

Оглавление

| | |
|---|-----|
| Лабораторная работа №1. Шифры перестановки | 2 |
| Лабораторная работа №2. Шифры замены..... | 18 |
| Лабораторная работа №3. Шифры гаммирования..... | 51 |
| Лабораторная работа №4. Электронная цифровая подпись | 83 |
| Лабораторная работа №5. Стеганография | 96 |
| Лабораторная работа №6. Перестановочные шифры..... | 128 |
| Лабораторная работа №7. Шифрование с помощью аналитических преобразований | 135 |
| Вопросы к зачету по предмету «Программно-аппаратные средства защиты информации..... | 142 |

Лабораторная работа №1. Шифры перестановки

Основы шифрования

Перестановка представляет собой способ шифрования, при котором для получения шифрограммы символы исходного сообщения меняют местами. Типичным примером перестановки являются анаграммы, ставшие популярными в XVII в. Анаграмма (греч. *ανα* - «снова» и *γράφω* - «запись») - литературный приём, состоящий в перестановке букв или звуков определённого слова (или словосочетания), что в результате даёт другое слово или словосочетание. Например: апельсин - спаниель, полковник - клоповник, горилка - рогалик, лепесток - телескоп.

Прародителем анаграммы однако считают поэта и грамматика Ликофрона, который жил в Древней Греции в III веке до н. э. Как сообщал византийский автор Иоанн Цец, из имени царя Птолемея он составил первую из известных нам анаграмм: Ptolemaios - Apo Melitos, что в переводе означает «из мёда», а из имени царицы Арсинои: Arsinoe - Ion Eras («фиалка Геры»). В XVII—XIX вв. среди естествоиспытателей было принято зашифровывать свои открытия в виде анаграмм, что служило двум нуждам: скрыть гипотезу до её окончательной проверки и утвердить авторство на открытие, когда оно будет подтверждено. Так, в 1610 г. Галилео Галилей для закрепления авторства на открытие спутников Сатурна зашифровал латинскую фразу «*Altissimum planetam tergeminum observavi*» («Высочайшую планету тройную наблюдал») следующим образом: «*Smaismrmilmepoetaleumibunenugttauiras*» (буквы «v» и «u» в латинских текстах часто считались взаимозаменяемыми).

Доподлинно не известно, когда появился шифр перестановки, но вполне возможно, что писцы в древности переставляли буквы в имени своего царя ради того, чтобы скрыть его подлинное имя или в ритуальных целях.

Все шифры перестановки делятся на два подкласса:

- шифры одинарной (простой) перестановки. При шифровании символы перемещаются с исходных позиций в новые один раз;

- шифры множественной (сложной) перестановки. При шифровании символы перемещаются с исходных позиций в новые несколько раз.

В те времена самой дальней из известных («высочайшей») планет был Сатурн. В действительности, в силу несовершенства телескопа, используемого Галилеем, он наблюдал не спутники, а кольца Сатурна, которые выступали по краям планеты. Эти выступы («ушки») и были приняты им за спутники. Свою гипотезу о них в виде анаграммы Галилей отослал Иоганну Кеплеру, который, потратив множество сил, перевел ее как «*Salve umbistineum geminatum Martia proles*» (лат., «Возрадуйтесь, два протуберанца - сыны Марса»). Кеплер не обратил внимание на то, что в его переводе была лишняя буква, т.к. по его соображениям у Марса должны были быть два спутника, неоткрытые на тот момент. Спутники Марса (Фобос и Деймос) были открыты американским астрономом Асафом Холлом позже - в 1877 г.

Шифры одинарной перестановки

В общем случае для данного класса шифров при шифровании и дешифровании используется таблица перестановок.

| | | | | |
|-------|-------|-------|-----|-------|
| 1 | 2 | 3 | ... | n |
| I_1 | I_2 | I_3 | ... | I_n |

Рисунок 1 - Таблица перестановок

В первой строке данной таблицы указывается позиция символа в исходном сообщении, а во второй – его позиция в шифрограмме. Таким образом, максимальное количество ключей для шифров перестановки равно $n!$, где n – длина сообщения.

С увеличением числа n значение $n!$ растет очень быстро ($1! = 1$, $5! = 120$, $10! = 3628800$, $15! = 1307674368000$). При больших n для приближенного вычисления $n!$ можно воспользоваться формулой Стирлинга

$$n! \approx \sqrt{2\pi n} * \left(\frac{n}{e}\right)^n \quad (1)$$

Шифр простой одинарной перестановки. Для шифрования и дешифрования используется таблица перестановок, аналогичная показанной на рисунке 2.

| | | | | | | |
|---|---|---|---|---|---|---|
| 1 | 2 | 3 | 4 | 5 | 6 | 7 |
| 2 | 4 | 1 | 7 | 6 | 5 | 3 |

Рисунок 2- Таблица перестановок

Например, если для шифрования исходного сообщения «АБРАМОВ» использовать таблицу, представленную на рисунке 2, то шифрограммой будет «РАВБОМА». Для использования на практике такой шифр не удобен, так как при больших значениях n приходится работать с длинными таблицами и для сообщений разной длины необходимо иметь свою таблицу перестановок.

Шифр блочной одинарной перестановки. При использовании этого шифра задается таблица перестановки блока символов, которая последовательно применяется до тех пор, пока исходное сообщение не закончится. Если исходное сообщение не кратно размеру блока, тогда оно при шифровании дополняется произвольными символами.

| | | |
|---|---|---|
| 1 | 2 | 3 |
| 2 | 3 | 1 |

Рисунок 3- Таблица перестановок

Для примера выберем размер блока, равный 3, и примем таблицу перестановок, показанную на рисунке 3. Дополним исходное сообщение

«АБРАМОВ» буквами **Б** и **Э**, чтобы его длина была кратна 3. В результате шифрования получим «РАБОАМЭВЬ».

Количество ключей для данного шифра при фиксированном размере блока равно $m!$, где m – размер блока.

Шифры маршрутной перестановки. Широкое распространение получили шифры перестановки, использующие некоторую геометрическую фигуру (плоскую или объемную). Преобразования состоят в том, что в фигуру исходный текст вписывается по ходу одного маршрута, а выписывается по-другому. Один из таких шифров – шифр «Считала»:

Греческим поэтом Архилохом, жившим в VII веке до н.э., упоминается устройство под названием **считала** (греч. σκυτάλη - жезл). Достоверно известно, что считала использовалась в войне Спарты против Афин в конце V века до н. э. Оно представляет собой цилиндр (иногда жезл командующего) и узкую полоску пергамента, обматывавшуюся вокруг него по спирали, на которой в свою очередь писалось сообщение.



Рисунок 4 - Считала

Шифруемый текст писался на пергаментной ленте по длине палочки, после того как длина палочки оказывалась исчерпанной, она поворачивалась и текст писался далее, пока либо не заканчивался текст, либо не исписывалась вся пергаментная лента. В последнем случае использовался очередной кусок пергаментной ленты. Для расшифровки адресат использовал палочку такого же

диаметра, на которую он наматывал пергамент, чтобы прочесть сообщение. Античные греки и спартанцы в частности, использовали этот шифр для связи во время военных кампаний. Однако такой шифр может быть легко взломан. Например, метод взлома сцитары был предложен ещё Аристотелем. Он состоит в том, что не зная точного диаметра палочки, можно использовать конус, имеющий переменный диаметр и перемещать пергамент с сообщением по его длине до тех пор, пока текст не начнёт читаться - таким образом дешифруется диаметр сцитары.

Шифр табличной маршрутной перестановки. Наибольшее распространение получили шифры маршрутной перестановки, основанные на таблицах. При шифровании в такую таблицу вписывают исходное сообщение по определённому маршруту, а выписывают (получают шифрограмму) - по-другому. Для данного шифра маршруты вписывания и выписывания, а также размеры таблицы являются ключом.

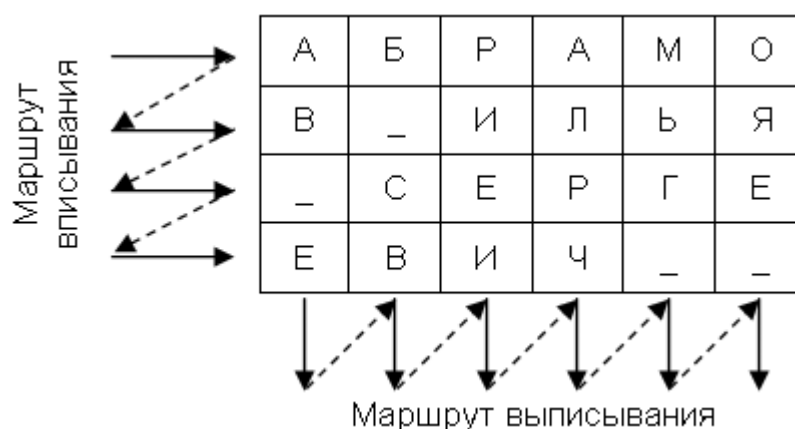


Рисунок 5 - Пример использования шифра маршрутной перестановки

Например, исходное сообщения «АБРАМОВ ИЛЬЯ СЕРГЕЕВИЧ» вписывается в прямоугольную таблицу размерами 4х6, маршрут вписывания — слева-направо сверху-вниз, маршрут выписывания — сверху-вниз слева-направо. Шифрограмма в этом случае выглядит «АВ_ЕБ_СВРИЕИАЛРЧМЫГ_ОЯЕ_».

Шифр вертикальной перестановки. Является разновидностью предыдущего шифра. К особенностям шифра можно отнести следующие:

- количество столбцов в таблице фиксируется и определяется длиной ключа;
- маршрут вписывания - строго слева-направо сверху-вниз;
- шифрограмма выписывается по столбцам в соответствии с их нумерацией (ключом).

| | | | | | | |
|-------|---|---|---|---|---|---|
| Ключ | Д | Я | Д | И | Н | А |
| | 2 | 6 | 3 | 4 | 5 | 1 |
| Текст | А | Б | Р | А | М | О |
| | В | – | И | Л | Ь | Я |
| | – | С | Е | Р | Г | Е |
| | Е | В | И | Ч | – | – |

Рисунок 6 - Пример использования шифра вертикальной перестановки

В качестве ключа можно использовать слово или фразу. Тогда порядок выписывания столбцов соответствует алфавитному порядку букв в ключе. Например, если ключевым словом будет «ДЯДИНА», то присутствующая в нем буква **А** получает номер 1, **Д** – 2 и т.д. Если какая-то буква входит в слово несколько раз, то ее появления нумеруются последовательно слева направо. В примере первая буква **Д** получает номер 2, вторая **Д** – 3.

При шифровании сообщения «АБРАМОВ ИЛЬЯ СЕРГЕЕВИЧ» результат будет «ОЯЕ_АВ_ЕРИЕИАЛРЧМЬГ_Б_СВ».

Шифр «Перекресток». Для перемешивания букв могут использоваться фигуры специального вида. Один из таких способов носит название «перекресток». В приведенном ниже примере рисуют крестообразные фигуры в

количестве, достаточном, чтобы разместить в них все буквы сообщения. Открытый текст записывают вокруг этих фигур заранее оговоренным способом - в нашем случае по часовой стрелке. Таким образом, сообщение «АБРАМОВ ИЛЬЯ СЕРГЕЕВИЧ» может выглядеть следующим образом:

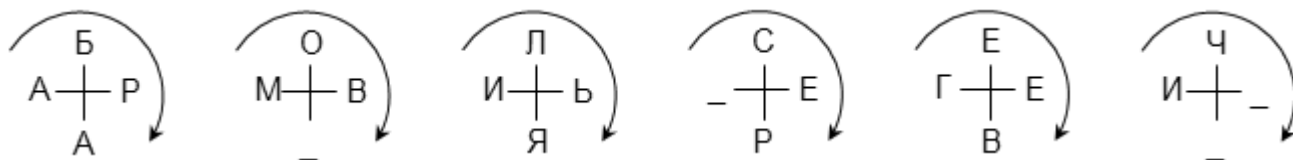


Рисунок 7 - Пример размещения открытого текста в шифре «Перекресток»

Буквы берутся построчно. Вначале берется оговоренное количество букв (N) из первой строки, затем удвоенное количество букв (2N) из второй и снова N букв из третьей строки. Например, при $N = 3$ шифрограмма будет выглядеть «БОЛАРМВИЬА_ЯСЕЧ_ЕГЕИ_РВ_».

Шифры с использованием треугольников и трапеций. Помочь выполнить перестановки могут как треугольники, так и трапеции. Открытый текст вписывается в эти фигуры в соответствии с количеством слов и формой выбранной фигуры, которая может быть растянута или сжата, чтобы в ней поместилось сообщение. Для первой фигуры, треугольника, открытый текст записывается построчно от вершины до основания.

Позднее был предложен шифр «поворотная решетка» или, как его еще называют, «решетка для вьющихся растений», поскольку она напоминала отверстия в деревянных решетках садовых строений. Этот шифр считают первым **транспозиционным** (геометрическим) шифром.

Несмотря на то, что между изначальным предложением Кардано и шифром «поворотная решетка» большая разница, методы сокрытия информации, основанные на использовании трафаретов, принято называть «решетками Кардано».

Для шифрования и дешифрования с помощью данного шифра изготавливается прямоугольный трафарет с четным количеством строк и столбцов. В трафарете вырезаются клетки таким образом, чтобы при наложении его на таблицу того же размера четырьмя возможными способами, его вырезы полностью покрывали все ячейки таблицы ровно по одному разу.

При шифровании трафарет накладывается на таблицу. В видимые ячейки таблицы выписываются буквы исходного текста слева-направо сверху-вниз. Далее трафарет поворачивается и вписывается следующая часть букв. Эта операция повторяется еще два раза. Шифрограмму выписывают из итоговой таблицы по определенному маршруту.

Таким образом, ключом при шифровании является трафарет, его исходное положение, порядок поворотов и маршрут выписывания.

Пример шифрования сообщения «АБРАМОВ+ДЯДИНА» показан на рисунок 8. Результат шифрования – «АДВ_МНРДБЯ+_ОААИ».

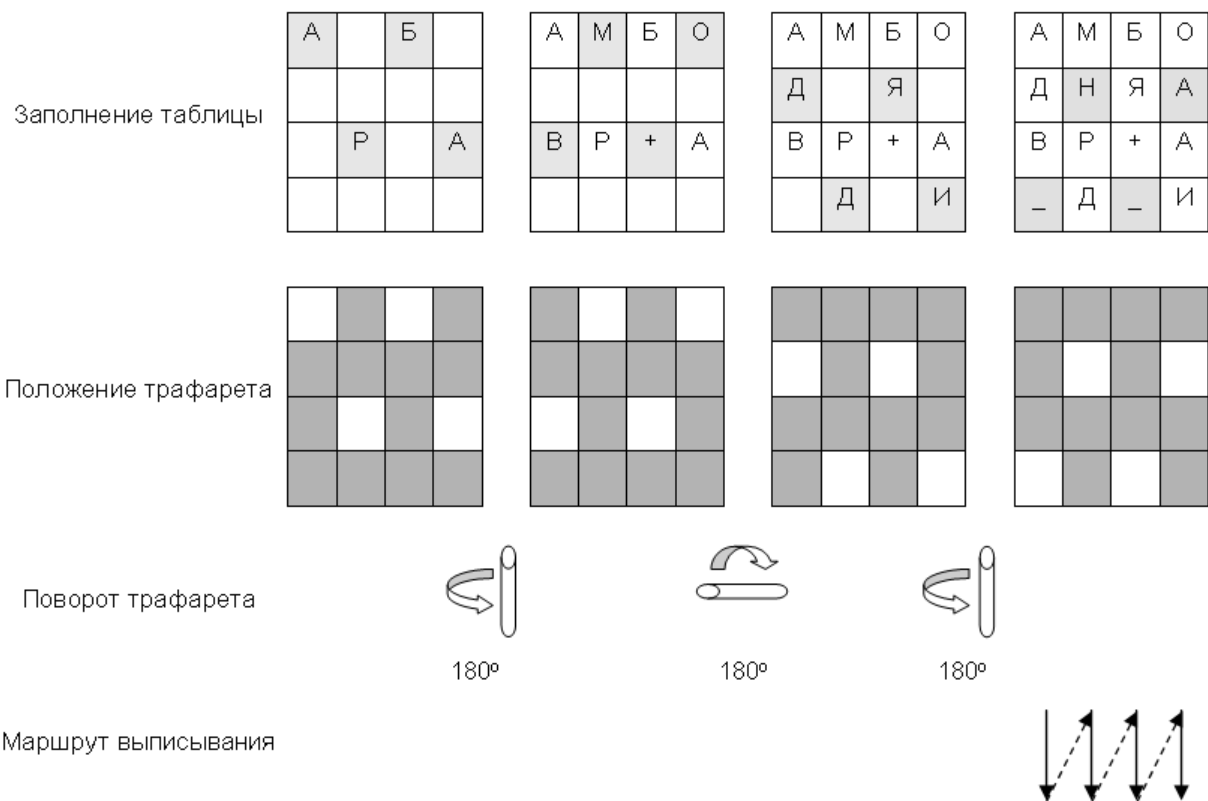


Рисунок 9 - Пример использования шифра «поворотная решетка»

Данный метод шифрования применялся нидерландскими правителями для секретных посланий в 1740-х гг. Он также использовался в армии кайзера Вильгельма в Первую мировую войну. Для шифрования немцы использовали решетки разных размеров, которым французские криптоаналитики дали собственные кодовые имена: Анна (25 букв), Берта (36 букв), Дора (64 буквы) и Эмиль (81 буква). Однако использовались решетки очень недолго (всего четыре месяца) к огромному разочарованию французов, которые только-только начали подбирать к ним ключи.

Магические квадраты. Магическими [нормальными] квадратами называются квадратные таблицы со вписанными в их ячейки последовательными натуральными числами начиная с 1, которые в сумме по каждому столбцу, каждой строке и главным диагоналям дают одно и то же число.

Впервые эти квадраты появились в Китае, где им и была приписана некоторая «магическая сила». По преданию, описанному в одной из пяти

канонических книг Древнего Китая - Шу-Цзин (Книге записанных преданий), в 2200 году до н.э. из реки Ло вышла огромная черепаха (по другой версии - дракон), символ вечности. На ее панцире были видны пятна, образовавшие удивительный рисунок.

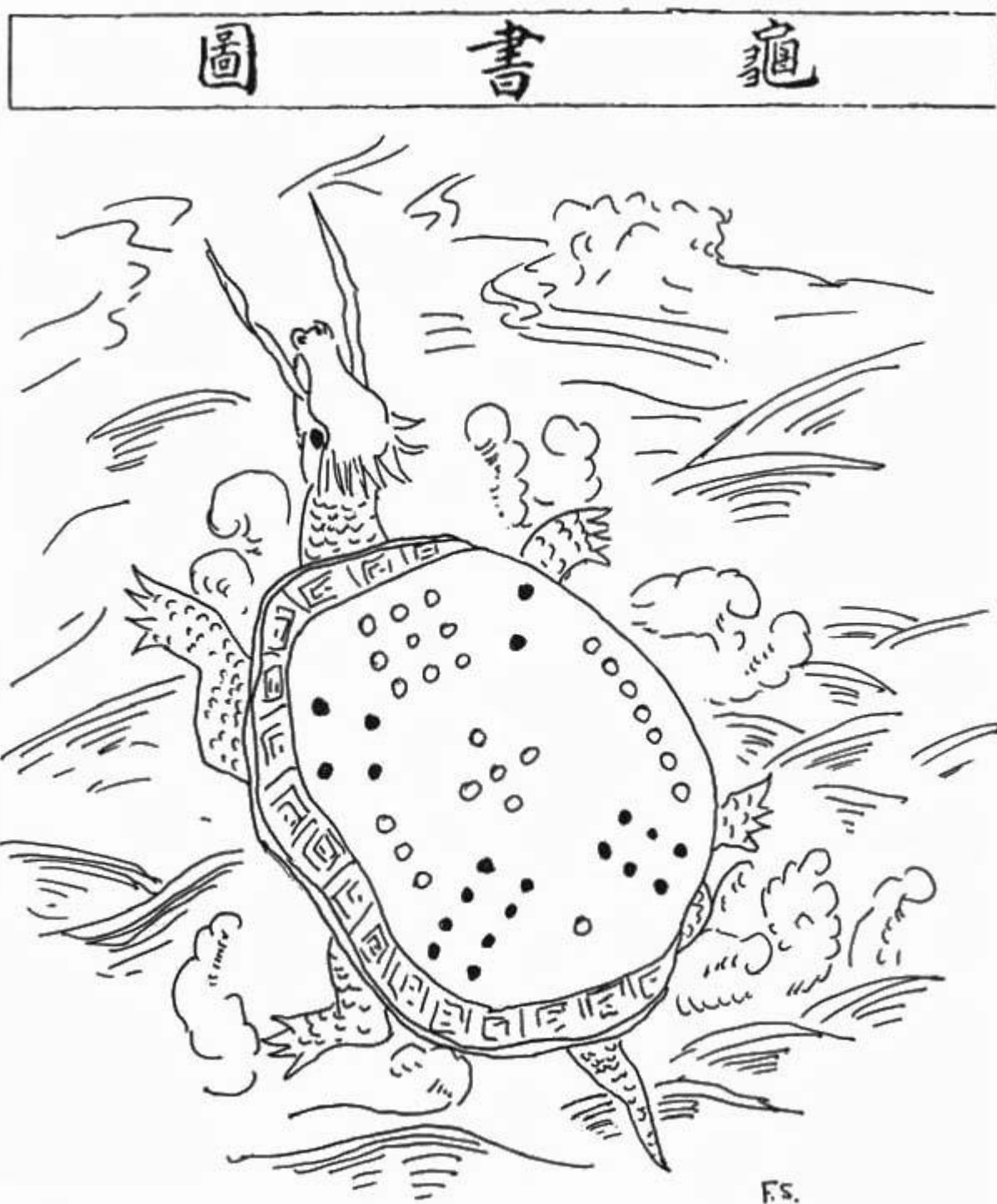


Рисунок 10 - Магический квадрат Ло Шу

Когда черепаха вышла из воды, высыхали лужи после недавнего ливня. Великий Юй взял эту черепаху и рассмотрел странный узор на ее панцире. Этот узор вдохновил его на создание трактата под названием «Хун Фань» («Великий план»), в котором говорилось о физике, астрологии, предсказаниях, морали, политике и религии.

Магические квадраты широко применялись для передачи секретной информации. При шифровании исходное сообщение вписывалось в квадрат по приведенной в них нумерации, после чего шифрограмма выписывалась по строкам. Количество возможных магических квадратов (ключей) быстро возрастает с увеличением их размера. Так, существует лишь один магический квадрат размером 3х3, если не принимать во внимание его повороты. Магических квадратов 4х4 насчитывается уже 880, а число магических квадратов размером 5х5 около 250000. Поэтому магические квадраты больших размеров могли быть хорошей основой для надежной системы шифрования того времени, потому что ручной перебор всех вариантов ключа для этого шифра был невыносим.

Рассмотрим квадрат размером 4х4. В него вписываются числа от 1 до 16. Его магия состоит в том, что сумма чисел по строкам, столбцам и полным диагоналям равняется одному и тому же числу - 34.

| | | | |
|----|----|----|----|
| 16 | 3 | 2 | 13 |
| 5 | 10 | 11 | 8 |
| 9 | 6 | 7 | 12 |
| 4 | 15 | 14 | 1 |

Рисунок 11 - Магический квадрат 4х4

Шифрование по магическому квадрату производилось следующим образом. Например, требуется зашифровать фразу: «АБРАМОВ+ДЯДИНА..».

Буквы этой фразы вписываются последовательно в квадрат согласно записанным в ячейках числам. В пустые клетки ставится точка или любая буква.

| | | | |
|-----|------|------|------|
| 16 | 3 Р | 2 Б | 13 Н |
| 5 М | 10 Я | 11 Д | 8 + |
| 9 Д | 6 О | 7 В | 12 И |
| 4 А | 15 . | 14 А | 1 А |

Рисунок 12- Пример шифрования с помощью магического квадрата

После этого шифрованный текст записывается в строку (считывание производится слева-направо сверху-вниз, построчно) – «.РБНМЯД+ДОВИА.АА».

Джелорамо Кардано (1501 – 1576 гг.) - итальянский математик, инженер, философ, медик и астролог. В его честь названы открытые Сципионом дель Ферро формулы решения кубического уравнения (Кардано первым их опубликовал) и карданный вал (известного ещё Леонардо да Винчи). Написал около 240 книг (131 из них была опубликована, 111 остались в виде рукописей).

Шифры множественной перестановки

В данном подклассе шифров используется идея повторного шифрования уже зашифрованного сообщения или многократной перестановки символов исходного сообщения перед попаданием в итоговую шифрограмму.

Шифр двойной перестановки. В таблицу по определенному маршруту записывается текст сообщения, затем переставляются столбцы, а потом переставляются строки. Шифрограмма выписывается по определенному маршруту.

Пример шифрования сообщения «АБРАМОВ+ДЯДИНА» показан на следующем рисунке. Результат шифрования – «ОАБЯ+_АИВ_РДМНАД».



Рисунок 13 - Пример использования шифра двойной перестановки

Ключом к шифру являются размеры таблицы, маршруты вписывания и выписывания, а также порядки перестановки столбцов и строк. Если маршруты являются фиксированными величинами, то количество ключей равно $n! \cdot m!$, n и m – количество столбцов и строк в таблице.

Несмотря на многоступенчатую процедуру шифрования, включая двойную перестановку, данный шифр может быть эквивалентно заменен шифром простой одинарной перестановки. На следующем рисунке приведена таблица эквивалентных одинарных перестановок для примера шифрования, приведенного на рисунке 13.

| | | | | | | | | | | | | | | | |
|----|---|----|---|----|---|---|---|----|----|----|----|----|----|----|----|
| 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 | 14 | 15 | 16 |
| А | Б | Р | А | М | О | В | + | Д | Я | Д | И | Н | А | – | – |
| 15 | 3 | 11 | 7 | 13 | 1 | 9 | 5 | 16 | 4 | 12 | 8 | 14 | 2 | 10 | 6 |
| О | А | Б | Я | + | – | А | И | В | – | Р | Д | М | Н | А | Д |

Рисунок 14 - Таблица эквивалентных одинарных перестановок

Аналогичную замену на шифр простой одинарной перестановки можно выполнить и для других шифров: табличная маршрутная перестановка, «поворотная решетка», «магический квадрат» и др.

Задания для самостоятельного выполнения

В лабораторной работе необходимо зашифровать свою фамилию имя отчество и номер группы и подгруппы (в текстовом виде) с помощью следующих шифров:

1. простой одинарной перестановки;
2. блочной одинарной перестановки;
3. табличной маршрутной перестановки;
4. вертикальной перестановки;
5. поворотной решетки;
6. магический квадрат (размер квадрата - 4x4);
7. двойной перестановки;
8. шифра «Перекресток»;
9. шифры с использованием треугольника.
10. табличной маршрутной перестановки;
11. поворотной решетки;
12. шифра «Перекресток»;
13. магический квадрат (размер квадрата - 4x4);
14. шифры с использованием треугольника.
15. вертикальной перестановки;
16. шифры с использованием треугольника.

При оформлении отчета необходимо привести исходное сообщение (фамилию имя отчество и номер группы и подгруппы (в текстовом виде), таблицы, ключевые слова (выбираются произвольно), маршруты вписывания и выписывания, повороты решетки и зашифрованное сообщение. Привести алгоритм (блок схему и текстовое описание), скриншоты выполнения

программы и текст кода. Язык программирования выбирается любой. Вместе с отчетом прикрепляется исходники кода.

Вопросы для самопроверки

1. В чем заключается основная идея криптографических преобразований шифров перестановки?
2. Перечислите основные разновидности шифров перестановки.
3. Дайте характеристику разновидностям шифров перестановки.

Лабораторная работа №2. Шифры замены

Основы шифрования

Сущность шифрования методом замены заключается в следующем [9]. Пусть шифруются сообщения на русском языке и замене подлежит каждая буква этих сообщений. Тогда, букве **А** исходного алфавита сопоставляется некоторое множество символов (шифрозамен) M_A , **Б** – M_B , ..., **Я** – M_Y . Шифрозамены выбираются таким образом, чтобы любые два множества (M_i и M_j , $i \neq j$) не содержали одинаковых элементов ($M_i \cap M_j = \emptyset$).

Таблица, приведенная на рисунок 1, является ключом шифра замены. Зная ее, можно осуществить как шифрование, так и расшифрование.

| | | | |
|-------|-------|-----|-------|
| А | Б | ... | Я |
| M_A | M_B | ... | M_Y |

Рисунок 1 - Таблица шифрозамен

При шифровании каждая буква **А** открытого сообщения заменяется любым символом из множества M_A . Если в сообщении содержится несколько букв **А**, то каждая из них заменяется на любой символ из M_A . За счет этого с помощью одного ключа можно получить различные варианты шифрограммы для одного и того же открытого сообщения. Так как множества M_A , M_B , ..., M_Y попарно не пересекаются, то по каждому символу шифрограммы можно однозначно определить, какому множеству он принадлежит, и, следовательно, какую букву открытого сообщения он заменяет. Поэтому расшифрование возможно и открытое сообщение определяется единственным образом.

Приведенное выше описание сущности шифров замены относится ко всем их разновидностям за исключением полиалфавитных шифров, в которых для зашифрования разных символов исходного алфавита могут использоваться одинаковые шифрозамены (т.е. $M_i \cap M_j \neq \emptyset$, $i \neq j$).

Метод замены часто реализуется многими пользователями при работе на компьютере. Если по забывчивости не переключить на клавиатуре набор символов с латиницы на кириллицу, то вместо букв русского алфавита при вводе текста будут печататься буквы латинского алфавита («шифрозамены»).

