**Лабораторная работа №5**

**Тема: Программирование алгебраических алгоритмов**

Введение

Для обеспечения защиты информации в настоящее время не существует какого-то одного технического приема или средства, однако общим в решении многих проблем безопасности является использование криптографии и криптоподобных преобразований информации.

1. Цель работы

Исследование и разработка классических методов симметричных криптосистем

2. Краткие сведения из теории

**- Шифры простой замены. Система шифрования Цезаря** - частный случай шифра простой замены. Метод основан на замене каждой буквы сообщения на другую букву того же алфавита, путем смещения от исходной буквы на K букв.

Известная фраза Юлия Цезаря VENI VINI VICI – пришел, увидел, победил, зашифрованная с помощью данного метода, преобразуется в SBKF SFAF SFZF (при смещении на 4 символа).

**- Шифры сложной замены. Шифр Гронсфельда** состоит в модификации шифра Цезаря числовым ключом. Для этого под буквами сообщения записывают цифры числового ключа. Если ключ короче сообщения, то его запись циклически повторяют. Шифротекст получают примерно также, как в шифре Цезаря, но отсчитывают не третью букву по алфавиту (как в шифре Цезаря), а ту, которая смещена по алфавиту на соответствующую цифру ключа.

Пусть в качестве ключа используется группа из трех цифр – 314, тогда

Сообщение СОВЕРШЕННО СЕКРЕТНО

Ключ 3143143143143143143

Шифровка ФПИСЬИОССАХИЛФИУСС

**- Гаммирование**

Процесс зашифрования заключается в генерации гаммы шифра и наложении этой гаммы на исходный открытый текст. Перед шифрованием открытые данные разбиваются на блоки Т(0)*i*одинаковой длины (по 64 бита). Гамма шифра вырабатывается в виде последовательности блоков Г(ш)*i* аналогичной длины (Т(ш)*i*=Г(ш)*i*+Т(0)*i*, где + - побитовое сложение, *i* =1-*m*).

Процесс расшифрования сводится к повторной генерации шифра текста и наложение этой гаммы на зашифрованные данные T(0)*i*=Г(ш)*i*+Т(ш)*i*.

В **шифрах многоалфавитной замены** для шифрования каждого символа исходного сообщения применяется свой шифр простой замены (свой алфавит).

|  |  |
| --- | --- |
|  | АБВГДЕЁЖЗИКЛМНОПРСТУФХЧШЩЪЫЬЭЮЯ\_ |
| А | АБВГДЕЁЖЗИКЛМНОПРСТУФХЧШЩЪЫЬЭЮЯ\_ |
| Б | \_АБВГДЕЁЖЗИКЛМНОПРСТУФХЧШЩЪЫЬЭЮЯ |
| В | Я\_АБВГДЕЁЖЗИКЛМНОПРСТУФХЧШЩЪЫЬЭЮ |
| Г | ЮЯ\_АБВГДЕЁЖЗИКЛМНОПРСТУФХЧШЩЪЫЬЭ |
| . | ………… |
| Я | ВГДЕЁЖЗИКЛМНОПРСТУФХЧШЩЪЫЬЭЮЯ\_АБ |
| \_ | БВГДЕЁЖЗИКЛМНОПРСТУФХЧШЩЪЫЬЭЮЯ\_А |

Каждая строка в этой таблице соответствует одному шифру замены аналогично шифру Цезаря для алфавита, дополненного пробелом. При шифровании сообщения его выписывают в строку, а под ним ключ. Если ключ оказался короче сообщения, то его циклически повторяют. Шифротекст получают, находя символ в колонке таблицы по букве текста и строке, соответствующей букве ключа. Например, используя ключ АГАВА, из сообщения ПРИЕЗЖАЮ ШЕСТОГО получаем следующую шифровку:

|  |  |
| --- | --- |
| Сообщение | ПРИЕЗЖАЮ\_ШЕСТОГО |
| Ключ | АГАВААГАВААГАВАА |
| Шифровка | ПНИГЗЖЮЮЮАЕОТМГО |

В компьютере такая операция соответствует сложению кодов ASCII символов сообщения и ключа по модулю 256.

**- Шифр Виженера.**

Наиболее известной и по праву одной из старейших многоалфавитных (одному шифруемому символу соответствует более одного символа) криптосистем является система известного французского криптографа графа Блейза Виженера (1523-1596).

