Ф СО ПГУ 7.18.1/02

Министерство образования и науки Республики Казахстан

Павлодарский государственный университет им. С. Торайгырова

Факультет физики, математики и информационных технологий

МЕТОДИЧЕСКИЕ УКАЗАНИЯ К ЛАБОРАТОРНЫМ ЗАНЯТИЯМ

Информационная безопасность и защита информации

Павлодар

Ф СО ПГУ 7.18.1/14

УТВЕРЖДАЮ
Декан ФФМиИТ
_____Ж.К. Нурбекова
«__»_____2010 г.

Составитель: старший преподаватель Токкожина М.А.
(должность, уч. степень, звание, подпись)

Кафедра Информатика и информационные системы

МЕТОДИЧЕСКИЕ УКАЗАНИЯ К ПРАКТИЧЕСКИМ ЗАНЯТИЯМ

Информационная безопасность и защита информации
(полное наименование дисциплины по рабочему учебному плану)

для студентов специальности (ей) 050602 «Информатика» 050703, Информационные системы
(шифр и полное наименование специальности)
Рекомендована на заседании кафедры от «__»_____2010 г.
Протокол №_____

Заведующий кафедрой_____Асаинова А.Ж.
(подпись)
Одобрена методическим советом факультета ФФМиИТ
«___»_____2010 г. Протокол №_____
Председатель МС_____ Муканова Ж.Г..
(подпись)

Лабораторная работа №1

Тема: симметричные криптосистемы.

Цель работы: Разработать криптографическую защиту информации, содержащейся в файле данных, с помощью алгоритма шифрования, указанного в варианте. Для этого:

1. Разработать алгоритмы шифрования и дешифрования блока (потока) открытого текста заданной длины из алфавита Z_n на заданном ключе с помощью метода, указанного в варианте(Если это позволяет алгоритм, длину блока взять кратной 8 бит).
2. Определить алфавит криптосистемы (открытого текста и шифртекста). Если алфавит не задан в варианте, выбрать его самостоятельно, так, чтобы он включал в себя символы используемого в примере открытого текста. Например, русский, английский, ASCII. Поставить символам исходного алфавита в соответствие символы из алфавита Z_n (n – основание алфавита).
3. Написать программу генерации случайных ключей шифра, оценить размерность ключевого пространства.
4. Написать програму, реализующую шифрование на заданном ключе открытого текста, состоящего из символов заданного алфавита. Открытый текст, ключ и шифртекст должны быть представлены отдельными файлами.
5. Написать програму для реализации алгоритма дешифрования полученного файла шифртекста при известном ключе.
6. Провести тестирование программ
   - на коротких тестовых примерах.
   - на текстах в несколько страниц

Лабораторная работа №2

Тема: криптоанализ симметричных криптосистем.

Провести эксперимент по определению практической стойкости, алгоритма, разработанного в лабораторной работе №1.

Считать, что противнику известен алгоритм шифрования. Выбрать наилучший с его точки зрения алгоритм подбора ключа и обосновать свой выбор. Использовать методы:

анализа статистических свойств шифртекста (частот появления букв).

силовую атаку (полный перебор ключей).

другие (если есть более эффективные)

С помощью программы, реализующей выбранный алгоритм криптоанализа провести экперимент по вскрытию шифртекстов различного размера.

При использовании статистического криптоанализа использовать таблицы, приведенные в приложении или подсчитать частоты появления букв используемого алфавита в тексте, частью которого является текст примера.

Для проверки на «осмысленность» полученного текста создать мини-словарь из части слов, встречающихся в тексте примера.

Построить графики зависимости времени криптоанализа от параметров алгоритма шифрования (длины или других параметров ключа, размера шифр-текста или др., в зависимости от алгоритмов шифрования и криптоанализа).

В результате эксперимента определить параметры алгоритма шифрования (размер передаваемого текста, размер и характеристики ключа, объем ключевого пространства и другие параметры алгоритма шифрования), необходимые для практической криптостойкости разработанного в лабораторной работе №1 алгоритма ширования.

Практической криптостойкостью в данной работе будем считать невозможность взлома шифра противником, имеющим в распоряжении один ПК мощности, равной мощности компьютера, на котором делалась работа и один час времени.

Лабораторная работа №3

Тема: Криптографические протоколы на основе асимметричных криптосистем..