Для записи исходных и зашифрованных сообщений используются строго определенные алфавиты. Алфавиты для записи исходных и зашифрованных сообщений могут отличаться. Символы обоих алфавитов могут быть представлены буквами, их сочетаниями, числами, рисунками, звуками, жестами и т.п. В качестве примера можно привести пляшущих человечков из рассказа А.

Конан Дойла (👤👤👤👤👤) и рукопись рунического письма (1 11 1) из романа Ж. Верна «Путешествие к центру Земли».

Шифры замены по особенностям процедур преобразования сообщения можно разделить на следующие **подклассы** (типы, разновидности).

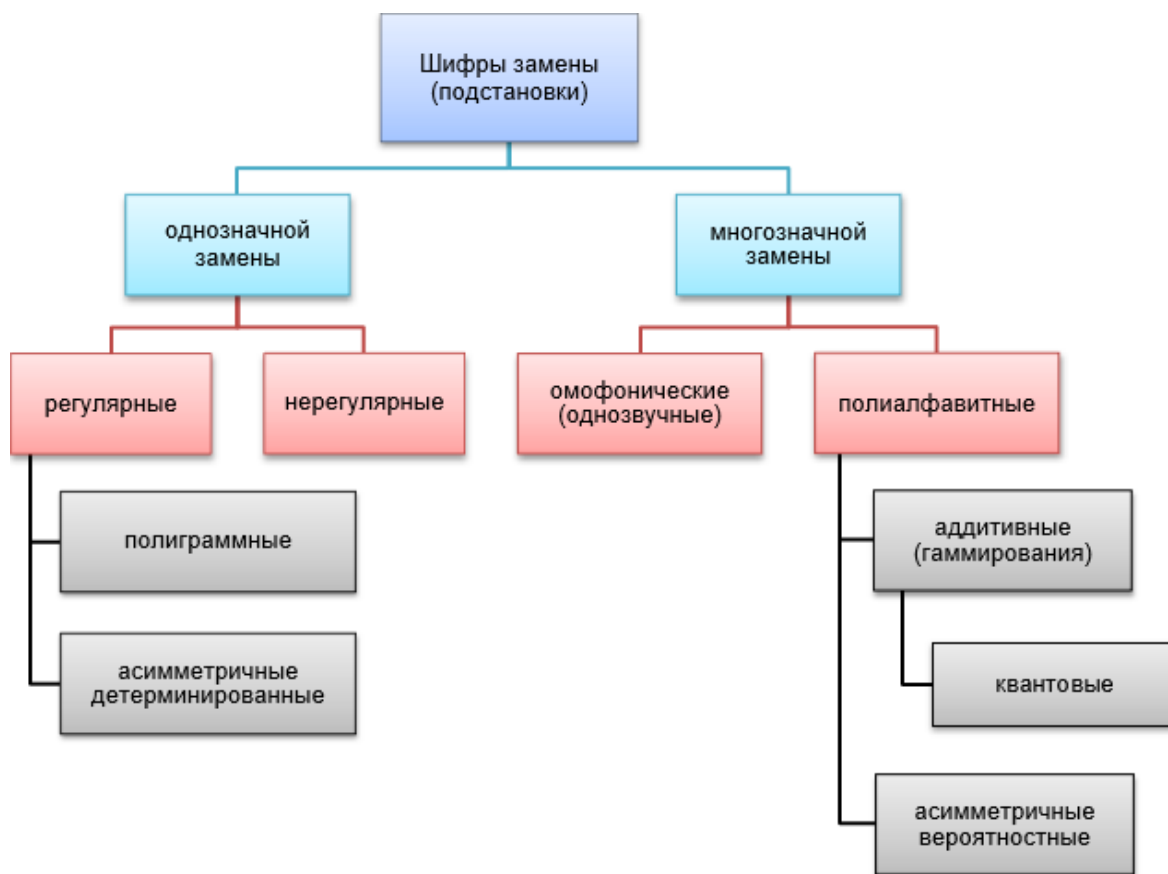


Рисунок 2 - Классификация шифров замены

На рисунке серым фоном представлены подгруппы шифров, которые не образуют полную вышележащую группу шифров, но получившие широкое применение на практике и описаны в этой или отдельных лекциях.

В следующий таблице приведена краткая характеристика типов шифров замены.

Таблица 1. Типы шифров замены

| Тип шифра | | | Краткая характеристика | Примеры шифров |
|--|------------|---------------------------------|--|---|
| однозначной замены (моноалфавитные, простые подстановочные) | | | Количество шифрозамен во множестве M для каждого символа или блока символов исходного алфавита равно 1 ($ M_i = 1$ для одного i -го символа или блока символов). | |
| однозначной замены | регулярные | | Шифрозамены состоят из одинакового количества символов или отделяются друг от друга разделителем (пробелом, точкой, тире и т.п.). | шифр Цезаря, лозунговый шифр, тюремный шифр |
| | регулярные | полиграммные | Шифрозамене соответствует блок символов исходного алфавита ($ M_i = 1$ для одного i -ого блока символов). | биграммный шифр Порты, шифр Хилла |
| | | асимметричные детерминированные | При зашифровании одного и того же открытого сообщения одним и тем же открытым ключом всегда будет получаться одна и та же шифрограмма. Т.е. для заданного открытого ключа один и тот же символ (блок символов) открытого сообщения всегда будет представляться | <u>RSA</u> , <u>шифр на основе задачи об укладке ранца</u> |

| | | | | |
|---------------------|----------------------------------|--|---|--|
| | | | одной и той же шифрозаменой. | |
| | нерегулярные | | Шифрозамены состоят из разного количество символов, записываемых без разделителей. | совмещенный шифр |
| многозначной замены | | | Количество шифрозамен во множестве М для отдельных символов или блока символов исходного алфавита больше 1 ($ M_i \geq 1$ для одного i-го символа или блока символов). | |
| многозначной замены | омофонические (однозвучные) | | Шифрозамены для разных символов или блоков символов исходного алфавита не повторяются ($M_i \cap M_j = \emptyset$ для двух разных i-го и j-го символов или блоков символов). | система омофонов, книжный шифр |
| | полиалфавитные (многоалфавитные) | | Исходному алфавиту для записи открытых сообщений соответствует несколько алфавитов шифрозамен. Выбор варианта алфавита шифрозамен для зашифрования отдельного символа или блока символов зависит от особенностей шифра. Одна и та же шифрозамена может использоваться для разных символов или блоков символов исходного алфавита ($M_i \cap M_j \neq \emptyset$ для двух разных i-го и j-го символов или блоков символов). | <u>диск Альберти,</u> <u>система Виженера</u> |

| | | | | |
|--|----------------|------------------------------|---|---|
| | полиалфавитные | аддитивные (гаммирования) | При зашифровании символы исходного алфавита в открытом сообщении заменяются числами, к которым добавляются числа секретной случайной числовой последовательности (гаммы), после чего берется остаток от деления по модулю (операция mod). | шифрование сложением по модулю N, шифр Вернама |
| | | квантовые | Являются разновидностью шифров гаммирования, где в качестве носителей информации используются элементарные частицы (пучки элементарных частиц). | |
| | | асимметричные вероятностные | При зашифровании одного и того же открытого сообщения одним и тем же открытым ключом могут получаться разные шифрограммы. Т.е. для заданного открытого ключа один и тот же символ (блок символов) открытого сообщения может представляться разными шифрозаменами. Это достигается за счет использования случайной величины при зашифровании символа (блока символов), что эквивалентно переключению алфавитов шифрозамен. | схема Эль-Гамала, шифр на основе эллиптических кривых |

2. Регулярные шифры однозначной замены

Максимальное количество ключей для любого шифра этого типа не превышает $n!$, где n – количество символов в алфавите. При больших n для приближенного вычисления $n!$ можно воспользоваться формулой Стирлинга:

$$n! \approx \sqrt{2\pi n} * \left(\frac{n}{e}\right)^n \quad (1)$$

Шифр Цезаря. Согласно описаниям историка Светония в книге «Жизнь двенадцати цезарей» данный шифр использовался Гаем Юлием Цезарем для секретной переписке со своими генералами (I век до н.э.). Применительно к русскому языку суть его состоит в следующем. Выписывается исходный алфавит (А, Б, ..., Я), затем под ним выписывается тот же алфавит, но с циклическим сдвигом на 3 буквы влево.

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

Рисунок 3 - Таблица шифрозамен для шифра Цезаря

При зашифровке буква А заменяется буквой Г, Б - на Д и т. д. Так, например, исходное сообщение «АБРАМОВ» после шифрования будет выглядеть «ГДУГПСЕ». Получатель сообщения «ГДУГПСЕ» ищет эти буквы в нижней строке и по буквам над ними восстанавливает исходное сообщение «АБРАМОВ».

Ключом в шифре Цезаря является величина сдвига нижней строки алфавита. Количество ключей для всех модификаций данного шифра применительно к алфавиту русского языка равно 33. Существуют различные модификации шифра Цезаря, в частности атбаш и лозунговый шифр.

Атбаш. В Ветхом Завете существует несколько фрагментов из священных текстов, которые зашифрованы с помощью шифра замены, называемого атбаш. Этот шифр состоит в замене каждой буквы другой буквой, которая находится в алфавите на таком же расстоянии от конца алфавита, как оригинальная буква - от начала. Например, в русском алфавите буква **А** заменяется на **Я**, буква **Б** - на **Ю** и т.д. В оригинальном Ветхом Завете использовались буквы еврейского алфавита. Так, в книге пророка Иеремии (25:26) слово «Бабель» (Вавилон) зашифровано как «Шешах».

Лозунговый шифр. Для данного шифра построение таблицы шифрозамен основано на лозунге (ключе) – легко запоминаемом слове. Вторая строка таблицы шифрозамен заполняется сначала словом-лозунгом (причем повторяющиеся буквы отбрасываются), а затем остальными буквами, не вошедшими в слово-лозунг, в алфавитном порядке. Например, если выбрано слово-лозунг «ДЯДИНА», то таблица имеет следующий вид.

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

Рисунок 4 - Таблица шифрозамен для лозунгового шифра

При шифровании исходного сообщения «АБРАМОВ» по приведенному выше ключу шифрограмма будет выглядеть «ДЯПДКМИ».

В качестве лозунга рекомендуется выбирать фразу, в которой содержатся конечные буквы алфавита. В общем случае, количество вариантов нижней строки (применительно к русскому языку) составляет $33! (\geq 10^{35})$.

Полибианский квадрат. Шифр изобретен греческим государственным деятелем, полководцем и историком Полибием (203-120 гг. до н.э.). Применительно к русскому алфавиту и индийским (арабским) цифрам суть

шифрования заключалась в следующем. В квадрат 6х6 выписываются буквы (необязательно в алфавитном порядке).

| | | | | | | |
|---|---|---|---|---|---|---|
| | 1 | 2 | 3 | 4 | 5 | 6 |
| 1 | А | Б | В | Г | Д | Е |
| 2 | Ё | Ж | З | И | Й | К |
| 3 | Л | М | Н | О | П | Р |
| 4 | С | Т | У | Ф | Х | Ц |
| 5 | Ч | Ш | Щ | Ъ | Ы | Ь |
| 6 | Э | Ю | Я | - | - | - |

Рисунок 5 - Таблица шифрозамен для полибианского квадрата

Шифруемая буква заменяется на координаты квадрата (строка-столбец), в котором она записана. Например, если исходное сообщение «АБРАМОВ», то шифрограмма – «11 12 36 11 32 34 13». В Древней Греции сообщения передавались с помощью оптического телеграфа (с помощью факелов). Для каждой буквы сообщения вначале поднималось количество факелов, соответствующее номеру строки буквы, а затем номеру столбца.

Тюремный шифр. Эта звуковая разновидность полибианского квадрата была разработана заключенными. Система состояла из нескольких ударов, обозначающих строки и столбцы в таблице с буквами алфавита. Один удар, а потом еще два соответствовали строке 1 и столбцу 2, т.е. букве **Б**. Пауза служила разделителем между строками и столбцами. Таким образом, зашифровать исходное сообщение «АБРАМОВ» можно следующим образом.

| | |
|---|---|
| А | тук ____ тук |
| Б | тук ____ тук, тук |
| Р | тук, тук, тук ____ тук, тук, тук, тук, тук, тук |

| | |
|---|---------------------------------------|
| А | тук ____ тук |
| М | тук, тук, тук ____ тук, тук |
| О | тук, тук, тук ____ тук, тук, тук, тук |
| В | тук ____ тук, тук, тук |

Рисунок 6 - Пример использования тюремного шифра

Шифрующая система Трисемуса (Тритемия). 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. На рисунок 7 изображена таблица с ключевым словом «ДЯДИНА».

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

Рисунок 7 - Таблица шифрозамен для шифра Трисемуса

Каждая буква открытого сообщения заменяется буквой, расположенной под ней в том же столбце. Если буква находится в последней строке таблицы, то для ее шифрования берут самую верхнюю букву столбца. Например, исходное сообщение «АБРАМОВ», зашифрованное – «ЖЗЦЖУФЙ».

Шифр масонов. В XVIII в. масоны создали шифр, чтобы скрыть от общественности свои коммерческие сделки. Как поведали те, кто прежде состоял в рядах этого общества, масоны пользовались способом засекречивания, весьма похожим на шифр розенкрейцеров. В «решетке» и в углах находятся точки, которыми заменяются буквы:

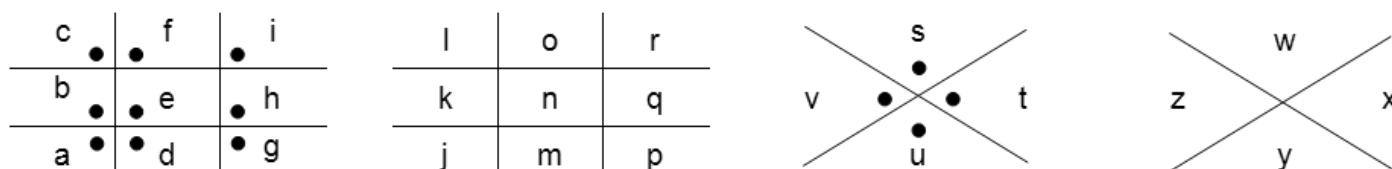


Рисунок 8 - Шифрозамены шифра масонов

Так как клятвы хранить тайну нарушались не раз, большинство Великих лож масонов в США больше не пользуются письменными шифрами, предпочитая передавать устные инструкции во время закрытых ритуалов.

С помощью шифра масонов можно легко расшифровать следующую фразу.



Рисунок 9 - Пример использования шифра масонов

Это первый уровень, на котором находятся все впервые вступившие в общество члены: Blue Lodge (рус. «Голубая (Синяя) ложа»).

Одним из существенных **недостатков шифров однозначной замены** является их легкая вскрываемость. При вскрытии шифрограмм используются различные приемы, которые даже при отсутствии мощных вычислительных средств позволяют добиться положительного результата. Один из таких приемов базируется на том, что в шифрограммах остается информация о частоте встречаемости букв исходного текста. Если в открытом сообщении часто встречается какая-либо буква, то в зашифрованном сообщении также часто

будет встречаться соответствующий ей символ. Еще в 1412 г. Шихаба аль-Калкашанди в своем труде «Заря для подслеповатого в искусстве писания» привел таблицу частоты появления арабских букв в тексте на основе анализа текста Корана. Для разных языков мира существуют подобные таблицы. Так, например, для букв русского алфавита по данным "Национального корпуса русского языка" такая таблица выглядит следующим образом.

Таблица 2. Частота появления букв русского языка в текстах

| № п/п | Буква | Частота, % | № п/п | Буква | Частота, % |
|-------|-------|------------|-------|-------|------------|
| 1 | О | 10.97 | 18 | Ь | 1.74 |
| 2 | Е | 8.45 | 19 | Г | 1.70 |
| 3 | А | 8.01 | 20 | З | 1.65 |
| 4 | И | 7.35 | 21 | Б | 1.59 |
| 5 | Н | 6.70 | 22 | Ч | 1.44 |
| 6 | Т | 6.26 | 23 | Й | 1.21 |
| 7 | С | 5.47 | 24 | Х | 0.97 |
| 8 | Р | 4.73 | 25 | Ж | 0.94 |
| 9 | В | 4.54 | 26 | Ш | 0.73 |
| 10 | Л | 4.40 | 27 | Ю | 0.64 |
| 11 | К | 3.49 | 28 | Ц | 0.48 |
| 12 | М | 3.21 | 29 | Щ | 0.36 |
| 13 | Д | 2.98 | 30 | Э | 0.32 |
| 14 | П | 2.81 | 31 | Ф | 0.26 |
| 15 | У | 2.62 | 32 | Ъ | 0.04 |
| 16 | Я | 2.01 | 33 | Ё | 0.04 |
| 17 | Ы | 1.90 | | | |

Существуют подобные таблицы для пар букв (биграмм). Например, часто встречаемыми биграммами являются «то», «но», «ст», «по», «ен» и т.д. Другой прием вскрытия шифрограмм основан на исключении возможных сочетаний букв. Например, в текстах (если они написаны без орфографических ошибок) нельзя встретить сочетания «чя», «щы», «ьъ» и т.п.

Для усложнения задачи вскрытия шифров однозначной замены еще в древности перед шифрованием из исходных сообщений исключали пробелы

и/или гласные буквы. Другим способом, затрудняющим вскрытие, является шифрование **биграммами** (парами букв).

Полиграммные шифры

Полиграммные шифры - шифры, в которых одна шифрозамена соответствует сразу нескольким символам исходного сообщения.

Биграммный шифр Порты. Шифр Порты, представленный им в виде таблицы, является первым известным биграммным шифром. Размер его таблицы составлял 20 x 20 ячеек; наверху горизонтально и слева вертикально записывался стандартный алфавит (в нем не было букв J, K, U, W, X и Z). В ячейках таблицы могли быть записаны любые числа, буквы или символы - сам Джованни Порты пользовался символами - при условии, что содержимое ни одной из ячеек не повторялось. Применительно к русскому языку таблица шифрозамен может выглядеть следующим образом.

| | А | Б | В | Г | Д | Е (Ё) | Ж | З | И (Й) | К | Л | М | Н | О | П | Р | С | Т | У | Ф | Х | Ц | Ч | Ш | Щ | Ъ | Ы | Ь | Э | Ю | Я |
|----------|-------------|-------------|-------------|-------------|-------------|-------------|-------------|-------------|-------------|-------------|-------------|-------------|-------------|-------------|-------------|-------------|-------------|-------------|-------------|-------------|-------------|-------------|-------------|-------------|-------------|-------------|-------------|-------------|-------------|-------------|-------------|
| А | 0 0 1 | 0 0 2 | 0 0 3 | 0 0 4 | 0 0 5 | 0 0 6 | 0 0 7 | 0 0 8 | 0 0 9 | 0 1 0 | 0 1 1 | 0 1 2 | 0 1 3 | 0 1 4 | 0 1 5 | 0 1 6 | 0 1 7 | 0 1 8 | 0 1 9 | 0 2 0 | 0 2 1 | 0 2 2 | 0 2 3 | 0 2 4 | 0 2 5 | 0 2 6 | 0 2 7 | 0 2 8 | 0 2 9 | 0 3 0 | 0 3 1 |
| Б | 0 3 2 | 0 3 3 | 0 3 4 | 0 3 5 | 0 3 6 | 0 3 7 | 0 3 8 | 0 3 9 | 0 4 0 | 0 4 1 | 0 4 2 | 0 4 3 | 0 4 4 | 0 4 5 | 0 4 6 | 0 4 7 | 0 4 8 | 0 4 9 | 0 5 0 | 0 5 1 | 0 5 2 | 0 5 3 | 0 5 4 | 0 5 5 | 0 5 6 | 0 5 7 | 0 5 8 | 0 5 9 | 0 6 0 | 0 6 1 | 0 6 2 |
| В | 0 6 3 | 0 6 4 | 0 6 5 | 0 6 6 | 0 6 7 | 0 6 8 | 0 6 9 | 0 7 0 | 0 7 1 | 0 7 2 | 0 7 3 | 0 7 4 | 0 7 5 | 0 7 6 | 0 7 7 | 0 7 8 | 0 7 9 | 0 8 0 | 0 8 1 | 0 8 2 | 0 8 3 | 0 8 4 | 0 8 5 | 0 8 6 | 0 8 7 | 0 8 8 | 0 8 9 | 0 9 0 | 0 9 1 | 0 9 2 | 0 9 3 |
| Г | 0 9 4 | 0 9 5 | 0 9 6 | 0 9 7 | 0 9 8 | 0 9 9 | 1 0 0 | 1 0 1 | 1 0 2 | 1 0 3 | 1 0 4 | 1 0 5 | 1 0 6 | 1 0 7 | 1 0 8 | 1 0 9 | 1 1 0 | 1 1 1 | 1 1 2 | 1 1 3 | 1 1 4 | 1 1 5 | 1 1 6 | 1 1 7 | 1 1 8 | 1 1 9 | 1 2 0 | 1 2 1 | 1 2 2 | 1 2 3 | 1 2 4 |
| Д | 1 2 5 | 1 2 6 | 1 2 7 | 1 2 8 | 1 2 9 | 1 3 0 | 1 3 1 | 1 3 2 | 1 3 3 | 1 3 4 | 1 3 5 | 1 3 6 | 1 3 7 | 1 3 8 | 1 3 9 | 1 4 0 | 1 4 1 | 1 4 2 | 1 4 3 | 1 4 4 | 1 4 5 | 1 4 6 | 1 4 7 | 1 4 8 | 1 4 9 | 1 5 0 | 1 5 1 | 1 5 2 | 1 5 3 | 1 5 4 | 1 5 5 |
| Е (Ё) | 1 5 6 | 1 5 7 | 1 5 8 | 1 5 9 | 1 6 0 | 1 6 1 | 1 6 2 | 1 6 3 | 1 6 4 | 1 6 5 | 1 6 6 | 1 6 7 | 1 6 8 | 1 6 9 | 1 7 0 | 1 7 1 | 1 7 2 | 1 7 3 | 1 7 4 | 1 7 5 | 1 7 6 | 1 7 7 | 1 7 8 | 1 7 9 | 1 8 0 | 1 8 1 | 1 8 2 | 1 8 3 | 1 8 4 | 1 8 5 | 1 8 6 |

| | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
|----------|-----|-----|-----|-----|-----|-----|-----|-----|-----|-----|-----|-----|-----|-----|-----|-----|-----|-----|-----|-----|-----|-----|-----|-----|-----|-----|-----|-----|-----|-----|-----|
| Ж | 187 | 188 | 189 | 190 | 191 | 192 | 193 | 194 | 195 | 196 | 197 | 198 | 199 | 200 | 201 | 202 | 203 | 204 | 205 | 206 | 207 | 208 | 209 | 210 | 211 | 212 | 213 | 214 | 215 | 216 | 217 |
| З | 218 | 219 | 220 | 221 | 222 | 223 | 224 | 225 | 226 | 227 | 228 | 229 | 230 | 231 | 232 | 233 | 234 | 235 | 236 | 237 | 238 | 239 | 240 | 241 | 242 | 243 | 244 | 245 | 246 | 247 | 248 |
| И (Й) | 249 | 250 | 251 | 252 | 253 | 254 | 255 | 256 | 257 | 258 | 259 | 260 | 261 | 262 | 263 | 264 | 265 | 266 | 267 | 268 | 269 | 270 | 271 | 272 | 273 | 274 | 275 | 276 | 277 | 278 | 279 |
| К | 280 | 281 | 282 | 283 | 284 | 285 | 286 | 287 | 288 | 289 | 290 | 291 | 292 | 293 | 294 | 295 | 296 | 297 | 298 | 299 | 300 | 301 | 302 | 303 | 304 | 305 | 306 | 307 | 308 | 309 | 310 |
| Л | 311 | 312 | 313 | 314 | 315 | 316 | 317 | 318 | 319 | 320 | 321 | 322 | 323 | 324 | 325 | 326 | 327 | 328 | 329 | 330 | 331 | 332 | 333 | 334 | 335 | 336 | 337 | 338 | 339 | 340 | 341 |
| М | 342 | 343 | 344 | 345 | 346 | 347 | 348 | 349 | 350 | 351 | 352 | 353 | 354 | 355 | 356 | 357 | 358 | 359 | 360 | 361 | 362 | 363 | 364 | 365 | 366 | 367 | 368 | 369 | 370 | 371 | 372 |
| Н | 373 | 374 | 375 | 376 | 377 | 378 | 379 | 380 | 381 | 382 | 383 | 384 | 385 | 386 | 387 | 388 | 389 | 390 | 391 | 392 | 393 | 394 | 395 | 396 | 397 | 398 | 399 | 400 | 401 | 402 | 403 |
| О | 404 | 405 | 406 | 407 | 408 | 409 | 410 | 411 | 412 | 413 | 414 | 415 | 416 | 417 | 418 | 419 | 420 | 421 | 422 | 423 | 424 | 425 | 426 | 427 | 428 | 429 | 430 | 431 | 432 | 433 | 434 |
| П | 435 | 436 | 437 | 438 | 439 | 440 | 441 | 442 | 443 | 444 | 445 | 446 | 447 | 448 | 449 | 450 | 451 | 452 | 453 | 454 | 455 | 456 | 457 | 458 | 459 | 460 | 461 | 462 | 463 | 464 | 465 |
| Р | 466 | 467 | 468 | 469 | 470 | 471 | 472 | 473 | 474 | 475 | 476 | 477 | 478 | 479 | 480 | 481 | 482 | 483 | 484 | 485 | 486 | 487 | 488 | 489 | 490 | 491 | 492 | 493 | 494 | 495 | 496 |
| С | 497 | 498 | 499 | 500 | 501 | 502 | 503 | 504 | 505 | 506 | 507 | 508 | 509 | 510 | 511 | 512 | 513 | 514 | 515 | 516 | 517 | 518 | 519 | 520 | 521 | 522 | 523 | 524 | 525 | 526 | 527 |
| Т | 528 | 529 | 530 | 531 | 532 | 533 | 534 | 535 | 536 | 537 | 538 | 539 | 540 | 541 | 542 | 543 | 544 | 545 | 546 | 547 | 548 | 549 | 550 | 551 | 552 | 553 | 554 | 555 | 556 | 557 | 558 |
| У | 559 | 560 | 561 | 562 | 563 | 564 | 565 | 566 | 567 | 568 | 569 | 570 | 571 | 572 | 573 | 574 | 575 | 576 | 577 | 578 | 579 | 580 | 581 | 582 | 583 | 584 | 585 | 586 | 587 | 588 | 589 |
| Ф | 590 | 591 | 592 | 593 | 594 | 595 | 596 | 597 | 598 | 599 | 600 | 601 | 602 | 603 | 604 | 605 | 606 | 607 | 608 | 609 | 610 | 611 | 612 | 613 | 614 | 615 | 616 | 617 | 618 | 619 | 620 |
| Х | 621 | 622 | 623 | 624 | 625 | 626 | 627 | 628 | 629 | 630 | 631 | 632 | 633 | 634 | 635 | 636 | 637 | 638 | 639 | 640 | 641 | 642 | 643 | 644 | 645 | 646 | 647 | 648 | 649 | 650 | 651 |

| | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
|---|-------------|-------------|-------------|-------------|-------------|-------------|-------------|-------------|-------------|-------------|-------------|-------------|-------------|-------------|-------------|-------------|-------------|-------------|-------------|-------------|-------------|-------------|-------------|-------------|-------------|-------------|-------------|-------------|-------------|-------------|-------------|-------------|
| Ц | 6 5 2 | 6 5 3 | 6 5 4 | 6 5 5 | 6 5 6 | 6 5 7 | 6 5 8 | 6 5 9 | 6 6 0 | 6 6 1 | 6 6 2 | 6 6 3 | 6 6 4 | 6 6 5 | 6 6 6 | 6 6 7 | 6 6 8 | 6 6 9 | 6 7 0 | 6 7 1 | 6 7 2 | 6 7 3 | 6 7 4 | 6 7 5 | 6 7 6 | 6 7 7 | 6 7 8 | 6 8 9 | 6 8 0 | 6 8 1 | 6 8 2 | 6 8 3 |
| Ч | 6 8 3 | 6 8 4 | 6 8 5 | 6 8 6 | 6 8 7 | 6 8 8 | 6 8 9 | 6 9 0 | 6 9 1 | 6 9 2 | 6 9 3 | 6 9 4 | 6 9 5 | 6 9 6 | 6 9 7 | 6 9 8 | 6 9 9 | 7 0 0 | 7 0 1 | 7 0 2 | 7 0 3 | 7 0 4 | 7 0 5 | 7 0 6 | 7 0 7 | 7 0 8 | 7 0 9 | 7 1 0 | 7 1 1 | 7 1 2 | 7 1 3 | 7 1 4 |
| Ш | 7 1 4 | 7 1 5 | 7 1 6 | 7 1 7 | 7 1 8 | 7 2 9 | 7 2 0 | 7 2 1 | 7 2 2 | 7 2 3 | 7 2 4 | 7 2 5 | 7 2 6 | 7 2 7 | 7 2 8 | 7 2 9 | 7 3 0 | 7 3 1 | 7 3 2 | 7 3 3 | 7 3 4 | 7 3 5 | 7 3 6 | 7 3 7 | 7 3 8 | 7 3 9 | 7 4 0 | 7 4 1 | 7 4 2 | 7 4 3 | 7 4 4 | 7 4 5 |
| Щ | 7 4 5 | 7 4 6 | 7 4 7 | 7 4 8 | 7 4 9 | 7 5 0 | 7 5 1 | 7 5 2 | 7 5 3 | 7 5 4 | 7 5 5 | 7 5 6 | 7 5 7 | 7 5 8 | 7 5 9 | 7 6 0 | 7 6 1 | 7 6 2 | 7 6 3 | 7 6 4 | 7 6 5 | 7 6 6 | 7 6 7 | 7 6 8 | 7 6 9 | 7 7 0 | 7 7 1 | 7 7 2 | 7 7 3 | 7 7 4 | 7 7 5 | |
| Ъ | 7 7 6 | 7 7 7 | 7 7 8 | 7 7 9 | 7 8 0 | 7 8 1 | 7 8 2 | 7 8 3 | 7 8 4 | 7 8 5 | 7 8 6 | 7 8 7 | 7 8 8 | 7 8 9 | 7 9 0 | 7 9 1 | 7 9 2 | 7 9 3 | 7 9 4 | 7 9 5 | 7 9 6 | 7 9 7 | 7 9 8 | 7 9 9 | 8 0 0 | 8 0 1 | 8 0 2 | 8 0 3 | 8 0 4 | 8 0 5 | 8 0 6 | 8 0 7 |
| Ы | 8 0 7 | 8 0 8 | 8 0 9 | 8 1 0 | 8 1 1 | 8 1 2 | 8 1 3 | 8 1 4 | 8 1 5 | 8 1 6 | 8 1 7 | 8 1 8 | 8 1 9 | 8 2 0 | 8 2 1 | 8 2 2 | 8 2 3 | 8 2 4 | 8 2 5 | 8 2 6 | 8 2 7 | 8 2 8 | 8 2 9 | 8 3 0 | 8 3 1 | 8 3 2 | 8 3 3 | 8 3 4 | 8 3 5 | 8 3 6 | 8 3 7 | 8 3 8 |
| Ь | 8 3 8 | 8 3 9 | 8 4 0 | 8 4 1 | 8 4 2 | 8 4 3 | 8 4 4 | 8 4 5 | 8 4 6 | 8 4 7 | 8 4 8 | 8 4 9 | 8 5 0 | 8 5 1 | 8 5 2 | 8 5 3 | 8 5 4 | 8 5 5 | 8 5 6 | 8 5 7 | 8 5 8 | 8 5 9 | 8 6 0 | 8 6 1 | 8 6 2 | 8 6 3 | 8 6 4 | 8 6 5 | 8 6 6 | 8 6 7 | 8 6 8 | 8 6 9 |
| Э | 8 6 9 | 8 6 0 | 8 6 1 | 8 6 2 | 8 6 3 | 8 6 4 | 8 6 5 | 8 6 6 | 8 6 7 | 8 6 8 | 8 6 9 | 8 7 0 | 8 7 1 | 8 7 2 | 8 7 3 | 8 7 4 | 8 7 5 | 8 7 6 | 8 7 7 | 8 7 8 | 8 7 9 | 8 8 0 | 8 8 1 | 8 8 2 | 8 8 3 | 8 8 4 | 8 8 5 | 8 8 6 | 8 8 7 | 8 8 8 | 8 8 9 | 8 8 0 |
| Ю | 9 0 0 | 9 0 1 | 9 0 2 | 9 0 3 | 9 0 4 | 9 0 5 | 9 0 6 | 9 0 7 | 9 0 8 | 9 0 9 | 9 1 0 | 9 1 1 | 9 1 2 | 9 1 3 | 9 1 4 | 9 1 5 | 9 1 6 | 9 1 7 | 9 1 8 | 9 1 9 | 9 2 0 | 9 2 1 | 9 2 2 | 9 2 3 | 9 2 4 | 9 2 5 | 9 2 6 | 9 2 7 | 9 2 8 | 9 2 9 | 9 2 0 | 9 2 1 |
| Я | 9 3 1 | 9 3 2 | 9 3 3 | 9 3 4 | 9 3 5 | 9 3 6 | 9 3 7 | 9 3 8 | 9 3 9 | 9 4 0 | 9 4 1 | 9 4 2 | 9 4 3 | 9 4 4 | 9 4 5 | 9 4 6 | 9 4 7 | 9 4 8 | 9 4 9 | 9 5 0 | 9 5 1 | 9 5 2 | 9 5 3 | 9 5 4 | 9 5 5 | 9 5 6 | 9 5 7 | 9 5 8 | 9 5 9 | 9 5 0 | 9 5 1 | 9 5 2 |

Рисунок 10 - Таблица шифрозамен для шифра Порты

Шифрование выполняется парами букв исходного сообщения. Первая буква пары указывает на строку шифрозамены, вторая - на столбец. В случае нечетного количества букв в исходном сообщении к нему добавляется вспомогательный символ («пустой знак»). Например, исходное сообщение «АБ РА МО В», зашифрованное – «002 466 355 093». В качестве вспомогательного символа использована буква «Я».