Для преобразования строится алфавитный квадрат с построчным сдвигом символов в каждом последующем ряду (рисунок 1.5)

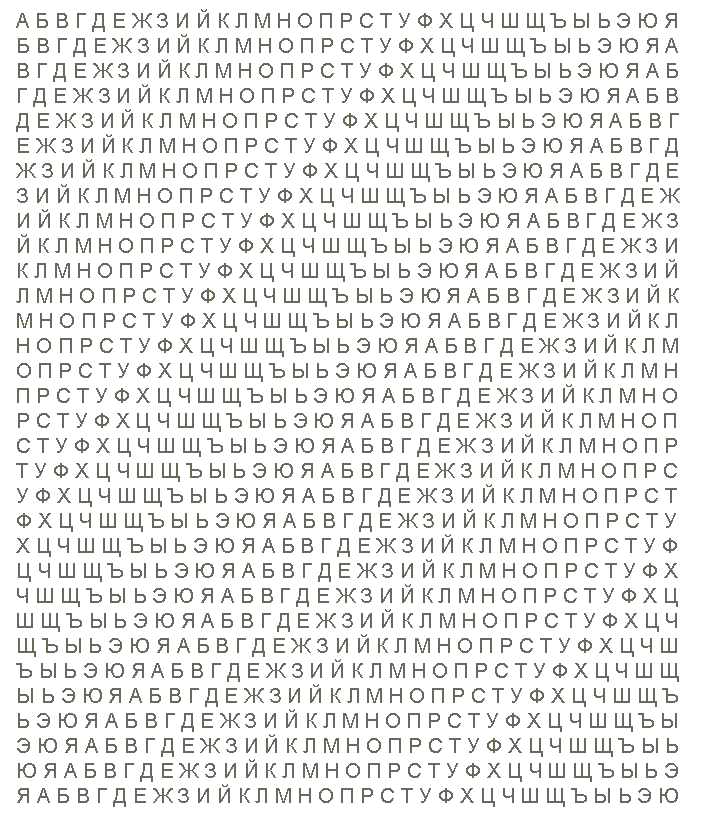


Рисунок 1.5 – Квадрат Виженера

Далее выбирается ключ. Затем пишется шифруемая фраза, а под ней циклически записывается ключ. Преобразование производится так: шифруемому символу соответствует символ, находящийся на пересечении буквы ключа (столбец) и буквы исходного текста (строка).

Одним и тем же буквам исходного текста соответствуют не всегда одинаковые символы, то есть символы могут принимать различные значения, что является несомненным плюсом в плане криптостойкости зашифрованного текста.

Далее выбирается ключ, например “ГРАФДРАКУЛА”. Затем пишется шифруемая фраза, а под ней циклически записывается ключ. Для примера возьмем фразу “ОТРЯД ЖДЕТ УКАЗАНИЙ” и исключим из нее пробелы:

“ОТРЯДЖДЕТУКАЗАНИЙ” – исходный текст, “ГРАФДРАКУЛАГРАФДР” – циклический ключ. Преобразование производится так: шифруемому символу соответствует символ, находящийся на пересечении буквы ключа (столбец) и буквы исходного текста (строка).

Получим: “СВРУИЦДПЕЮКГЧАБМЩ”. Как видно, одним и тем же буквам исходного текста соответствуют не всегда одинаковые символы, то есть символы могут принимать различные значения, что является несомненным плюсом в плане криптостойкости зашифрованного текста.

Квадрат может быть каким угодно, главное, чтобы он был легко воспроизводимым и левый столбец, так же как и верхний ряд, соответствовали всему алфавиту. В качестве альтернативного варианта это может быть известный квадрат Френсиса Бьюфорта, где строки – зеркальное отражение строк квадрата Виженера. Для усложнения строки могут быть переставлены местами в определенном порядке и т. д. Усложненной разновидностью этого метода является метод шифрования с автоключом, предложенный математиком Дж. Кардано (XVI в.). Суть его в том, что, кроме циклического ключа, есть еще один, записываемый однократно перед циклическим ключом – первичный ключ. Этот нехитрый прием придает дополнительную стойкость алгоритму.