Разработать алгоритмы, реализующие криптографические протоколы (см. вариант) взаимодействия удаленных абонентов на основе асимметричных криптосистем.

Написать программы, реализующие эти протоколы для всех участников. Значения модуля криптосистемы выбирать не менее 50 бит. Для вычислений с большими числами можно использовать специальные программы.

Для проверки чисел на простоту использовать комбинированный алгоритм на основе тестов Леманна или Рабина-Миллера

Хеширование выполнять на основе любого блочного симметричного алгоритма (например с использованием сети Фейстеля или алгоритма из предыдущих лаб. работ) по одной из схем, данных в лекциях.

Проверить правильность выполнения протокола для малых значений параметров криптосистемы (контрольный пример).

Продемонстрировать выполнение протокола для нормальных значений параметров криптосистемы.

1. Варианты

К лабораторным работам № 1-2

Основные варианты:

Вариант 1. Шифрующие таблицы с числовым ключом

Вариант 2. Шифр Гронсфельда с ключевым словом

Вариант 3. Алгоритм, реализующий идею «диска Альберти» для русского алфавита

Вариант 4. Шифр Цезаря с ключевым словом

Вариант 5. Шифрующие таблицы с перестановкой по ключу –размеру таблицы.

Вариант 6. Полибианский квадрат для русского алфавита.

Вариант 7. Шифр Гронсфельда с числовым ключом

Вариант 8. Шифр Кардано без поворотов.

Вариант 9. Шифр Плейфера

Вариант 10. Шифрующие таблицы с ключевым словом

Вариант 11.Шифр Цезаря многоалфавитный

Вариант 12. Шифр гаммирования с линейным конгруэнтным генератором ключей

Вариант 13. Аффинная система подстановок Цезаря

Вариант 14. Шифр Вижинера с числовым ключом

Вариант 15. Шифр Хилла для 3-грамм

Вариант 16. Шифрующие таблицы Трисемуса

Вариант 17. Шифр Вернама.

Вариант 18. Алгоритм, реализующий идею «диска Альберти» для английского алфавита

Вариант 19. Шифр Вижинера с ключевым словом

Вариант 20. Шифр гаммирования с генератором ключей на основе датчика случайных чисел

Вариант 21. Полибианский квадрат для английского алфавита.

Вариант 22. Шифрующие таблицы с двойной перестановкой по ключевому слову.

Вариант 23. Шифр Уинстона

Вариант 24. Шифрующие таблицы с двойной перестановкой по числовому ключу.

Дополнительные варианты(повышенной сложности):

Вариант 25. Магические квадраты

Вариант 26. Шифр Кардано с поворотами.

К лабораторной работе № 3

1. Протокол обмена секретным документом комбинированным методом шифрования на основе криптосистемы RSA.
2. Протокол двустороннего подписания контракта на основе алгоритма цифровой подписи ГОСТ Р 34.10-94.

3. Протокол обмена несекретным документом с цифровой подписью на основе алгоритма RSA.
4. Протокол обмена секретным документом, зашифрованным с помощью алгоритма RSA.
5. Протокол идентификации абонента с помощью алгоритма цифровой подписи DSA.
6. Протокол обмена несекретным документом с невидимой цифровой подписью на основе алгоритма RSA.
7. Протокол византийского соглашения для трех участников на основе схемы Шамира проверяемого разделения секрета.
8. Протокол генерации сеансового секретного ключа на основе криптосистемы RSA.
9. Протокол обмена несекретным документом с цифровой подписью на основе алгоритма Эль Гамаля.
10. Протокол обмена несекретным документом со слепой цифровой подписью на основе алгоритма RSA.
11. Протокол аутентификации Шнорра.
12. Протокол идентификации абонента с помощью алгоритма цифровой подписи RSA.
13. Протокол двустороннего подписания контракта на основе алгоритма цифровой подписи Эль Гамаля.
14. Протокол вычисления ключа доступа при разделении секрета между тремя участниками по схеме Шамира проверяемого разделения секрета.
15. Протокол обмена несекретным документом с цифровой подписью DSA.
16. Протокол двустороннего подписания контракта на основе алгоритма цифровой подписи RSA.
17. Протокол обмена несекретным документом с цифровой подписью на основе алгоритма ГОСТ Р 34.10-94.
18. Протокол обмена секретным документом с цифровой подписью на основе алгоритма RSA.
19. Протокол идентификации абонента с помощью алгоритма цифровой подписи ГОСТ Р 34.10-94.
20. Протокол «подбрасывания монеты по телефону».
21. Протокол экпоненциального ключевого обмена по методу Диффи-Хеллмана.
22. Протокол вычисления дискретного логарифма со скрытием информации от оракула.
23. Протокол обмена секретным документом комбинированным методом шифрования на основе экпоненциального ключевого обмена по методу Диффи-Хеллмана.
24. Протокол двустороннего подписания контракта на основе алгоритма цифровой подписи DSA.