Шифр Playfair (англ. «Честная игра»). В начале 1850-х гг. Чарлз Уитстон придумал так называемый «прямоугольный шифр». Леон Плейфер, близкий друг Уитстона, рассказал об этом шифре во время официального обеда в 1854 г. министру внутренних дел лорду Пальмерстону и принцу Альберту. А поскольку Плейфер был хорошо известен в военных и дипломатических кругах, то за творением Уитстона навечно закрепилось название «шифр Плейфера».

Данный шифр стал первым буквенным биграммным шифром (в биграммной таблице Порты использовались символы, а не буквы). Он был предназначен для обеспечения секретности телеграфной связи и применялся британскими войсками в Англо-бурской и Первой мировой войнах. Им пользовалась также австралийская служба береговой охраны островов во время Второй мировой войны.

Шифр предусматривает шифрование пар символов (биграмм). Таким образом, этот шифр более устойчив к взлому по сравнению с шифром простой замены, так как затрудняется частотный анализ. Он может быть проведен, но не для 26 возможных символов (латинский алфавит), а для $26 \times 26 = 676$ возможных биграмм. Анализ частоты биграмм возможен, но является значительно более трудным и требует намного большего объема зашифрованного текста.

Для шифрования сообщения необходимо разбить его на биграммы (группы из двух символов), при этом, если в биграмме встретятся два одинаковых символа, то между ними добавляется заранее оговоренный вспомогательный символ (в оригинале – **X**, для русского алфавита – **Я**). Например, «зашифрованное сообщение» становится «за ш и ф р о в а н н о е с о **Я** о б щ е н и е **Я**». Для формирования ключевой таблицы выбирается лозунг и далее она заполняется по правилам шифрующей системы Трисемуса. Например, для лозунга «ДЯДИНА» ключевая таблица выглядит следующим образом.

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

| | | | | | |
|---|---|---|---|---|---|
| Ь | Э | Ю | - | 1 | 2 |
|---|---|---|---|---|---|

Рисунок 11 - Ключевая таблица для шифра Playfair

Затем, руководствуясь следующими правилами, выполняется зашифровывание пар символов исходного текста:

1. Если символы биграммы исходного текста встречаются в одной строке, то эти символы замещаются на символы, расположенные в ближайших столбцах справа от соответствующих символов. Если символ является последним в строке, то он заменяется на первый символ этой же строки.

2. Если символы биграммы исходного текста встречаются в одном столбце, то они преобразуются в символы того же столбца, находящимися непосредственно под ними. Если символ является нижним в столбце, то он заменяется на первый символ этого же столбца.

3. Если символы биграммы исходного текста находятся в разных столбцах и разных строках, то они заменяются на символы, находящиеся в тех же строках, но соответствующие другим углам прямоугольника.

Пример шифрования.

- биграмма «за» формирует прямоугольник – заменяется на «жб»;
- биграмма «ши» находятся в одном столбце – заменяется на «юе»;
- биграмма «фр» находятся в одной строке – заменяется на «хс»;
- биграмма «ов» формирует прямоугольник – заменяется на «йж»;
- биграмма «ан» находятся в одной строке – заменяется на «ба»;
- биграмма «но» формирует прямоугольник – заменяется на «ам»;
- биграмма «ес» формирует прямоугольник – заменяется на «гт»;
- биграмма «оя» формирует прямоугольник – заменяется на «ка»;
- биграмма «об» формирует прямоугольник – заменяется на «па»;
- биграмма «ще» формирует прямоугольник – заменяется на «шё»;
- биграмма «ни» формирует прямоугольник – заменяется на «ан»;
- биграмма «ея» формирует прямоугольник – заменяется на «ги».

Шифрограмма – «жб юе хс йж ба ам гт ка па шё ан ги».

Для расшифровки необходимо использовать инверсию этих правил, откидывая символы **Я** (или **Х**), если они не несут смысла в исходном сообщении.

Шифр Хилла. Первый практически реализуемый способ шифрования с использованием алгебры был придуман в 1929 г. математиком Лестером Хиллом - профессором из Хантер-колледжа в Нью-Йорке, статья которого «Cryptography in an Algebraic Alphabet» была опубликована в журнале «The American Mathematical Monthly».

Каждой букве алфавита сопоставляется число. Для русского алфавита можно использовать простейшую схему: А = 0, Б = 1, ..., Я = 32. Для зашифрования блок исходного сообщения из **n** букв рассматривается как **n**-мерный вектор чисел и умножается на матрицу размером **n x n** по модулю 33. Данная матрица, совместно с кодовой таблицей сопоставления букв алфавита с числами, является ключом зашифрования. Для расшифрования применяется обратная матрица по модулю.

Например, для триграммных замен могут использоваться следующие матрицы зашифрования/ расшифрования.

$$\begin{array}{c} \left| \begin{array}{ccc} 6 & 27 & 1 \\ 13 & 16 & 32 \\ 28 & 17 & 15 \end{array} \right| \quad \left| \begin{array}{ccc} 2 & 26 & 17 \\ 26 & 20 & 4 \\ 13 & 30 & 21 \end{array} \right| \\ \text{матрица} \quad \quad \text{матрица} \\ \text{зашифрования} \quad \text{расшифрования} \end{array}$$

Рис.5.12. Матрицы зашифрования/ расшифрования

Исходное сообщение «АБРАМОВ», дополненное двумя вспомогательными буквами «яя» (для кратности трем), после сопоставления букв с числами будет выглядеть следующим образом «0 1 17 0 13 15 2 32 32». После перемножения троек чисел на матрицу зашифрования шифрограмма примет следующий вид «11 32 8 3 28 17 17 11 24» (или в буквенном эквиваленте «КЯЗ ГЪР РКЧ»).

АБР - 0 1 17

$$(6 * 0 + 27 * 1 + 1 * 17) \bmod 33 = 11 \quad (\text{К})$$

$$(13 * 0 + 16 * 1 + 32 * 17) \bmod 33 = 32 \quad (\text{Я})$$

$$(18 * 0 + 17 * 1 + 15 * 17) \bmod 33 = 8 \quad (\text{З})$$

АМО - 0 13 15

$$(6 * 0 + 27 * 13 + 1 * 15) \bmod 33 = 3 \quad (\text{Г})$$

$$(13 * 0 + 16 * 13 + 32 * 15) \bmod 33 = 28 \quad (\text{Ђ})$$

$$(28 * 0 + 17 * 13 + 15 * 15) \bmod 33 = 17 \quad (\text{Р})$$

Вяя - 2 32 32

$$(6 * 2 + 27 * 32 + 1 * 32) \bmod 33 = 17 \quad (\text{Р})$$

$$(13 * 2 + 16 * 32 + 32 * 32) \bmod 33 = 11 \quad (\text{К})$$

$$(28 * 2 + 17 * 32 + 15 * 32) \bmod 33 = 24 \quad (\text{Ч})$$

Для расшифрования тройки чисел шифрограммы необходимо умножить на матрицу расшифрования.

КЯЗ - 11 32 8

$$(2 * 11 + 26 * 32 + 17 * 8) \bmod 33 = 0 \quad (\text{А})$$

$$(26 * 11 + 20 * 32 + 4 * 8) \bmod 33 = 1 \quad (\text{Б})$$

$$(13 * 11 + 30 * 32 + 21 * 8) \bmod 33 = 17 \quad (\text{Р})$$

ГЪР - 3 28 17

$$(2 * 3 + 26 * 28 + 17 * 17) \bmod 33 = 0 \quad (\text{А})$$

$$(26 * 3 + 20 * 28 + 4 * 17) \bmod 33 = 13 \quad (\text{М})$$

$$(13 * 3 + 30 * 28 + 21 * 17) \bmod 33 = 15 \quad (\text{О})$$

РКЧ - 17 11 24

$$(2 * 17 + 26 * 11 + 17 * 24) \bmod 33 = 2 \quad (\text{В})$$

$$(26 * 17 + 20 * 11 + 4 * 24) \bmod 33 = 32 \quad (\text{Я})$$

$$(13 * 17 + 30 * 11 + 21 * 24) \bmod 33 = 32 \quad (\text{Я})$$

В результате будет получен набор чисел «0 1 17 0 13 15 2 32 32», соответствующий исходному сообщению со вспомогательными символами «АБРАМОВяя».

Полиграммные (др.-греч. πολύς – многочисленный и греч. γράμμα – знак, буква).

Обратная матрица – матрица A^{-1} , при умножении на которую, исходная матрица A дает в результате единичную матрицу E .

Нерегулярные шифры

Еще одним направлением повышения стойкости шифров замены заключается в использовании нерегулярных шифров. В приведенных выше шифрах (**регулярных**) шифрозамены состоят из строго определенного количества символов (букв, цифр, графических элементов и т.д.) или в шифрограмме они отделяются друг от друга специальными символами (пробелом, точкой, запятой и т.д.). В нерегулярных шифрах шифрозамены состоят из разного количества символов и записываются в шифрограмме подряд (без выделения друг от друга), что значительно затрудняет криптоанализ.

Совмещенный шифр (совмещенная таблица) [43]. Данный шифр применялся еще семейством Ардженти - криптологами, разрабатывавшими шифры для Папы Римского в XVI в. В XX столетии этим способом пользовались коммунисты в ходе гражданской войны в Испании. В начале войны противники фашизма в Испании контролировали большинство крупных городов и защищали свою связь, включая радиопередачи, с помощью различных методов шифрования, в том числе совмещенных шифров.

Вариант коммунистов получил название «совмещенный» из-за необычного использования одно- и двухцифровых шифрозамен, благодаря чему сообщение приобретало дополнительную защиту от потенциального дешифровальщика. Некоторые буквы зашифровывались одной цифрой, другие же - парой цифр. При этом криптоаналитик противника совершенно не представлял, где в перехваченных сообщениях находятся одноцифровые, а где двухцифровые шифрозамены.

Таблица шифрозамен состоит из 10 столбцов с нумерацией 0, 9, 8, 7, 6, 5, 4, 3, 2 и 1. В начальную строку вписывается ключевое слово без повторяющихся букв. В последующие строки вписываются по десять не вошедших в него букв по порядку следования в алфавите. Строки, за исключением начальной, нумеруются по порядку, начиная с 1.

| | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|
| | 0 | 9 | 8 | 7 | 6 | 5 | 4 | 3 | 2 | 1 |
| | Д | Я | И | Н | А | | | | | |
| 1 | Б | В | Г | Е | Ё | Ж | З | Й | К | Л |
| 2 | М | О | П | Р | С | Т | У | Ф | Х | Ц |

| | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|
| 3 | ч | ш | щ | ъ | ы | ь | э | ю | - | - |
|---|---|---|---|---|---|---|---|---|---|---|

Рисунок 13 - Пример таблицы шифрозамен совмещенного шифра с ключевым словом «ДЯДИНА»

При шифровании буквы исходного сообщения, входящие в ключевое слово, заменяются на одну цифру (номер столбца), остальные – двумя (номера строки и столбца). Например, для приведенной выше таблицы шифрозамен исходное сообщение «АБРАМОВ» будет зашифровано как «610276202919».

При получении шифрограммы адресат знает, что когда появляются цифры 1, 2 или 3, с ними обязательно связана еще одна цифра, поскольку они представляют собой цифровую пару. Так что 35 - это, несомненно, пара, а 53 - нет, ведь в таблице нет строки с номером 5. Перехват такого сообщения третьей стороной даст ей всего лишь ряд цифр, потому что криптоаналитик противника не имеет ни малейшего представления, какие цифры одиночные, а какие входят в состав пар.

Омофонические шифры

Другое направление повышения стойкости шифров замены состоит в том, чтобы каждое множество шифрообозначений M_i для отдельного i -го символа исходного алфавита содержало более одного элемента. При использовании такого шифра одну и ту же букву (если она встречается несколько раз в сообщении) заменяют на разные шифрозамены из M_i . Это позволяет скрыть истинную частоту встречаемости букв открытого сообщения.

Система омофонов. В 1401 г. Симеоне де Крема стал использовать таблицы омофонов для сокрытия частоты появления гласных букв в тексте при помощи более чем одной шифрозамены. Такие шифры позже стали называться **шифрами многозначной замены** или **омофонами**³. Они получили развитие в XV веке. В книге «Трактат о шифрах» Леона Баттисты Альберти

(итальянский ученый, архитектор, теоретик искусства, секретарь папы Климентия XII), опубликованной в 1466 г., приводится описание шифра замены, в котором каждой букве ставится в соответствие несколько эквивалентов, число которых пропорционально частоте встречаемости буквы в открытом тексте. Так, если ориентироваться на табл.5.2, то число шифрозамен для буквы **О** должно составлять 110, для буквы **Е** – 85 и т.д. При этом каждая шифрозамена должна состоять из 3 цифр и их общее количество равно 1000. На рис.5.12 представлен фрагмент таблицы шифрозамен.

| № п/п | А | Б | В | ... | М | ... | О | ... | Р | ... | Я |
|-------|-----|-----|-----|-----|-----|-----|-----|-----|-----|-----|-----|
| 1 | 311 | 128 | 175 | ... | 037 | ... | 248 | ... | 064 | ... | 266 |
| 2 | 357 | 950 | 194 | ... | 149 | ... | 267 | ... | 189 | ... | 333 |
| ... | ... | ... | ... | ... | ... | ... | ... | ... | ... | ... | ... |
| 16 | 495 | 990 | 199 | ... | 349 | ... | 303 | ... | 374 | ... | 749 |
| ... | ... | | ... | ... | ... | ... | ... | ... | ... | ... | ... |
| 20 | 519 | | 427 | ... | 760 | ... | 306 | ... | 469 | ... | 845 |
| ... | ... | | ... | ... | ... | ... | ... | ... | ... | | |
| 32 | 637 | | 524 | ... | 777 | ... | 432 | ... | 554 | | |
| ... | ... | | ... | | | | ... | ... | ... | | |
| 45 | 678 | | 644 | | | | 824 | ... | 721 | | |
| ... | ... | | | | | | ... | ... | ... | | |
| 47 | 776 | | | | | | 828 | ... | 954 | | |
| ... | ... | | | | | | ... | | | | |
| 80 | 901 | | | | | | 886 | | | | |
| ... | | | | | | | ... | | | | |
| 110 | | | | | | | 903 | | | | |

Рисунок 14 - Фрагмент таблицы шифрозамен для системы омофонов

При шифровании символ исходного сообщения заменяется на любую шифрозамену из своего столбца. Если символ встречается повторно, то, как правило, используют разные шифрозамены. Например, исходное сообщение

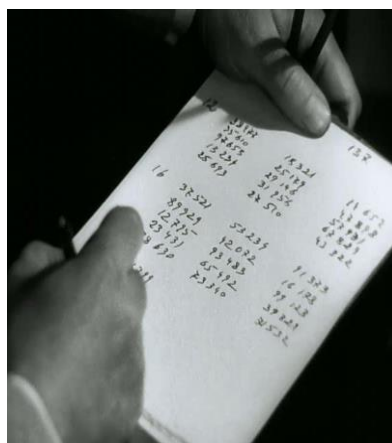
«АБРАМОВ» после шифрования может выглядеть «357 990 374 678 037 828 175».

Книжный шифр. Заметным вкладом греческого ученого Энея Тактика в криптографию является предложенный им так называемый книжный шифр, описанный в сочинении «Об обороне укреплённых мест». Эней предложил прокалывать малозаметные дырки в книге или в другом документе над буквами секретного сообщения. Интересно отметить, что в Первой мировой войне германские шпионы использовали аналогичный шифр, заменив дырки на точки, наносимые симпатическими чернилами⁴ на буквы газетного текста. Описанные способы передачи секретных сообщений (с помощью точек) относятся к стеганографическим методам сокрытия информации.

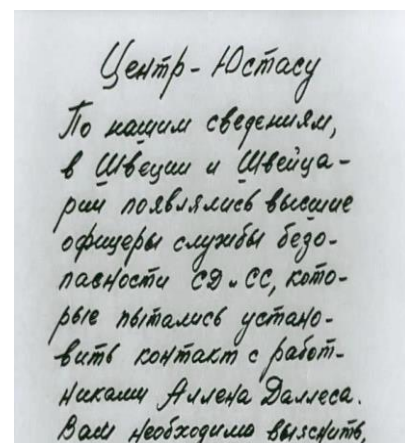
После Первой мировой войны книжный шифр приобрел иной вид. Шифрозамена для каждой буквы определялась набором цифр, которые указывали на номер страницы, строки и позиции в строке.



а) ключ



б) шифрограмма



в) сообщение

(4-й том собрания
сочинений Ф.Шиллера)

Рисунок 15 - Пример использования книжного шифра
(кадры из советского сериала «Семнадцать мгновений весны»)

Количество книг, изданных за всю историю человечества, является величиной ограниченной (по крайней мере, явно меньше, чем 15!). Однако

отсутствие полной электронной базы по изданиям делает процедуру вскрытия шифрограмм почти не выполнимой.

Вариантные шифры. Вариантные шифры напоминают полибианский квадрат, но для каждой строки и столбца используется по два буквенных идентификатора. В квадрат (прямоугольник) шифрозамен вначале записывается ключевое слово без повторяющихся букв, а затем дополняется не вошедшими в него буквами по порядку следования в алфавите. Каждой строке и столбцу квадрата ставится в соответствие по две буквы алфавита. Буквы для идентификации строк и столбцов не должны повторяться.

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

Рисунок 16 - Пример таблицы шифрозамен вариантного шифра с ключевым словом «ДЯДИНА»

Комбинации букв-идентификаторов строки и столбца дают по восемь шифрозамен для каждой буквы исходного текста. Например, для буквы Д возможны шифрозамены: **ФЙ, ЙФ, ФЦ, ЦФ, ЫЙ, ЙЫ, ЫЦ** и **ЦЫ**. Для таблицы шифрозамен, приведенной на рис.5.16, исходное сообщение «АБРАМОВ» может быть зашифровано как «ЫЗ ЫХ ОЦ ЗФ ГР РЩ АЙ».

Омофоны (греч. ὁμός – одинаковый и φωνή – звук) – слова, которые звучат одинаково, но пишутся по-разному и имеют разное значение.

Симпатические (невидимые) чернила – чернила, записи которыми являются изначально невидимыми и становятся видимыми только при определенных условиях (нагрев, освещение, химический проявитель и т. д.).

Полиалфавитные шифры

В полиалфавитных шифрах используется нескольких алфавитов шифрозамен. Выбор варианта алфавита шифрозамен для зашифрования отдельного символа или блока символов зависит от особенностей шифра.

Диск Альберти. В «Трактате о шифрах» Альберти приводит первое точное описание многоалфавитного шифра на основе шифровального диска.



Рисунок 17 - Реплика диска Альберти, используемого Конфедерацией во время Гражданской войны в Америке [www.cryptomuseum.com]

Он состоял из двух дисков – внешнего неподвижного и внутреннего подвижного дисков, на которые были нанесены буквы алфавита. Процесс шифрования заключался в нахождении буквы открытого текста на внешнем диске и замене ее на букву с внутреннего диска, стоящую под ней. После этого

внутренний диск сдвигался на одну позицию и шифрование второй буквы производилось уже по новому шифралфавиту. Ключом данного шифра являлся порядок расположения букв на дисках и начальное положение внутреннего диска относительно внешнего.

Таблица Трисемуса. Одним из шифров, придуманных немецким аббатом Трисемусом, стал многоалфавитный шифр, основанный на так называемой «таблице Трисемуса» - таблице со стороной равной n , где n – количество символов в алфавите. В первой строке матрицы записываются буквы в порядке их очередности в алфавите, во второй – та же последовательность букв, но с циклическим сдвигом на одну позицию влево, в третьей – с циклическим сдвигом на две позиции влево и т.д.

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

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

Рисунок 18 - Таблица Трисемуса

Первая строка является одновременно и алфавитом для букв открытого текста. Первая буква текста шифруется по первой строке, вторая буква по второй и так далее. После использования последней строки вновь возвращаются к первой. Так сообщение «АБРАМОВ» приобретет вид «АВТГРУЗ».

Система шифрования Виженера. В 1586 г. французский дипломат Блез Виженер представил перед комиссией Генриха III описание простого, но довольно стойкого шифра, в основе которого лежит таблица Трисемуса.

Перед шифрованием выбирается ключ из символов алфавита. Сама процедура шифрования заключается в следующем. По *i*-ому символу открытого сообщения в первой строке определяется столбец, а по *i*-ому символу ключа в крайнем левом столбце – строка. На пересечении строки и столбца будет находиться *i*-ый символ, помещаемый в шифрограмму. Если длина ключа меньше сообщения, то он используется повторно. Например, исходное сообщение «АБРАМОВ», ключ – «ДЯДИНА», шифрограмма – «ДАФИЪОЁ».

Справедливости ради, следует отметить, что авторство данного шифра принадлежит итальянцу Джованни Батиста Беллазо, который описал его в 1553 г. История «проигнорировала важный факт и назвала шифр именем Виженера,

несмотря на то, что он ничего не сделал для его создания». Беллазо предложил называть секретное слово или фразу **паролем** (ит. password; фр. parole - слово).

В 1863 г. Фридрих Касиски опубликовал алгоритм атаки на этот шифр, хотя известны случаи его взлома шифра некоторыми опытными криптоаналитиками и ранее. В частности, в 1854 г. шифр был взломан изобретателем первой аналитической вычислительной машины Чарльзом Бэббиджем, хотя этот факт стал известен только в XX в., когда группа ученых разбирала вычисления и личные заметки Бэббиджа. Несмотря на это шифр Виженера имел репутацию исключительно стойкого к «ручному» взлому еще долгое время. Так, известный писатель и математик Чарльз Лютвидж Доджсон (Льюис Кэрролл) в своей статье «Алфавитный шифр», опубликованной в детском журнале в 1868 г., назвал шифр Виженера невзламываемым. В 1917 г. научно-популярный журнал «Scientific American» также отзывался о шифре Виженера, как о неподдающемся взлому.

Роторные машины. Идеи Альберти и Беллазо использовались при создании электромеханических роторных машин первой половины XX века. Некоторые из них использовались в разных странах вплоть до 1980-х годов. В большинстве из них использовались роторы (механические колеса), взаимное расположение которых определяло текущий алфавит шифрозамен, используемый для выполнения подстановки. Наиболее известной из роторных машин является немецкая машина времен Второй мировой войны «Энигма» [8].

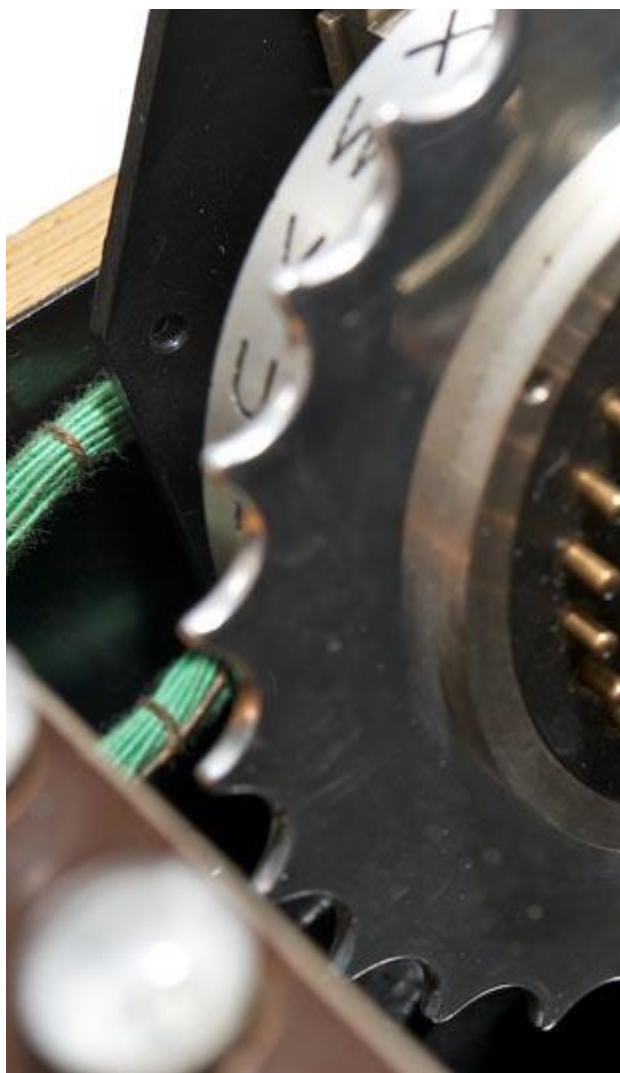


Рисунок 19 - Энигма [www.cryptomuseum.com]

Выходные штыри одного ротора соединены с входными штырями следующего ротора и при нажатии символа исходного сообщения на клавиатуре замыкали электрическую цепь, в результате чего загоралась лампочка с символом шифрозамены.



а) четыре последовательно соединённых ротора



б) штыри ротора

Рисунок 20 - Роторная система Энигмы [www.cryptomuseum.com]

Шифрующее действие «Энигмы» показано для двух последовательно нажатых клавиш - ток течёт через роторы, «отражается» от рефлексора, затем снова через роторы.

