МИНОБРНАУКИ РОССИИ

Орский гуманитарно-технологический институт (филиал)
федерального государственного бюджетного образовательного учреждения
высшего образования «Оренбургский государственный университет»
(Орский гуманитарно-технологический институт (филиал) ОГУ)

Кафедра программного обеспечения

Методические указания по выполнению и защите лабораторных и практических работ по дисциплине «Б1.Д.В.2 Защита информации»

Уровень высшего образования

БАКАЛАВРИАТ

Направление подготовки

09.03.01 Информатика и вычислительная техника

(код и наименование направления подготовки)

Программное обеспечение средств вычислительной техники и автоматизированных систем

(наименование направленности (профиля) образовательной программы)

Тип образовательной программы

Программа бакалавриата

Квалификация

Бакалавр

Форма обучения

Очная

Год начала реализации программы (набора)

2019

г. Орск 2018

Методические указания предназначены для обучающихся очной формы обучения направления подготовки 09.03.01 Информатика и вычислительная техника профилю Программное обеспечение средств вычислительной техники и автоматизированных систем по дисциплине «Б1.Д.В.2 Защита информации»

Составитель _____ В.С. Богданова
_____ О.В. Подсобляева

Методические указания рассмотрены и одобрены на заседании кафедры программного обеспечения, протокол № 1 от «01» сентября 2018 г.

Заведующий кафедрой _____ Е.Е. Сурина

Согласовано:
Председатель методической комиссии по направлению подготовки 09.03.01 Информатика и вычислительная техника
_____ Е.Е.Сурина
«12» сентября 2018 г.

Пояснительная записка

В результате изучения дисциплины «Б1.Д.В.Э.3.1 Практикум по проектированию информационных систем» у обучающихся должны быть сформированы знания, умения и навыки:

- изучение программно-аппаратных средств защиты информации, методов анализа и планирования информационной защиты компьютерных систем, сетей и их компонентов, средств защиты сетевых служб;
- формирование базовых знаний в области информационной защиты телекоммуникационных и компьютерных систем и сетей на основе современных программных и операционных систем.

Одной из наиболее эффективных форм закрепления теоретических знаний и выработки навыков самостоятельной работы являются лабораторные занятия.

Целью проведения лабораторных занятий является:

- закрепление знаний студентов по основам проектной деятельности,
- формирование у студентов навыков использования современных технических средств и технологий для решения проектных и исследовательских задач.

Тематический план

Таблица 1 – Тематический план выполнения лабораторных и практических работ по дисциплине «Б1.Д.В.Э.3.2Практикум по проектированию информационных систем» для обучающихся направления подготовки 09.03.01 Информатика и вычислительная техника профиль подготовки Программное обеспечение средств вычислительной техники и автоматизированных систем

Лабораторные работы

№ ЛР	№ раздела	Наименование лабораторных работ	Кол-во часов
№ 1	1	Ключевые аспекты и вопросы формирования информационной безопасности современного предприятия	4
№ 2	2	Защищенная информационная система. Уровни и структура ИБ	4
№ 3	3	Модели и стандарты в сфере ИБ и управления рисками ИБ	4
№ 4	4	Технологии и методы реализации ИБ. Комплексная защита информационной инфраструктуры	6
		Итого:	18

Практические занятия

№ занятия	№ раздела	Тема	Кол-во часов
№ 1	1	Применение информационных технологий для изучения вопросов организационно-правового обеспечения информационной безопасности	4
№ 2	2	Использование криптографических средств защиты информации	2
№ 3	2	Реализация работы инфраструктуры открытых ключей	2
№ 4	2	Средства стеганографии для защиты информации	2
№ 5	3	Настройка безопасного сетевого соединения	2
№ 7	4	Антивирусные средства защиты информации	2
		Итого:	16

Методические указания по выполнению и оформлению лабораторных и практических работ

Лабораторные и практические работы по дисциплине «Защита информации» предполагают решение задач по темам, представленным в тематическом плане.

В практической и лабораторной работе должны быть выполнены все предусмотренные задания. В работе должна просматриваться логическая последовательность и взаимная увязка основных частей работы.