**- Шифр Плейфейра.**

Назван так в честь своего разработчика. Алгоритм заключается в следующем: сначала составляется равносторонний алфавитный квадрат. Для русского алфавита подойдет квадрат 5х6. Задается ключевая фраза без повторов букв, например “БАРОН ЛИС”. Фраза вписывается в квадрат без пробелов, далее последовательно вписываются недостающие буквы алфавита в правильной последовательности. Одну букву придется исключить для выполнения условия равносторонности. Пусть это будет Ъ. Примем допущение, что Ъ=Ь. Итак, получился квадрат, который легко восстановить по памяти:

Теперь условия для преобразования:

1. Текст должен иметь четное количество букв и делиться на биграммы (сочетания по две буквы), недостающую часть текста дополняем самостоятельно одним (любым) символом. Например, текст “ОСЕНЬ” преобразуется в “ОСЕНЬА”.
2. Биграмма не должна содержать одинаковых букв – “СОСНА” – “СО СН АБ”.

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

Рисунок 1.6 – Пример алфавитного квадрата для шифрования методом Плейфера

Правила преобразования:

Если биграмма не попадает в одну строку или столбец, то мы смотрим на буквы в углах прямоугольника, образованного рассматриваемыми буквами. Например: “ДИ” = “ЛЕ”, “ЬУ” = “МЮ” и т. д.

Если биграмма попадает в одну строку (столбец), мы циклично смещаемся на одну букву вправо (вниз). Например, “ЛС”=“ИВ”, “ТЭ”=“ЧР”.

Итак, мы готовы преобразовать текст. Приступим к шифрованию:

“СОВЕЩАНИЕ СОСТОИТСЯ В ПЯТНИЦУ” – первоначально преобразуется в биграммы: “СО ВЕ ЩА НИ ЕС ОС ТО ИТ СЯ ВП ЯТ НИ ЦУ”. Выполнив преобразование по вышеизложенным правилам, получим биграммы: “РВ ЗИ НЦ ГА ИЖ ВР РУ ПС ЭГ УИ ФЭ ГА ПШ”.

Обратите внимание на то, что одинаковые буквы на входе дали разные буквы на выходе криптосистемы, а одинаковые буквы на выходе совсем не соответствуют одинаковым на входе. Таким образом, криптотекст “РВЗИНЦГАИЖВРРУПСЭГУИ” выглядит гораздо более “симпатично”, чем после прямой замены моноалфавитной криптосистемы.

Правила преобразования могут значительно варьироваться. Алфавит может быть упрощен до логического минимума с целью сокращения квадрата. Например, можно переводить текст в транслитерацию и писать латинскими буквами, тогда квадрат будет размером 5х5.

**- Система Вернама.**

В 1949 году, Шеннон сформулировал и доказал свою «пессимистическую теорему»: шифр является абсолютно криптостойким тогда и только тогда, когда энтропия ключа больше либо равна энтропии исходного текста. Из теоремы следует, что длина ключа должна быть соразмерна с длиной текста. Если быть более точным, длина ключа должна равняться длине текста.

На основе этой теоремы построена система Вернама. Каждый бит ключа этой системы равновероятно равен 0 либо 1. Длина ключа равна длине текста. Ключ используется только один раз. Доказано, что этот шифр абсолютно не вскрываем. Не будем этого доказывать, но обоснуем.

Для вскрытия шифрованного сообщения необходимо перебрать все возможные комбинации ключей (это единственный способ, так как ключ используется лишь единожды), и среди полученных значений текста выбрать исходный, пусть это будет текст на русском языке. Допустим, что злоумышленник может это сделать мгновенно, то есть опустим временную сложность такой задачи. Для текста любой длины, будет много бессмысленных результатов и их можно отбросить, но злоумышленник получит все возможные тексты заданной длины, в том числе наш текст. Но ничто и никогда не укажет на то, какой из текстов является исходным.

Рассмотрим это на примере четырех буквенных имен. Пусть зашифровано имя «Даша», а ключ «АБВГ». Если используется кодировка ASCII, то зашифрованный текст выглядит следующим образом: ♦!j#. Как говорилось ранее, единственный способ дешифровать текст, полный перебор всех возможных ключей. Но очевидно, что существует такой ключ, суммирование с которым зашифрованного текста даст в результате «Маша», или даже «Миша». Но действительно, невозможно ответить на вопрос, какое из имен является исходным.

