**Лабораторная работа №1**

**Тема: Программирование арифметических алгоритмов**

Введение

По мере развития и усложнения средств, методов и форм автоматизации процессов обработки информации повышается зависимость общества от степени безопасности используемых им информационных технологий, которая определяется степенью защищенности и устойчивости как компьютерных систем в целом, так и отдельных программ.

1. Цель работы

Исследование и разработка основных методов симметричных криптосистем.

2. Краткие сведения из теории

***Криптография*** – обеспечивает сокрытие смысла сообщения с помощью шифрования и открытия его расшифрованием, которые выполняются по специальным алгоритмам с помощью ключей.

***Ключ*** – конкретное секретное состояние некоторых параметров алгоритма криптографического преобразования данных, обеспечивающее выбор только одного варианта из всех возможных для данного алгоритма.

***Криптоанализ*** – занимается вскрытием шифра без знания ключа (проверка устойчивости шифра).

***Кодирование*** – (не относится к криптографии) – система условных обозначений, применяемых при передаче информации. Применяется для увеличения качества передачи информации, сжатия информации и для уменьшения стоимости хранения и передачи.

Криптосистемы разделяются на ***симметричные*** и *с* ***открытым ключом***.

В ***симметричных криптосистемах*** и для шифрования, и для дешифрования используется ***один и тот же ключ***.

В ***системах с открытым ключом*** используются два ключа - ***открытый*** и ***закрытый***, которые математически связаны друг с другом. Информация шифруется с помощью открытого ключа, который доступен всем желающим, а расшифровывается с помощью закрытого ключа, известного только получателю сообщения.

Криптографические преобразования имеют цель обеспечить недоступность информации для лиц, не имеющих ключа, и поддержание с требуемой надежностью обнаружения несанкционированных искажений. Большинство средств защиты информации базируется на использовании криптографических шифров и процедур шифрования - расшифрования. В соответствии со стандартом ГОСТ 28147-89 под **шифром** понимают совокупность обратимых преобразований множества открытых данных на множество зашифрованных данных, задаваемых ключом и алгоритмом преобразования.

В криптографии используются следующие основные алгоритмы шифрования:

* алгоритм замены (подстановки) – символы шифруемого текста заменяются символами того же или другого алфавита в соответствии с заранее обусловленной схемой замены;
* алгоритм перестановки – символы шифруемого текста переставляются по определенному правилу в пределах некоторого блока этого текста;
* гаммирование – символы шифруемого текста складываются с символами некоторой случайной последовательности;
* аналитическое преобразование – преобразование шифруемого текста по некоторому аналитическому правилу (формуле).

Процессы шифрования и расшифрования осуществляются в рамках некоторой криптосистемы. Для **симметричной** криптосистемы характерно применение одного и того же ключа, как при шифровании, так и при расшифровании сообщений. В **асимметричных** криптосистемах для зашифрования данных используется один (общедоступный) ключ, а для расшифрования – другой (секретный) ключ.

Симметричные криптосистемы.

Шифры перестановки. В шифрах средних веков часто использовались таблицы, с помощью которых выполнялись простые процедуры шифрования, основанные на перестановке букв в сообщении. Ключом в данном случае является размеры таблицы. Например, сообщение “Сегодня новый день” записывается в таблицу из 4 строк и 4 столбцов по столбцам.

|  |  |  |  |
| --- | --- | --- | --- |
| С | Д | О | Д |
| Е | Н | В | Е |
| Г | Я | Ы | Н |
| О | Н | Й | Ь |

Для получения шифрованного сообщения текст считывается по строкам и группируется по 4 букв: СДОД\_ЕНВЕ \_ГЯЫН\_ОНЙЬ

