ЛАБОРАТОРНАЯ РАБОТА № 2

ИССЛЕДОВАНИЕ РАЗЛИЧНЫХ МЕТОДОВ ЗАЩИТЫ ТЕКСТОВОЙ ИНФОРМАЦИИ И ИХ СТОЙКОСТИ НА ОСНОВЕ ПОДБОРА КЛЮЧЕЙ

Цель работы: изучение методов шифрования/расшифрования перестановкой символов, подстановкой, гаммированием, использованием таблицы Виженера. Исследование и сравнение стойкости различных методов на основе атак путем перебора всех возможных ключей.

В лабораторной работе рассматривается способ вскрытия шифра, основанный на переборе всех вариантов ключа. Критерием правильности варианта служит наличие в тексте «вероятного слова». Перебирается множество всех возможных ключей, шифрованный текст расшифровывается на каждом ключе. В получившемся «псевдооткрытом» тексте ищется вероятное слово. Если такого слова нет, текущий текст бракуется и осуществляется переход к следующему ключу. Если такое слово найдено, на экран выводится вариант ключа. Затем перебор ключей продолжается до тех пор, пока не исчерпается все множество вариантов. Возможно обнаружение нескольких ключей, при которых в «псевдооткрытых текстах» имеется вероятное слово.

После завершения перебора необходимо расшифровать текст на найденных ключах. «Псевдооткрытый текст» выводится на экран для визуального контроля. Если оператор признает текст открытым, то работа по вскрытию заканчивается. Иначе данный вариант ключа бракуется и осуществляется переход к следующему ключу.

Описание лабораторной работы. Для выполнения лабораторной работы необходимо запустить программу **LAB_RAB.exe**, используемую для шифрования/расшифрования, а также дешифрования (методом протяжки вероятного слова) файлов.

Система реализует следующие функции:

- ввод, удаление и селекция ключей пользователя;
- поддержка списка ключей;
- шифрование и расшифрование текста;
- дешифрование текста путем подбора ключей, методом протяжки вероятного слова.

Система поддерживает следующие методы криптографического преобразования информации:

- замена;
- перестановка;

- гаммирование;
- таблица Виженера.

При запуске утилит шифрования и расшифрования у пользователя запрашивается подтверждение на правильность выбранного метода для работы и соответствия заданного ключа целям пользователя (также всегда при изменении файла в текстовом редакторе выдается запрос на сохранение изменений при каждом шаге, дальнейшее развитие которого приведет к необратимым изменениям в файле и потере изначальной информации).

Описание интерфейса:

- окно текстового редактора с широким набором дополнительных функций;
- таблица всех ключей, введенных в систему с быстрым доступом для ввода, удаления или выбора текущего ключа;
- список всех методов шифрования для быстрого и удобного переключения между ними;
- основное меню (вверху экрана);
- дополнительное меню (вызывается нажатием правой кнопки мыши);
- набор вспомогательных кнопок для быстрого и удобного интерфейса;
- поля вывода текущего состояния системы:
  — текущий ключ,
  — вероятное слово,
  — сила ключа для протяжки.

Пример работы с программой

Внимание! Будьте внимательны при установке параметров работы, так как в процессе вычисления по ходу работы эти параметры изменить уже не удастся. После запуска программы абсолютно все рабочие поля пустые и необходимо провести первоначальные настройки для работоспособности системы.

Алгоритм работы с программой:

1) вводится список ключей;
2) вводится вероятное слово (необязательно вначале, до его ввода все меню запуска протяжки все равно недоступны);
3) выбирается необходимый метод шифрования;
4) загружается исходный или зашифрованный файл (открываются соответствующие меню для шифрования и расшифрования);
5) запускается необходимый процесс:
   — шифрование,
   — расшифрование,
   — протяжка вероятного слова,
   — конвертация текста;
6) продолжение работы в любом порядке в соответствии с описанными пунктами;
7) при завершении работы не забудьте сохранить необходимые результаты (при закрытии и загрузке новых файлов система автоматически запрашивает подтверждение на запись).

Шифрование:

1. Открыть файл.
2. Внести необходимые изменения.
3. Настроить соответствующие параметры:
   - тип шифрования;
   - ключ, пр.
4. Запустить процесс шифрования через пункт меню УТИЛИТЫ/ЗАШИФРОВАТЬ F5.

Внимание! При шифровании файла все внесенные пользователем изменения до текущего момента времени будут сохранены на жестком диске.

Расшифрование:

1. Открыть файл.
2. Произвести необходимые изменения.
3. Настроить соответствующие параметры: тип шифрования, пр.
4. Запустить процесс расшифрования через пункт меню УТИЛИТЫ/РАСШИФРОВАТЬ F6.

Внимание! При расшифровании файла все проведенные пользователем изменения до текущего момента времени будут сохранены на жестком диске.