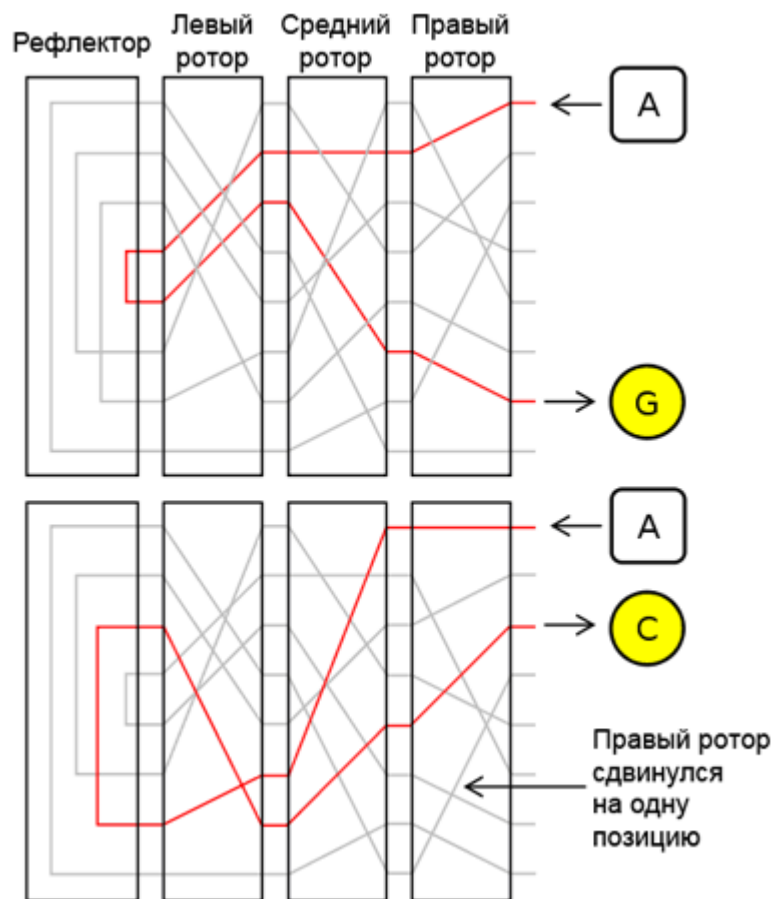


Рисунок 21 - Схема шифрования

Примечание. Серыми линиями показаны другие возможные электрические цепи внутри каждого ротора. Буква **А** шифруется по-разному при последовательных нажатиях одной клавиши, сначала в **Г**, затем в **С**. Сигнал идет по другому маршруту за счёт поворота одного из роторов после нажатия предыдущей буквы исходного сообщения.

Шифры Тени. Главными развлечениями для американцев тридцатых годов XX века были бульварное чтение и радио. Для раскрутки своих книжек издательство Street & Smith спонсировало радиопередачу, ведущим в которой был Тень (англ. Shadow), загадочный рассказчик со зловещим голосом, который в начале каждого выпуска заявлял: «Кто знает, что за зло прячется в сердцах людей? Тень знает!». Успех радиопередачи подтолкнул издательство к решению начать выпускать серию книг, в которой главным героем был бы Тень. Свои услуги предложил Уолтер Гибсон, большой любитель фокусов и

головоломок. Под псевдонимом Максвелл Грант он принялся писать роман за романом, да с такой скоростью, что за свою жизнь написал почти 300 книжек о грозе тех, кто нечист помыслами. В новелле «Цепочка смерти» супергерой воспользовался так называемым кодом направления, хотя на самом деле он действует скорее как шифр, чем как код.
























| | | | | | | | | |
|---|---|---|---|--|---|---|---|---|
|  |  |  |  |  |  |  |  |  |
| a | b | c | d | e | f | g | h | |
|  |  |  |  |  |  |  |  |  |
| n | o | p | q | r | s | t | u | |
|  | |  |  |  |  | | | |
| пробел | | 1 | 2 | 3 | 4 | | | |

Рисунок 22 - Таблица шифрозамен и управляющих символов

Управляющие символы в последней строке таблицы служат для изменения кода зашифрования/дешифрования (выбора шифралфавита). Линии внутри управляющего символа указывают адресату, как держать лист бумаги для дешифрования очередного символа шифрограммы. Символ 1 означает, что лист надо держать как обычно: верх и низ расположены на своих местах. Символ 2 требует для дешифрования очередного символа поворота листа на 90° вправо. Управляющие символы могут появляться перед любой строчкой текста, а также в ее середине.

Из нижеприведенного примера можно узнать настоящие имя и фамилию супергероя.

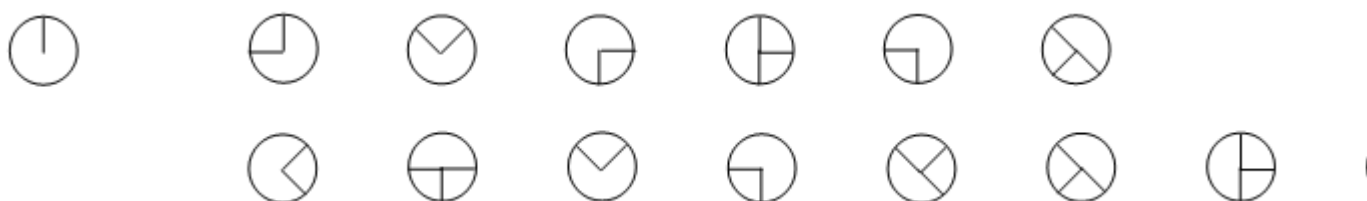


Рисунок 23 - Настоящие имя и фамилия Тени

Согласно первому управляющему символу, лист следует держать обычным образом, не поворачивая, и после замены буквы образуют «Lamont Cranston» (Ламонт Крэнстон).

Задания для самостоятельного выполнения

В лабораторной работе необходимо зашифровать свою фамилию имя отчество и номер группы и подгруппы (в текстовом виде) с помощью следующих шифров:

1. шифра Цезаря;
2. лозунгового шифра;
3. полибианского квадрата;
4. шифрующей системы Трисемуса;
5. шифра Playfair;
6. системы омофонов (допускается для каждой буквы алфавита привести всего по две шифрозамены, т.е. принять, что все буквы имеют одинаковую вероятность появления в текстах);
7. шифра Виженера;
8. шифра масонов;
9. биграммного шифра Порты;
10. шифра Хилла;
11. вариантного шифра;
12. шифра Тени;
13. совмещенного шифра.
14. шифрующей системы Трисемуса;
15. шифра Playfair;
16. шифра Виженера.

При оформлении отчета необходимо привести исходное сообщение (фамилию имя отчество, номер группы и номер подгруппы (в текстовом виде), таблицу шифрозамен, ключ (если таблица шифрозамен не является ключом) и зашифрованное сообщение. Привести алгоритм (блок схему и текстовое

описание), скриншоты выполнения программы и текст кода. Язык программирования выбирается любой. Вместе с отчетом прикрепляется исходники кода.

Вопросы для самопроверки

1. В чем заключается основная идея криптографических преобразований шифров замены?
2. Перечислите основные разновидности шифров замены.
3. Дайте характеристику разновидностям шифров замены.
4. Назовите основной недостаток шифра однозначной замены

Лабораторная работа №3. Шифры гаммирования

Основы шифрования

Шифры гаммирования (аддитивные шифры) являются самыми эффективными с точки зрения стойкости и скорости преобразований (процедур зашифрования и дешифрования). По стойкости данные шифры относятся к классу совершенных. Для зашифрования и дешифрования используются элементарные арифметические операции – открытое/зашифрованное сообщение и гамма, представленные в числовом виде, складываются друг с другом по модулю (**mod**). Напомним, что результатом сложения двух целых чисел по модулю является остаток от деления (например, $5+10 \bmod 4 = 15 \bmod 4 = 3$).

В литературе шифры этого класса часто называют потоковыми, хотя к потоковым относятся и другие разновидности шифров. В шифрах гаммирования может использоваться сложение по модулю N (общий случай) и по модулю 2 (частный случай, ориентированный на программно-аппаратную реализацию).

Сложение по модулю N. В 1888 г. француз маркиз де Виари в одной из своих научных статей, посвященных криптографии, доказал, что при замене букв исходного сообщения и ключа на числа справедливы формулы:

$$C_i = (P_i + K_i) \bmod N, \quad (1)$$

$$P_i = (C_i + N - K_i) \bmod N, \quad (2)$$

где P_i , C_i - i -ый символ открытого и зашифрованного сообщения;

N - количество символов в алфавите;

K_i - i -ый символ гаммы (ключа).

Данные формулы позволяют выполнить зашифрование / расшифрование по Виженеру при замене букв алфавита числами согласно следующей таблице (применительно к русскому алфавиту):

Таблица 1. Таблица кодирования символов

| | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|
| А | Б | В | Г | Д | Е | Ё | Ж | З | И | Й | К | Л | М | Н | О | П | Р | С | Т | У | Ф | Х | Ц | Ч | Ш | Щ | Ъ | Ы | Ь | Э | Ю | Я |
| 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 | 14 | 15 | 16 | 17 | 18 | 19 | 20 | 21 | 22 | 23 | 24 | 25 | 26 | 27 | 28 | 29 | 30 | 31 | 32 |

Например, для шифрования используется русский алфавит ($N = 33$), открытое сообщение – «АБРАМОВ», гамма – «ЖУРИХИН». При замене символов на числа буква **А** будет представлена как 0, **Б** – 1, ..., **Я** – 32. Результат шифрования показан в следующей таблице.

Таблица 2. Пример аддитивного шифрования по модулю $N = 33$

| | | | | | | | | |
|--------------------------------------|----------------------------|---|----|----|---|----|----|----|
| С и м м о д у л | открытого сообщения, P_i | А | Б | Р | А | М | О | В |
| | | 0 | 1 | 17 | 0 | 13 | 15 | 2 |
| | гаммы, K_i | Ж | У | Р | И | Х | И | Н |
| | | 7 | 20 | 17 | 9 | 22 | 9 | 14 |
| | шифrogramмы, C_i | Ж | Ф | Б | И | В | Ч | П |
| | | 7 | 21 | 1 | 9 | 2 | 24 | 16 |

Сложение по модулю 2 (шифр Вернама). Значительный успех в криптографии связан с именем американца Гильберто Вернама. В 1917 г. он, будучи сотрудником телеграфной компании АТ&Т, совместно с Мейджором Джозефом Моборном предложил идею автоматического шифрования телеграфных сообщений. Речь шла о своеобразном наложении гаммы на знаки алфавита, представленные в соответствии с телетайпным кодом Бодо пятизначными «импульсными комбинациями». Например, буква **А** представлялась комбинацией («— — — + +»), а комбинация («+ + — + +») означала переход от букв к цифрам. На бумажной ленте, используемой при работе телетайпа, знаку «+» соответствовало наличие отверстия, а знаку «—» - его отсутствие. При считывании с ленты металлические щупы проходили через отверстия, замыкали электрическую цепь и, тем самым, посылали в линию импульс тока.



Рисунок 1 - Шифровальная машина Siemens M-190

[www.cryptomuseum.com]

Вернам предложил электромеханически покоординатно складывать «импульсы» знаков открытого текста с «импульсами» гаммы, предварительно нанесенными на ленту. Сложение проводилось «по модулю 2» (\oplus , для булевых величин аналог этой операции – XOR, «Исключающее ИЛИ»). Имеется в виду, что если «+» отождествить с 1, а «-» с 0, то сложение определяется двоичной арифметикой:

| | | |
|----------|---|---|
| \oplus | 0 | 1 |
| 0 | 0 | 1 |
| 1 | 1 | 0 |

Таким образом, при данном способе шифрования символы текста и гаммы представляются в двоичном виде, а затем каждая пара двоичных разрядов складывается по модулю 2. Процедуры шифрования и дешифрования выполняются по следующим формулам:

$$C_i = P_i \oplus K_i, \quad (6.3)$$

$$P_i = C_i \oplus K_i. \quad (6.4)$$

Вернам сконструировал и устройство для такого сложения. Замечательно то, что процесс шифрования оказался полностью автоматизированным. Кроме

того, оказались слитыми воедино процессы зашифрования / расшифрования и передачи по каналу связи.

В 1918 г. два комплекта соответствующей аппаратуры были изготовлены и испытаны. Испытания дали положительные результаты. Единственное неудовлетворение специалистов - криптографов было связано с гаммой. Дело в том, что первоначально гамма была нанесена на ленту, склеенную в кольцо. Несмотря на то, что знаки гаммы на ленте выбирались случайно, при зашифровании длинных сообщений гамма регулярно повторялась. Этот недостаток так же отчетливо осознавался, как и для шифра Виженера. Уже тогда хорошо понимали, что повторное использование гаммы недопустимо даже в пределах одного сообщения. Попытки удлинить гамму приводили к неудобствам в работе с большим кольцом. Тогда был предложен вариант с двумя лентами, одна из которых шифровала другую, в результате чего получалась гамма, имеющая длину периода, равную произведению длин исходных периодов.

Шифры гаммирования стали использоваться немцами в своих дипломатических представительствах в начале 1920-х гг., англичанами и американцами – во время Второй мировой войны. Разведчики-нелегалы ряда государств использовали **шифрблокноты**. Шифр Вернама применялся на правительственной «горячей линии» между Вашингтоном и Москвой, где ключевые материалы представляли собой перфорированные бумажные ленты, производившиеся в двух экземплярах.



Рис.6.2. Одноразовый шифровальный блокнот (СССР, ГДР, 1960-е гг.)
[www.cryptomuseum.com]

Перед иллюстрацией использования шифра приведем таблицу кодов символов Windows 1251 и их двоичное представление.

Таблица 3. Коды символов Windows 1251 и их двоичное представление

| Буква | Дес-код | Bin-код | Буква | Дес-код | Bin-код | Буква | Дес-код | Bin-код |
|-------|---------|-----------|-------|---------|-----------|-------|---------|-----------|
| А | 192 | 1100 0000 | Л | 203 | 1100 1011 | Ц | 214 | 1101 0110 |
| Б | 193 | 1100 0001 | М | 204 | 1100 1100 | Ч | 215 | 1101 0111 |
| В | 194 | 1100 0010 | Н | 205 | 1100 1101 | Ш | 216 | 1101 1000 |
| Г | 195 | 1100 0011 | О | 206 | 1100 1110 | Щ | 217 | 1101 1001 |
| Д | 196 | 1100 0100 | П | 207 | 1100 1111 | Ъ | 218 | 1101 1010 |
| Е | 197 | 1100 0101 | Р | 208 | 1101 0000 | Ы | 219 | 1101 1011 |
| Ж | 198 | 1100 0110 | С | 209 | 1101 0001 | Ь | 220 | 1101 1100 |
| З | 199 | 1100 0111 | Т | 210 | 1101 0010 | Э | 221 | 1101 1101 |
| И | 200 | 1100 1000 | У | 211 | 1101 0011 | Ю | 222 | 1101 1110 |
| Й | 201 | 1100 1001 | Ф | 212 | 1101 0100 | Я | 223 | 1101 1111 |
| К | 202 | 1100 1010 | Х | 213 | 1101 0101 | | | |

Примечание. Дес-код – десятичный код символа, Bin-код – двоичный код символа.

Пример шифрования сообщения «ВОВА» с помощью ключа «ЮЛЯ» показан в следующей таблице. Так как длина ключа меньше длины открытого сообщения, то для генерации гаммы он циклически повторяется.

Таблица 4. Пример аддитивного шифрования по модулю 2

| | | | | | |
|---------------------------|---------|-----------|-----------|-----------|-----------|
| Открытое сообщение, P_i | Буква | В | О | В | А |
| | Дес-код | 194 | 206 | 194 | 192 |
| | Bin-код | 1100 0010 | 1100 1110 | 1100 0010 | 1100 0000 |
| Гамма, K_i | Буква | Ю | Л | Я | Ю |
| | Дес-код | 222 | 203 | 223 | 222 |
| | Bin-код | 1101 1110 | 1100 1011 | 1101 1111 | 1101 1110 |
| Шифрограмма, C_i | Дес-код | 28 | 5 | 29 | 30 |
| | Bin-код | 0001 1100 | 0000 0101 | 0001 1101 | 0001 1110 |

Шифрование по модулю 2 обладает замечательным свойством - вместо истинной гаммы противнику можно сообщить ложную гамму, которая при наложении на шифрограмму даст осмысленное выражение.

Таблица 5. Пример использования ложной гаммы

| | | | | | |
|---|---------|-----------|-----------|-----------|-----------|
| Шифрограмма, C_i | Дес-код | 28 | 5 | 29 | 30 |
| | Bin-код | 0001 1100 | 0000 0101 | 0001 1101 | 0001 1110 |
| Ложная гамма, K'_i | Буква | Ю | Е | М | Б |
| | Дес-код | 222 | 197 | 204 | 193 |
| | Bin-код | 1101 1110 | 1100 0101 | 1100 1100 | 1100 0001 |
| Ложное открытое сообщение, P'_i | Дес-код | 194 | 192 | 209 | 223 |
| | Bin-код | 1100 0010 | 1100 0000 | 1101 0001 | 1101 1111 |
| | Буква | В | А | С | Я |

Пример, представленный в таблице, иллюстрирует совершенность шифров гаммирования. Для перехваченной шифрограммы противник может подобрать большое количество гамм, дающих при расшифровании осмысленные сообщения и не имеющих ничего общего с истинным открытым сообщением. Более того, под любое ложное открытое сообщение найдется ложная гамма.

Стойкость аддитивных шифров определяется, главным образом, качеством гаммы, которое зависит от длины периода и случайности распределения по периоду.

Длиной периода гаммы называется минимальное количество символов, после которого последовательность начинает повторяться. **Случайность распределения символов по периоду** означает отсутствие закономерностей между появлением различных символов в пределах периода.

Для обеспечения абсолютной стойкости необходимо, чтобы последовательность символов в пределах периода гаммы обладала следующими свойствами:

- была случайной (должна отсутствовать закономерность в появлении символов гаммы);

- распределение символов алфавита гаммы должно быть близко к равномерному (равновероятному);
- совпадала по размеру или была больше исходного открытого текста;
- применялась только один раз.

Первые два свойства (требования) проверяются с помощью различных тестов. Наиболее популярный и авторитетный из них «Набор статистических тестов для генераторов случайных и псевдослучайных чисел для криптографических приложений» (англ. NIST SP 800-22 «A statistical test suite for random and pseudorandom number generators for cryptographic applications»), включающий в себя 15 тестов.

Классический одноразовый шифровальный блокнот - большой неповторяющийся случайный набор символов ключа, написанный на листах бумаги, склеенных в блокнот. Шифровальщик при личной встрече снабжался блокнотом, каждая страница которого содержала ключ. Такой же блокнот имелся и у принимающей стороны. Использованные страницы после однократного использования уничтожались.

Генерация случайных последовательностей

Несмотря на все достоинства шифров гаммирования, одной из ключевых проблем их применения на практике является получение качественных гамм. Для процедур зашифрования/дешифрования можно использовать истинно случайные или псевдослучайные гаммы (последовательности).

Псевдослучайная последовательность – последовательность чисел, которая была вычислена по определённой процедуре, но имеет все свойства случайной последовательности чисел в рамках решаемой задачи. Отличие истинно случайных последовательностей от псевдослучайных заключается в невозможности предсказания (расчета, определения) символов в ней. Таким образом, любой алгоритмически устроенный программно-аппаратный комплекс не может генерировать истинно случайные последовательности, т.к. он работает по строго определенным правилам, а значит результат (гамма) предсказуем. Как

сказал Джон фон Нейман, «всякий, кто питает слабость к арифметическим методам получения случайных чисел, грешен вне всяких сомнений» [63].

Истинно случайные гаммы могут быть получены путем оцифровки случайных физических или антропогенных процессов.

Псевдослучайные гаммы получают путем применения рекуррентных формул или полноценных алгоритмов. При этом отсутствие истинной случайности не мешает получать криптографически стойкие последовательности, в т.ч. и с бесконечным периодом.

Рекуррентная формула - формула вида $a_n = f(n, a_{n-1}, a_{n-2}, \dots, a_{n-p})$, определяющая каждый член последовательности a_n , как функцию от p предыдущих членов и возможно номера члена последовательности n .

Генерация истинно случайных последовательностей

Как было отмечено выше, генерация истинно случайных последовательностей возможна путем оцифровки случайных физических или антропогенных процессов.

Среди **физических процессов**, которые рассматривались в качестве источника случайных последовательностей, можно выделить следующие:

- **дробовый шум** – беспорядочные изменения (флуктуации) принимаемого или передаваемого сигнала относительно его среднего значения, вызванные дискретностью потоков фотонов и электронов в оптических и радиоэлектронных устройствах;

- **тепловой шум** – равновесный шум, обусловленный тепловым движением носителей заряда в проводнике, в результате чего на концах проводника возникает флуктуирующая разность потенциалов. В микропроцессорах Intel с архитектурой Ivy Bridge для аппаратной генерации случайных последовательностей используется тепловой шум в кристаллах кремния. Для усиления энтропии поток битов проходит дополнительную фильтрацию и шифрование AES в режимах CBC и CRT;



Рисунок 3 - Микропроцессор Core i7-3770 с архитектурой Ivy Bridge и инструкцией генерации случайных чисел RdRand

- движение жидкостей в лавовых лампах. Компания CloudFlare, через сеть которой проходит до 10% трафика Интернета, в качестве одного из источников случайных последовательностей использует стену с сотней лавовых ламп;

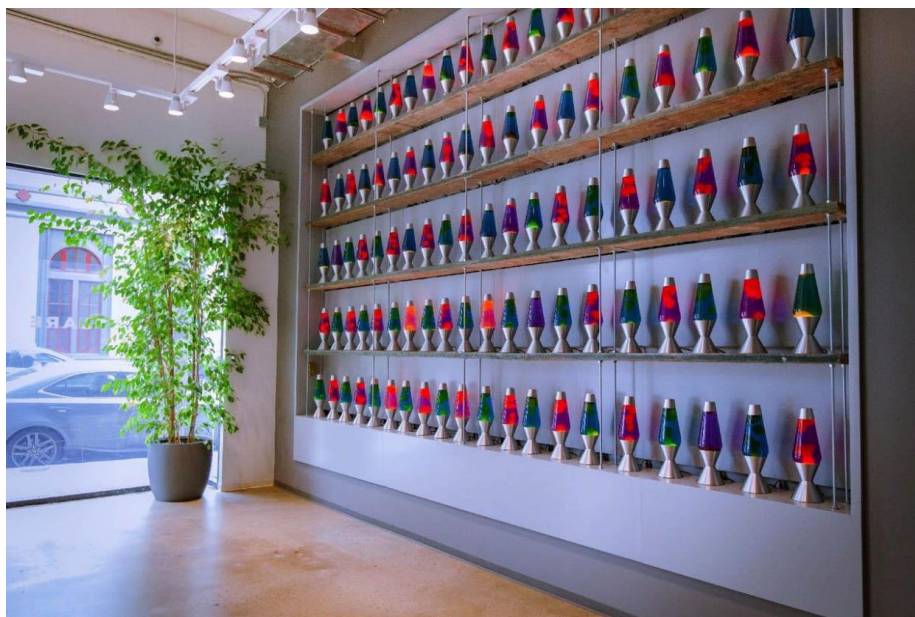


Рисунок 4 - «Стена энтропии» в компании CloudFlare

- движение ленточек в потоке воздуха вентилятора;



Рисунок 5 - Хаотичное движение ленточек в потоке воздуха

- **радиоактивный распад** – спонтанное изменение состава или внутреннего строения нестабильных атомных ядер путём испускания элементарных частиц, гамма-квантов и/или ядерных фрагментов. Компания CloudFlare в качестве одного из источников случайных последовательностей использует радиоактивный элемент;



Рисунок 6 - Счетчик Гейгера

- **электромагнитное излучение** – электромагнитные волны, возникающие при возмущении магнитного или электрического поля. Генераторы случайных

последовательностей на базе квантовых явлений предлагает большое количество компаний (ID Quantique, QuintessenceLabs, ComScire и др.);



Рисунок 7 - Квантовый генератор случайных чисел
[www.idquantique.com/random-number-generation/overview]

- **лавинный пробой в полупроводниках** – электрический пробой р-п-перехода, вызванный лавинным размножением носителей заряда под действием сильного электрического поля;

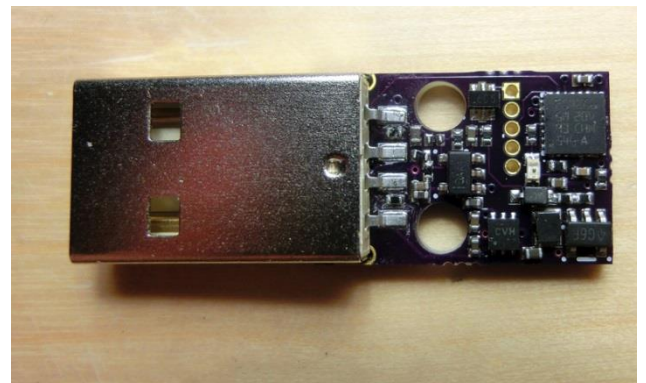


Рисунок 8 - Устройство ChaosKey [altusmetrum.org/ChaosKey]

- нестабильная частота свободно работающего осциллятора. Компания RAND использовала это явление для публикации в 1955 г. книги «Миллион случайных цифр со стандартным отклонением 100 000», а компания AT&T в 1986 г. представила коммерческую микросхему-генератор.

К **антропогенным процессам**, используемых в качестве источника случайных последовательностей, можно отнести следующие:

- время между нажатиями клавиш;

- движения компьютерной мыши;
- изменение скорости вращения жесткого диска, вызванного турбулентностью воздуха;
- время между принятыми пакетами в сети (например, пинг сайта Google).

Для большинства рассмотренных выше генераторов на базе физических и антропогенных процессов характерны определенные **недостатки**:

- необходимость передачи гаммы всем участникам обмена данными. Так как гамма генерируется в одном месте и она случайна, то принимающая данные сторона для расшифровки предварительно должна получить эту гамму (проблема обмена ключами);
- медленная скорость генерации числовых последовательностей;
- антропогенные процессы могут иметь скрытые зависимости – каждый пользователь обладает своим «подчерком» работы с компьютером.

В заключение обзора генераторов истинно случайных последовательностей рассматривается оригинальный метод, предложенный в 2013 г. учеными Корнельского университета. Кратко принцип нового метода шифрования заключается в том, что отправитель и получатель (Алиса и Боб) во время встречи формируют общий ключ, облучая кусочки стекла изображением-паттерном с ID_i (внешне он напоминает QR-код). В результате отражения и преломления, характер которого индивидуален для каждого куска стекла, у Алисы и Боба получаются собственные случайные изображения, которые затем оцифровываются (получаются ключи $keyA_i$ и $keyB_i$). Из этих изображений и составляется общий ключ ($keyAB_i = keyA_i \oplus keyB_i$).

Схема генерации одного общего ключа показана на следующем рисунке.

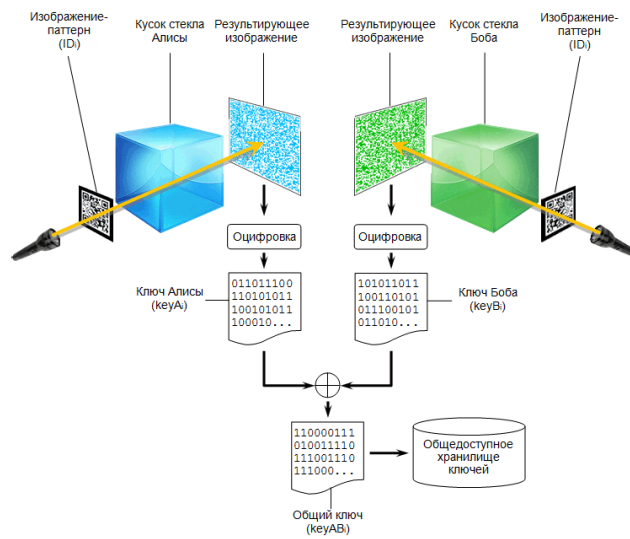


Рисунок 9 - Схема генерации одного общего ключа

Как и в классической системе Вернама, каждый случайный паттерн (ключи $keyA_i$, $keyB_i$ и $keyAB_i$) можно использовать лишь однажды. В связи с этим Алиса и Боб должны сформировать достаточное количество ключей, облучая свои куски стекла разными паттернами. После генерации общие ключи $keyAB_i$ помещаются в общедоступное хранилище.

Процедура обмена шифрограммами выглядит следующим образом.

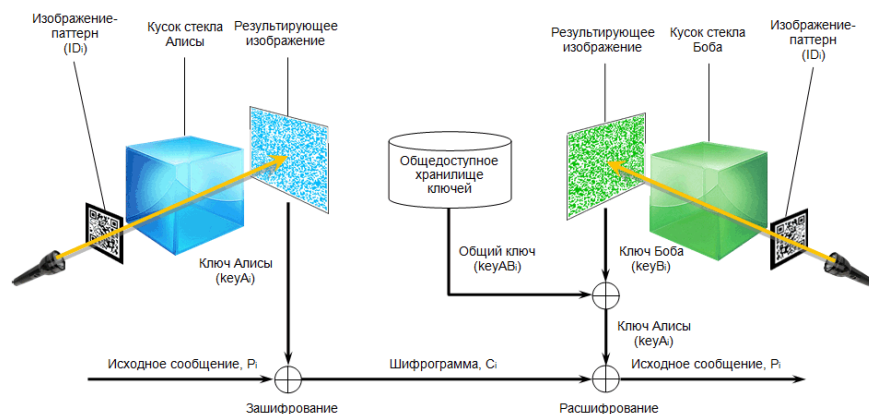


Рисунок 10 - Схема зашифрования и дешифрования сообщения

1) Алиса выбирает паттерн с ID_i , облучает свой кусочек стекла и оцифровывает полученное изображение, получая ключ $keyA_i$.

2) Исходное сообщение P_i Алиса складывает по модулю 2 с ключом $keyA_i$ ($C_i = P_i \oplus keyA_i$) и отправляет шифрограмму C_i с идентификатором паттерна ID_i Бобу.

