибегают к более простому управлению ключевой последовательностью, но это приводит к некоторому снижению надежности шифра. Например, ключ определяется указанием места в книге, известной отправителю и получателю сообщения. Ключевая последовательность начинается с указанного места этой книги и используется таким же образом, как в системе Вижинера. Иногда такой шифр называют шифром с бегущим ключом. Управление ключевой последовательностью в таком варианте шифра намного проще, так как длинная ключевая последовательность может быть представлена в компактной форме. Но с другой стороны, эти ключи не будут случайными. Поэтому у криптоаналитика появляется возможность использовать информацию о частотах букв исходного естественного языка.

**Шифрование методом Вернама**

Система шифрования Вернама является в сущности частным случаем системы шифрования Вижинера при значении модуля m = 2. Конкретная версия этого шифра, предложенная в 1926 г. Гилбертом Вернамом, сотрудником фирмы AT&T США, использует двоичное представление символов исходного текста.

Каждый символ исходного открытого текста из английского алфавита {А, В, С, D, ..., Z}, расширенного шестью вспомогательными символами (пробел, возврат каретки и т.п.), сначала кодировался в 5-битовый блок (b0, b1, …, b4) телеграфного кода Бодо.

Случайная последовательность двоичных ключей k0,k1,k2,... заранее записывалась на бумажной ленте.

Схема передачи сообщений с использованием шифрования методом Вернама показана ниже. Шифрование исходного текста, предварительно преобразованного в последовательность двоичных символов x, осуществлялось путем сложения по модулю 2 символов x с последовательностью двоичных ключей k.

Символы шифртекста

y=x Еk

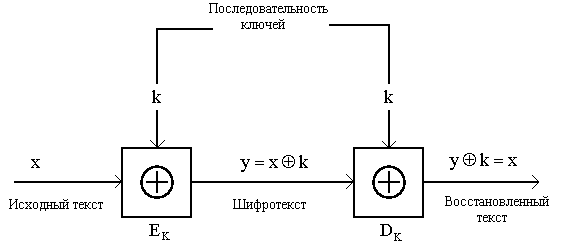


Схема шифрования и расшифрования сообщений по методу Вернама

Расшифрование состоит в сложении по модулю 2 символов у шифртекста с той же последовательностью ключей k:

y Е k = x Е k Е k = x.

При этом последовательности ключей, использованные при шифровании и расшифровании, компенсируют друг друга (при сложении по модулю 2), и в результате восстанавливаются символы x исходного текста.

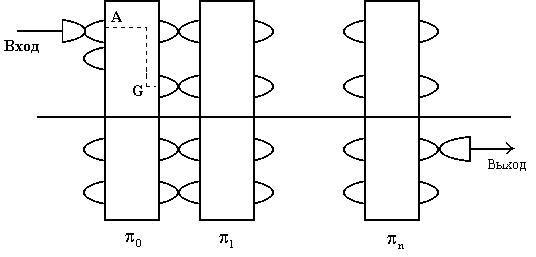
При разработке своей системы Вернам проверял ее с помощью закольцованных лент, установленных на передатчике и приемнике для того, чтобы использовалась одна и та же последовательность ключей.

Следует отметить, что метод Вернама не зависит от длины последовательности ключей и, кроме того, он позволяет использовать случайную последовательность ключей. Однако при реализации метода Вернама возникают серьезные проблемы, связанные с необходимостью доставки получателю такой же последовательности ключей, как у отправителя, либо с необходимостью безопасного хранения идентичных последовательностей ключей у отправителя и получателя. Эти недостатки системы шифрования Вернама преодолены при шифровании методом гаммирования.

**Роторные машины**

В 20-х годах XX века были изобретены электромеханические устройства шифрования, автоматизирующие процесс шифрования. Принцип работы таких машин основан на многоалфавитной замене символов исходного текста по длинному ключу согласно версии шифра Вижинера. Большинство из них - американская машина SIGABA (М-134), английская TYPEX, немецкая ENIGMA, японская PURPLE были роторными машинами.

Главной деталью роторной машины является ротор (или колесо) с проволочными перемычками внутри. Ротор имеет форму диска (размером с хоккейную шайбу). На каждой стороне диска расположены равномерно по окружности m электрических контактов, где m - число знаков алфавита (в случае латинского алфавита m = 26). Каждый контакт на передней стороне диска соединен с одним из контактов на задней стороне. В результате электрический сигнал, представляющий знак, будет переставлен в соответствии с тем, как он проходит через ротор от передней стороны к задней. Например, ротор можно закоммутировать проволочными перемычками для подстановки G вместо A, U вместо В, L вместо С и т.д.



Банк роторов

При повороте ротора из одного положения в другое подстановка, которую он осуществляет в приходящем сигнале, будет изменяться. В общем случае эту подстановку можно записать в виде

T = C j p C -j

где p - подстановка, реализуемая ротором в его начальном положении; С - циклический сдвиг на одну позицию; C j - циклический сдвиг на j позиций.

Например, если начальная подстановка ротора p(А) = G и ротор сдвигается на три позиции (j = 3), то открытый текст D будет против того контакта ротора, который используется

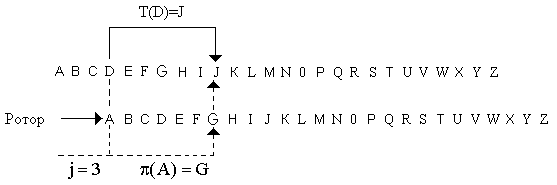


Схема формирования подстановки при сдвиге ротора (j =3) для представления открытого текста А, а шифрованный текст J окажется против того контакта ротора, который используется для представления шифрованного текста G , и результирующая подстановка Т(D) = G при j = 3. Алгебраически это записывается в виде

Т (D) = С3pС-3 (D) = С3 p (А) = С3 (G) = J.

