Шифрование методами замены

Допустим, что устройства читателя подвергаются атаке со стороны неизвестного хакера.

Нарушитель, хакер, злоумышленник не ограничивается выводом из строя устройств. Он их перепрограммирует с целью принудить владельца выполнять какие-то требования либо банального вымогательства у владельца устройств некоторой денежной суммы. Объявляет о требованиях, например, звонком по сотовому телефону и диктует условия (цену) за восстановление работоспособного состояния устройства. Информационная подсистема приборов защищена шифрами разной сложности. Нарушитель использует свои параметры этих разных шифров для затруднения владельцу самостоятельно восстановить работоспособность устройств.

Некоторые положения теории криптологии

***Математическая модель*** произвольного ***шифра*** замены SА = (Х, К, Y, E, D), где

X – символ (фрагмент) открытого текста в алфавите А, |A| = n;

Y– символ шифртекста в алфавите В, |B| = m;

K – ключ шифра k =1(1)K; Ek – преобразование зашифрования с ключом kз;

Dk – преобразование расшифрования с ключом kp.

Правило зашифрования произвольного шифра замены yj ∊ фk(хj), j = 1(1)J , j = 1(1)J.

***Требования к криптографической системе*** (КГС)

* реализуемость и неизменность шифралгоритма программная и аппаратная;
* преобразования, используемые в шифралгоритме должны быть обратимыми;
* владение шифралгоритмом не должно способствовать вскрытию ключ;
* совпадение объемов (длина шифрованного равна длине исходного) текстов;
* любой возможный ключ должен обеспечивать равновероятную защиту;
* отсутствие просто устанавливаемых зависимостей между ключами в сеансах связи;
* прочтение шифртекста только с соответствующим ключом;
* малые изменения ключа должны существенно менять шифртекст прежнего исходного;
* малые изменения исходного текста при одном ключе существенно меняют шифртекст;
* дополнительные символы к исходному тексту надежно скрываются в шифтексте;
* число операций в атаке перебором ключей ограничивается возможностями компьютера;
* число операций при атаке на ключ должно быть не меньше числа возможных ключей.

Требования к криптографическим примитивам.

* биективность (при n=m), регулярность или (n,m,k)-эластичность векторного отображения;
* высокая степень корреляционной иммунности;
* большая алгебраическая степень и высокая нелинейность;
* низкие автокорреляционные показатели, обеспечение строгого лавинного критерия.

***Классификация шифров***. Признак - тип преобразования зашифрования открытого текста порождает при замене символа (фрагмента) Х на эквивалентный символ Y шифртекста: *шифр замены*; получение шифртекста перестановкой символов открытого текста порождает *шифр перестановки*; зашифрование последовательно открытого текста двумя или более разными шифрами порождает *композиционный шифр*.

При совпадении ключей зашифрования и расшифрования kз= kр в шифрах замены возникает *симметричный шифр;* при несовпадении ключей kз*≠* kр *асимметричный шифр*. Если в преобразованиях используются неоднозначные функции возникает шифр *многозначной замены* (*пропорциональной* *замены*, *омофоны*); *шифр однозначной замены* (*шифр гаммирования*) возникает в случае использования однозначных функций. Правило зашифрования для шифра однозначной замены yj = ф(хj), j = 1(1)J , j = 1(1)J.

*Шифр равнозначной замены* возникает при выборе шифрующего символа yi из алфавита В, |B| = m, yi ∊ Вq, i =1(1)N; иначе возникает *шифр разнозначной замены*. Для шифров замены часто используют V∊Ар, для некоторого р∊N. При р = 1 возникают *поточные шифры*; при р>1 возникают *блочные шифры замены*.

При использовании в процессе шифрования единственного алфавита шифр замены называют *одноалфавитным шифром замены* или *шифром простой замены*. В других случаях - *многоалфавитным шифром замены*. С шифрами перестановки ситуация более простая. Открытый текст размещают перед шифрованием в таблицу, например, a×b =4×7. Шифрованный текст пишем по столбцам пнотртйаиупнмреоешрвррекмаси. Это *шифр маршрутной перестановки*.