3) Боб по полученному идентификатору ID_i из общедоступного хранилища считывает общий ключ $keyAB_i$ и, облучая паттерн с ID_i и свой кусочек стекла, генерирует собственный ключ $keyB_i$.

4) Складывая по модулю 2 ключи $keyAB_i$ и $keyB_i$, Боб получает ключ $keyA_i$ ($keyA_i = keyAB_i \oplus keyB_i$).

5) Для прочтения исходного сообщения P_i Боб складывает по модулю 2 шифрограмму C_i и ключ $keyA_i$ ($P_i = C_i \oplus keyA_i$).

По утверждению авторов схемы, взломать шифр Вернама можно только украв сами кусочки полупрозрачного стекла. Однако даже в этом случае у Алисы и Боба будет около 24 часов на определение факта кражи, поскольку злоумышленнику потребуется определить структуру стеклянного образца. Другие возможные проблемы при использовании данной схемы:

- потеря кусочка стекла;
- появление сколов и царапин на стекле;
- необходимость точного взаимного расположения и ориентации источника света, изображения-паттерна, кусочка стекла и полотна с результирующим изображением при оцифровке гаммы.

Информационная энтропия — мера неопределённости или непредсказуемости информации, неопределённость появления какого-либо символа первичного алфавита.

Генерация псевдослучайных последовательностей

Генераторы псевдослучайных последовательностей получили наибольшее распространение. По схеме использования они делятся на синхронные и самосинхронизирующиеся.

Схема шифрования с использованием **синхронных генераторов** представлена на следующем рисунке.

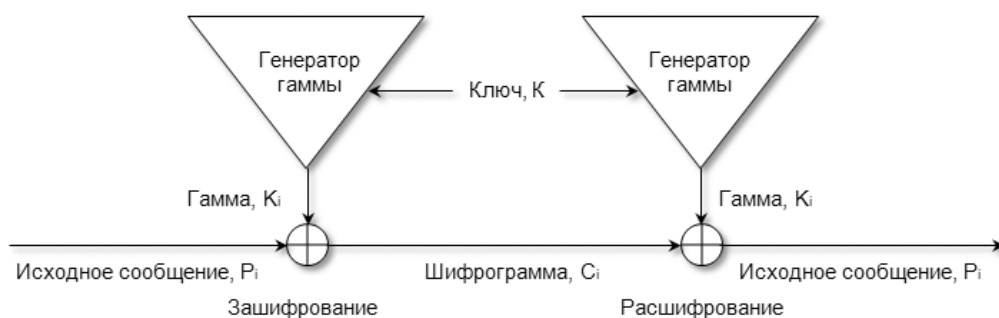


Рисунок 11 - Схема шифрования с использованием синхронных генераторов

При этом генератор гаммы, как правило, состоит из трех основных блоков.

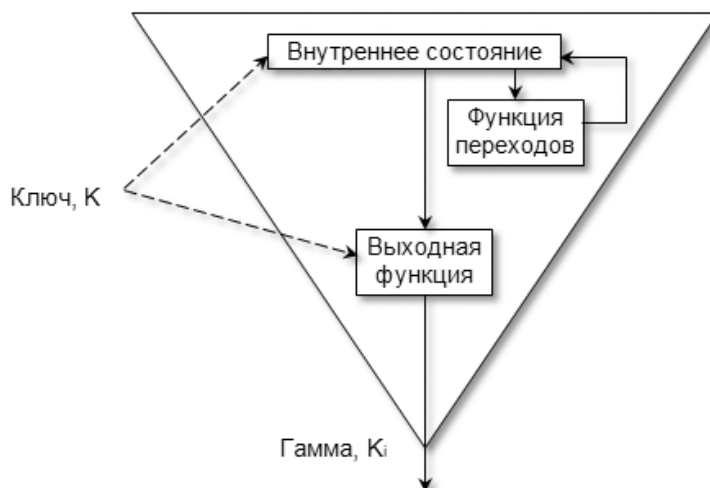


Рисунок 12 - Устройство генератора гаммы с внутренней обратной связью

Внутреннее состояние описывает текущее состояние генератора гаммы. **Начальное внутреннее состояние**, как правило, определяется ключом **К**. Два генератора, с одинаковым ключом и одинаковым внутренним состоянием, создают одинаковые гаммы. **Функция переходов** считывает текущее внутреннее состояние и генерирует новое внутреннее состояние. **Выходная функция** считывает внутреннее состояние и генерирует бит (биты) гаммы **K_i** .

В другой разновидности, так называемых **генераторах типа счетчик**, отсутствует блок с функцией переходов. В отличие от генераторов с обратной

связью, они позволяют вычислить i -й бит гаммы, не вычисляя всех предыдущих битов. Для этого генератор устанавливается в i -е внутреннее состояние, после чего вычисляется соответствующий ему i -й бит гаммы. Это свойство полезно использовать для обеспечения произвольного доступа к файлам данных, что позволяет расшифровать отдельный фрагмент данных, не расшифровывая файл полностью.

В синхронном генераторе гамма генерируется независимо от потока сообщения. На шифрующей стороне генератор гаммы последовательно выдает биты гаммы K_i . На расшифровывающей стороне другой генератор гаммы один за другим выдает идентичные биты гаммы. Эта схема работает нормально, если оба генератора синхронизированы.

Недостаток синхронного генератора. Если один из генераторов пропускает один из циклов или бит шифрограммы теряется при передаче, то все символы шифрограммы, следующие за ошибкой, расшифровываются некорректно. В этом случае отправитель и получатель должны синхронизировать генераторы и заново передать некорректно расшифрованную часть сообщения.

Достоинство синхронного генератора. Отсутствие распространения ошибок. Если во время передачи бит C_i изменит свое значение, что намного вероятнее его потери, то некорректно расшифровывается только один измененный бит.

В самосинхронизирующемся генераторе каждый бит гаммы представляет собой функцию фиксированного числа предыдущих битов шифрограммы. Используемые при таком шифровании генераторы гаммы называют генераторами с обратной связью по шифрограмме (шифртексту).

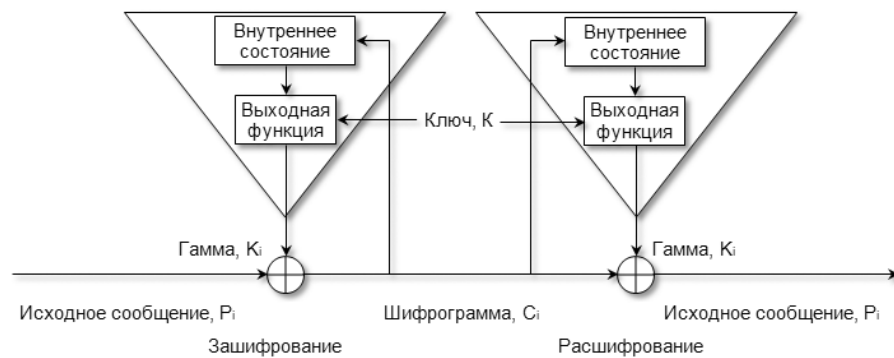


Рисунок 13 - Схема шифрования с использованием самосинхронизирующихся генераторов гаммы

Внутреннее состояние зависит от n предыдущих битов шифрограммы. Каждое сообщение начинается случайным заголовком (**вектор инициализации, синхропосылка**) длиной n бит, после прохождения которого оба генератора гаммы синхронизируются.

Недостатки самосинхронизирующегося генератора.

1. Распространение ошибки. Для каждого бита шифрограммы, искаженного при передаче, расшифровывающий генератор выдает n некорректных битов гаммы. Следовательно, измененный бит влияет на внутреннее состояние, каждой ошибке шифрограммы будет соответствовать n ошибок открытого текста.

2. При потере бита C_i необходимо заново передать часть сообщения, но в отличие от синхронных генераторов, синхронизация намного проще.

Для генерации псевдослучайных последовательностей используют рекуррентные формулы или полноценные алгоритмы. В первом случае члены числовой последовательности не только рассчитываются рекуррентно, но и впоследствии становятся частью гаммы. Во втором случае для генерации гаммы используются более сложные правила, в т.ч. для повышения энтропии гаммы могут применять хеш-функции и шифрование.

В качестве иллюстрации ниже приведены некоторые из них.

А) Рекуррентные формулы:

- линейный конгруэнтный генератор;
- инверсный конгруэнтный генератор;
- аддитивный генератор;
- регистр сдвига с линейной обратной связью.

А.1) Линейный конгруэнтный генератор – генератор псевдослучайных чисел, в котором новый член последовательности рассчитывается на базе предыдущего через линейную зависимость. В общем случае линейный конгруэнтный генератор задается выражением:

$$X_{i+1} = (a X_i + b) \bmod m, \quad (5)$$

где a , b и m – некоторые коэффициенты.

Алгоритм RANDU - один из вариантов линейного конгруэнтного генератора псевдослучайных чисел, десятилетиями использовавшийся на мейнфреймах. Он определяется рекуррентным соотношением:

$$X_{i+1} = (65539 X_i) \bmod 2^{31}, \quad (6)$$

где X_0 - нечётное.

Пример псевдослучайной последовательности, порождаемой алгоритмом RANDU при начальном значении $X_0 = 1$:

| | |
|-------------|-------------------------------------|
| 1 | |
| 65 | 539 |
| 393 | 225 |
| 1 | 769 499 |
| 7 | 077 969 |
| 26 | 542 323 |
| ... | |
| 388 | 843 697 |
| 238 606 867 | (повтор для элемента № 536 870 913) |

79 531 577

477 211 307

1

К сожалению, линейные конгруэнтные генераторы нельзя использовать в криптографии, т.к. они предсказуемы. Впервые линейные конгруэнтные генераторы были взломаны Джимом Ридсом, а затем Джоан Бояр [8]. Ей удалось также вскрыть **квадратичные генераторы**

$$X_{i+1} = (a X_i^2 + b X_i + c) \bmod m \quad (7)$$

и кубические генераторы

$$X_{i+1} = (a X_i^3 + b X_i^2 + c X_i + d) \bmod m. \quad (8)$$

А.2) Инверсный конгруэнтный генератор (генератор Эйхенауэра – Лена) – генератор псевдослучайных чисел, в котором новый член последовательности рассчитывается как обратное число к предыдущему по модулю. Общая формула генератора выглядит следующим образом:

$$X_{i+1} = (a X_i^{-1} + b) \bmod m, \quad (9)$$

где a , b и m – некоторые коэффициенты, $0 \leq a < m$, $0 \leq b < m$.

Как и в случае с линейным конгруэнтным генератором получаемая последовательность периодична с максимальным периодом m . Данные генераторы считаются более стойкими, но требуют значительных вычислений.

А.3) Аддитивный генератор (запаздывающий генератор Фибоначчи) – генератор псевдослучайных чисел, в котором новый член последовательности зависит более чем от одного из предшествующих. Одна из ранних реализаций

генератора последовательности Фибоначчи с запаздыванием была предложена 1958 г. Дж. Ж. Митчелом и Д. Ф. Муром:

$$X_{i+1} = (X_{i-a} + X_{i-b}) \bmod m, \quad (10)$$

где $a = 24, b = 55$ – запаздывание, $b > a \geq 1$;

$X_0 \dots X_{54}$ – произвольные целые числа;

m – чётное число.

Более сложные реализации аддитивных генераторов применяются в алгоритмах Fish, Pike, Mush и др.

А.4) Регистр сдвига с линейной обратной связью (РСЛОС) – упорядоченный набор битов, у которого значение входного (вдвигаемого слева, старшего) бита равно линейной булевой функции от значений остальных битов регистра до сдвига. Теорию последовательности регистров сдвига разработал в 1965 г. главный криптограф норвежского правительства Эрнст Селмер [8].

Длиной регистра называется количества битов в нем. В качестве булевой функции для РСЛОС чаще всего используют сложение по модулю 2. Такие РСЛОС обычно записывают в виде многочлена (полинома) или упорядоченной последовательности. Запись $x^8 + x^4 + x^3 + x^2 + 1$ или (8, 4, 3, 2, 0) означает, что длина регистра 8 битов, а входной бит рассчитывается по формуле $b_7 = b_4 \oplus b_3 \oplus b_2 \oplus b_0$ (для битов нумерация начинается справа и с нулевой позиции). Выходной (выдвигаемый справа, младший) бит будет являться частью генерируемой гаммы. Расчет требуемой гаммы осуществляется в цикле, на каждой итерации которого выполняются следующие операции.

1. Добавление выходного бита b_0 к гамме.
2. Расчет входного бита b_{n-1} по формуле.
3. Сдвиг битов регистра вправо на одну позицию.
4. Занесение рассчитанного входного бита b_{n-1} в позицию $n-1$.

В следующей таблице приведен пример генерации гаммы для регистра, инициализированного значением 10001100_2 .

Таблица 6. Пример генерации гаммы для РСЛОС $x^8 + x^4 + x^3 + x^2 + 1$

| № п/п | Исходное состояние регистра | Бит гаммы, b_0 | Входной бит, $b_7 = b_4 \oplus b_3 \oplus b_2 \oplus b_0$ | Сдвиг регистра вправо на одну позицию | Занесение входного бита b_7 в регистр |
|-------|-----------------------------|------------------|---|---------------------------------------|---|
| 0 | 1 0 0 0 1 1 0 0 | 0 | $0 \oplus 1 \oplus 1 \oplus 0 = 0$ | 1 0 0 0 1 1 0 | 0 1 0 0 0 1 1 0 |
| 1 | 0 1 0 0 0 1 1 0 | 0 | $0 \oplus 0 \oplus 1 \oplus 0 = 1$ | 0 1 0 0 0 1 1 | 1 0 1 0 0 0 1 1 |
| 2 | 1 0 1 0 0 0 1 1 | 1 | $0 \oplus 0 \oplus 0 \oplus 1 = 1$ | 1 0 1 0 0 0 1 | 1 1 0 1 0 0 0 1 |
| 3 | 1 1 0 1 0 0 0 1 | 1 | $1 \oplus 0 \oplus 0 \oplus 1 = 0$ | 1 1 0 1 0 0 0 | 0 1 1 0 1 0 0 0 |
| 4 | 0 1 1 0 1 0 0 0 | 0 | $0 \oplus 1 \oplus 0 \oplus 0 = 1$ | 0 1 1 0 1 0 0 | 1 0 1 1 0 1 0 0 |
| ... | ... | ... | ... | ... | ... |
| Гамма | | 00110... | | | |

Для регистра длиной n максимальное количество состояний составляет $2^n - 1$. Это число равно $2^n - 1$, а не 2^n , поскольку заполнение РСЛОС нулями влечет вывод регистром бесконечной последовательности нулей, что совершенно бесполезно. Таким образом, максимально возможная длина периода гаммы в битах составляет $(2^n - 1)$, если из регистра для гаммы на каждой итерации брать один бит. Для получения такого максимального периода многочлен должен быть примитивным по модулю

2. Примитивный многочлен степени n – неприводимый многочлен, который является делителем $x^{2^n-1} + 1$, но не является делителем $x^d + 1$ для всех d , являющихся делителями $2^n - 1$. Чем больше битов регистра используются для расчета входного бита, тем лучше (повышается стойкость). Многочлены с большим количеством членов называют **плотными**, с малым – **разреженными**.

РСЛОС обладают высокой скоростью генерации чисел, хорошими статистическими свойствами, а также возможностью простой реализации на аппаратном уровне. Исследователями предложено несколько десятков различных вариантов реализации генераторов на базе РСЛОС, в т.ч. с применением комбинации нескольких РСЛОС одновременно и разных функций расчета входного или выходного бита (регистры сдвига с нелинейной обратной связью, обобщенной обратной связью, обратной связью по переносу и т.д.).

Б) Алгоритмы:

- алгоритм Блум - Блум - Шуба;
- RC4;
- Trivium;
- генератор на базе иррациональных чисел.

Б.1) Алгоритм Блум - Блум - Шуба (англ. Algorithm Blum - Blum - Shub, BBS) предложен в 1986 г. Ленор Блум, Мануэлем Блюмом и Майклом Шубом.

Рекуррентная формула BBS выглядит следующим образом:

$$X_{i+1} = X_i^2 \bmod m, \quad (11)$$

где $m = p * q$ – является произведением двух больших простых p и q , сравнимых с 3 по модулю 4.

На каждом шаге алгоритма гамма получают из X_i путём взятия либо паритетного бита, либо одного или более младших битов X_i . Начальное значение X_0 должно быть **взаимно простым** с m – в противном случае у генерируемой последовательности быстро появляется период.

Пример с использованием двух малых простых чисел.

$$p = 7 \ (7 \bmod 4 = 3) \text{ и } q = 19 \ (19 \bmod 4 = 3).$$

$$m = 7 * 19 = 133.$$

$$X_0 = 53.$$

Таблица 7. Пример генерации гаммы по алгоритму BBS

| № п/п | X | | Четный паритетный бит | Младший бит | 2 младших бита |
|-------|---------|---------|-----------------------------|----------------|-------------------|
| | Дес-код | Bin-код | | | |
| 0 | 53 | 110101 | 0 | 1 | 01 |
| 1 | 16 | 10000 | 1 | 0 | 00 |
| 2 | 123 | 1111011 | 0 | 1 | 11 |
| 3 | 100 | 1100100 | 1 | 0 | 00 |
| 4 | 25 | 11001 | 1 | 1 | 01 |
| ... | ... | ... | ... | ... | ... |
| Гамма | | | 01011... | 10101... | 0100110001... |

Как было отмечено выше, X_0 должно быть взаимно простым с m . Если для генерации последовательности с параметрами $p = 7$, $q = 19$ и $m = 133$ выбрать $X_0 = 57 = 3 * 19$, то она будет состоять из одних $X_i = 57$ ($57^2 \bmod 133 = 57$). Таким образом, период последовательности будет равным 1, что не лучшим образом сказывается на качестве гаммы. Слишком малый период может возникать и в случае, когда X_0 и m взаимно просты. Например, если при тех же параметрах выбрать $X_0 = 130$, то последовательность будет выглядеть: 130, 9, 81, 44, 74, 23, 130, ...

Особенностью этого алгоритма является то, что для получения X_n необязательно вычислять все $n - 1$ предыдущих чисел, если известно начальное состояние генератора X_0 и числа p и q , то n -ное значение может быть вычислено по формуле:

$$X_n = X_0^{2^n \bmod ((p-1)(q-1))} \bmod m. \quad (12)$$

Б.2) RC4 (от англ. Rivest cipher или Ron's code) был создан сотрудником компании «RSA Security» Рональдом Ривестом в 1987 г. В течение семи лет шифр являлся коммерческой тайной, и точное описание алгоритма предоставлялось только после подписания соглашения о неразглашении, но в сентябре 1994 г. его описание было анонимно отправлено в список рассылки «Cypherpunks».

Этап 1. Инициализация S-блока.

Перед генерацией гаммы выполняется инициализация **S-блока** длиной L_s . Обычно L_s выбирается кратно 8 битов ($2^8 = 256$, $2^{16} = 65536$ и т.п.). Для инициализации используется ключ **K** длиной L_K от 40 до 2048 битов по следующему алгоритму.

1. Цикл А. Для $i := 0$ до $L_s - 1$
 - 1.1. $S[i] := i$
2. $j := 0$
3. Цикл В. Для $i := 0$ до $L_s - 1$
 - 3.1. $j := (j + S[i] + K[i \bmod L_K]) \bmod L_s$
 - 3.2. Поменять местами $S[i]$ и $S[j]$

Этап 2. Генерация гаммы.

Непосредственная генерация гаммы выполняется циклически блоками по L_s битов до достижения необходимой длины псевдослучайной последовательности L_g . Алгоритм генерации следующий.

1. $i := 0$
2. $j := 0$
3. $L := 0$
4. Цикл. Пока $L < L_g$
 - 4.1. $i := (i + 1) \bmod L_s$
 - 4.2. $j := (j + S[i]) \bmod L_s$
 - 4.3. Поменять местами $S[i]$ и $S[j]$
 - 4.4. $t := (S[i] + S[j]) \bmod L_s$
 - 4.5. Блок гаммы $:= S[t]$

$$4.6. L := L + L_s$$

RC4 получил широкое распространение в криптосистемах и протоколах, в частности:

- WEP (англ. Wired Equivalent Privacy) — алгоритм для обеспечения безопасности сетей Wi-Fi;
- WPA (англ. Wi-Fi Protected Access) — обновленный алгоритм сертификации устройств сетей Wi-Fi;
- BitTorrent protocol encryption — протоколы пиринговых файлообменных сетей;
- SSL (англ. Secure Sockets Layer) — криптографический протокол передачи данных в сети;
- Kerberos — сервер аутентификации Kerberos;
- PDF (англ. Portable Document Format) — межплатформенный формат электронных документов, разработанный фирмой Adobe Systems;
- Skype — программное обеспечение IP-телефонии;
- и др.

Обнаруженные уязвимости в стандартной реализации RC4 привели к отказу от его использования в некоторых криптосистемах и протоколах, а также появлению различных его модификаций: RC4A, RC4+, VMPC, Spritz.

Б.3) Trivium был представлен в 2008 г. как часть европейского проекта eSTREAM по профилю 2 (аппаратно ориентированные шифры) и в настоящий момент имеет статус международного стандарта «ISO/IEC 29192-3:2012. Информационные технологии - Методы безопасности - Легкая криптография - Часть 3: Поточные шифры» (англ. «ISO/IEC 29192-3:2012. Information technology - Security techniques - Lightweight cryptography - Part 3: Stream ciphers»). Авторами генератора (шифра) являются Кристоф Де Канньер и Барт Пренел.

По аналогии с RC4 процедура выработки гаммы состоит из двух этапов: инициализации S-блока и непосредственно генерации гаммы.

Этап 1. Инициализация S-блока.

Длина **S-блока** составляет 288 битов. При этом он условно делится на 3 части длинами 93, 84 и 111 битов. В первую часть S_1 заносится 80-битовый ключ **K** с добавлением 13 нулевых битов, во вторую часть S_2 заносится 80-битовый вектор инициализации **IV** с добавлением 4 нулевых битов и в последнюю часть S_3 заносятся нулевые биты за исключением трех последних единичных битов. После первоначальной инициализации в цикле осуществляется связывание битов из разных частей со сдвигами битов вправо в каждой из них. Весь алгоритм инициализации выглядит следующим образом.

$$1. S_1 = (s_1, s_2, \dots, s_{93}) := (K_1, K_2, \dots, K_{80}, 0, \dots, 0)$$

$$2. S_2 = (s_{94}, s_{95}, \dots, s_{177}) := (IV_1, IV_2, \dots, IV_{80}, 0, \dots, 0)$$

$$3. S_3 = (s_{178}, s_{179}, \dots, s_{288}) := (0, \dots, 0, 1, 1, 1)$$

4. Цикл. Для $i := 1$ до 288

$$4.1. t_1 := s_{66} \oplus (s_{91} \wedge s_{92}) \oplus s_{93} \oplus s_{171}$$

$$4.2. t_2 := s_{162} \oplus (s_{175} \wedge s_{176}) \oplus s_{177} \oplus s_{264}$$

$$4.3. t_3 := s_{243} \oplus (s_{286} \wedge s_{287}) \oplus s_{288} \oplus s_{69}$$

$$4.4. \text{Сдвиг первой части на один бит вправо } S_1 := (_, s_1, s_2, \dots, s_{92})$$

$$4.5. \text{Занесение } t_3 \text{ в первую позицию первой части } S_1 := (t_3, s_1, s_2, \dots, s_{92})$$

$$4.6. \text{Сдвиг второй части на один бит вправо } S_2 := (_, s_{94}, s_{95}, \dots, s_{176})$$

$$4.7. \text{Занесение } t_1 \text{ в первую позицию второй части } S_2 := (t_1, s_{94}, s_{95}, \dots, s_{176})$$

$$4.8. \text{Сдвиг третьей части на один бит вправо } S_3 := (_, s_{178}, s_{179}, \dots, s_{287})$$

$$4.9. \text{Занесение } t_2 \text{ в первую позицию третьей части } S_3 := (t_2, s_{178}, s_{179}, \dots, s_{287})$$

Этап 2. Генерация гаммы.

Для генерации гаммы длиной L_g в каждой итерации цикла на основе 6 битов **S-блока** вычисляется один бит гаммы и выполняются операции, идентичные рассмотренным в инициализации **S-блока**. Алгоритм генерации следующий.

$$1. L := 0$$

2. Цикл. Пока $L < L_g$

$$2.1. \text{Бит гаммы} := s_{66} \oplus s_{93} \oplus s_{162} \oplus s_{177} \oplus s_{243} \oplus s_{288}$$

- 2.2. $t_1 := s_{66} \oplus (s_{91} \wedge s_{92}) \oplus s_{93} \oplus s_{171}$
- 2.3. $t_2 := s_{162} \oplus (s_{175} \wedge s_{176}) \oplus s_{177} \oplus s_{264}$
- 2.4. $t_3 := s_{243} \oplus (s_{286} \wedge s_{287}) \oplus s_{288} \oplus s_{69}$
- 2.5. Сдвиг первой части на один бит вправо $S_1 := (_, s_1, s_2, \dots, s_{92})$
- 2.6. Занесение t_3 в первую позицию первой части $S_1 := (t_3, s_1, s_2, \dots, s_{92})$
- 2.7. Сдвиг второй части на один бит вправо $S_2 := (_, s_{94}, s_{95}, \dots, s_{176})$
- 2.8. Занесение t_1 в первую позицию второй части $S_2 := (t_1, s_{94}, s_{95}, \dots, s_{176})$
- 2.9. Сдвиг третьей части на один бит вправо $S_3 := (_, s_{178}, s_{179}, \dots, s_{287})$
- 2.10. Занесение t_2 в первую позицию третьей части $S_3 := (t_2, s_{178}, s_{179}, \dots, s_{287})$
- 2.11. $L := L + 1$

Существуют упрощенные модификации генератора гаммы Univium, Bivium, Trivium-toy и Bivium-toy.

Б.4) Иррациональное число – вещественное число, которое не является рациональным, т.е. не может быть представлено в виде обыкновенной дроби $\pm \frac{m}{n}$, где m, n – натуральные числа. К наиболее известным иррациональным числам относятся $\sqrt{2}, \sqrt{3}, \sqrt{5}, \ln 2, e$ и π [17].

Иррациональное число может быть представлено в виде бесконечной непериодической десятичной дроби. Другими словами в дробной части такого числа бесконечное количество цифр и в их записи отсутствует период. Это говорит о том, что любая конечная случайная числовая последовательность рано или поздно обязательно будет являться частью иррационального числа. Данные обстоятельства могут сделать иррациональные числа ценным источником псевдослучайных последовательностей. Для генерации гаммы можно будет указать номер позиции в дробной части, с которой следует начать выбирать последовательность цифр для гаммы. Очевидно, что данный номер должен быть очень большим, чтобы потенциальный противник не смог за приемлемое время его определить методом перебора.

К **проблемам** использования иррациональных чисел в качестве псевдослучайных числовых последовательностей относятся:

- отсутствие доказательства нормальности чисел;
- относительно сложный алгоритм расчета, подразумевающий, как правило, использование рекуррентных процедур;
- наличие в своем составе «плохих» последовательностей (например, последовательностей требуемой для гаммы длины, но состоящих из одних нулей или имеющих легко определяемый период).

В качестве примера рассмотрим число π .

Равновероятность появления цифр в записи (= нормальность) числа π не доказана, хотя анализ первых 200 млрд. десятичных цифр говорит в пользу этого.

Таблица 8. Количество появлений десятичных цифр в первых 200 млрд. знаках числа π

| Цифра | Количество появлений |
|-------|----------------------|
| 0 | 20 000 030 841 |
| 1 | 19 999 914 711 |
| 2 | 20 000 136 978 |
| 3 | 20 000 069 393 |
| 4 | 19 999 921 691 |
| 5 | 19 999 917 053 |
| 6 | 19 999 881 515 |
| 7 | 19 999 967 594 |
| 8 | 20 000 291 044 |
| 9 | 19 999 869 180 |

Для расчета цифр числа π можно использовать приближенные формулы, ряды, пределы, интегралы и т.п. В первом случае получается неточное значение и, как правило, с периодом («теряется» иррациональность), в других требуется сложная процедура расчета с получением всех предшествующих цифр, начиная с первой.

Важным достижением в области расчетов числа π стала формула Бэйли – Боруэйна – Плаффа, открытая в 1997 г. Саймоном Плаффом и названная в честь авторов статьи, в которой она впервые была опубликована.

$$\pi = \sum_{k=0}^{\infty} \frac{1}{16^k} \left(\frac{4}{8k+1} - \frac{2}{8k+4} - \frac{1}{8k+5} - \frac{1}{8k+6} \right) \quad (13)$$

Эта формула примечательна тем, что она позволяет извлечь любую конкретную шестнадцатеричную или двоичную цифру числа π без вычисления предыдущих. К сожалению, расчеты по этой формуле достаточно медлительны, но это уже значительный шаг вперед для использования иррациональных чисел в практической криптографии.

Взаимно простые числа – целые числа, не имеющие общих делителей, кроме ± 1 , т.е. наибольший общий делитель которых равен 1.

Отличие ключа от гаммы

Очень часто понятия «ключ» и «гамма» отождествляют, но между ними есть принципиальные отличия. Напомним, **ключ** – минимально необходимая информация (за исключением сообщения, алфавитов и алгоритма), используемая для шифрования и дешифрования сообщений. **Гаммой** является вся числовая последовательность, используемая для шифрования или дешифрования сообщения с длиной не менее этого сообщения.

Для иллюстрации отличий приведена следующая таблица.