Несколько большей стойкостью к раскрытию обладает **метод одиночной перестановки** по ключу. Он отличается от предыдущего тем, что столбцы таблицы переставляются по ключевому слову, фразе или набору чисел длиной в строку таблицы. Используя в качестве ключа слово Ваза, получим следующую таблицу

|  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| В | А | З | А |  |  |  |  | А | А | В | З |
| 3 | 1 | 4 | 2 |  |  |  |  | 1 | 2 | 3 | 4 |
| С | Д | О | Д |  |  |  |  | Д | Д | С | О |
| Е | Н | В | Е |  |  |  |  | Н | Е | Е | В |
| Г | Я | Ы | Н |  |  |  |  | Я | Н | Г | Ы |
| О | Н | Й | Ь |  |  |  |  | Н | Ь | О | Й |

До перестановки. После перестановки

В верхней строке левой таблицы записан ключ, а номера под буквами ключа определены в соответствии с естественным порядком соответствующих букв ключа в алфавите. Если в ключе встретились бы одинаковые буквы, они бы нумеровались слева направо. Получается шифровка: ДДСО\_НЕЕВ\_ЯНГЫ\_НЬОЙ.

Для обеспечения дополнительной скрытности можно повторно шифровать сообщение, которое уже было зашифровано. Для этого размер второй таблицы подбирают так, чтобы длины ее строк и столбцов отличались от длин строк и столбцов первой таблицы. Лучше всего, если они будут взаимно простыми.

Кроме алгоритмов одиночных перестановок применяются **алгоритмы двойных перестановок**. Сначала в таблицу записывается текст сообщения, а потом поочередно переставляются столбцы, а затем строки. При расшифровке порядок перестановок будет обратный. Число вариантов двойной перестановки достаточно быстро возрастает с увеличением размера таблицы: для таблицы 3 х 3 их 36, для 4 х 4 их 576, а для 5\*5 их 14400.

Пример данного метода шифрования показан в следующих таблицах. Ключом к шифру служат номера столбцов 2413 и номера строк 4123 исходной таблицы :

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  | 2 | 4 | 1 | 3 |  |  | 1 | 2 | 3 | 4 |  |  | 1 | 2 | 3 | 4 |
| 4 | С | Е | Г | О |  | 4 | Г | С | О | Е |  | 1 | Я | Д | Н | Н |
| 1 | Д | Н | Я | Н |  | 1 | Я | Д | Н | Н |  | 2 | Ы | О | Й | В |
| 2 | О | В | Ы | Й |  | 2 | Ы | О | Й | В |  | 3 | Н | Д | Ь | Е |
| 3 | Д | Е | Н | Ь |  | 3 | Н | Д | Ь | Е |  | 4 | Г | С | О | Е |

Двойная перестановка столбцов и строк

В результате перестановки получена шифровка: ЯДННЫОЙВНДЬЕГСОЕ. В средние века для шифрования применялись и **магические квадраты**. Магическими квадратами называются квадратные таблицы с вписанными в их клетки последовательными натуральными числами, начиная с единицы, которые дают в сумме по каждому столбцу, каждой строке и каждой диагонали одно и то же число. Для шифрования необходимо вписать исходный текст по приведенной в квадрате нумерации и затем переписать содержимое таблицы по строкам. В результате получается шифротекст, сформированный благодаря перестановке букв исходного сообщения.

|  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 16 | 3 | 2 | 13 |  |  | О | И | Р | Т |
| 5 | 10 | 11 | 8 |  |  | З | Ш | Е | Ю |
| 9 | 6 | 7 | 12 |  |  | \_ | Ж | А | С |
| 4 | 15 | 14 | 1 |  |  | Е | Г | О | П |

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| П | Р | И | Е | З | Ж | А | Ю | \_ | Ш | Е | С | Т | О | Г | О |
| 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 | 14 | 15 | 16 |

Число магических квадратов очень резко возрастает с увеличением размера его сторон: для таблицы 3\*3 таких квадратов -1; для таблицы 4\*4 - 880; а для таблицы 5\*5-250000.

3. Порядок выполнения работы

На языке DELPHI, VBA С++ или C# 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.

Вопросы для самопроверки

1. Цель и задачи криптографии.
2. Шифры одиночной перестановки и перестановки по ключевому слову.
3. Шифры двойной перестановки. Шифрование с помощью магического квадрата.