Открытый текст прочитывается в первой строке, затем последний символ второй строки и далее справа налево, не прерываясь, в третьей и четвертой строках. Слова в клетки вписаны без пробелов

Аналогично формируются *столбцовые (строчные) перестановки*.Усложнение возможно путем введения ключа k = <3,5,7,1,4,2,6>, указывающего порядок чтения столбцов, или "хитрого" обхода ячеек таблицы, например, таблицу a×b =8×8 обходом шахматного коня.

Для защиты информационной подсистемы «умного» устройства используется простая криптографической система, использующая алфавит естественного языка (русского). В сценарии участвуют два субъекта: владелец устройства и хакер. Владелец знает, что алфавит естественного языка (ЕЯ) предварительно подвергается преобразованию путем умножения на известную ему перестановку 32 степени. Буквы е и ё считаются одной буквой поэтому размерность алфавита не 33, а 32 буквы. Тексты пишутся без пробелов.

Задача читателя, который получил доступ к смешанному алфавиту, состоит в полном восстановлении работоспособности умного устройством (текстов команд), получении возможности замены смешанного алфавита другим (собственным) и зашифровании на его основе текстов (команд управления), которые появляются на экране устройства.

Отметим, что при работе с шифрами учитываются ***законы естественных языков*** (ЕЯ):

* закон избыточности текстов,
* закон частоты встречаемости элементов (букв, слов, n-грамм ) текста,
* закон Ципфа-Мандельброта.

Простая одноалфавитная замена (без ключа)

Задача №1

Устройство перестало подчиняться командам (отказало), подверглось атаке нарушителя. После простейших проверок наличия внешних дефектов, энергоинтерфейсов, запаха горелой проводки изоляции не чувствуется, а на экранчике дисплея появилось (см. ниже

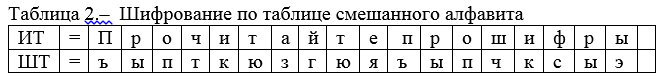
Зашифрованное сообщение №1

ъ ы п т к ю з г ю я ъ ы п ч к с ы э

Это набор из 18 символов {ъыпткюзгюяъыпчксыэ}, кажущийся бессмысленным. Но на самом деле нарушитель что-то сообщает владельцу на экране и исключает возможность использования устройства по назначению. Попробуем расшифровать оставленное злоумышленником сообщение. Для этого сформируем в таблице 1 перестановку, т.е. последовательность символов (букв) смешанного алфавита (четвертая строка).

Вторая строка частота встречаемости букв (в тысячных долях) естественного алфавита (третья строка), последняя (четвертая строка) содержит переставленные перестановкой Р 32 степени буквы ЕЯ

**Шифрование текста нарушителем.** В регистр загружается открытый текст и заменяем каждую его букву символом из 4-й строки (табл. 1), этот символ появляется на экране устройства (вторая строка таблицы 2)

При расшифровании символы верхней строки вписываются по мере их раскрытия, а вторая строка заполняется, считывается с экрана, взломанного устройства

Частоты встречаемости символов каждой пары «***х***и» → «***у***ш» в этом шифре совпадают, но так как шифртекст имеет малый объем, то частоты его символов накапливаются по многим шифртекстам. Здесь обозначены «***х***и» - символ исходного, а «***у***ш» – символ шифрованного текстов.

**Расшифрование текста с экрана.** С каждым символом хакерского шифртекста экрана последовательно входим в таблицу 1 (нижняя строка) и в третьей ее строке находим соответствующий символ исходного (не шифрованного, открытого) текста хакера. Пройдя все 18 символов удается восстановить текст от хакера, его пожелание владельцу устройства "прочитайте про шифры".

Одноалфавитная замена с ключом

Задача №2

Для увеличения стойкости шифра к атакам, использующим частотный закон ЕЯ, в этом шифре используется не только смешанный алфавит, но вводится новый элемент в алгоритм шифрования, называемый ключом.

**Определение.** Ключом называется секретная последовательность символов алфавита (слово) фиксированной длины, возможно осмысленная, что совсем не обязательно, используемая при преобразовании открытого текста в шифрованный и обратно.