Таблица 9. Отличия ключа от гаммы

| Метод генерации гаммы | Ключ | Гамма |
|--|--------------------------|--|
| На базе случайных физических или антропогенных процессов | Ключ соответствует гамме | |
| На базе слова или фразы (см. табл. 6.2 и 6.4) | Слово или фраза | Циклически повторяющееся слово или фраза |

| | | |
|--|--|--|
| Линейный или инверсный конгруэнтный генератор | Начальное число и коэффициенты формул | Генерируемая числовая последовательность |
| Регистр сдвига с линейной обратной связью | Вид полинома и исходное состояние регистра | Генерируемая числовая последовательность |
| RC4 | Ключ К | Числовая последовательность из частей S-блока |
| На базе числа π | Номер начальной позиции в дробной части, с которой выбираются цифры числа π | Последовательность цифр числа π , начиная с заданной позиции |

Стандарты и спецификации США

Развитая система стандартов и спецификаций по генерации и тестированию псевдослучайных последовательностей существует в США. ANSI (Американский национальный институт стандартов – англ. American national standards institute) и NIST (Американский национальный институт стандартизации – англ. National Institute of Standards and Technology) разработали следующие документы:

- стандарты ANSI серии X9.82:
- ANSI X9.82 «Random Number Generation. Part 1: Overview and Basic Principles» (рус. «Генерация случайных чисел. Часть 1: Обзор и основные принципы»);
- ANSI X9.82 «Financial Services - Random Number Generation. Part 2: Entropy Sources» (рус. «Финансовые услуги – Генерация случайных чисел. Часть 2: Источники энтропии»);
- ANSI X9.82 «Random Number Generation. Part 3: Deterministic Random Bit Generators» (рус. «Генерация случайных чисел. Часть 3: Детерминированные генераторы случайных битов»);

- ANSI X9.82 «Random Number Generation. Part 4: Random Bit Generator Constructions» (рус. «Генерация случайных чисел. Часть 4: Конструкции генератора случайных битов»);
- специальные публикации NIST серии 800:
- NIST SP 800-22 Rev.1a «A Statistical Test Suite for Random and Pseudorandom Number Generators for Cryptographic Applications» (рус. «Набор статистических тестов для генераторов случайных и псевдослучайных чисел для криптографического приложений»);
- NIST SP 800-90A «Recommendation for Random Number Generation Using Deterministic Random Bit Generators» (рус. «Рекомендации для генерации случайных чисел с использованием детерминированных генераторов случайных битов»).

Задания для самостоятельного выполнения

В лабораторной работе необходимо зашифровать свою фамилию имя отчество и номер группы и подгруппы (в текстовом виде) с помощью следующих шифров:

1. гаммирования по модулю N;
2. гаммирования модулю 2;
3. сгенерировать гамму с помощью регистра сдвига с линейной обратной связью (принять полином $x^8 + x^4 + x^3 + x^2 + 1$);
4. алгоритма Блум - Блум – Шуба;
5. алгоритма RC4;
6. шифра Вернама;
7. алгоритма Trivium;
8. алгоритма генератор на базе иррациональных чисел;
9. алгоритма Блум - Блум – Шуба;
10. гаммирования по модулю N;
11. алгоритма генератор на базе иррациональных чисел;
12. сгенерировать гамму с помощью регистра сдвига с линейной обратной связью (принять полином $x^8 + x^4 + x^3 + x^2 + 1$);

13. алгоритма Trivium;
14. шифра Вернама;
15. гаммирования по модулю N;
16. алгоритма RC4.

При оформлении отчета необходимо привести исходное сообщение свою фамилию имя отчество и номер группы и подгруппы (в текстовом виде), расчет исходного значения и таблицы генерации гамм для 10 итераций (см. таблицы 6 и 7). Исходное значение определить сложением по модулю 2 всех букв фамилии в соответствии с кодировкой Windows 1251.

Например, для фамилия "АБРАМОВ" расчет исходного значения для генераторов гамм будет выглядеть следующим образом.

| | | |
|----------|------------------|---------------------|
| | 1100 0000 | A |
| | 1100 0001 | Б |
| | 1101 0000 | Р |
| \oplus | 1100 0000 | A |
| | 1100 1100 | М |
| | 1100 1110 | О |
| | <u>1100 0010</u> | В |
| | 1101 0001 | = 209 ₁₀ |

Привести алгоритм (блок схему и текстовое описание), скриншоты выполнения программы и текст кода. Язык программирования выбирается любой. Вместе с отчетом прикрепляется исходники кода.

Вопросы для самопроверки

1. В чем заключается основная идея криптографических преобразований аддитивных шифров?
2. Назовите основные характеристики гаммы.
3. При каких условиях применения гаммы аддитивный шифр можно считать совершенным.
4. Опишите схемы шифрования с использованием синхронных и самосинхронизирующихся потоковых шифров.

Лабораторная работа №4. Электронная цифровая подпись

Протоколы электронной цифровой подписи

Общие сведения

Протоколы ЭЦП с одной стороны относят к протоколам аутентификации, т.к. гарантируют, что сообщение поступило от достоверного отправителя, а с другой стороны к протоколам контроля целостности, т.к. гарантируют, что сообщение пришло в неискаженном виде. Более того, получатель в дальнейшем может использовать ЭЦП как доказательство достоверности сообщения третьим лицам (арбитру) в том случае, если отправитель впоследствии попытается отказаться от него.

Электронная цифровая подпись – реквизит электронного документа, предназначенный для защиты данного документа от подделки, полученный в результате криптографического преобразования информации с использованием закрытого ключа ЭЦП и позволяющий идентифицировать владельца сертификата ключа подписи, а также установить отсутствие искажения информации в электронном документе (Федеральный закон № 1 -ФЗ "Об электронной цифровой подписи" от 10.01.2002г.).

Электронная цифровая подпись – информация в электронной форме, которая присоединена к другой информации в электронной форме (подписываемой информации) или иным образом связана с такой информацией и которая используется для определения лица, подписывающего информацию (Федеральный закон № 63-ФЗ "Об электронной подписи" от 06.04.2011г.).

[Электронная цифровая] подпись – строка бит, полученная в результате процесса формирования подписи (ISO/IEC 14888-1:2008 "Информационные технологии. Методы защиты. Цифровые подписи с приложением. Часть 1. Общие положения" и ГОСТ Р 34.10-2012 "Информационная технология. Криптографическая защита информации. Процессы формирования и проверки

электронной цифровой подписи"). По ГОСТ понятия "Электронная цифровая подпись", "электронная подпись" и "цифровая подпись" являются синонимами.

Из приведенных определений наихудшим является определение, приведенное в стандарте ISO/IEC 14888-1:2008 (ГОСТ Р 34.10-2012) – строку бит можно получить обыкновенным сканированием рукописной подписи. Наиболее семантически адекватным является определение, приведенное в Федеральном законе № 1-ФЗ от 10.01.2002г. Единственная неточность этого определения заключается в том, что ЭЦП позволяет не идентифицировать, а аутентифицировать владельца - идентификатор владельца (подписавшего, отправителя) сообщается получателю в явном виде. Таким образом, ЭЦП характеризуется следующими **свойствами**.

1. ЭЦП – это дополнение (реквизит) к подписываемому документу, которое может быть представлено как в битовом виде, так и в другой системе счисления (например, шестнадцатеричной).

2. ЭЦП гарантирует целостность подписанного документа – защищает его от преднамеренного искажения (подделки) и случайного искажения в результате пересылки по сети или хранения на материальном носителе.

3. ЭЦП позволяет аутентифицировать подписавшего (владельца закрытого ключа, владельца сертификата ключа подписи) – по идентификатору подписавшего подтверждается, что ЭЦП к документу принадлежит именно подписавшему. В силу этого подписавший впоследствии не может отказаться от своей подписи (неотрицание авторства).

4. ЭЦП неразрывно связано с документом – ЭЦП к одному документу нельзя выдать за подпись к другому документу. В то же время, в силу особенностей алгоритмов ассиметричного вероятностного шифрования, один и тот же владелец к одному и тому же документу может сгенерировать разные ЭЦП, которые будут равнозначны (см. ГОСТ 34.10-94 и ГОСТ Р 34.10-2012).

Говоря о схеме электронной подписи, обычно имеют в виду следующую классическую ситуацию:

- отправитель знает содержание сообщения, которое он подписывает;

- получатель, зная открытый ключ проверки подписи, может проверить правильность подписи полученного сообщения в любое время без какого-либо разрешения и участия отправителя;

- безопасность схемы подписи гарантируется.

При создании электронной подписи по классической схеме отправитель:

- применяет к исходному сообщению T хеш-функцию $h(T)$ и получает хеш-образ сообщения r ;

- вычисляет электронную подпись s по хеш-образу r с использованием своего закрытого ключа;

- посылает сообщение T вместе с электронной подписью s получателю.

Получатель, отделив электронную подпись от сообщения, выполняет следующие действия:

- применяет к полученному сообщению T хеш-функцию $h(T)$ и получает хеш-образ сообщения r' ;

- расшифровывает хеш-образ r из электронной подписи s с использованием открытого ключа отправителя;

- проверяет соответствие хеш-образов r' и r и если они совпадают, то отправитель действительно является тем, за кого себя выдает, и сообщение при передаче не подверглось искажению.

Как видно из этой схемы, при выработке и проверке ЭЦП существуют два принципиальных отличия от классического асимметричного зашифрования/расшифрования информации (обеспечения конфиденциальности).

1. При обеспечении конфиденциальности используются ключи получателя, в протоколах ЭЦП – отправителя (подписавшего, владельца).

2. Порядок использования ключей обратный. Для обеспечения конфиденциальности информация зашифровывается открытым ключом получателя, расшифровывается закрытым ключом получателя. При выработке и проверке ЭЦП информация (хеш-образ) зашифровывается закрытым ключом отправителя, расшифровывается открытым ключом отправителя.

Существует несколько схем ЭЦП, которые, как правило, применяются совместно с определенными хеш-функциями. Некоторые из них приведены в таблице.

Таблица 1. Схемы ЭЦП

| Схема цифровой подписи | Задача, лежащая в основе стойкости | Хеш-функция |
|---|---|--|
| RSA | Разложение числа на множители | MD4 или MD5 (Message Digest Algorithm - алгоритм краткого изложения сообщения, Р. Ривест) |
| DSS (NIST ¹ . FIPS Publication 186: Digital Signature Standard (DSS). May 1994) DSS – Федеральный стандарт цифровой подписи США | Дискретное логарифмирование по схеме Эль-Гамала | SHA-1 (NIST. FIPS Publication 180: Secure Hash Standard (SHS). May 1993) SHS – стандарт хэш-функции США SHA - Secure Hash Algorithm – алгоритм хеш-функции |
| ECDSA (Elliptic Curve Digital Signature Algorithm) - алгоритм цифровой подписи на эллиптических кривых. Принят в качестве стандарта ISO ² 14888-3 в 1998 г., ANSI ³ X9.62 – 1999 г., IEEE ⁴ 1363 – 2000 г. и NIST 186-2 – 2000 г. (последняя редакция – NIST. FIPS Publication 186-3: Digital Signature Standard (DSS). June 2009) | Дискретное логарифмирование в группе точек эллиптической кривой | SHA (NIST. FIPS 180-3: Secure Hash Standard (SHS). October 2008) |
| ГОСТ 34.10-94 (Информационная технология. Криптографическая защита информации. Процедуры выработки и проверки электронной цифровой подписи на базе асимметричного | Дискретное логарифмирование по схеме Эль-Гамала | ГОСТ 34.11-94 (Информационная технология. Криптографическая защита информации. Функция хэширования) |

| | | |
|---|---|---|
| криптографического алгоритма) | | |
| ГОСТ Р 34.10-2001 (Информационная технология. Криптографическая защита информации. Процессы формирования и проверки электронной цифровой подписи) | Дискретное логарифмирование в группе точек эллиптической кривой | ГОСТ 34.11-94 (Информационная технология. Криптографическая защита информации. Функция хэширования) |
| ГОСТ Р 34.10-2012 (Информационная технология. Криптографическая защита информации. Процессы формирования и проверки электронной цифровой подписи) | Дискретное логарифмирование в группе точек эллиптической кривой | ГОСТ Р 34.11-2012 (Информационная технология. Криптографическая защита информации. Функция хэширования) |

Примечания.

¹NIST - Национальный Институт стандартов и технологий, США (The National Institute of Standards and Technology).

²ISO - Международная организация по стандартизации (International Organization for Standardization).

³ANSI - Американский национальный институт стандартов (American National Standards Institute).

⁴IEEE - Институт инженеров по электротехнике и электронике (Institute of Electrical and Electronics Engineers).

Протокол на базе алгоритма RSA

Этап 1. Отправитель **A** генерирует открытый $\{e=5, n=91\}$ и закрытый $\{d=29\}$ ключи, публикует открытый ключ.

Этап 2. Отправка сообщения и электронной подписи (выполняет отправитель **A**).

Таблица 2. Отправка сообщения и ЭЦП на базе алгоритма RSA

| № п/п | Описание операции | Пример |
|----------|---|---------------------------------|
| 1 | Вычисление хеш-образа $h = h(T)$, где T – исходное сообщение; $h(T)$ – хеш-функция (для MD5 длина хеш-образа 128 бит). | $h = 7$ |
| 2 | Выработка электронной подписи $s = h^d \bmod n$, Где d – закрытый ключ отправителя А; N – часть открытого ключа отправителя А. | $s = 7^{29} \bmod 91$ $= 63$ |
| 3 | Отправка получателю Б исходного сообщения T и электронной подписи s . | |

Этап 3. Получение сообщения и проверка электронной подписи (выполняет получатель Б).

Таблица 3. Получение сообщения и проверка ЭЦП на базе алгоритма RSA

| № п/п | Описание операции | Пример |
|----------|---|------------------------------|
| 1 | Вычисление хеш-образа по полученному сообщению $h' = h(T')$, где T' – полученное сообщение. | $h' = 7$ |
| 2 | Вычисление хеш-образа из электронной подписи $h = s^e \bmod n$, где e и n – открытый ключ отправителя А. | $h = 63^5 \bmod 91$ $= 7$ |
| 3 | Если $h' = h$, то получатель Б делает вывод, что полученное сообщение $T' = T$ и оно действительно отправлено А. | $7 = 7$ |

Алгоритм цифровой подписи ГОСТ 34.10-94

Алгоритм цифровой подписи ГОСТ 34.10-94 похож на DSS-94 и является вариацией схемы Эль-Гамала.

Этап 1. Выработка ключей (выполняет отправитель А).

Таблица 4. Выработка ключей для ЭПЦ по ГОСТ 34.10-94

| № п/п | Описание операции | Пример |
|----------|---|----------------------------------|
| 1 | Выбор простого числа p (по ГОСТ – $2^{509} < p < 2^{512}$ либо $2^{1020} < p < 2^{1024}$). | $p = 79$ |
| 2 | Выбор простого числа q , являющегося делителем $(p - 1)$ (по ГОСТ – $2^{254} < q < 2^{256}$). | $q = 13 [(79 - 1) \bmod 13 = 0]$ |
| 3 | Выбор a ($0 < a < p - 1$), для которого $a^q \bmod p = 1$. | $a = 8 [8^{13} \bmod 79 = 1]$ |
| 4 | Выбор закрытого ключа x ($0 < x < q$). | $x = 4$ |
| 5 | Вычисление $y = a^x \bmod p$. | $y = 8^4 \bmod 79 = 67$ |
| 6 | Публикация открытого ключа $\{p, q, a, y\}$. Первые три параметра p, q и a - открыты и могут совместно использоваться пользователями сети, y – персональный открытый ключ для одного пользователя (отправителя А). | |

Этап 2. Отправка сообщения и электронной подписи (выполняет отправитель А).

Таблица 5. Отправка сообщения и ЭЦП по ГОСТ 34.10-94

| № п/п | Описание операции | Пример |
|----------|--|--|
| 1 | Вычисление хеш-образа $h = h(T)$ (по ГОСТ длина хеш-образа 256 бит). | $h = 7$ |
| 2 | Выбор k ($0 < k < q$). | $k = 11$ |
| 3 | Вычисление двух значений: $w = a^k \bmod p$ и $w' = w \bmod q$ (по ГОСТ длина w' 256 бит). Если $w' = 0$, перейти к этапу 2 и выбрать другое значение числа k . | $w = 8^{11} \bmod 79 = 21$ $w' = 21 \bmod 13 = 8$ |
| 4 | Вычисление $s = (x w' + k h) \bmod q$ (по ГОСТ длина s 256 бит). Если $s = 0$, перейти к этапу 2 и выбрать другое значение числа k . | $s = (4 * 8 + 11 * 7) \bmod 13 = 5$ |
| 5 | Отправка получателю Б исходного сообщения T и электронной подписи $\{w', s\}$. | |

Этап 3. Получение сообщения и проверка электронной подписи (выполняет получатель Б).

Таблица 6. Получение сообщения и проверка ЭЦП по ГОСТ 34.10-94

| № п/п | Описание операции | Пример |
|-------|--|---|
| 1 | Вычисление хеш-образа по полученному сообщению $h' = h(T')$, где T' – полученное сообщение. Если $T = T'$, то должно быть $h = h'$. | $h' = 7$ |
| 2 | Вычисление $v = h'^{q-2} \bmod q$. | $v = 7^{11} \bmod 13 = 2$ |
| 3 | Вычисление двух значений: $z_1 = (s \cdot v) \bmod q$ и $z_2 = ((q - w') \cdot v) \bmod q$. | $z_1 = (5 \cdot 2) \bmod 13 = 10$ $z_2 = ((13 - 8) \cdot 2) \bmod 13 = 10$ |
| 4 | Вычисление $u = ((a^{z_1} \cdot y^{z_2}) \bmod p) \bmod q$. | $u = ((8^{10} \cdot 67^{10}) \bmod 79) \bmod 13 = 8$ |
| 5 | Если $u = w'$, то получатель Б делает вывод, что полученное сообщение $T' = T$ и оно действительно отправлено А. | $8 = 8$ |

Алгоритм цифровой подписи ГОСТ Р 34.10-2001 и ГОСТ Р 34.10-2012

Алгоритмы цифровой подписи ГОСТ Р 34.10-2001 и ГОСТ Р 34.10-2012 совпадают и похожи на ECDSA.

Этап 1. Отправитель А генерирует открытый $\{(A, B) = (3, 7), P(x_p, y_p) = P(7, 17), q = 47, Q(x_q, y_q) = Q(36, 20)\}$ и закрытый $\{d = 10\}$ ключи, публикует открытый ключ.

Этап 2. Отправка сообщения и электронной подписи (выполняет отправитель А).

Таблица 7. Отправка сообщения и ЭЦП по ГОСТ 34.10-2001 (34.10-2012)

| № п/п | Описание операции | Пример |
|----------|---|-----------------------------------|
| 1 | Вычисление хеш-образа $h = h(T)$ (по ГОСТ длина хеш-образа 256 бит). | $h = 7$ |
| 2 | Вычисление $e = h \bmod q$. | $e = 7 \bmod 47 = 7$ |
| 3 | Выбор k ($0 < k < q$). | $k = 11$ |
| 4 | Определение точки эллиптической кривой $C(x_c, y_c) = k P(x_p, y_p)$. | $C = 11 * P(7, 17) = (16, 16)$ |
| 5 | Вычисление $r = x_c \bmod q$. Если $r = 0$, перейти к этапу 2 и выбрать другое значение числа k . | $r = 16 \bmod 47 = 16$ |
| 6 | Вычисление $s = (r d + k e) \bmod q$. Если $s = 0$, перейти к этапу 2 и выбрать другое значение числа k . | $s = (16*10 + 11*7) \bmod 47 = 2$ |
| 7 | Отправка получателю Б исходного сообщения T и электронной подписи $\{r, s\}$. | |

Этап 3. Получение сообщения и проверка электронной подписи (выполняет получатель Б).

Таблица 8. Получение сообщения и проверка ЭЦП по ГОСТ 34.10-2001 (34.10-2012)

| № п/п | Описание операции | Пример |
|----------|--|---|
| 1 | Вычисление хеш-образа по полученному сообщению $h' = h(T')$, где T' – полученное сообщение. Если $T = T'$, то должно быть $h = h'$. | $h' = 7$ |
| 2 | Вычисление $e' = h' \bmod q$. | $e' = 7 \bmod 47 = 7$ |
| 3 | Вычисление $v = e'^{-1} \bmod q$, где e'^{-1} – обратное число к e' по модулю q . | $e'^{-1} = 27 [(7 * 27) \bmod 47 = 1] v = 27 \bmod 47 = 27$ |
| 4 | Вычисление двух значений: $z_1 = (s v) \bmod q$ и $z_2 = ((q - r) v) \bmod q$. | $z_1 = (2 * 27) \bmod 47 = 7$ $z_2 = ((47 - 16) * 27) \bmod 47 = 38$ |
| 5 | Определение точки эллиптической кривой $C'(x_c, y_c) = z_1 P(x_p, y_p) + z_2 Q(x_q, y_q)$. | $C' = 7 P(7, 17) + 38 Q(36, 20) = (22, 26) + (11, 31) = (16, 16)$ |

| | | |
|---|---|--------------------------------|
| 6 | Вычисление $r' = x_c \cdot \text{mod } q$. | $r' = 16 \text{ mod } 47 = 16$ |
| 7 | Если $r' = r$, то получатель Б делает вывод, что полученное сообщение $T' = T$ и оно действительно отправлено А. | $16 = 16$ |

Разновидности ЭЦП

Кроме классической схемы ЭЦП различают еще несколько специальных:

- схема "конфиденциальной" (неотвергаемой) подписи – подпись не может быть проверена без участия сгенерировавшего ее лица;
- схема подписи "вслепую" ("затемненной" подписи) - отправитель не знает подписанного им сообщения;
- схема "мультиподписи" - вместо одного отправителя сообщение подписывает группа из нескольких участников;
- схема "групповой" подписи - получатель может проверить, что подписанное сообщение пришло от члена некоторой группы отправителей, но не знает, кем именно из членов группы оно подписано. В то же время, в случае необходимости, отправитель может быть определен;
- и др.

Юридические основания использования ЭЦП

10 января 2002 г. Президент Российской Федерации В.В. Путин подписал Федеральный закон № 1-ФЗ "Об электронной цифровой подписи". Цель Федерального закона № 1-ФЗ - обеспечение правовых условий использования ЭЦП в электронных документах, при соблюдении которых ЭЦП в электронном документе признается равнозначной собственноручной подписи в документе на бумажном носителе.

В настоящий момент действует Федеральный закон № 63-ФЗ "Об электронной подписи" от 06.04.2011 г. Сфера действия (цель) Федерального закона № 63-ФЗ - регулирует отношения в области использования электронных подписей при совершении гражданско-правовых сделок, оказании

государственных и муниципальных услуг, исполнении государственных и муниципальных функций, при совершении иных юридически значимых действий, в том числе в случаях, установленных другими федеральными законами.

В системах, где число пользователей исчисляется сотнями и тысячами, для проверки ЭЦП используются так называемые сертификаты ЭЦП (ЭП).

Сертификат ЭЦП – открытый ключ с некоторой дополнительной информацией о его владельце (регистрационный номер сертификата, ФИО владельца, срок действия и т.д.), подписанный ключом Центра сертификации (ЦС, Certificate Authority, СА, Удостоверяющий центр, УЦ).

В Федеральном законе "Об электронной подписи" даны следующие определения.

Сертификат ключа проверки электронной подписи – электронный документ или документ на бумажном носителе, выданные УЦ либо доверенным лицом УЦ и подтверждающие принадлежность ключа проверки ЭП владельцу сертификата ключа проверки ЭП.

Квалифицированный сертификат ключа проверки электронной подписи – сертификат ключа проверки ЭП, выданный аккредитованным УЦ или доверенным лицом аккредитованного УЦ либо федеральным органом исполнительной власти, уполномоченным в сфере использования ЭП.

При получении документа, подписанного ЭЦП, вначале подается запрос в ЦС, который высылает сертификат ЭЦП, информацию об окончании срока его действия или информацию об отсутствии сертификата. Если ЦС выслал сертификат, то считается, что документ послал именно тот, кто указан в сертификате. Для автоматизации деятельности ЦС применяется системы, называемые системы поддержки инфраструктуры открытых ключей (Public Key Infrastructure, PKI).

Впервые ссуда под ЭЦП (на покупку дома) была выдана в США 25 июля 2000г.

Задания для самостоятельного выполнения

В лабораторной работе необходимо привести последовательность выполнения процедур генерации и проверки ЭЦП с использованием следующих способов:

- 1) на базе алгоритма RSA;
- 2) по ГОСТ 34.10-94;
- 3) по ГОСТ 34.10-2001.

При оформлении отчета необходимо привести таблицы генерации ключей, отправки сообщения с ЭЦП и получения сообщения с ЭЦП. В качестве хеш-образа исходного сообщения $h(T)$ принять коды, соответственно, 1-ой, 2-ой и 3-ей буквы своей фамилии имени и отчества, номера группы и подгруппы.

Варианты заданий для применения следующих способов:

1. 3
2. 2
3. 1
4. 3
5. 2
6. 2
7. 1
8. 3
9. 2
10. 1
11. 2
12. 3
13. 1
14. 3
15. 2
16. 1

Вопросы для самопроверки

1. Дайте определение понятию "электронная цифровая подпись".
2. Опишите последовательность действий участников протокола при отправке и проверке ЭЦП.
3. Какой порядок использования ключей (открытый; закрытый) при отправке и проверке ЭЦП?
4. Опишите схему протокола ЭЦП на основе алгоритма RSA.
5. Перечислите специальные схемы ЭЦП.
6. Назовите цель введения в действие Федерального закона "Об электронной цифровой подписи".

Лабораторная работа №5. Стеганография

Компьютерные стеганографические методы как самостоятельно, так и совместно с криптографией, получили широкое распространение в целях защиты конфиденциальной информации. В лабораторной работе рассматривается стеганографическое сокрытие секретных сообщений в текстовых документах редактора Microsoft Word за счет специфического форматирования символов текста. Принципы сокрытия базируются на других известных стеганографических методах.

1. Микроточки. Использование микроточек для передачи секретных сообщений описал греческий ученый Эней Тактик в сочинении «Об обороне укрепленных мест». Суть предложенного им так называемого «книжного шифра» заключалась в прокалывании малозаметные дырок в книге или в другом документе над буквами секретного сообщения. Во время Первой мировой войны германские шпионы использовали аналогичный шифр, заменив дырки на точки, наносимые симпатическими чернилами на буквы газетного текста.

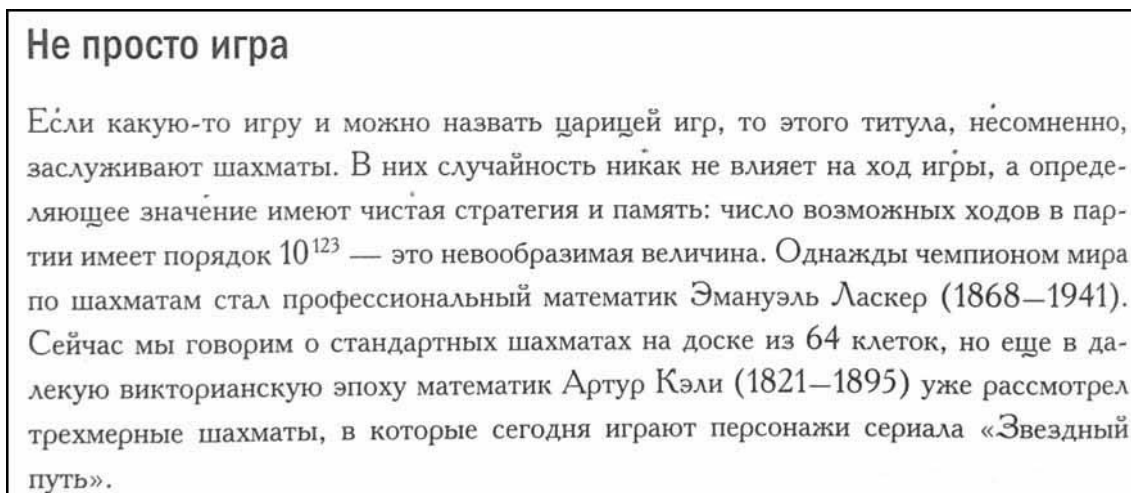


Рисунок 1 - Сокрытие сообщения «секрет» в тексте за счет малозаметных точек (Хоакин Наварро. Тайная жизнь чисел. Мир математики – том 31)

По аналогии с микроточками скрывающаяся в тексте секретная информация специальным образом помечается (форматируется).

2. Использование особенностей человеческого зрения. Подобные методы широко используются для сокрытия информации в мультимедийных файлах (в частности, метод LSB, Least Significant Bit - наименьший значащий бит) за счет их избыточности. По аналогии с ними, в обычном тексте символы, составляющие секретное сообщение, могут форматируются так, что это будет незаметно для глаза неискушенного читателя текста. В частности, символы секретного сообщения могут выделяться другим цветом, незначительно отличающегося от цвета остальных символов.