Рекомендуемая структура работ:

1) цель работы;

2) задание в соответствии с выбранным вариантом;

3) теоретическая часть, включающая краткое изложение теоретических положений по теме практической работы, формулы для решения задания;

4) практическая часть, включающая решение задания по теме практической работы. Дополнительно для наглядности расчетный материал может быть представлен в виде таблиц, графиков;

5) выводы по работе;

6) список использованной литературы.

Работы могут быть оформлены:

- машинописным текстом на листах формата А4.

Титульный лист оформляется на основе СТО 02069024. 101 – 2014 «РАБОТЫ СТУДЕНЧЕСКИЕ. Общие требования и правила оформления».

Работа защищается устно и принимается к зачету, если нет замечаний по ее выполнению и оформлению. При отсутствии зачтенных лабораторных работ студент не допускается к зачету по дисциплине «Б1.Д.В.Защита информации».

Лабораторная работа №1 Ключевые аспекты и вопросы формирования информационной безопасности современного предприятия

Порядок оформления:

1. Ознакомьтесь с описанием деятельности компании в соответствии с вашим вариантом.
2. Шрифт Tahoma 10. Интервал 1,5. Поля стандартные. Страницы работы должны быть пронумерованы. Формат документов MS Office полностью совместимым с версией 97-2003
3. Каждая таблица и рисунок должны быть пронумерованы и иметь название;
4. На каждую таблицу или рисунок должны быть ссылки из текста. При этом таблица или рисунок должны начинаться не далее следующей страницы;
5. Пункт не должен начинаться или заканчиваться списком, таблицей, рисунком;
6. Материал должен иметь четкую структуру изложения
7. Работы в электронном виде отправляются на ящик преподавателя. Тема письма «Практикум ИБ».
8. Крайний срок сдачи лабораторного практикума для проверке преподавателем за 3 календарных дня до проведения итогового мероприятия.
9. Работы, оформленные не в соответствии с требованиями или сданные после завершения срока сдачи работ, к защите не принимаются.

1. Ознакомление с представленными средства инструментального контроля

а) Изучение возможностей представленных средств контроля.

б) Проведение пробных проверок систем/компьютеров установленных в учебном классе.

в) Получение одного либо нескольких отчётов и подготовка предложений по устранению выявленных несоответствий.

2. Подготовка плана мероприятий по аудиту информационной безопасности

а) Выбор одной из представленных компаний.
б) Формулирование требований аудита на основании одного из стандартов информационной безопасности.
в) Разработка плана мероприятий с указанием сроков, подразделений и видов проверок для выбранной компании.

3. Разработка итогового отчёта по результатам аудита

а) Подготовка простейшей методики анализа результатов аудита.
б) Подготовка формы аудиторского отчёта с указанием персонала, его заполняющего, и плана проведения повторных проверок.

Варианты компаний:

1. Компания имеет 5 представительств, все пять в разных странах (.com, .ru и тд). Имеет 5 представительств в каждом от 50-100 чел. Головная компания 1000 чел в России. Отдел продаж в региональное представительство, административный отдел и отдел обработки данных. Направление деятельности компании - транснациональные грузовые перевозки.
2. Компания имеет одно представительство в России, которое является компанией, купленной годом ранее, занимающееся разработкой ПО. Головная компания до 500 чел. Представительство - до 300 чел. (Разные бренды). 2 домена – 2 бренда
3. Компания имеет головной офис со штатом 300 чел. Занимается продажей сотовых телефонов. По всей России 2000-3000 представительств – магазинах, есть упр. Менеджер (локальный отд. продаж) и тарифный отдел и отд. логистики.
4. Компания – 100 чел. Сфера деятельности аутсорсинг, услуги администрирования различных систем на базе Майкрософт. Клиенты в большинстве стран мира. Компания обеспечивает полную поддержку инфраструктуры клиента.
5. Компания состоит из 3-х филиалов на территории РФ. ЦО в Москве. Численность ЦО 100 чел., в филиалах 20 чел. Занимается производством и разработкой средств аутентификации. Производство в филиалах, ЦО выполняет только административные действия.
6. Компания - холдинг с центральным офисом в г. Москве. Занимается созданием и разработкой интернет сайтов и в неё входит ещё 4 компании, находящиеся в 4 странах мира. В каждой компании до 50 человек.