Таким образом, к характеристикам ключа относятся:

* доступность – закрытый, открытый (в двухключевых шифрах),
* алфавит – языка страны,
* длина – число букв (символов),
* состав – названия всех букв ключа,
* порядок – следование букв состава ключа (осмысленный или нет),
* срок – длительность использования.

Введение в алгоритм шифрования нового элемента «ключа» способствует при замене символа «х» открытого текста символом «у» шифрованного текста при очередном повторном появлении символа «х» заменить его не символом «у», как первый раз, а каким-то другим, на который укажет символ ключа. Подсчет нарушителем встречаемости символов открытого и шифрованного текста, не позволяет ему правильно сопоставлять пары таких символов, так как частота символов шифртекста стала отличной от прежней. Действительно, одному символу открытого текста стали соответствовать несколько разных символов шифртекста. Наглядно это увидим на конкретном примере.

Пусть, как и раньше, на экране устройства хакер написал свой текст (он изменился):

Зашифрованное сообщение №2

ю я и ю ю я и ю ю я и ю ю я и ю ю я

Этот текст возник иначе, чем в задаче 1, т.е. другим путем (с использованием ключа) отличным от способа шифрования в задаче 1. В качестве ключа используется короткое 4-х буквенное слово «ТЕСТ».

**Шифрование.** В таблице 3 верхняя строка заполнена открытым текстом хакера, а под ней выписан многократно без пробелов ключ ТЕСТ. В третью строку вписываются символы шифрованного текста, взятые из последней строки таблицы 1

Заливкой выделены повторяющиеся группы из 4-х символов, что может указывать на длину ключа

Шифртекст получился «не очень» впечатляющим, так сработал усовершенствованный новый алгоритм шифра. Действительно одной букве шифртекста стали соответствовать разные буквы открытого текста и наоборот - букве открытого несколько букв шифртекста.

**Расшифрование текста с экрана**. В тексте легко выделяются повторяющиеся части (юяию -4 символа). Это наводит на мысль, что породил такие части не исходный текст, а именно ключ. Этот ключ содержит 4 символа, причем 1-й и 4-й символы, по-видимому, совпадают. Частоты символов позволяют установить состав букв ключа. Легко в ключе определяется только его длина. Состав символов и их порядок определится путем рассмотрения допустимых сочетаний по 4 символа из алфавита ЕЯ.

Задача №3

**Шифрование.** Для увеличения стойкости шифра к атакам, использующим частотный закон ЕЯ, в этом шифре используется не только смешанный алфавит, но вводится новый элемент в алгоритм шифрования, называемый ключом. Как влияет длина ключа на шифртекст? Изменим (увеличим на 1 символ) длину ключа. В таблице 4 верхняя строка заполнена открытым текстом хакера, а под ней выписан многократно без пробелов ключ ТЕКСТ. В третью строку вписываются символы смешанного алфавита, взятые из последней строки таблицы 1

Пусть, как и раньше, на экране устройства хакер (нарушитель) написал свой текст:

Зашифрованное сообщение №3 (текст опять изменился)

ю я л и ю ю я л и и ю ю я л и ю ю я л



Получилась очень похожая на предыдущую картинка, просто повторов стало меньше, а длина ключа возросла на 1 символ.

**Расшифрование текста с экрана.** В тексте легко выделяются повторяющиеся части (юялию - 5 символов). Это наводит на мысль, что породил такие части не сам исходный текст, а именно новый ключ. Этот ключ содержит 5 символов, причем 1-й и 5-й символы, по-видимому, совпадают. Частоты символов позволяют установить состав букв ключа. О новом ключе можно сказать практически то же самое. Ключ имеет длину 5-символов, и его 1-й и 5-й символы совпадают. Состав подбирается путем допустимых сочетаний по 5 символов из алфавита ЕЯ.

**Многоалфавитная замена с ключом, гаммирование**

Рассмотрение проблемы с атакой на шифры, которая использует частотные зависимости ЕЯ, привело к мысли использовать в алгоритме шифрования не только ключ, что как мы видели в задачах 2,3 оказалось не очень удачным решением (легко определяется длина ключа, повторяющиеся символы), но и более чем один (множество) смешанных алфавитов.