25. Протокол идентификации абонента с помощью алгоритма цифровой подписи Эль Гамаля.

26. Протокол обмена секретным документом, зашифрованным с помощью алгоритма Эль Гамаля.

2. Приложение .

Приложение 1: Таблица вероятностей букв в русских текстах.

буква	пробел		**е** или **ё**	**а**	**и**	**н**	**т**	**с**	**р**	**в**	**л**
вер-ть	0,175	,090	,072	,062	,062	,053	,053	,045	,040	,038	,035
буква	**к**		**д**	**п**			**у**	**я**	**з**	**ы**	**б**
вер-ть	0,028	,026	,025	,023	,021	,018	,016	,016	,014	,014	,013
буква	**ъ** или **ь**		**х**	**ж**	**ш**	**ю**	**ц**	**щ**	**э**	**ф**	
вер-ть	0,012	,010	,009	,007	,006	,004	,003	,003	,002		
					,006						

***Приложение* 2. Таблица вероятностей букв в английских текстах.**

буква	пр-л	**e**	**t**	**a**	**o**	**n**	**i**	**s**	**r**
вер-ть	,185	,097	,076	,064	,062	,057	,056	,052	,047
буква	**h**	**l**	**d**	**c**	**u**	**p**	**f**	**м**	**w**
вер-ть	,04	,031	,028	,025	,018	,018	,018 ,017	,016	
буква	**y**	**в**	**g**	**v**	**к**	**q**	**x**	**j**	**z**
вер-ть	,015	,013	,013	,007	,039	,002	,002	,001	,001

Лабораторная работа №6

Тема: **Алгоритм защиты БД MS Access**

1. Создать новую уникальную рабочую группу.

2. Создать новую учетную запись администратора. Подключится к новой рабочей группе; открыть любую БД; в меню – сервис выбрать защиту и пользователей группы; создать нового пользователя, ввести имя и код

учетной записи (это не пароль); в списке имеющейся группы выбрать: Admins – добавить.

3. Удалить из группы администраторов пользователя Admin.
4. Выйти из Access и войти новым пользователем в Access; обязательно ввести пароль на данную учетную запись.
5. Создать заново БД, которую хотим защитить.
6. Выполнить импорт объектов из исходной БД в БД, созданную на предыдущем шаге.
7. Выполнить распределение прав на необходимые объекты.

8. Порядок выполнения и результаты работы

Защита на уровне пароля

Откройте БД, в пункте меню ***Сервис*** выберите ***Защита/Задать пароль базы данных*** (см. рис.1)