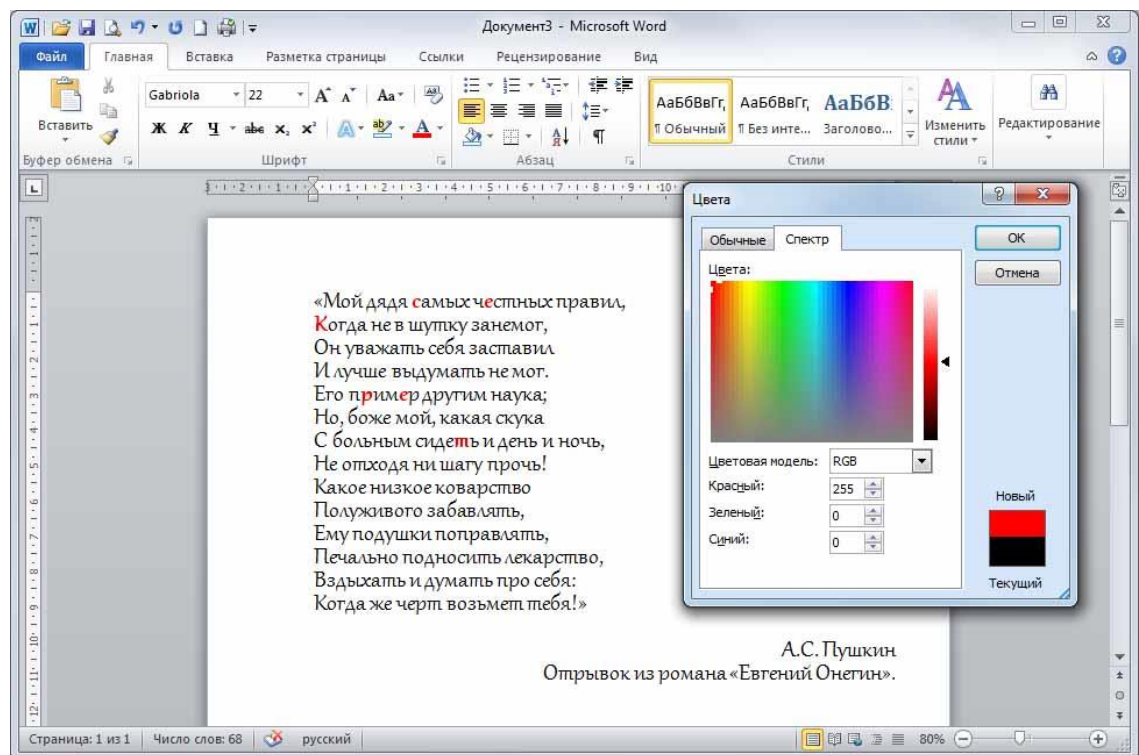


Рисунок 2 - Принцип форматирования символов секретного сообщения
«секрет» (цвет символов красный – RGB(255, 0, 0))

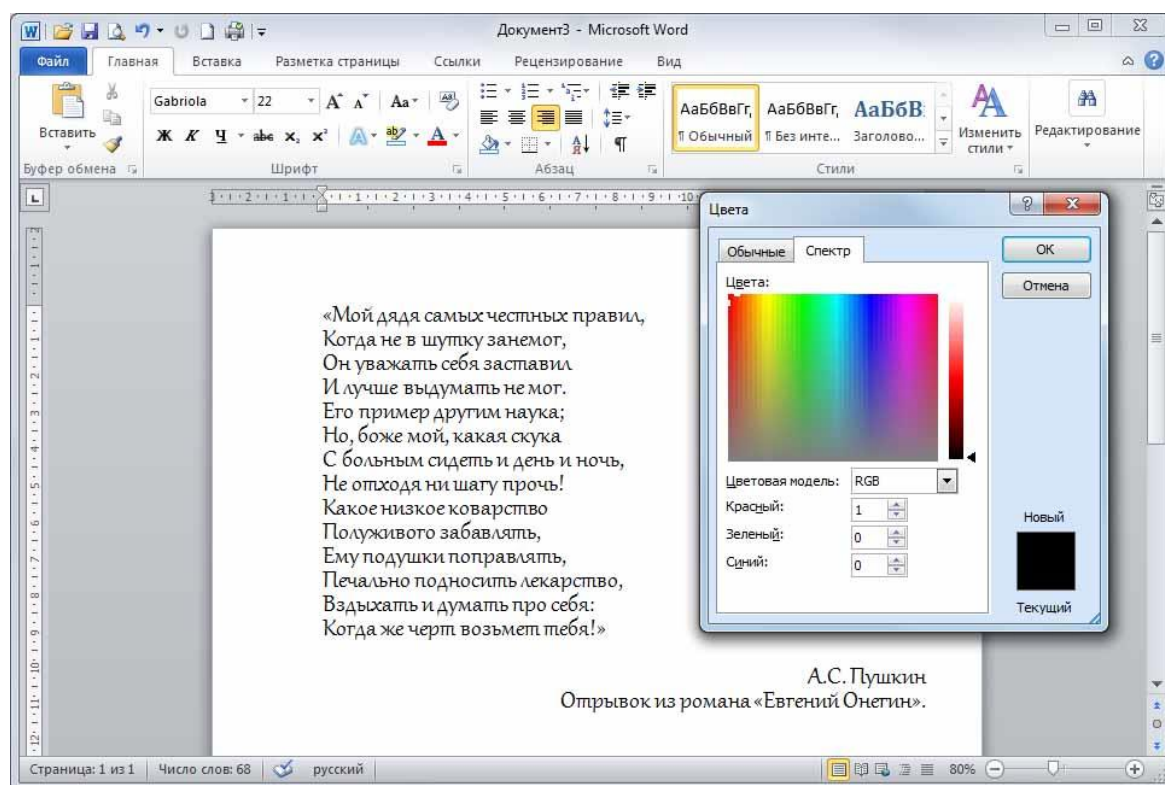


Рисунок 3 - Стеганографическое сокрытие символов секретного сообщения «секрет» (цвет символов «почти черный» – RGB(1, 0, 0))

На рисунке 3 цвет символов секретного сообщения RGB(1, 0, 0) практически не отличается от цвета символов остального текста RGB(0, 0, 0).

3. Семаграммы и кодирование. Предыдущий метод можно усилить за счет использования предварительного кодирования символов секретного сообщения (например, азбукой Морзе или Windows 1251). Перед форматированием символы секретного сообщения вначале кодируются битовыми строками длиной n согласно принятой кодировке. В исходном тексте выбираются n первых символов, которые будут соответствовать битовому представлению первого символа секретного сообщения. Для нулей битовой строки оставляют исходное форматирование, для единиц – незначительно меняют (см. рисунок 3). Процедуру последовательно повторяют для оставшихся символов секретного сообщения. Например, слово «секрет» согласно кодировке Windows 1251 в битовом представлении будет выглядеть $11110001\ 11100101\ 11101010\ 11110000\ 11100101\ 11110010_2$.

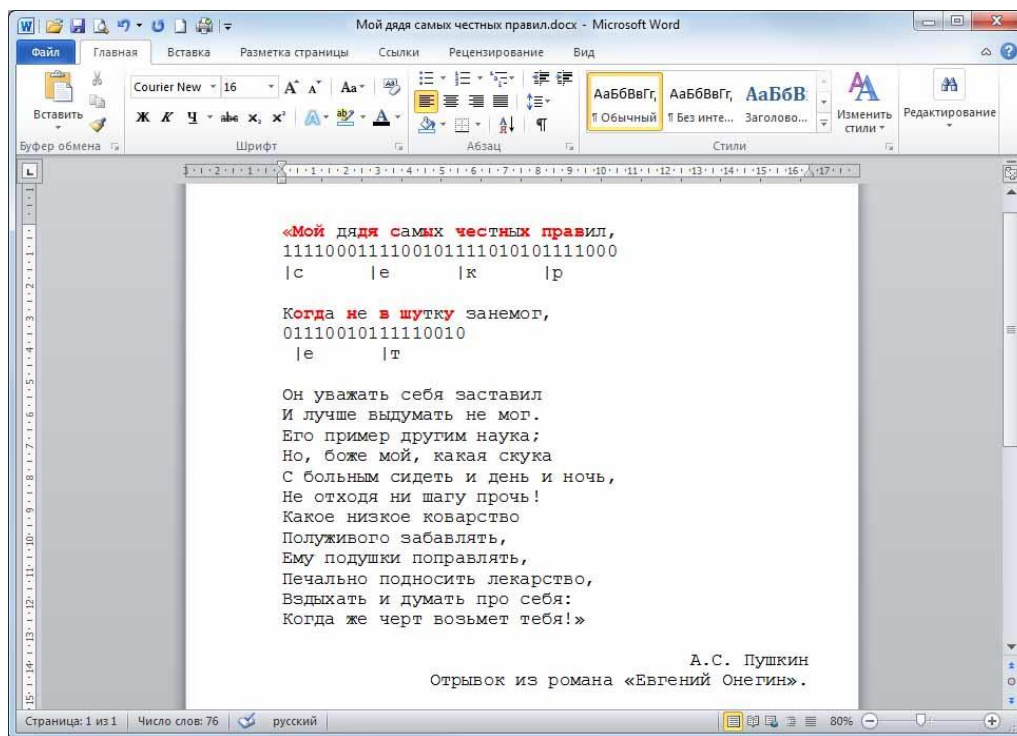


Рисунок 4 - Принцип кодирования и форматирования символов секретного сообщения «секрет» (цвет нулей черный – RGB(0, 0, 0); цвет единиц красный – RGB(255, 0, 0))

КОДИРОВАНИЕ ИНФОРМАЦИИ

Кодирование – представление информации в альтернативном виде. По своей сути кодовые системы (или просто коды) аналогичны шифрам однозначной замены, в которых элементам кодируемой информации соответствуют кодовые обозначения. Отличие заключается в том, что в шифрах присутствует переменная часть (ключ), которая для определенного исходного сообщения при одном и том же алгоритме шифрования может выдавать разные шифртексты. В кодовых системах переменной части нет. Поэтому одно и то же исходное сообщение при кодировании, как правило, всегда выглядит одинаково¹. Другой отличительной особенностью кодирования является применение кодовых обозначений (замен) целиком для слов, фраз или чисел (совокупности цифр). Замена элементов кодируемой информации кодовыми обозначениями может быть выполнена на основе соответствующей таблицы (наподобие таблицы шифрозамен) либо определена посредством функции или алгоритма кодирования.

В качестве элементов кодируемой информации могут выступать:

- буквы, слова и фразы естественного языка;
- различные символы, такие как знаки препинания, арифметические и логические операции, операторы сравнения и т.д. Следует отметить, что сами знаки операций и операторы сравнения – это кодовые обозначения;

- числа;
- аудиовизуальные образы;
- ситуации и явления;
- наследственная информация;
- и т.д.

Кодовые обозначения могут представлять собой:

- буквы и сочетания букв естественного языка;
- числа;
- графические обозначения;
- электромагнитные импульсы;
- световые и звуковые сигналы;
- набор и сочетание химических молекул;
- и т.д.

Кодирование может выполняться в целях:

- удобства хранения, обработки и передачи информации (как правило, закодированная информация представляется более компактно, а также пригодна для обработки и передачи автоматическими программно-техническими средствами);

- удобства информационного обмена между субъектами;
- наглядности отображения;
- идентификации объектов и субъектов;
- сокрытия секретной информации;
- и т.д.

Кодирование информации бывает одно- и многоуровневым. Примером одноуровневого кодирования служат световые сигналы, подаваемые светофором (красный – стой, желтый – приготовиться, зеленый – вперед). В качестве

многоуровневого кодирования можно привести представление визуального (графического) образа в виде файла фотографии. Вначале визуальная картинка разбивается на составляющие элементарные элементы (пикселы), т.е. каждая отдельная часть визуальной картинки кодируется элементарным элементом. Каждый элемент представляется (кодируется) в виде набора элементарных цветов (RGB: англ. red – красный, green – зеленый, blue – синий) соответствующей интенсивностью, которая в свою очередь представляется в виде числового значения. Впоследствии наборы чисел, как правило, преобразуются (кодируются) с целью более компактного представления информации (например, в форматах jpeg, png и т.д.). И наконец, итоговые числа представляются (кодируются) в виде электромагнитных сигналов для передачи по каналам связи или областей на носителе информации. Следует отметить, что сами числа при программной обработке представляются в соответствии с принятой системой кодирования чисел.

Кодирование информации может быть обратимым и необратимым. При обратимом кодировании на основе закодированного сообщения можно однозначно (без потери качества) восстановить кодируемое сообщение (исходный образ). Например, кодирование с помощью азбуки Морзе или штрихкода. При необратимом кодировании однозначное восстановление исходного образа невозможно. Например, кодирование аудиовизуальной информации (форматы jpeg, mp3 или avi) или хеширование.

Различают общедоступные и секретные системы кодирования. Первые используются для облегчения информационного обмена, вторые – в целях сокрытия информации от посторонних лиц.

В некоторых секретных кодовых системах присутствуют элементы, позволяющие получать разные закодированные сообщения для определенного исходного сообщения (аддитивные числа, многозначные замены, правила перешифрования).

Общедоступные кодовые системы

Код Бодо - цифровой 5-битный код. Был разработан Эмилем Бодо в 1870 г. для своего телеграфа. Код вводился прямо клавиатурой, состоящей из пяти

клавиш, нажатие или ненажатие клавиши соответствовало передаче или непередаче одного бита в пятибитном коде. Существует несколько разновидностей (стандартов) данного кода (ССИТТ-1, ССИТТ-2, МТК-2 и др.). В частности, МТК-2 представляет собой модификацию международного стандарта ССИТТ-2 с добавлением букв кириллицы.

| Управляющие символы | | | | |
|----------------------------------|----------------|-----------------|---------------|------------------------|
| Двоичный код | Десятичный код | Назначение | | |
| 01000 | 8 | Возврат каретки | | |
| 00010 | 2 | Перевод строки | | |
| 11111 | 31 | Буквы латинские | | |
| 11011 | 27 | Цифры | | |
| 00100 | 4 | Пробел | | |
| 00000 | 0 | Буквы русские | | |
| Буквы, цифры и остальные символы | | | | |
| Двоичный код | Десятичный код | Латинская буква | Русская буква | Цифры и прочие символы |
| 00011 | 3 | A | А | - |
| 11001 | 25 | B | Б | ? |
| 01110 | 14 | C | Ц | : |
| 01001 | 9 | D | Д | Кто там? |
| 00001 | 1 | E | Е | 3 |
| 01101 | 13 | F | Ф | Э |
| 11010 | 26 | G | Г | Ш |
| 10100 | 20 | H | Х | Щ |
| 00110 | 6 | I | И | 8 |
| 01011 | 11 | J | Й | Ю |
| 01111 | 15 | K | К | (|
| 10010 | 18 | L | Л |) |
| 11100 | 28 | M | М | . |
| 01100 | 12 | N | Н | , |
| 11000 | 24 | O | О | 9 |

| | | | | |
|-------|----|---|---|---|
| 10110 | 22 | P | П | 0 |
| 10111 | 23 | Q | Я | 1 |
| 01010 | 10 | R | Р | 4 |
| 00101 | 5 | S | С | ' |
| 10000 | 16 | T | Т | 5 |
| 00111 | 7 | U | У | 7 |
| 11110 | 30 | V | Ж | = |
| 10011 | 19 | W | В | 2 |
| 11101 | 29 | X | Ь | / |
| 10101 | 21 | Y | Ы | 6 |
| 10001 | 17 | Z | З | + |

Рисунок 5 - Стандарт кода Бодо МТК-2

На рисунке 6 показана телетайпная перфолента с сообщением, переданным с помощью кода Бодо.

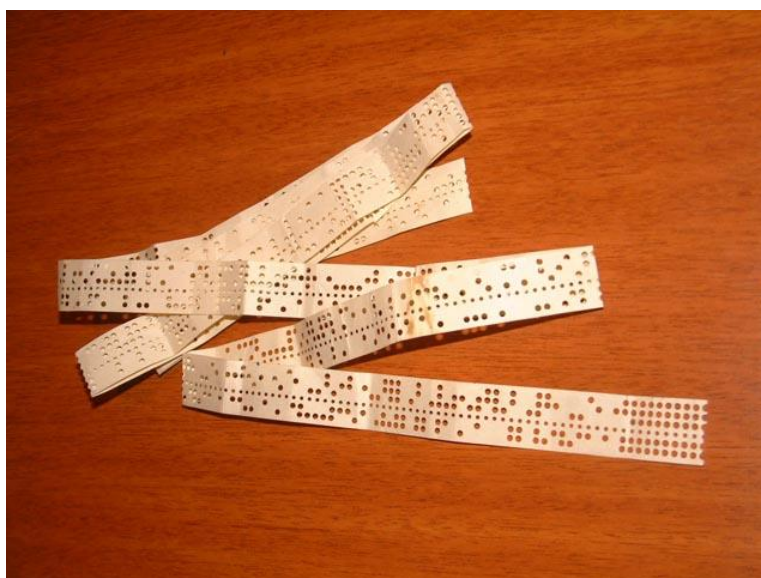


Рисунок 3 - Перфолента с кодом Бодо

Следует отметить два интересных факта, связанных с кодом Бодо.

1. Сотрудники телеграфной компании АТ&Т Гильберто Вернам и Мейджор Джозеф Моборн в 1917 г. предложили идею автоматического

шифрования телеграфных сообщений на основе кода Бодо. Шифрование выполнялось методом гаммирования по модулю 2.

2. Соответствие между английским и русским алфавитами, принятое в МТК-2, было использовано при создании компьютерных кодировок КОИ-7 и КОИ-8.

Задания для самостоятельного выполнения

В качестве текстов использованы стихи Агнии Барто, секретных сообщений – японские пословицы и поговорки.

Способы форматирования символов, применяемые для секретных сообщений (символов целиком, нулей или единиц) по вариантам:

1. цвет символов;
2. цвет фона;
3. размер шрифта;
4. масштаб шрифта;
5. межсимвольный интервал.
6. без кодировки;
7. код Бодо (МТК-2);
8. КОИ-8R;
9. cp866;
10. Windows 1251.
11. масштаб шрифта;
12. cp866;
13. цвет символов;
14. цвет фона;
15. межсимвольный интервал.
16. код Бодо (МТК-2).

Отчет по лабораторной работе должен содержать:

- код программы;

- алгоритм программы;
- фрагмент стиха, содержащий секретное сообщение (см. рисунок 4):
- с подчеркиванием символов, соответствующих единицам (вместо выделения красным цветом);
- с битовыми строками;
- с символами секретного сообщения;
- вывод (например, «В тексте.....», скрыта фраза «Один бог забыл - другой поможет.» посредством использования кодировки sr866 и размера символов: для нулей – 14пт, для единиц – 14.5пт»).

В ЭС прикреплять отчет и исходник файла.

Варианты индивидуальных заданий:

Вариант 1

Как Вовка стал старшим братом

— У меня есть старший брат,

Очень умный парень! —

Уверяет всех ребят

Таня на бульваре.—

В красном галстуке он ходит,

В пионерской форме,

Сорняки на огороде

Вырывает с корнем!

И толстушка Валечка

Старшим братом хвалится:

— Если кто меня обидит —

Старший брат в окно увидит.

Если я заплакала —

Он проучит всякого.

Он готов меня спасти

И от тигра лютого.

Десять лет ему почти,

Павликом зовут его.

Катя в красном платице
Как расплатится:
— Я одна ничья сестра,—
Цапнул кот меня вчера.
Что ж, меня кусай, царапай...
Я одна у мамы с папой,
Нет у братьев у меня,
Папа с мамой — вся родня.
К ней подходит не спеша
Вовка — добрая душа.
Объявляет он ребятам:
— Буду Кате старшим братом.
С понедельника, с утра,
Будешь ты моя сестра.

Агния Барто.

Вариант 2

Королева

Если до сих пор нигде вы
Не встречали королевы,-
Поглядите - вот она!
Среди нас живет она.
Всем, направо и налево,
Объявляет королева:
- Где мой плащ? Его повесьте!
Почему он не на месте?
У меня портфель тяжелый -
Донесешь его до школы!
Я дежурной поручаю
Принести мне кружку чая
И купите мне в буфете
Каждый, каждый по конфете.

Королева - в третьем классе,
А зовут ее Настасьей.
Бант у Насти
Как корона,
Как корона
Из капрона.

Агния Барто.

Вариант 3

В школу
Почему сегодня Петя
Просыпался десять раз?
Потому что он сегодня
Поступает в первый класс.
Он теперь не просто мальчик,
А теперь он новичок.
У него на новой куртке
Отложной воротничок.
Он проснулся ночью темной,
Было только три часа.
Он ужасно испугался,
Что урок уж начался.
Он оделся в две минуты,
Со стола схватил пенал.
Папа бросился вдогонку,
У дверей его догнал.
За стеной соседи встали,
Электричество зажгли,
За стеной соседи встали,
А потом опять легли.
Разбудил он всю квартиру,
До утра заснуть не мог.
Даже бабушке приснилось,
Что твердит она урок.

Даже дедушке приснилось,
Что стоит он у доски
И не может он на карте
Отыскать Москвы-реки.
Почему сегодня Петя
Просыпался десять раз?
Потому что он сегодня
Поступает в первый класс.

Агния Барто.

Вариант 4

Девочка-рёвушка
Что за вой? Что за рёв?
Там не стадо ли коров?
Нет, там не коровушка -
Это Ганя-рёвушка
Плачет,
Заливается,
Платьем утирается...
УУ-УУ-У!..
Вышла рёва на крыльцо,
Рёва сморщила лицо:
- Никуда я не пойду!
Мне не нравится в саду.
Уу-уу-у!...-
Вот вернулась Ганя в дом,
Слёзы катятся ручьём:
- Ой, пойду обратно!
Дома неприятно!
Оо-оо-о!..
Дали Гане молока.
- Эта кружка велика!
В этой не могу я!
Дайте мне другую!
УУ-УУ-У!..
Дали рёвушке в другой,

Рёва топнула ногой:
- В этой не желаю!
Лучше дайте чаю!
Аа-аа-а!..-
Уложили Ганю спать,
Плачет рёвушка опять:
- Ой, не буду спать я!
Ой, наденьте платье!
уу-уу-у!..
Тут сбежался народ.
Чтоб узнать: кто ревёт?
Кто всё время плачет?
Что всё это значит?
Видят - девочка стоит,
Очень странная на вид:
Нос распух, что свёкла,
Платье всё промокло.
Оо-оо-о!..
уу-уу-у!..
- Что ты плачешь, рёвушка,
Рёвушка-коровушка?
На тебе от сырости
Плесень может вырасти.

Агния Барто.

Варианты 5

Его семья
У Вовы двойка с минусом -
Неслыханное дело!
Он у доски не двинулся.
Не взял он в руки мела!
Стоял он будто каменный:
Он стоял как статуя.

- Ну как ты сдашь экзамены?
Волнуется вожатая.-
Твою семью, отца и мать,
На собрание упрекать
Директор будет лично!
У нас хороших двадцать пять
И три семьи отличных,
Но твоей семьей пока
Директор недоволен:
Она растить ученика
Не помогает школе.
- Ну при чем моя семья? -
Он говорит вздыхая.-
Получаю двойки я -
И вдруг семья плохая!
Упреки он бы перенес,
Не показал бы виду,
Но о семье идет вопрос -
Семью не даст в обиду!
Будут маму упрекать:
"У нас хороших двадцать пять
И три семьи отличных,
А вы одна - плохая мать!" -
Директор скажет лично.
Печально Вова смотрит вдаль,
Лег на сердце камень:
Стало маму очень жаль...
Нет, он сдаст экзамен!
Скажет маме: "Не грусти,
На меня надейся!
Нас должны перевести

В хорошее семейство!"

Агния Барто.

Вариант 6.

Жарко

У солнышка есть правило:

Оно лучи расправило,

Раскинуло с утра —

И на земле жара.

Оно по небу синему

Раскинуло лучи —

Жара такая сильная,

Хоть караул кричи!

Изнемогают жители

В Загорске-городке.

Они всю воду выпили

В киоске и в ларьке.

Мальчишки стали неграми,

Хоть в Африке и не были.

Жарко, жарко, нету сил!

Хоть бы дождь поморосил.

Жарко утром, жарко днем,

Влезть бы в речку, в водоем,

Влезть бы в речку, в озерцо,

Вымыть дождиком лицо.

Кто-то стонет: — Ой, умру!

Трудно в сильную жару,

Например, толстухам:

Стали падать духом.

А девчонка лет пяти

Не смогла пешком идти —

На отце повисла,

Будто коромысло.

Жарко, жарко, нету сил!
Хоть бы дождь поморосил.
Вовка вызвал бы грозу —
Не сговоришься с тучей.
Она — на небе, он — внизу.
Но он на всякий случай
Кричит: — Ну где же ты, гроза?
Гремишь, когда не надо! —
И долго ждет, подняв глаза,
Он у калитки сада.
Жарко, жарко, нету сил!..
Пить прохожий попросил:
— Вовка — добрая душа,
Дай напиться из ковша!
Вовка — добрая душа
Носит воду не дыша,
Тут нельзя идти вприпрыжку —
Расплескаешь полковша.
— Вовка, — просят две подружки, —
Принеси и нам по кружке!
— Я плесну вам из ведра,
Подставляйте горсти...
...Тридцать градусов с утра
В городе Загорске,
И все выше, выше ртуть...
Надо сделать что-нибудь,
Что-то сделать надо,
Чтоб пришла прохлада,
Чтоб не вешали носы
Люди в жаркие часы.
Вовка — добрая душа
Трудится в сарае,
Что-то клеит не спеша,
Мастерит, стараясь.
Вовка — добрая душа
Да еще три малыша.

Паренькам не до игры:
Предлагает каждый,
Как избавить от жары
Разомлевших граждан.
В городе Загорске
Горки да пригорки,
Что ни улица — гора.
Шла старушка в гору,
Причитала: — Ох, жара!
Помереть бы впору.
Вдруг на горке, на откосе,
Ей подарок преподносит,
Подает бумажный веер
Вовка — парень лет пяти.
Мол, шагайте поживее,
Легче с веером идти.
Обмахнетесь по пути.
Вовка — добрая душа
Да еще три малыша,
Да еще мальчишек восемь
Распевают на откосе:
— Получайте, граждане,
Веера бумажные,
Получайте веера,
Чтоб не мучила жара.
Раздаем бесплатно,
Не берем обратно.
На скамью старушка села,
Обмахнулась веером,
Говорит: — Другое дело —
Ветерком повеяло.—
Обмахнулся веером
Гражданин с бородкой,
Зашагал уверенной,
Деловой походкой.
И пошло конвейером:

Каждый машет веером.
Веера колышутся —
Людям легче дышится.

Агния Барто.

Вариант 7

Жил на свете самосвал

Жил на свете самосвал,
Он на стройке побывал,
Подкатил с утра к воротам,
Сторожа спросили: — Кто там?

Самосвал ответил так:
— Я привез отличный шлак.

Молодчина самосвал,
Где он только не бывал!
Он кирпич возил и гравий,
Но, увы, застрял в канаве!

Буксовал он, буксовал,
Еле вылез самосвал,
Говорит: — Меня не троньте,
Я сегодня на ремонте,
У меня помята рама!

— Алексей! — сказала мама.—
Ты успел в канаву влезть?

Дело в том, что самосвалом
Был Алеша, славный малый.
Сколько лет ему?

Лет шесть!

Самосвал сигналит громко:

— У меня сейчас поломка,

Но с утра я снова в путь.

— Хорошо,— сказала мама,—

Но пока Алешей будь!

Молока попьешь, и спать! —

Что ж, пришлось Алешей стать!

Где Алеша? Спит уже,

Дома спит, не в гараже.

Агния Барто.

Вариант 8

Вам не нужна сорока

Вам не нужна сорока,

Сорока без крыла?

Она у нас два срока —

Два месяца жила.

Ее нашли в июне,

Ее назвали Дуней.

Скакала как зайчонок

Сорока по траве,

Любила у девчонок

Сидеть на голове.

Она однажды ложку

Стащила со стола,

Но, поиграв немножко,

Андрюшке отдала.

Он был ее любимцем,
Андрюша Челноков,
Она ему гостинцы
Носила — червячков.

Мы к ней привыкли очень,
А Дуня, в тихий час,
Твердила по-сорочьи:
«Скучаю я без вас...»

Но осень, осень скоро,
В саду желтеет лист,
Уже уехал в город
Володя-баянист.

И мы уедем... Осень...
Но как мы Дуню бросим?

Она у нас два срока —
Два месяца жила...
Вам не нужна сорока,
Сорока без крыла?

Агния Барто.

Вариант 9.

Я выросла

Мне теперь не до игрушек -
Я учусь по букварю,
Соберу свои игрушки
И Сереже подарю.

Деревянную посуду

Я пока дарить не буду.
Заяц нужен мне самой -
Ничего, что он хромой,

А медведь измазан слишком...
Куклу жалко отдавать:
Он отдаст ее мальчишкам
Или бросит под кровать.

Паровоз отдать Сереже?
Он плохой, без колеса...
И потом, мне нужно тоже
Поиграть хоть полчаса!

Мне теперь не до игрушек -
Я учусь по букварю...
Но я, кажется, Сереже
Ничего не подарю.

Агния Барто.

Вариант 10

Блинчики

Всюду Павлику почет:
Павлик блинчики печет.
Он провел беседу в школе -
Говорил, открыв тетрадь,
Сколько соды, сколько соли,
Сколько масла нужно брать.

Доказал, что вместо масла
Можно брать и маргарин.
Решено единогласно:
Он прекрасно говорил.

Кто сказал такую речь,
Сможет блинчиков напечь!

Но, товарищи, спешите -
Нужно дом спасать скорей!
Где у вас огнетушитель?
Дым валит из-под дверей!

А соседи говорят:
- Это блинчики горят!
Ох, когда дошло до дела,
Осрамился наш герой -
Девять блинчиков сгорело,
А десятый был сырой!
Говорить нетрудно речь,
Трудно блинчиков напечь!

Агния Барто.

Вариант 11

Снегирь

На Арбате, в магазине,
За окном устроен сад.
Там летает голубь синий,
Снегири в саду свистят.

Я одну такую птицу
За стеклом видал в окне,
Я видал такую птицу,
Что теперь не спится мне.

Ярко-розовая грудка,
Два блестящие крыла...
Я не мог ни на минутку

Оторваться от стекла.

Из-за этой самой птицы
Я ревел четыре дня.
Думал, мама согласится -
Будет птица у меня.

Но у мамы есть привычка
Отвечать всегда не то:
Говорю я ей про птичку,
А она мне про пальто.

Что в карманах по дыре,
Что дерусь я во дворе,
Что поэтому я должен
Позабыть о снегире.

Я ходил за мамой следом,
Подждал ее в дверях,
Я нарочно за обедом
Говорил о снегирях.