Ниже мы подробно рассмотрим схему шифрования с этими нововведениями и некоторые факторы, влияющие на стойкость шифра к атакам

Задача №4

В этой задаче используется множество смешанных алфавитов, организованных в квадрат Виженера, а ключи используются прежние.

Для увеличения стойкости шифра к атакам, использующим частотный закон ЕЯ, в этом шифре используется не единственный смешанный алфавит, а их множество с применением циклического сдвига каждого последующего на один символ относительно предыдущего. Вытолкнутый циклическим сдвигом символ из начала алфавита помещается в конец списка букв алфавита так, что полная длина алфавите не меняется.

При одноалфавитной замене без ключа всегда символ «х» (буква) исходного (открытого) текста заменялась одной и той же буквой «у» смешанного алфавита, и частота использования х и у была одинаковой, совпадающей с частотой встречаемости символа «х» в ЕЯ. При многоалфавитной замене нарушитель понимает, что символ «х» при каждом очередном появлении в открытом тексте заменяется разными буквами из разных смешанных алфавитов. Этот факт не дает возможности нарушителю напрямую воспользоваться частотным законом ЕЯ, так как частота встречаемости символов открытого текста осталась прежней, но частота встречаемости символов шифрованного текста стала совершенно другой.

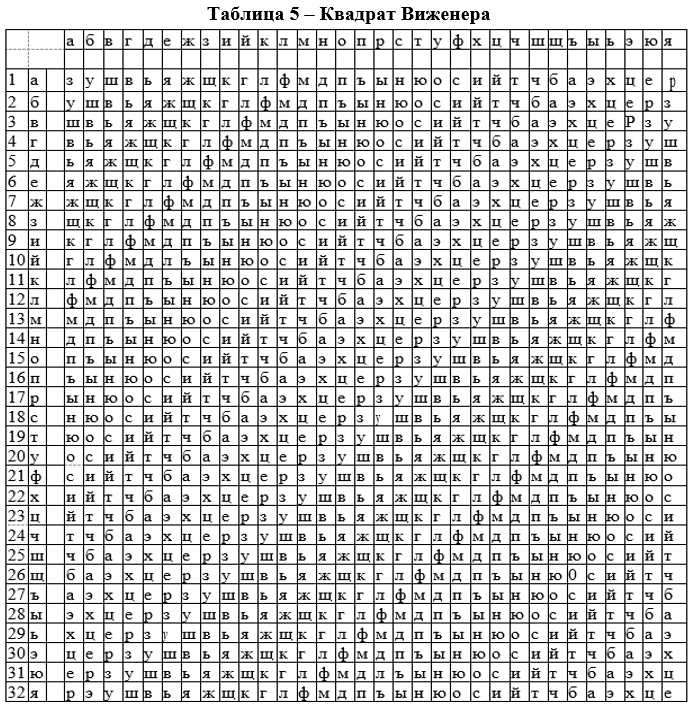
Зашифрованное сообщение №4 (текст опять изменился)

у и р г а т н э ь л з ш з ц ч ж ш з

Что же такое нарушитель желает сообщить владельцу «умного» устройства? Стремление разобраться в шифрованном сообщении приводит к необходимости детального анализа ситуации с шифрами и текстами открытыми и шифрованными. Прежде всего, необходимо уяснить как будет использоваться множество смешанных алфавитов, какое их количество задействуется в алгоритме и как эти алфавиты соотносятся друг с другом. Ответ на эти вопросы помогает найти новая таблица 5, названная квадратом ***32×32*** (таблицей) Виженера. Сколько смешанных алфавитов следует привлекать в алгоритме шифра? Как выбрать ключ шифра?

Строкам таблицы Виженера соответствуют символы (буквы) ключа. Из этого следует, что при шифровании используются столько строк квадрата Виженера, сколько букв содержит ключ шифра (при условии отсутствия повторов). Так как ключом может быть произвольная последовательность букв, то строкам квадрата соответствует полный алфавит. Колонкам квадрата соответствуют символы исходного текста – также полный алфавит.