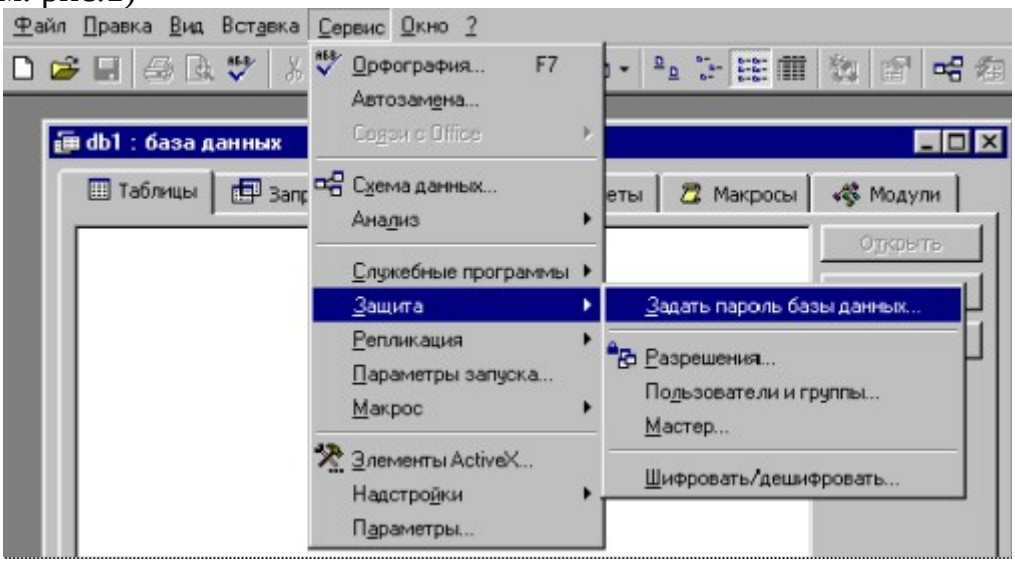

Рис.1 Защита БД при помощи пароля

Появится окно, в котором вас попросят ввести пароль и повторить его (рис.2).

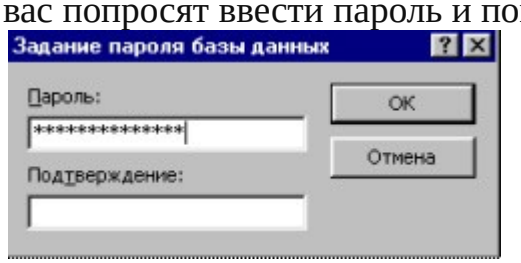

Рис.2 Ввод пароля

Рекомендации по выбору пароля:

- не желательно в качестве пароля использовать такие данные, как ваше имя, дата рождения и т.д.;
- не стоит выбирать короткий пароль, так как он может быть подобран при помощи специальных программ за достаточно короткое время;
- нежелательна комбинация букв и цифр, так как это затрудняет подбор пароля и делает бесполезной атаку по словарю.

Защита на уровне пользователя

Для этого вида защиты необходимо сначала создать новую рабочую группу (если вы будете использовать старую, то БД легко можно будет вскрыть, т.к. в этом случае для алгоритма защиты будут браться данные, указанные при установке Windows или MS Access).
Для создания новой рабочей группы запустите программу WRKGADM.EXE, находящуюся в каталоге WINDOWS/SYSTEM, и нажмите кнопку ***Создать*** (рис.3).

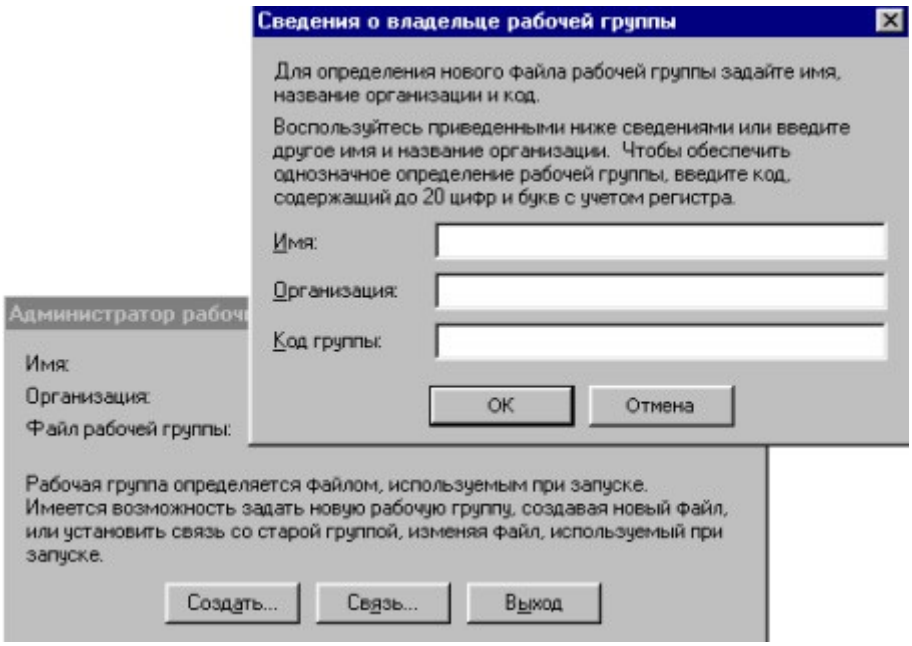

Рис.3 Создание новой рабочей группы

В появившемся диалоге введите запрашиваемую информацию и нажмите кнопку ***OK.*** Задайте имя новой рабочей группы, например MY_GR.MDW (рис.4).