Протяжка вероятного слова (дешифрование)

Внимание! Мощность ключа задастся заранее в опции «сила ключа». Длина ключа значительно влияет на время протяжки вероятного слова (в худшем случае имеем дело с логарифмическим алгоритмом).

1. Вводится вероятное слово (длиной от 1(3) до 9).
2. Для отделения вновь найденных ключей от предыдущих между ними добавляется надпись «подбор».
3. Перебираются ключи.
4. Расшифровывается вся первая строка текста по текущему ключу.
5. Порциями, равными длине вероятного слова, сравнивается содержимое этой строки со значением вероятного слова.
6. Если найдено хоть одно совпадение, запоминается ключ.

7. Переход к новому ключу.
8. Переход к следующей строке.
9. Результаты должны содержаться в списке ключей. Если совпадений не найдено, в список ключей ничего не добавляется.

Операции с ключами. С базой ключей могут осуществляться следующие действия:

- добавить новый ключ;
- удалить одну запись;
- изменить активную запись;
- очистить всю таблицу введенных ключей.

Примечание. Под словами «работа с таблицей ключей» имеются в виду ключи, введенные для использования в двух методах (гаммирования и таблица Виженера).

Ключи для перестановки. В каждый момент времени в системе может быть только один текущий ключ для перестановки.

Правила ввода ключа для перестановки:

1) при переключении в списке поддерживаемых системой методов шифрования на пункт «Перестановка» вызывается окно ввода ключа перестановки. Окно состоит из двух кнопок (ОТМЕНЫ и ВЫХОДА без изменений и кнопки ENTER — подтверждение установленной длины ключа) и окна задания длины ключа для перестановки;
2) в окне задания длины ключа необходимо выбрать необходимую длину (параметры заменяются в пределах 1...9) и подтвердить желание использовать ключ именно такой длины;
3) после подтверждения в окне высветятся кнопки с цифрами на лицевой стороне (в количестве, равном длине ключа), при нажатии на кнопку происходит фиксация кнопки (ее обесцвечивание) для невозможности ее дальнейшего использования (так как все цифры в ключе перестановки должны быть неповторяющимися);
4) после перебора всех кнопок система запоминает введенный ключ, выводит его в поле ввода ключей и выходит из окна ввода ключа перестановки в окно основной программы.

Задание

1. Ознакомиться с описанием лабораторной работы и заданием.
2. Выполнить настройку программы: выбрать метод шифрования, ввести ключи для всех методов, ввести вероятное слово, осуществить все остальные системные настройки.

3. Для метода замены (одноалфавитного метода):

- выбрать данный алгоритм в списке доступных методов шифрования;
- установить необходимое смещение;
- открыть произвольный файл;
- просмотреть содержимое исходного файла;
- выполнить для этого файла шифрование (при необходимости можно задать имя зашифрованного файла);
- просмотреть в редакторе зашифрованный файл;
- ввести вероятное слово;
- ввести вероятную длину ключа (кроме метода замены);
- подобрать ключ;
- выполнить расшифрование со всеми найденными ключами;
- найти в каком-либо из расшифрованных файлов правильно расшифрованное ключевое слово;
- расшифровать файл исходным ключом;
- проверить результат.

4. Для метода перестановки:

- выбрать метод перестановки;
- в открывшемся окне ввода ключа перестановки символов указать сначала длину этого ключа, а затем из появившихся кнопок составить необходимую комбинацию для ключа, нажимая на кнопки в заданном порядке; при этом уже использованные кнопки становятся недоступными для предотвращения их повторного ввода;
- далее действия полностью соответствуют изложенным в п. 3.

5. Для метода гаммирования:

- выбрать метод;
- ввести ключ;
- полностью повторить п. 3.

6. Для таблицы Виженера все действия повторяются из п. 5 (метод гаммирования).

В отчете для каждого метода шифрования описывается последовательность выполняемых действий, указываются имена всех использованных файлов, исходные и найденные ключи, описывается процесс дешифрования.

Преподавателю предоставляется отчет о проделанной работе и все использованные файлы.

7. Привести в отчете ответы на контрольные вопросы в соответствии с номером варианта, указанным преподавателем (табл. 1.2).

Таблица 1.2

Номер варианта	Контрольные вопросы
1, 5, 7, 3, 9, 18, 28	Чем отличается псевдооткрытый текст (текст, полученный при расшифровке по ложному ключу) от настоящего открытого текста?
2, 4, 6, 8, 20, 22, 24, 26, 30	Как зависит время вскрытия шифра описанным выше способом подбора ключей от длины вероятного слова?
11, 13, 15, 10, 17, 19, 27	Зависит ли время вскрытия шифра гаммирования (или таблицы Виженера) от мощности алфавита гаммы?
12, 14, 16, 21, 23, 25, 29	В чем недостатки метода дешифрования с использованием протяжки вероятного слова?