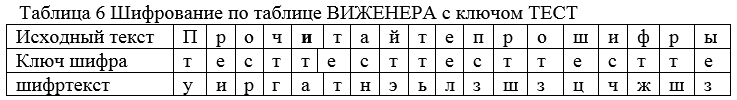
Таким образом, в этом квадрате размещаются 32 смешанных алфавита (см таблица 1) по горизонтали и по вертикали. Каждый алфавит в этих линиях сдвигается (изменяется) на один символ относительно предыдущей линии, и этот символ вписывается после последнего символа в конце списка. Верхняя строка и вторая колонка – это алфавит ЕЯ с исходным упорядочением букв, т.е. каждая строка и столбец помечены буквой стандартного алфавита.



Из множества возможных перемешиваний алфавита Б. Виженер предложил использовать только ***n = 32***. Способ их получения из первого путем циклического сдвига на каждом шаге на одну позицию.

**Процесс шифрования.** Исходный текст без пробелов вписывается в линейный регистр. Каждой букве отводится своя ячейка регистра. Ниже этого регистра помещается другой регистр, в который вписывается ключ ТЕСТ шифра. Если ключ шифра короче текста, то ключ вписывается многократно один за другим без пробелов. Таким образом, каждая буква исходного текста соответствует некоторой букве ключа. Это можно отобразить так «хи» → «хk».

Шифртекст представленный на экране (у и р г а т н э ь л з ш з ц ч ж ш з) устройства - это 3-я строка таблицы 6.



Первой букве открытого (столбец) текста соответствует первая буква ключа (строка) «хи =П»→«хk=т». Переходим в квадрат Виженера. Строка квадрата обозначена буквой «т» ключа, а столбец квадрата определяется буквой открытого текста «П». В клетке пересечения выбранных линий (строки, столбца) находится буква шифртекста «уш = у». Формально эти действия описываются цепочкой «хk = т» → «хи = П» → «уш = у» из трех символов: тПу.

Дальше все повторяется до исчерпания открытого текста. Результатом такого шифрования является третья строчка таблицы 6. Именно она появляется на экране дисплея умного устройства.

**Анализ текста с экрана**. Из примера для ключа "ТЕСТ" видим, что первая буква ИТ П заменяется на У, которая взята в строке квадрата, помеченной буквой Т ключа, и в колонке квадрата, соответствующей (помеченной) букве П.

Второй раз, когда буква П встречается в ИТ замена (буква 3) для нее берется в строке, ключа, помеченной буквой С (не как раньше буквой т), и в той же самой колонке для буквы П. Уже отсюда видим, что подсчет частот встречаемости буквы П в исходном тексте и символов замены для этой буквы в шифрованном тексте не совпадают, что не позволяет напрямую воспользоваться законом частоты повторяемости букв при вскрытии шифртекста.

Здесь же укажем, что при использовании ключа происходит многоалфавитная замена. Количество используемых при шифровании алфавитов в общем случае соответствует числу различных букв в ключе, но, понятно, что не более ***n = 32***. Отсюда, как казалось-бы, напрашивается вывод - больше длина ключа - надежнее шифр. К сожалению, это не всегда так.

Во-первых, в ключе могут быть повторяющиеся буквы и для них используется одна и та же строка квадрата Виженера:

Во-вторых, не исключается возможность совпадений (наложений) одинаковых непрерывных участков ИТ на одинаковые непрерывные участки ключа.

К чему это может привести будет рассмотрено на примере оцифровки для второго более длинного ключа "ТЕКСТ".

Анализ исходного текста и шифртекста с ключом ТЕСТ показывает следующее: в ИТ имеются две повторяющиеся триграммы "ПРО", в скобках за буквами пишем какими буквами они заменились в шифртексте: Р(И, Ш, Ш) встречается три раза; буквы П (У, З), О(Р З), Т(Т, Ь), И(А, Б) – по два раза; Ч(Г), А(Н),Й(Э),Е(Л),Ш(Ц),Ф(Ж),Ы(З).