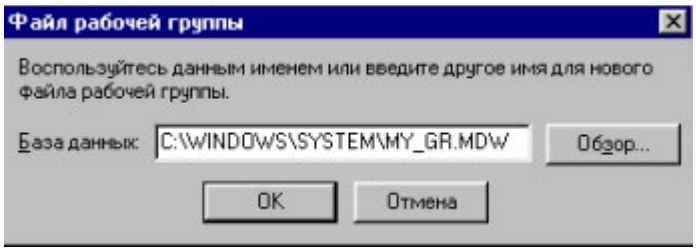

Рис.4 Ввод имени новой рабочей группы

В случае правильного введения данных и их подтверждения появится сообщение о завершении создания рабочей группы. Теперь можно выйти из программы *Администратор рабочих групп.*
Запустите БД, которую необходимо защитить. В пункте меню ***Сервис*** выберите ***Защита/Пользователи и группы*** (рис.5).

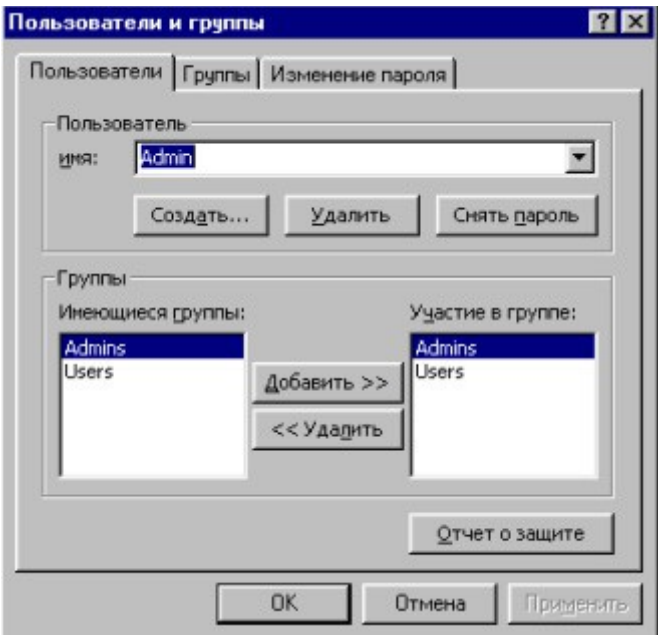

Рис.5 Окно свойств пользователей и групп

Нажмите кнопку ***Создать…*** и введите имя нового пользователя, например *user1*, укажите его код. По умолчанию запись войдет в группу *Users.* Повторите эти действия для всех пользователей, которые будут работать с БД. Перейдите в вкладку ***Изменение пароля.*** Задайте пароль администратора, после чего при каждом запуске *Access* будет появляться окно, предлагающее ввести имя пользователя и пароль (рис.6).

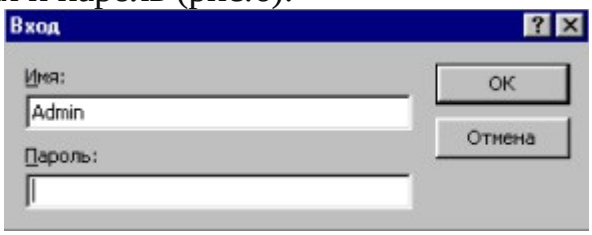

Рис.6 Запрос имени и пароля пользователя

В пункте меню ***Сервис*** выберите ***Защита/Разрешения*** (рис.7). Выберете защищаемый объект, например Таблица1. Задайте разрешения для группы *Users*, а затем и для каждого из пользователей.
Ну вот и все, остается каждому пользователю самому ввести свой пароль. Для этого необходимо зайти в БД под своим имением и выполнить действия как при создании пароля Администратора.