Роторы можно объединить в банк роторов таким образом, чтобы выходные контакты одного ротора касались входных контактов следующего ротора. При этом электрический импульс от нажатой клавиши с буквой исходного текста, входящий с одного конца банка роторов, будет переставляться каждым из роторов, до тех пор, пока не покинет банк.

Такой банк может реализовывать большое число подстановок, соответствующих различным комбинациям положений роторов. Для получения сильной криптографической системы расположение роторов должно меняться при переходе от знака к знаку сообщения.

Роторная машина состоит из банка роторов и механизма для изменения положения роторов с каждым зашифрованным знаком, объединенного с устройствами ввода и вывода, такими как устройство считывания с перфоленты и печатающее устройство.

Простейшее из возможных движений ротора - это движение по принципу одометра; оно использовалось в немецкой машине Enigma во время второй мировой войны. При шифровании одного знака правое крайнее колесо поворачивается на одну позицию. Когда это (и любое другое) колесо переместится на m позиций и совершит полный оборот, колесо, расположенное слева от него, передвинется на одну позицию, и процесс будет повторяться. Этот процесс проведет банк роторов сквозь все его возможные положения, прежде чем цикл повторится. Поскольку все роторы перемещаются с разными скоростями, период n-роторной машины составляет 26n (при m = 26).

Для закона движения ротора желательны следующие характеристики:

* период должен быть большим;
* после шифрования каждого знака все роторы или большая их часть должны повернуться друг относительно друга.

Движение по принципу одометра оптимально в смысле первого требования, но совершенно неудовлетворительно в отношении второго требования. Улучшение движения по принципу одометра можно получить, если поворачивать каждый ротор более чем на одну позицию. Если смещения каждого ротора не имеют общих множителей с объемом алфавита m, то период останется максимальным.

Другое решение заключается в ограничении числа допустимых остановочных мест для каждого ротора за счет введения внешнего фиксирующего кольца, на котором определенным способом зафиксированы места остановок. При использовании латинского алфавита можно заставить машины поворачиваться и останавливаться следующим образом. Первому колесу разрешается останавливаться в каждой из 26 позиций, второму колесу - только в 25 позициях, третьему колесу - только в 23 позициях, и так далее до шестого колеса, которому разрешается останавливаться только в 17 позициях. Период такой роторной машины теперь составляет 101 млн, а не 266»309 млн, как в случае движения по принципу одометра. Потеря в длине периода с успехом окупается полученной сложностью движения роторов. Теперь второе требование удовлетворяется довольно хорошо, поскольку каждое из колес перемещается после шифрования каждого знака и многие колеса могут двигаться друг относительно друга.

Роторная машина может быть настроена по ключу изменением любых ее переменных:

* роторов;
* порядка расположения роторов;
* числа мест остановки на колесо;
* характера движения и т.д.

Поскольку перекоммутировать роторы трудно, то обычно на практике машины обеспечивали комплектом роторов, в котором находилось больше роторов, чем можно одновременно поместить в машину. Первичная настройка по ключу производилась выбором роторов, составляющих комплект. Вторичная настройка по ключу производилась выбором порядка расположения роторов в машине и установкой параметров, управляющих движением машины. С целью затруднения расшифрования шифртекстов противником роторы ежедневно переставляли местами или заменяли. Большая часть ключа определяла начальные положения роторов (2б3=17576 возможных установок) и конкретные перестановки на коммутационной доске, с помощью которой осуществлялась начальная перестановка исходного текста до его шифрования (26!= 4·1026 возможностей).

Роторные машины были самыми важными криптографическими устройствами во время второй мировой войны и доминировали по крайней мере до конца 50-х годов.

**Варианты заданий:**

1) Реализовать шифрование текстового сообщения, используя любой нестандартный метод перестановки, например, менять местами четные и не четные символы. Использование данного метода в этом варианте лабораторной работы не запрещается, но желательно проявить инициативу.

2) Реализовать шифрование текстового сообщения, используя метод шифрования с подстановкой степени *n*.

3) Реализовать шифрование текстового сообщения, используя метод шифрования с любой маршрутной перестановкой.

4) Реализовать шифрование текстового сообщения, используя шифр «Сцитала».

5) Реализовать шифрование текстового сообщения, используя шифр «Поворотная решетка».

6) Реализовать шифрование текстового сообщения, используя шифр вертикальной перестановки.

7) Реализовать шифрование текстового сообщения, используя шифр «Полибианский квадрат».

8) Реализовать шифрование текстового сообщения, используя систему шифрования Цезаря.

9) Реализовать шифрование текстового сообщения, используя аффинную систему подстановок Цезаря.

10) Реализовать шифрование текстового сообщения, используя систему Цезаря с ключевым словом.

11) Реализовать шифрование текстового сообщения, используя шифрующие таблицы Трисемуса.

12) Реализовать шифрование текстового сообщения, используя биграммный шифр Плейфейра.

13) Реализовать шифрование текстового сообщения, используя систему омофонов.

14) Реализовать шифрование текстового сообщения, используя шифр Гронсфельда.

15) Реализовать шифрование текстового сообщения, используя систему шифрования Вижинера .

16) Реализовать шифрование текстового сообщения, используя шифр «двойной квадрат» Уитстона.

17) Реализовать шифрование текстового сообщения, используя метод одноразовой системы шифрования.

18) Реализовать шифрование текстового сообщения, используя шифрование методом Вернама.

19) Реализовать шифрование текстового сообщения, используя шифр «Роторные машины».