Наш ограниченного объема пример позволил продемонстрировать все возможности замен. Хотя ключ ТЕСТ содержит четыре буквы, но различных среди них только три. Следовательно, при шифровании будут использованы только три различных смешанных алфавита.

Задача №5

**Процесс шифрования.** В этой задаче также используется множество смешанных алфавитов, организованных в квадрат Виженера. Используется более длинный ключ ТЕКСТ.

Первой букве открытого текста соответствует первая буква ключа «хи =П»→«хk=т».

Переходим в квадрат Виженера. Строка квадрата обозначена буквой «т» ключа, а столбец квадрата определяется буквой открытого текста «П». В клетке пересечения выбранных строки и столбца находится буква шифртекста «уш = у». Формально эти действия описываются цепочкой «хk = т» → «хи = П» → «ущ = у» из трех символов: тПу.

Дальше все повторяется до исчерпания открытого текста. Результатом такого шифрования является третья строчка таблицы 7. Именно она появляется на экране дисплея умного устройства.

Зашифрованное сообщение №5

у и ч к а ь я о в т у и ч г а ж и я

Будем пытаться прочесть это сообщение в ходе анализа шифртекста.

**Анализ и дешифрование текста с экрана**. Ключ ТЕКСТ содержит пять букв, из них различных только четыре, и с этим ключом будут использованы четыре различных смешанных алфавита. Какой же из ключей обеспечивает большую устойчивость к взлому (расшифрованию)?

Казалось-бы, тот шифр, который использует большее число различных алфавитов, что приводит к замене одной и той же буквы ИТ большим числом других букв, и лучше ее маскирует. Но, увы, это не общее правило. Наш пример призван это подтвердить.

Криптоаналитики стремятся использовать разнообразные и всесторонние подходы к задачам вскрытия шифровок. Так, например, они выявляют в ШТ повторяющиеся отрезки текста даже если шифрование было многоалфавитным. Эти отрезки могут быть однобуквенными - монограммы, двухбуквенными - биграммы, трехбуквенными - триграммы и т. д. Подсчитываем число повторяющихся отрезков и интервалы (в числе символов) между ними. Что это дает? Очень даже много.

В ШТ встречаются буквы У(П,П), Ч(О,О), А(И,И), Я(А, Ы) – по два раза, И(РРР) - 3 раза. 18 позиций сообщения представлены 12 буквами ИТ и 12 буквами ШТ, но состав этих 12 букв различен. Совпадение количества букв, конечно, случайное.

Все ситуации замены при шифровании могут быть описаны следующим перечнем:

* одинаковые буквы ИТ (П(УУ), Р(ИИИ), О(ЧЧ), И(АА),) заменяются одинаковыми в ШТ (У, И, Ч, А);
* одинаковые буквы ИТ (Т) заменяются разными в ШТ (Ь, В);
* разные буквы ИТ(Ч, А, Й, Е, Ш, Ф, Ы) заменяются разными в ШТ(К, Я, О, Т, Г, Ж, Я);
* разные буквы ИТ (А, Ы) заменяются одинаковыми в ШТ (Я).

*Определение длины ключа*. Причиной появления одной и той же буквы Y в ШТ может быть либо совпадение буквы X в ИТ и буквы ключа под ней; либо на Y была заменена другая буква из ИТ при использовании сдвинутого смешанного алфавита.

В первом случае интервалы между повторениями буквы Y в ШТ будут совпадать с числовыми значениями *кратными длине ключа*; во-втором, - понятно, совпадения ожидать не приходится. Аналогичная ситуация может иметь место и для других повторяющихся в ШТ букв.



Действительно, в исходном тексте буква Р попадает трижды на букву Е ключа ТЕКСТ во ***2***-й, ***12***-й и ***17***-й позициях и заменяется буквой И из одного и того же смешанного циклически сдвинутого алфавита. Этот алфавит в квадрате Виженера соответствует строке, помеченной буквой Е ключа. Интервалы между повторениями буквы И кратны числу ***5***. Все три интервала кратны ***5***.  
  