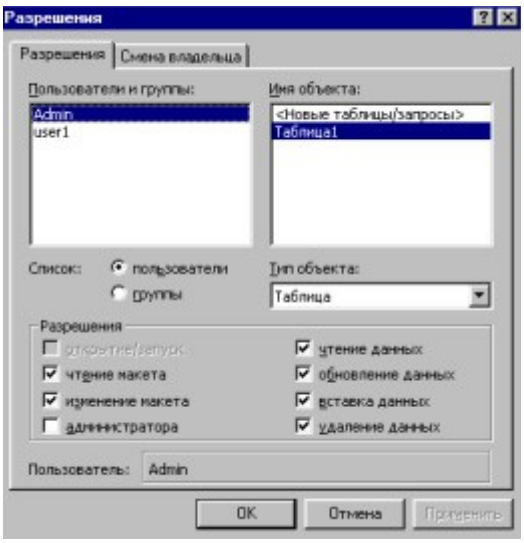

Рис.7 Окно определения прав доступа для каждого пользователя

6. Вопросы для самопроверки

1. Способы защиты информации в БД Access.
2. Группы и пользователи БД Access . Файл рабочей группы.
3. Объекты БД Access и права доступа к объектам. Понятие владельца объекта.
4. Алгоритм защиты БД Access.
5. Система безопасности SQL Server. Группы и пользователи SQL Server.
6. Понятие хранимых процедур и их достоинства. Создание хранимых процедур.
7. Основные операторы, которые используются в хранимых процедурах. Определение и использование переменных.
8. Права доступа к объектам БД SQL Server. Операторы Grand и Revoke.
9. Уровни безопасности операционных систем.
10. Пользователи и группы в Windows NT. Защищаемые объекты Windows NT.
11. Принцип действия систем безопасности в Windows NT.

Лабораторная работа №7

Тема: **Дешифрование**

Цель работы Исследование основных методов криптографической зашиты информации.

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.

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. Ключем в данном случае является размеры таблицы. Например, сообщение “Неясное становится еще более непонятным” записывается в таблицу из 5 строк и 7 столбцов по столбцам.

Н; О; Н; С; Б; Н; Я
Е; Е; О; Я; О; Е; Т
Я; С; В; Е; Л; П; Н
С; Т; И; Щ; Е; О; Ы
Н; А; Т; Е; Е; Н; М

Для получения шифрованного сообщения текст считывается по строкам и группируется по 5 букв:

НОНСБ НЯЕЕО ЯОЕТЯ СВЕЛП НСТИЩ ЕОЫНА ТЕЕНМ

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 ЛУНАТИК, получим следующую таблицу

Л; У; Н; А; Т; И; К; ; ; А; И; К; Л; Н; Т; У
4; 7; 5; 1; 6; 2; 3; ; ; 1; 2; 3; 4; 5; 6; 7
Н; О; Н; С; Б; Н; Я; ; ; С; Н; Я; Н; Н; Б; О
Е; Е; О; Я; О; Е; Т; ; ; Я; Е; Т; Е; О; О; Е
Я; С; В; Е; Л; П; Н; ; ; Е; П; Н; Я; В; Л; С
С; Т; И; Щ; Е; О; Ы; ; ; Щ; О; Ы; С; И; Е; Т
Н; А; Т; Е; Е; Н; М; ; ; Е; Н; М; Н; Т; Е; А

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: СНЯНН БОЯЕТ ЕООЕЕ ПНЯВЛ СЩОЫС ИЕТЕН МНТЕА. 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 был обратный. Пример данного метода шифрования показан в следующих таблицах:

; 2; 4; 1; 3; ; ; 1; 2; 3; 4; ; ; 1; 2; 3; 4
4; П; Р; И; Е; ; 4; И; П; Е; Р; ; 1; А; 3; Ю; Ж
1; 3; Ж; А; Ю; ; 1; А; 3; Ю; Ж; ; 2; Е; _ ; С; Ш
2; _; Ш; Е; С; ; 2; Е.; _; С; Ш; ; 3; Г; Т; О; О
3; Т; О; Г; О; ; 3; Г; Т; О; О; ; 4; И; П; Е; Р

Двойная перестановка столбцов и строк

В результате перестановки получена шифровка АЗЮЖЕ_СШГТООИПЕР. Ключом к шифру служат номера столбцов 2413 и номера строк 4123 исходной таблицы.

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.

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.

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 К 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).

