**Лабораторная работа №1**

**Тема:** Шифр Цезаря.

**Задание:** Имеется шифрованный текст (см. табл. 1), полученный с помощью шифра Цезаря. Величина используемого при этом сдвига неизвестна. Расшифруйте сообщение.

Таблица 1. Варианты л\р1

|  |  |
| --- | --- |
| № вар | Задание |
|  | ИЦРХЭЫЩШШЩРЬЩЩМДРШУРМЮПРЭЪЩЬЭРЪРШШЩТЛЧ РШКЭЗЩМЖВШЩРМЮЧЛСШЩРЬЩЩМДРШУР |
|  | ФГМКРОНФЩЗТЪЦФЫКШНФНХРТЦЛМИЩЪШИХГЙЫМЫЪЧНШНЩН ЯНХГЩНЪЗФРЧНШНМИЯРМИХХГЭ |
|  | ВЦЫБЦГЮМЦСФЦЮГВГУСЩЭЦПГХЯВГДАЫЖЯБЯЙЦЪЫБЩАГЯФБСЕ ЩИЦВЫЯЪГЦЖЮЯЬЯФЩЩ |
|  | КЭЧУЙЧБЗЪАДЮНЮКБИЭКЗШФДЙНОЮБМЬЙББЙБДИБЗДАКНОПЛЬЖЖ МДЛОКЯМЬРДУБНЖДИОБСЙКЗКЯДЫИЮКБЙЙКЯКПМКЮЙЫ |
|  | ТБВРЭФРАВЭЛЕЪАШЯВЮУАРДШЗХБЪШЕБШБВХЬРЕШБЯЮЫМЧГХВБП ЮФШЭШВЮВЦХЪЫОЗШФЫПИШДАЮТРЭШПШФЫПАРБИШДАЮТЪШ |
|  | ШАЖЮЕИДЩЖЦКЮНЫЗАДЯЗЮЗИЫВЫЗДИАЖСИСВАБФНДВАЦЬЪСЯЮ ВЫЫИЪШЦЗШХЭЦГГСЛШЭЦЮВГДАБФНЦ |
|  | ШОФТЙЧШЩМЕТУЖЦВЮБУАШЬТ,ЯТУЩОЫЫЙЧЯЭЬЪЬЗКМТЮБСЬСЬ ШЩМЕО |
|  | ПМЯПРАГЛЛЩЗПГИОГРЛЩЗИЙЬХМРНОЮАЖРГЙЭКМДГРЯЩРЪЖПНМЙ ЪЕМАЮЛВЙЭЦЖТОМАИЖПММЯЧГЛЖЭ |
|  | ЙЧСЦЮЬЪЩЩМЛЫЪРЫФЭИЭЪЪНЕСЩФЛРЪЦМУЗОМСЮГЮЪЪЮЫЬМО ФЮСЧСШНЗЧРСХЭЮОФЮСЧИЩЪЭЪУРМЮСЧИЭЪЪНЕСЩФЛ |
|  | ЖКВИУКУЭВГЦПАНИШЕЧКЙЧЪЪАЬЭЙЭИКАМАВШКЖЪВГЦПЭБВЖКЖ ИУЭЪВГЦПШЦКЪЙЭЩЧАЬЭЕКАМАВШКЖИЗЖГФЯЖЪШКЭГЧ |

**Пояснения:**

*Шифр Цезаря.*

Самым древним и самым простым из известных подстановочных шифров является шифр, использовавшийся Юлием Цезарем. В шифре цезаря каждая буква алфавита заменяется буквой, которая находится на три позиции дальше в этом же алфавите. При этом алфавит считается «циклическим», т.е. за буквой Я следует буква А. Например, для алфавита

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 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 |

шифрование происходит следующим образом:

|  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Открытый текст: | К | Р | И | П | Т | О | Г | Р | А | Ф | И | Я |
| Шифрованный текст: | Н | У | Л | Т | Х | С | Ж | У | Г | Ч | Л | В |

Определить преобразование можно, перечислив все варианты, как показано ниже.

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Открытый текст: | 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 |
| Шифрованный текст: | 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 |

Если каждой букве назначить числовой эквивалент (А = 1, Б = 2 и т.д.), то алгоритм шифрования можно выразить следующими формулами. Каждая буква открытого текста *P* заменяется буквой шифрованного текста *C*:

C = E(P) = (P+3) mod (26).

В общем случае сдвиг может быть любым, поэтому общий алгоритм Цезаря записывается формулой

C = E(P) = (P+k) mod (26),

где *k* принимает значения в диапазоне от 1 до 31 (для рассмотренного алфавита). Алгоритм дешифрования также прост:

P = D(C) = (C-k) mod (26).

Если известно, что определенный текст был зашифрован с помощью шифра Цезаря, то с помощью простого перебора всех вариантов раскрыть шифр очень просто – для этого достаточно проверить 31 возможный вариант ключа.

Применение метода последовательного перебора всех возможных вариантов оправдано следующими тремя важными характеристиками данного шифра.

1. Известны алгоритмы шифрования и дешифрования.
2. Необходимо перебрать всего 31 вариант.
3. Язык открытого текста известен и легко узнаваем.

В большинстве случаев, когда речь идет о защите компьютерной информации, можно предполагать, что алгоритм известен. Единственное, что делает криптоанализ на основе метода последовательного перебора практически бесполезным – это применение алгоритма, для которого требуется перебрать слишком много ключей.

**Контрольные вопросы:**

1. Что представляет собой ключ в этом методе?
2. Как сообщение записывается при шифрации?
3. Как закодированное сообщение считывается при шифрации?
4. Как закодированное сообщение записывается при дешифрации?
5. Как восстановленное сообщение считывается при дешифрации?
6. Можно ли организовать дешифрацию с неизвестным ключом?
7. Можно ли программно определить правильный вариант сообщения после дешифрации?
8. Алгоритм шифрации.
9. Алгоритм дешифрации.
10. Анализ метода.

**Содержание отчета**

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