***17 – 12 = 5, 17 – 2 = 15, 12 – 2 = 10.***

Аналогично с буквой У в ***1*** и ***11***- й позициях ШТ, интервал ***11 – 1=10*** кратен ***5***; с буквой Ч в ***3***-й и в ***13***-й позициях ШТ; интервал равен ***13 – 3 = 10***, что также кратно ***5***. Буква Я в позициях 7-й и 18-й ШТ не удовлетворяет общему правилу ***18 – 7=11***, что не кратно ***5***, а вот буква А в ШТ в позициях 5-й и 15-й опять подчинена правилу, интервал ***15 – 5 = 10*** кратен ***5***.

Повторение буквы Я в ШТ можно считать случайностью, тем более, что мы это знаем. Правильнее было бы сказать, что это норма. Именно это и требуется для нарушения закона частоты. Для такого маленького примера многовато совпадений, но ведь он и подобран специально. Каким же может быть объяснение подобных совпадений? При таком числе совпадений на ШТ из ***18*** букв следует однозначный вывод - длина ключа равна ***5*** символам.

Как только решен этот вопрос сразу же становится возможным определение списков букв ШТ, которые были зашифрованы одним и тем же смешанным алфавитом. Не зная самого ключа, мы должны полагать, что используются пять различных алфавитов (по числу букв в ключе), т.е. пять строк квадрата Виженера.

Множество всех букв ШТ теперь можно расчленить на ***L = 5*** групп, таким образом, что в каждой группе соберутся буквы из одной строки квадрата Виженера, т. е. из одного смешанного алфавита. Таким образом удается свести задачу к нескольким последовательным, но одноалфавитной замены для каждого. А это уже задача из числа успешно решаемых. Как же осуществить разбиение букв?

Очень просто. Первая буква Т ключа ТЕКСТ соответствует некоторой строке квадрата. С другой стороны, в примере эта буква стоит в позициях ***1***-й*,* **6**- й, ***11***-й, ***16***-й. Все буквы ШТ в этих позициях заменялись буквами из одной и той же строки. Обозначим длину ключа символом ***L***, тогда в каждую ***m***-ю группу, (***m*** соответствует порядковому номеру буквы в ключе) попадают все буквы ШТ из позиций с номерами ***m + L\*i, i = 0(1)4,*** ***m = 1(1) L,*** где переменная ***i*** - порядковый номер буквы в списке букв выбираемом из одной строки квадрата Виженера. Эту часть анализа удобно представить таблицей.



Данная таблица содержит две колонки, помеченные одинаковой буквой Т ключа. Это означает, что размещенные в этих колонках буквы выбирались из одной строки квадрата Виженера. Для продолжения криптоанализа эти колонки необходимо слить вместе. Далее для всех колонок подсчитывается количество одинаковых букв в каждой - кратность ее использования в ШТ. Таблица 4 после слияния колонок для буквы Т примет следующий вид.



На этом этапе вскрытия шифрограммы перед нами встает задача выбора дальнейшего пути исследования. Если бы выборки в каждой группе были значительными (более 700 букв), то используя закон частоты встречаемости буквы, сопоставив частоту появления букв в русском языке и в каждой группе, а также учитывая семантику вскрываемого текста можно было бы и завершить решение задачи, но при малых выборках ожидать успеха на этом пути не приходится.

Что еще кроме длины можно установить по ШТ о ключе? Конечно, интерес представляет само слово или выражение, но подступы к таким данным пока не просматриваются. Имеется информация о том, что интервалы между буквами ключа в стандартном алфавите связаны со сдвигами смешанных алфавитов в квадрате Виженера. Да это так. Каждая буква стандартного алфавита имеет свой порядковый номер. Интервалы между буквами ключа могут быть вычислены. Для нашего примера эти интервалы удобно представить в виде квадратных матриц. Шапка и боковик таблиц заполняются буквами ключа, а значения в клетках -разности номеров букв в стандартном алфавите. Эти матрицы описывают величины сдвигов между используемыми смешанными.