Было сухо, но галоши
Я послушно надевал,
До того я был хорошим -
Сам себя не узнавал.

Я почти не спорил с дедом,
Не вертелся за обедом,
Я "спасибо" говорил,
Всех за все благодарил.

Трудно было жить на свете,
И, по правде говоря,
Я терпел мученья эти
Только ради снегиря.

До чего же я старался!
Я с девчонками не дрался.

Как увижу я девчонку,
Погрожу ей кулаком
И скорей иду в сторонку,
Будто я с ней незнаком.

Мама очень удивилась:
- Что с тобой, скажи на милость?
Может, ты у нас больной -
Ты не дрался в выходной!

И ответил я с тоской:
- Я теперь всегда такой.

Добивался я упрямо,
Повозился я не зря.
- Чудеса,- сказала мама
И купила снегиря.

Я принес его домой.
Наконец теперь он мой!
Я кричал на всю квартиру:
- У меня снегирь живой!

Я им буду любоваться,
Будет петь он на заре...
Может, снова можно драться
Завтра утром во дворе?

Агния Барто.

Вариант 12

Медвежонок невежа

Был сынок у маменьки —
Медвежонок маленький.
В маму был фигурой —
В медведицу бурую.

Уляжется медведица
Под деревом в тени,
Сын рядом присоседится,
И так лежат они.

Он упадет.— Ах, бедненький! —
Его жалеет мать.—
Умнее в заповеднике
Ребенка не сыскать!

Сыночек дисциплины
Совсем не признает!
Нашел он мед пчелиный —
И грязной лапой в мед!

Мать твердит:
— Имей в виду —
Так нельзя
Хватать еду! —
А он как начал чавкать,
Измазался в меду.

Мать за ним ухаживай,
Мучайся с сынком:
Мой его, приглаживай
Шерстку языком.

Родители беседуют —
Мешает он беседе.

Перебивать не следует
Взрослого медведя!

Вот он примчался к дому
И первый влез в берлогу —
Медведю пожилому
Не уступил дорогу.

Вчера пропал куда-то,
Мамаша сбилась с ног!

Взъерошенный, лохматый
Пришел домой сынок
И заявляет маме:
— А я валялся в яме!

Ужасно он воспитан,
Всю ночь ревет, не спит он!

Он мать изводит просто.
Тут разве хватит сил?
Пошел сыночек в гости —
Хозяйку укусил,
А медвежат соседки
Столкнул с высокой ветки.

Медведица бурая
Три дня ходила хмурая,
Три дня горевала:
— Ах, какая дура я —
Сынка избаловала!

Советоваться к мужу
Медведица пошла:
— Сынок-то наш все хуже,
Не ладятся дела!

Не знает он приличий —
Он дом разрушил птичий,
Дерется он в кустах,
В общественных местах.

Заревел в ответ медведь:
— Я при чем тут, женка?
Это мать должна уметь
Влиять на медвежонка!
Сынок — забота ваша.
На то вы и мамаша.

Но вот дошло и до того,
Что на медведя самого,
На родного папу,
Мишка поднял лапу.

Отец, сердито воя,
Отшлепал сорванца.
(Задело за живое,
Как видно, и отца.)

А медведица скулит,
Сына трогать не велит:
— Бить детей недопустимо!
У меня душа болит...

Нелады в семье
Медвежьей —
А сынок
Растет невежей!

Я знаю понаслышке,
И люди говорят,
Что такие мишки

Есть среди ребят.

Агния Барто.

Вариант 13.

Про Вовку, черепаху и кошку

Случилось вот какое дело —
Черепаха похудела!

— Стала маленькой головка,
Хвостик слишком тонок! —
Так сказал однажды Вовка,
Насмешил девчонок.

— Похудела? Ну, едва ли! —
Девочки смеются. —
Молока мы ей давали,
Выпила всё блюдце.

Черепаха панцирь носит!
Видишь, высунула носик
И две пары ножек!
Черепаха панцирь носит,
Похудеть не может.

— Черепаха похудела! —
Уверяет Вова. —
Нужно выяснить, в чем дело,
Может, нездорова?

Смотрит Вовка из окошка,
Видит он — крадется кошка,
Подошла, лизнула блюдце...

Экая плутовка!
Нет, девчонки зря смеются!

— Вот,— кричит им Вовка,—
Поглядите, кошка съела
Завтрак черепаший!
Черепаха похудела
Из-за кошки вашей!

Агния Барто.

Варианты 14

Я с ней дружу

Я осторожно по бревну
Иду через речонку,
А за собой тяну, тяну
Смешливую девчонку.

Она вопит: — Ой, утону!—
Она хохочет звонко,
А я тяну ее, тяну,
Как малого ребенка.

Потом мы мчимся под дождем...
Мы прыгаем по лужам,
Мы под дождем
Друг друга ждем.
Да, я с девчонкой дружен.

Кричат мальчишки мне:
— Жених!—
Я злюсь, конечно,
Злюсь на них,
Но чувств своих не выдам —
Иду с небрежным видом.

Пускай хоть в школьный «Крокодил»
Строчат они заметку,—
Я с ней дружу, я с ней ходил
И в лыжную разведку.

Она летит с горы крутой,
Летит и не поморщится,
А мне кричит:
— Боюсь!
Постой!—
Такая уж притворщица.

Агния Барто.

Секретные сообщения

1. Баклажан на стебле дыни не вырастет
2. Баловать ребенка - всё равно, что бросить его
3. Беда не приходит одна
4. Без шлифовки и алмаз не блестит
5. Бездельник болтлив
6. Бери зонтик раньше, чем промокнешь
7. Бесплезнее, чем писать цифры на текущей воде
8. Бесплезный, как фонарь днем
9. Бессердечные дети отчий дом хают
10. Благодарность помни не меньше обиды
11. Блеск золота ярче сияния Будды
12. Близ умного дети и не учась читают
13. Близкие духом тянутся друг к другу
14. Блохе голову топором не рубят
15. Бог живет в честном сердце
16. Богатство и знатность, полученные нечестным путем, исчезают, как

облако

17. Богач, что пепельница: чем полнее, тем грязнее
18. Более важно умение, а не сила
19. Большая удача вызовет много мелких неприятностей
20. Больше одной жизни не проживешь
21. Большие несчастья происходят от малых причин
22. Большой талант созревает поздно
23. Большому актеру - большая и сцена
24. Братья ссорятся между собой, но обороняются от чужих
25. Брод по указаниям младенца, которого несут на спине, не переходят
26. Брось будд, о богах не беспокойся
27. Будду слепил, да душу вдохнуть забыл
28. Будешь спать в лодке, распустив паруса, - не увидишь берега
29. Была бы вера, а боги найдутся
30. В больших делах мелкие недостатки не обдумывают
31. В деревне без птиц и летучая мышь – птица
32. В десять лет - вундеркинд, в двадцать - талант, а за тридцать - посредственность
33. В дом, где смеются, приходит счастье
34. В драке обе стороны виноваты
35. В дружбе тоже знай меру
36. В жизни семь неудач и семь удач
37. В жизни всё изменчиво
38. В избытке и лекарство – яд
39. В красивом платье и конюх хорош
40. В лохмотьях и царедворца за нищего примут, в шелках и конюх за князя сойдет

Лабораторная работа №6. Перестановочные шифры.

Цель работы: Изучить перестановочные шифры. Шифр «Лесенка». Шифр вертикальной перестановки. Шифр «Поворотная решетка».

Основные сведения

Все рассмотренные ранее методы основывались на замещении символов открытого текста различными символами шифрованного текста. Принципиально иной класс преобразований строится на использовании перестановок букв открытого текста. Шифры, созданные с помощью перестановок, называют перестановочными шифрами.

Шифр «Лесенка».

Простейший из таких шифров использует преобразование «лесенки», заключающейся в том, что открытый текст записывается вдоль наклонных строк определенной длины («ступенек»), а затем считывается построчно по горизонтали. Например, чтобы шифровать сообщение «шифр с использованием перестановки» по методу лесенки со ступеньками длиной 2, запишем это сообщение в виде

Ш Ф С С О Ь О А И М Е Е Т Н В И И Р И П Л З В Н Е П Р С
А О К

Шифрованное сообщение будет иметь следующий вид.

ШФССОЬОАИМЕЕТНВИИРИПЛЗВНЕПРСАОК

Шифр вертикальной перестановки.

Шифр «Лесенка» особой сложности для криптоанализа не представляет. Более сложная схема предполагает запись текста сообщения в горизонтальные строки одинаковой длины и последующее считывание текста столбец за

столбцом, но не по порядку, а в соответствии с некоторой перестановкой столбцов. Порядок считывания столбцов при этом становится ключом алгоритма. Ниже приведен 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 |

Шифрованный текст: ТОСАЛСААВЕТОРБКТЕОПЕКПЦСАНТМ

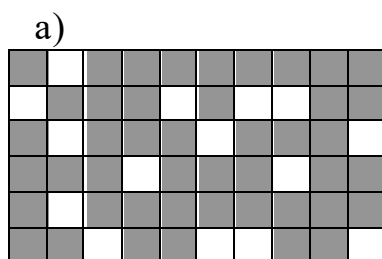
Шифр «Поворотная решетка».

Для использования шифра, называемого поворотной решеткой, изготавливается трафарет из прямоугольного листа клетчатой бумаги размером $2m \times 2n$ клеток. В трафарете вырезано $m \times n$ 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.

Рассмотрим процесс шифрования на примере. Пусть в качестве ключа используется решетка 6×10 , приведенная на рисунке 3, а. Зашифруем с ее помощью текст

ШИФРРЕШЕТКАЯВЛЯЕТСЯЧАСТНЫМСЛУЧАЕМШИФРАМАРШРУТНОЙ
ОЙПЕРЕСТАНОВКИ.



б)

| | | | | | | | | | |
|---|---|---|---|---|---|---|---|--|---|
| | Ш | | | | | | | | |
| И | | | | Ф | | Р | Р | | |
| | Е | | | | Ш | | | | Е |
| | | | Т | | | | К | | |
| | А | | | | | | | | |
| | | Я | | | В | Л | | | Я |

в)

| | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|
| Е | Ш | | Т | С | | | Я | | |
| И | | | | Ф | | Р | Р | Ч | |
| | Е | А | | | Ш | С | | | Е |
| | | | Т | Н | | | К | Ы | |
| | А | М | С | | Л | | | | У |
| | | Я | | | В | Л | | Ч | Я |

г)

| | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|
| Е | Ш | А | Т | С | Е | М | Я | | Ш |
| И | И | | | Ф | | Р | Р | Ч | |
| | Е | А | Ф | | Ш | С | Р | | Е |
| Т | А | | Т | Н | М | | К | Ы | А |
| Р | А | М | С | Ш | Л | Р | У | | У |
| | Т | Я | | | В | Л | | Ч | Я |

д)

| | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|
| Е | Ш | А | Т | С | Е | М | Я | Н | Ш |
| И | И | О | Й | Ф | П | Р | Р | Ч | Е |
| Р | Е | А | Ф | Е | Ш | С | Р | С | Е |
| Т | А | Т | Т | Н | М | А | К | Ы | А |
| Р | А | М | С | Ш | Л | Р | У | Н | У |
| О | Т | Я | В | К | В | Л | И | Ч | Я |

Рисунок 1 - Пример шифрования текста методом поворотной решетки.

Наложив решетку на лист бумаги, вписывается первые 15 (по числу вырезов) букв сообщения. Результат после снятия решетки изображен на рисунке 1, б. Повернув решетку на 180 градусов и вписав следующие 15 букв, получаем лист, изображенный на рисунке 1, в. Перевернув лист и проделав то же самое, шифруется остаток текста (рисунок 1, г и д).

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

Число трафаретов, то есть количество ключей шифра «решетка», составляет $T = 4^{mk}$. Этот шифр предназначен для сообщений длины $n = 4mk$. Уже при размере трафарета 8×8 число возможных решеток превосходит 4 миллиарда.

Задания для самостоятельного выполнения

Вариант задания определяется последней цифрой номера зачетной книжки (0 соответствует 10 варианту).

Сообщения создаются и шифруются на базе алфавита
АБВГДЕЖЗИЙКЛМНОПРСТУФХЦЧШЩЪЫЬЭЮЯ.

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

Таблица 1 - Варианты условий к заданию.

| № вари анта | Задание |
|-------------------|---------|
|-------------------|---------|

| | |
|-----|--|
| 1. | ВЩИТЗЪВЪЛОНЕНИУШИЗЕГАЕТСЮЕНОЙОСВЕПТПЫВЗШТРРО БОПАЕАОМНЛОЛОТМРЯЯЕЪЛОЛЕНА |
| 2. | ЛЕСЕПЕУЕОНЪНЯПЗННМИЪУИЩЮДТКРТЮБПОХЕИООИФАЕН ШЕИБЕВО ОИЩЕАСРНИЛВЯОЦСАЕЗТОЙИММРЕЗСТАИСЪАИРИТРНАЫ |
| 3. | МЕЕЕСНЪМТПЦСНРЧЯТЫЗДОЕЕТОБЕТИСООВЧЛИГЧСЕСIVКИ ЕОИЕКЛВ САУОНСЕЛОЪЯПНМБИТСОЙНЗОИЕЕЕНФВДОАЛЕНСМО |
| 4. | ВРОСМЕННАЗАРТМНММММММНИАКНФЦЯСОВУЕАДЕНАНСХ ТАОИЛЕЛО ЮЕЖОНФЦЫТЭРЯРЯАБЪДРБНКТОИХЕЛОИМВНЯОИАУЫУА |
| 5. | СААИАЕЪДЛЪЩКТСЕМИБСДОЧКЕЪХЕОЕИИАСЕНОБИОННРЪМ РСНЦТЗОЛ ЕВНЦОАСПНТФИЕОСЖСАФИСНЯЪОЕОИМПТНПТИАТЯВЮЙМР |
| 6. | ОЗСЗСЕСЕОИИИЩДАТОТТПНЙФИКЕНДЕПИСЕАИИСАНОАМА ЯЯЧДДКТСИЙЧЫСВОЕЕЕАООЯИСБНЛБНЖНЦЧОЗИЕОЯЕИНТИНБ |
| 7. | СЕЕАСБЕАЕМООЧЯРТОКЕАОЕИМЗСТЕЧЕВОСТЕОАЕТТРЧОНС АОНИСИТО ЖТРНТВЛФАЕИБИТЬПООПВЗНЪЕИПИЯАПДСЦЯ |
| 8. | ОИЯИОРИОМТБЕДННСТРЕВЕКОФНАЪОШАСОСОЫМОНАПНТР МИТНТЕТУМРЗПЕЕЧРПАЕБОГЛЕОАЦСАСОБНЛКИУВТВС |
| 9. | ПВАНЦОАЕИНРИЫЯТЗТЫАНРИИСРРТГЕДХВСРЕМСЫУЯТЯМ ОАДАИЛЯУ ЛИСЕШЗЫТКОРПАННЯРШЫИНЕАНХТНИЕЧНЕЮАИН |
| 10. | КЕЪИАНЗПДООИАЕИООНННЦААОАТЖЕЛССВНЦОФИЧЩТНВН ГИКСАФИС ОИАИОНОООТОЛНИАТРОЕТКЫЗСАИГЕИДЛЪМЗТУАХМТНЧОД Я |

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 - Варианты условий к заданию.

| № вари анта | Задание |
|-------------------|---|
| 1. | Зашифрованный текст: ФТБЕОЗРЬЩМАОСЕОИАОИНШВОНЖ Частично восстановленный ключ: XX5X1 |
| 2. | Зашифрованный текст: ПНОСОЕЕНМРЗОЮЯАЬБАПТКТБС Частично восстановленный ключ: 6XX1X4 |
| 3. | Зашифрованный текст: ОННАНЦОНДЛЬХФИСНИАТЫКЕЬД Частично восстановленный ключ: XX24X3 |
| 4. | Зашифрованный текст: СИВОСЕНЕЗОПЕОПТОЧЕБСЕСЙАИБЕТЕН Частично восстановленный ключ: 4XX13X |
| 5. | Зашифрованный текст: СНСКЫЕЕОАНОЕЕУАБЧДПНПITДМ Частично восстановленный ключ: 3XXX5 |
| 6. | Зашифрованный текст: АКДВСЕШНЛСООСИЫАЧЕФЯКЕТРИМИИ Частично восстановленный ключ: 63XX27X |
| 7. | Зашифрованный текст: ИАОТЮОЕРКМФНТЫЧРИКМОШВСЫЛ Частично восстановленный ключ: XX3X2 |
| 8. | Зашифрованный текст: ЛЩЕОЫЙМААТЛНТОАОЯСВКЗЕЗЛААТ Частично восстановленный ключ: 7XX3X24 |
| 9. | Зашифрованный текст: СУХЫЫМИЗЕМТРОТНАНЦПЙАЗИАЛЕИЩФИЬМЗИОИ Частично восстановленный ключ: 2XX3X6 |
| 10. | Зашифрованный текст: БСЕАГНМЗЛАЕООЯНПЛТБНАЕЕСЬБЕА Частично восстановленный ключ: 2X41XX7 |

Отчет по лабораторной работе должен содержать:

- исходный текст;
- полученный результат;
- код программы;
- описание алгоритма программы.

В ЭС прикреплять отчет и исходник файла.

Контрольные вопросы:

1. На чем основывается метод перестановок?
2. Оцените надежность шифра «Лесенка».
3. Дайте определение абсолютной защищенности.

Лабораторная работа №7. Шифрование с помощью аналитических преобразований

Цель работы

Исследование шифров, основанных на аналитических преобразованиях.

Теоретическая часть

Достаточно надежное закрытие информации может быть обеспечено при использовании для шифрования некоторых аналитических преобразований. Например, умножение матрицы на вектор по правилу:

$$\overline{C} = A \times \overline{B}; \quad \sum_{j=1}^N a_{ij} b_j \quad (1)$$

Если матрицу $A = (a_{ij})$ использовать в качестве ключа, а вместо компонента вектора $B = (b_j)$ подставить символы текста, то компоненты вектора $C = (c_j)$ будут представлять собой символы зашифрованного текста.

Пример.

Возьмем в качестве ключа квадратную матрицу третьего порядка

$$A = \begin{pmatrix} 14 & 8 & 3 \\ 8 & 5 & 2 \\ 3 & 2 & 1 \end{pmatrix}$$

Заменим буквы алфавита цифрами, соответствующими их порядковому номеру в алфавите: А–0, Б–1, В–2 и т.д. Тогда отрывку текста ВАТАЛА будет соответствовать 2, 0, 19, 0, 12, 0. По принятому алгоритму шифрования необходимо выполнить следующие действия:

$$\overline{C} = A \times \overline{B} = \begin{pmatrix} 14 & 8 & 3 \\ 8 & 5 & 2 \\ 3 & 2 & 1 \end{pmatrix} \times \begin{pmatrix} 2 \\ 0 \\ 19 \end{pmatrix} = \begin{pmatrix} 85 \\ 54 \\ 25 \end{pmatrix};$$

$$\overline{C} = A \times \overline{B} = \begin{pmatrix} 14 & 8 & 3 \\ 8 & 5 & 2 \\ 3 & 2 & 1 \end{pmatrix} \times \begin{pmatrix} 0 \\ 12 \\ 0 \end{pmatrix} = \begin{pmatrix} 96 \\ 60 \\ 24 \end{pmatrix}.$$

При этом зашифрованный текст будет иметь вид: 85, 54, 25, 96, 60, 24.

Дешифрование осуществляется с использованием указанного правила умножения матрицы на вектор, только в качестве ключа берется матрица, обратная той, с помощью которой проводится зашифровывание, а в качестве вектора-сомножителя – соответствующие фрагменты символов закрытого текста; тогда значениями вектора-результата будут цифровые эквиваленты знаков открытого текста.

Матрицей, обратной данной A , называется матрица A^{-1} , получающаяся из присоединения матрицы делением всех ее элементов на определитель данной матрицы. Присоединенной называется матрица, составленная из алгебраических дополнений A_{ij} , к элементам данной матрицы, которые вычисляются по формуле

$$A_{ij} = (-1)^{i+j} \Delta_{ij}, \quad (2)$$

где Δ_{ij} – определитель матрицы, получаемой вычеркиванием i -й строки и j -го столбца исходной матрицы.

Определителем матрицы называется алгебраическая сумма $n!$ членов (для определителя n -го порядка), составленная следующим образом:

членами служат всевозможные произведения n элементов матрицы, взятых по одному в каждой строке и в каждом столбце; причем член суммы берется со знаком «+», если его индексы составляют четную подстановку, и со знаком «-» – в противоположном случае. Для матрицы третьего порядка определитель вычисляется следующим образом:

$$\Delta_{ij} = a_{11}a_{22}a_{33} + a_{12}a_{23}a_{31} + a_{13}a_{21}a_{32} - a_{11}a_{23}a_{32} - a_{12}a_{21}a_{33} - a_{13}a_{22}a_{31}.$$

Процесс раскрытия выглядит так:

$$A^{-1} \times \overline{C} = \begin{pmatrix} 1 & -2 & 1 \\ -2 & 5 & -4 \\ 1 & -4 & 6 \end{pmatrix} \times \begin{pmatrix} 85 \\ 54 \\ 25 \end{pmatrix} = \begin{pmatrix} 1 \cdot 85 - 2 \cdot 54 + 1 \cdot 25 \\ -2 \cdot 85 + 5 \cdot 54 - 4 \cdot 25 \\ 1 \cdot 85 - 4 \cdot 54 + 6 \cdot 25 \end{pmatrix} = \begin{pmatrix} 2 \\ 0 \\ 19 \end{pmatrix};$$

$$A^{-1} \times \overline{C} = \begin{pmatrix} 1 & -2 & 1 \\ -2 & 5 & -4 \\ 1 & -4 & 6 \end{pmatrix} \times \begin{pmatrix} 96 \\ 60 \\ 24 \end{pmatrix} = \begin{pmatrix} 1 \cdot 96 - 2 \cdot 60 + 1 \cdot 24 \\ -2 \cdot 96 + 5 \cdot 60 - 4 \cdot 24 \\ 1 \cdot 96 - 4 \cdot 60 + 6 \cdot 24 \end{pmatrix} = \begin{pmatrix} 0 \\ 12 \\ 0 \end{pmatrix}.$$

Таким образом, получена последовательность знаков раскрытого текста 2, 0, 19, 0, 12, 0, что соответствует исходному тексту.

Ход работы

Реализуйте программный модуль в соответствии с полученным заданием.

После реализации программного модуля выполните статистический анализ текста до криптографического преобразования и после него.

Содержание отчёта

При оформлении отчета необходимо привести исходное сообщение (фамилию имя отчество и номер группы и подгруппы (в текстовом виде), таблицы, ключевые слова (выбираются произвольно), маршруты вписывания и выписывания, повороты решетки и зашифрованное сообщение. Привести алгоритм (блок схему и текстовое описание), скриншоты выполнения

программы и текст кода. Язык программирования выбирается любой. Вместе с отчетом прикрепляется исходники кода.

Варианты заданий

Вариант 1.

$$A = \begin{vmatrix} 1 & 2 & 0 \\ -1 & -3 & 4 \\ 2 & 5 & 6 \end{vmatrix}; T_0 = \langle \text{ЮМОРИСТИЧНЫЙ} \rangle$$

Вариант 2.

$$A = \begin{vmatrix} 5 & 3 & -1 \\ 3 & 2 & -1 \\ 1 & 1 & 0 \end{vmatrix}; T_0 = \langle \text{АЭРОДИНАМИКА} \rangle$$

Вариант 3.

$$A = \begin{vmatrix} 11 & 7 & -4 \\ 7 & 4 & -3 \\ 2 & 2 & -1 \end{vmatrix}; T_0 = \langle \text{БЛАГОВЕЩЕНИЕ} \rangle$$

Вариант 4.

$$A = \begin{vmatrix} -1 & 0 & -2 \\ -5 & 4 & -7 \\ 6 & -4 & -6 \end{vmatrix}; T_0 = \langle \text{ЭВОЛЮЦИОНИСТ} \rangle$$

Вариант 5.

$$A = \begin{vmatrix} 2 & 5 & 7 \\ 6 & 3 & 4 \\ 5 & -2 & -3 \end{vmatrix}; T_0 = \langle \text{ТЕРМИНОЛОГИЯ} \rangle$$

Вариант 6.

$$A = \begin{vmatrix} 1 & 2 & 3 \\ 2 & 1 & 2 \\ 3 & 1 & 3 \end{vmatrix}; T_0 = \langle \text{НАМОРАЖИВАТЬ} \rangle$$

Вариант 7.

$$A = \begin{vmatrix} 2 & 1 & 7 \\ 3 & -5 & 9 \\ -1 & 4 & 6 \end{vmatrix}; T_0 = \langle \text{ПЯТИУГОЛЬНИК} \rangle$$

Вариант 8.

$$A = \begin{vmatrix} 3 & 4 & 2 \\ 2 & -1 & -3 \\ 1 & 5 & 1 \end{vmatrix}; T_0 = \langle \text{ОБЩЕСТВЕННИК} \rangle$$

Вариант 9.

$$A = \begin{vmatrix} 2 & 5 & 1 \\ 3 & 8 & 2 \\ 1 & 2 & 0 \end{vmatrix}; T_0 = \langle \text{КРИПТОГРАФИЯ} \rangle$$

Вариант 10.

$$A = \begin{vmatrix} 2 & 7 & 3 \\ 3 & 9 & 4 \\ 1 & 5 & 3 \end{vmatrix}; T_0 = \langle \text{ЕЖЕНЕДЕЛЬНИК} \rangle$$

Вариант 11.

$$A = \begin{vmatrix} 2 & 2 & 7 \\ -3 & -2 & 5 \\ 4 & 3 & -1 \end{vmatrix}; T_0 = \langle \text{ЧЕРНОКНИЖНИК} \rangle$$

Вариант 12.

$$A = \begin{vmatrix} 5 & 7 & 4 \\ 8 & 3 & 4 \\ 7 & 2 & 3 \end{vmatrix}; T_0 = \langle \text{ЦАРЕУБИЙСТВО} \rangle$$

Вариант 13.

$$A = \begin{vmatrix} 7 & 4 & 9 \\ 3 & 4 & 7 \\ 2 & 3 & 6 \end{vmatrix}; T_0 = \langle \text{СПЕЦИФИКАЦИЯ} \rangle$$

Вариант 14.

$$A = \begin{vmatrix} 4 & 8 & 12 \\ 1 & 2 & 3 \\ 1 & 3 & 5 \end{vmatrix}; T_0 = \langle \text{УДИВИТЕЛЬНЫЙ} \rangle$$

Вариант 15.

$$A = \begin{vmatrix} 2 & 1 & 5 \\ 1 & 3 & 2 \\ 7 & 6 & 3 \end{vmatrix}; T_0 = \langle \text{ИМПРОВИЗАТОР} \rangle$$

Вариант 16.

$$A = \begin{vmatrix} 1 & 2 & 3 \\ 4 & 5 & 6 \\ 7 & 8 & 9 \end{vmatrix}; T_0 = \langle \text{МУСОРОПРОВОД} \rangle$$

Вариант 17.

$$A = \begin{vmatrix} 1 & 1 & 1 \\ 1 & 2 & 3 \\ 7 & 3 & 6 \end{vmatrix}; T_0 = \langle \text{РУКОВОДИТЕЛЬ} \rangle$$

Контрольные вопросы

1. В чем особенности метода аналитических преобразований.
2. Отличия метода посимвольного шифрования и шифрования текста биграммами.
3. Статистический анализ выполненного задания (минимум три примера).

4. Что такое шифрование данных?
5. К какому виду шифрования относится данный метод?
6. В чём сущность шифрования аналитическими методами?
7. Что такое присоединенная матрица?
8. Что такое транспонированная матрица?
9. Какие ещё методы шифрования вы знаете?

Вопросы к зачету по предмету «Программно-аппаратные средства защиты информации»

1. Секретные системы. Алгебра секретных систем. Совершенная секретность.
2. Энтропия. Ненадежность. Избыточность. Расстояние единственности. Идеальные системы.
3. Практическая секретность. Перемешивание. Перестановки, подстановки и линейные преобразования. Статистические методы раскрытия шифров. Распыление и запутывание. Метод вероятных слов.
4. Симметричные криптосистемы. Блочное шифрование. SP-сети. Принцип итеративирования. Конструкция Фейстеля.
5. Шифры DES и ГОСТ 28147-89.
6. Стандарт шифрования AES. Математические основы шифра Rijndael. Поля Галуа.
7. Режимы шифрования блочных шифров ECB, CBC, CFB, OFB.
8. Поточное шифрование. Регистры сдвига. Регистры сдвига с линейной обратной связью. Отводная последовательность. Шифры A5, RC4, SEAL.
9. Асимметричные криптосистемы.
10. Китайская теорема об остатках и ее применение для сокращения времени вычисления.
11. Проверка чисел на простоту. Стратегия построения больших простых чисел. Асимптотический закон распределения простых чисел. Проверка чисел на простоту. Тест Рабина - Миллера.
12. Криптосистема Диффи-Хеллмана. Односторонние функции. Атака «человек посередине».
13. Криптосистема RSA.
14. Односторонние функции с секретом. Сложность задачи факторизации.
15. Криптосистема Эль-Гамала: цифровая подпись, шифрование.
16. Стандарты цифровой подписи.
17. Хэш-функции. Определение, свойства. Парадокс задачи о днях рождения. Примеры применения хэш-функций.
18. Строение хэш-функций, функция сжатия.
19. Криптографические протоколы. Виды протоколов.
20. Доказательства с нулевым разглашением. Модель пещеры.
21. Электронная коммерция. Неотслеживаемость. Слепая подпись.
22. Вопросы управления ключами.
23. Распределение ключей. Сервер ключей. Kerberos.
24. Инфраструктура открытого ключа. Централизованное управление. Центры сертификации. Иерархия центров сертификации.