Греческим писателем Полибием за 100 лет до н.э. был изобретен так называемый **полибианский квадрат** размером 5*5, заполненный алфавитом в случайном порядке. Греческий алфавит имеет 24 буквы, а 25-м символом является пробел. Для шифрования на квадрате находили букву текста и записывали в шифротекст букву, расположенную ниже ее в том же столбце. Если буква оказывалась в нижней строке таблицы, то брали верхнюю букву из того же столбца.

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

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.

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 $Т(0)_i$=$Г(ш)_i$+$Т(ш)_i$.

Асимметричные криптосистемы

Схема шифрования Эль Гамаля

Алгоритм шифрования Эль Гамаля основан на применении больших чисел для генерации открытого и закрытого ключа, криптостойкость же обусловлена сложностью вычисления дискретных логарифмов.

Последовательность действий пользователя:

1. Получатель сообщения выбирает два больших числа P и G, причем $P > G$.
2. Получатель выбирает секретный ключ - случайное целое число $X < P$.
3. Вычисляется открытый ключ $Y= G^x \bmod P$.
4. Получатель выбирает целое число K, 1< K< P-1.
5. Шифрование сообщения (M): $a= G^K \bmod P$, $b=Y^K M \bmod P$, где пара чисел (a,b) является шифротекстом.

Криптосистема шифрования данных RSA

Предложена в 1978 году авторами Rivest, Shamir и Aldeman и основана на трудности разложения больших целых чисел на простые сомножители.

Последовательность действий пользователя:

1. Получатель выбирает 2 больших простых целых числа p и q, на основе которых вычисляет $N=pq$; $M=(p-1)(q-1)$.

2. Получатель выбирает целое случайное число d, которое является взаимопростым со значением M, и вычисляет значение e из условия $ed=1(\text{mod } M)$.

3. d и N публикуются как открытый ключ, e и M являются закрытым ключом.

4. Если S –сообщение и его длина: $1<\text{Len}(S)<N$, то зашифровать этот текст можно как $S'=S^d(\text{mod } N)$, то есть шифруется открытым ключом.

5. Получатель расшифровывает с помощью закрытого ключа: $S=S'^e(\text{mod } N)$.

3. Задание к работе

На языке VBA или C++ написать программу шифрования и дешифрования текстового файла методом, указанным преподавателем. В качестве примера в п. 4 приводится алгоритм шифрования методом гаммирования.

4. Порядок выполнения работы

Основные шаги шифрования текстового файла методом гаммирования.

1. Получить от пользователя ключ, имя входного и выходного файла.
2. Инициализировать генератор случайных чисел с помощью ключа. Открыть указанные файлы.
3. Прочитать строку из файла.
4. Получить случайное число.
5. Получить ASCII-код очередного символа строки и увеличить его на случайное число, полученное на шаге 4.
6. Проверить правильность (допустимый диапазон) нового ASCII-кода.
7. В выходную строку записать очередной символ, соответствующий ASCII-коду, полученному на шаге 6.
8. Если не достигли конца входной строки, то перейти к шагу 4.
9. Записать полученную строку в выходной файл.
10. Если не достигнут конец файла, то перейти к шагу 3.
11. Закрыть файлы.

Алгоритм дешифрации аналогичен алгоритму шифрации за исключением того, что из ASCII –кода вычитаем 256 и проверяем больше ноля или нет.

Open Filename For Input As # FileNumber –открытие файла для чтения.

Out Put –для вывода.

В ASCII –коде символы 10 и 13 (возврат каретки).

Надо открывать файлы как двоичные, ключевое слово Binary.

Line Input # FileNumber, A$ -переменная строковая.

Print –для записи.

Для чтения и записи двоичного файла объявляем переменную типа Variant.

Put # NF,, VA

Get # NF,, VA

Close –закрытие файла.

Содержание отчета

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

5. Вопросы для самопроверки

1. Цель и задачи криптографии.
2. Шифры одиночной перестановки и перестановки по ключевому слову. Шифр Гронфельда.
3. Шифры двойной перестановки. Шифрование с помощью магического квадрата.
4. Шифр многоалфавитной замены и алгоритм его реализации.
5. Алгоритм шифрации двойным квадратом. Шифр Enigma.
6. Алгоритм шифрования DES.
7. Алгоритм шифрования ГОСТ 28147-89.
8. Алгоритм шифрования RSA.
9. Алгоритм шифрования Эль Гамаля.
10. Задачи и алгоритмы электронной подписи.