Возможно, что аналитик знает часть текста, например, он знает что это договор на продажу недвижимости, но не знает цену. В результате перебора, если на это хватит времени, он получит все возможные цены «заданной длины». То есть если цена трехзначная, аналитиком будет получена девятьсот одна различная цена. Таким образом, взлом системы Вернама не приведет к получению новой информации и является абсолютно невскрываемым.

Недостаток этой системы – длина ключа. Сам Вернам предлагал пересылать ключ курьером. При этом если курьер не довез ключ, можно сгенерировать новый ключ и снова его отправить. Однако такой механизм чрезвычайно неудобен, поэтому эта система не используется в настоящее время.

Этот шифр при его идеальности лишен помехоустойчивости, потому как изменение одного бита, практически невозможно отследить.

3. Порядок выполнения работы

На выбранном языке написать программу шифрования и дешифрования текстового файла методом, указанным преподавателем.

Содержание отчета

1. Название работы.
2. Цель работы.
3. Блок-схему алгоритма шифрования.
4. Тексты программ.

4. Вопросы для самопроверки

1. Шифр Гронcфельда.
2. Шифры двойной перестановки. Шифрование с помощью магического квадрата.
3. Шифр многоалфавитной замены и алгоритм его реализации.

# Рекомендуемая литература

1. Жельников В. Криптография от папируса до компьютера. М.: ABF, 1997. – 336c.
2. Нильс Фергюсон, Брюс Шнайер «Практическая криптография», М.: Издательский дом «Вильямс», 2005г.-424с.
3. Петров А.А. «Компьютерная безопасность. Криптографические методы защиты», М.: ДМК, 2000г. -448с.
4. Коблиц Н. Курс теории чисел в криптографии. – М., Научное издательство ТВП, 2001 г.
5. Масленников А. Практическая криптография BHV – СПб 2003 г.
6. Шнайер Брюс Прикладная криптография. Протоколы, алгоритмы, исходные тексты на языке Си. Триумф-2002 г.
7. Баричев С. Основы современной криптографии. Учебный курс. Горячая линия Телеком 2002 г.

## ASCII таблица

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **ASCII** 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 | **Символ**  NUL SOH STX ETX EOT ENQ ACK BEL BS  TAB LF  VT  FF  CR  SO  SI  DLE DC1 DC2 DC3 DC4 NAK SYN ETB CAN EM  SUB ESC FS  GS  RS  US | **ASCII** 32 33 34 35 36 37 38 39 40 41 42 43 44 45 46 47 48 49 50 51 52 53 54 55 56 57 58 59 60 61 62 63 | **Символ** Space ! " # $ % & ' ( ) \* + , - . / 0 1 2 3 4 5 6 7 8 9 : ; < = > ? | **ASCII** 64 65 66 67 68 69 70 71 72 73 74 75 76 77 78 79 80 81 82 83 84 85 86 87 88 89 90 91 92 93 94 95 | **Символ** @ A B C D E F G H I J K L M N O P Q R S T U V W X Y Z [ \ ] ^ \_ | **ASCII** 96 97 98 99 100 101 102 103 104 105 106 107 108 109 110 111 112 113 114 115 116 117 118 119 120 121 122 123 124 125 126 127 | **Символ** ` a b c d e f g h i j k l m n o p q r s t u v w x y z ~ DEL | **ASCII** 128 129 130 131 132 133 134 135 136 137 138 139 140 141 142 143 144 145 146 147 148 149 150 151 152 153 154 155 156 157 158 159 | **Символ** Ђ Ѓ ‚ ѓ „ … † ‡ € ‰ Љ ‹ Њ Ќ Ћ Џ ђ ‘ ’ “ ” • – — ? ™ љ › њ ќ ћ џ | **ASCII** 160 161 162 163 164 165 166 167 168 169 170 171 172 173 174 175 176 177 178 179 180 181 182 183 184 185 186 187 188 189 190 191 | **Символ** Ў ў Ј ¤ Ґ ¦ § Ё © Є « ¬  ® Ї ° ± І і ґ µ ¶ · ё № є » ј Ѕ ѕ ї | **ASCII** 192 193 194 195 196 197 198 199 200 201 202 203 204 205 206 207 208 209 210 211 212 213 214 215 216 217 218 219 220 221 222 223 | **Символ** 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 | **ASCII** 224 225 226 227 228 229 230 231 232 233 234 235 236 237 238 239 240 241 242 243 244 245 246 247 248 249 250 251 252 253 254 255 | **Figu** 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 |