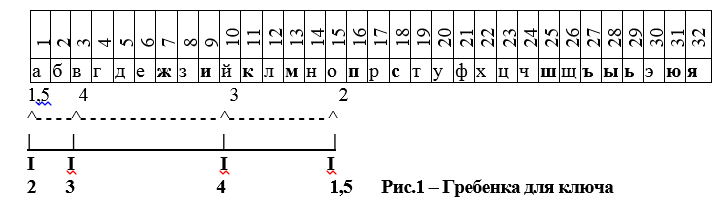
ненулевые клетки - значения расстояний между строками квадрата Виженера, задаваемые ключом

Можно ли каким-то образом получить такие матрицы, не располагая данными о ключе?

Эта информация может явиться той основой, которая позволит выявить сам ключ, т.е. слово. Ясно, что, зная величину сдвигов между алфавитами, можно пытаться подобрать слово из букв стандартного алфавита по маске, которая учитывает структуру самих сдвигов. Поиск может выполняться с использованием словарей или с визуальным контролем. Надо полагать, что ключ будет осмысленным словом или даже фразой. Это и должно использоваться при контроле в процессе поиска ключа.

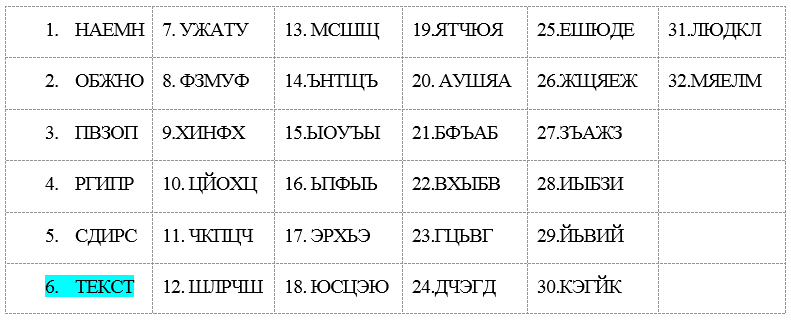
Покажем на нашем примере как такой поиск выполняется. Построим (гребенку (Рис. 1 которая будет играть роль движка или шаблона (маски). Разность между крайними отметками на гребенке равна модулю наибольшего сдвига между алфавитами. Отметим крайние положения (зубцы) гребенки номерами наиболее раздвинутых алфавитов (в примере наиболее удаленных друг от друга букв Т и Е ключа) как 1 и 2. Все другие положения на гребенке определяются относительными расстояниями (сдвигами) алфавитов, занимающих промежуточное положение между выявленными крайними.

Снабдим их соответствующей нумерацией 3, 4, 5. Теперь, если перемещать движок- гребенку вдоль стандартного алфавита, помещенного на полоске, склеенной в кольцо, и считывать буквы напротив зубцов, то оказывается, что различных положений у такого движка всего 32 по числу букв в алфавите. Соответственно и буквенных наборов, потенциально образующих ключ такое же число. Остается выяснить путем перебора какая совокупность букв с точки зрения семантики наиболее подходит в качестве ключа. Считаем, что лента с алфавитом склеена в кольцо и движок перемещается по окружности.



На самом деле вопрос о построении гребенки не так прост. В нашем примере мы знаем ключ и соответственно ему нумеровали рабочие алфавиты из квадрата Виженера. При неизвестном ключе мы можем построить гребенку, но нумерация зубцов остается невыясненной. Порядок букв в ключе (относительный) будет определен так. В примере мы крайний правый зубец гребенки снабдили номером 1, а крайний левый номером 2, что соответствует буквам Т и Е стандартного алфавита. Но, не зная ключа, можно было поместить зубцы и наоборот (зубцы на Рис.1 для второй возможности представлены в виде (“-^-“)

**Вскрытие ключа**. Приведем те совокупности букв, которые выявляются движком - гребенкой по первому варианту:



Беглый анализ этих совокупностей после прочтения показывает, что совсем непросто получить осмысленный текст при произвольном выборе гребенки. Даже похожих на осмысленные слова совокупностей практически нет. Первая совокупность могла бы быть подозрительной на ключ с учетом того, что допущена ошибка в длине ключа и ключом является слово НАЕМНИК.

Но среди всего этого имеется одно единственное вполне осмысленное слово ТЕКСТ (выделено заливкой) и, конечно, только оно может быть принято в качестве ключа.