Лабораторная работа №2 Защищенная информационная система. Уровни и структура ИБ

Цель работы: Исследование структуры алгоритма и методики практической реализации криптосистемы шифрования Эль - Гамаля.

Основные теоретические положения:

Схема шифрования Эль - Гамаля может быть использована как для формирования цифровых подписей, так и шифрования данных. Безопасность схемы Эль - Гамаля обусловлена сложностью вычисления дискретных логарифмов в конечном поле.

При использовании алгоритма шифрования Эль - Гамаля длина шифротекста вдвое больше длины исходного открытого текста ***M.***

В реальных схемах шифрования необходимо использовать в качестве модуля ***n*** большое простое число, имеющее в двоичном представлении длину ***512... 1024 бит***.

Следует отметить, что формирование каждой подписи по данному методу требует нового значения ***k***, причём это значение должно выбираться случайным образом. Если нарушитель раскроет значение ***k***, повторно используемое отправителем, то может раскрыть и секретный ключ ***x*** отправителя.

Схема алгоритма шифрования данных Эль - Гамаля

1. Определение открытого *"y"* и секретного *"x"* ключей

1.1. Выбор двух взаимно простых больших чисел ***p*** и ***q***, ***q < p***

1.2. Выбор значения секретного ключа $x, x < p$
1.3. Определение значения открытого ключа y из выражения:

$$y=q^x \ (mod\ p)$$

2. Алгоритм шифрования сообщения М
2.1. Выбор случайного числа k, удовлетворяющего условию:

$$0 < k < p-1 \text{ и } НОД\ (k,p-1) = 1$$

2.2. Определение значения a из выражения: $a = q^k \ (mod\ p)$
2.3. Определение значения b из выражения: $b = y^k\ M \ (mod\ p)$
2.4. Криптограмма C, состоящая из a и b, отправляется получателю
2.5. Получатель расшифровывает криптограмму с помощью выражениями:

$$Ma^x = b(mod\ p)$$

3. Процедуру шифрования данных рассмотрим на следующем примере (для удобства расчётов в данном примере использованы числа малой разрядности):
3.1. Выбираем два взаимно простых числа $p = 11$ и $q = 2;$
3.2. Выбираем значение секретного ключа $x, (x < p), x = 8$;
3.3. Вычисляем значение открытого ключа y из выражения

$$y=q^x \ (mod\ p) = 2^8 \ (mod\ 11) = 256 (mod\ 11) = 3$$

3.4.Выбираем значение открытого сообщения $M = 5$;
3.5. Выбираем случайное число $k = 9;\ НОД\ (9, 10) = 1;$
3.6. Определяем значение a из выражения:

$$a = q^к \ (mod\ p) = 2^9 \ (mod\ 11) = 512 \ (mod\ 11) = 6;$$

3.7. Определяем значение b из выражения:

$$b = y^k\ M \ (mod\ p) = 3^9 * 5 \ (mod\ 11) = 98415 \ (mod\ 11) = 9.$$

Таким образом, получаем зашифрованное сообщение как $(a, b) = (6, 9)$ и отправляем получателю.
3.8. Получатель расшифровывает данный шифротекст, используя секретный ключ x и решая следующее сравнение:

$$M*a^x = b \ (mod\ p) = 5*6^8 = 9 \ (mod\ 11) = 8398080 = 9 \ (mod\ 11)$$

Вычисленное значение сообщения $M = 5$ представляет собой заданное исходное сообщение.

4. Содержание отчёта
4.1. Составить блок-схему и программу алгоритма шифрования Эль - Гамаля.
4.2. Листинг программы шифрования заданного сообщения с использованием алгоритма Эль - Гамаля.

Лабораторная работа №3 Модели и стандарты в сфере ИБ и управления рисками ИБ

Цель работы: Исследование структуры алгоритма и методики практической реализации (ЭЦП) RSA.
Основные теоретические положения: Технология применения системы ЭЦП предполагает наличие сети абонентов, обменивающихся подписанными электронными документами. При обмене электронными документами по сети значительно снижаются затраты, связанные с их обработкой, хранением и поиском.

Одновременно при этом возникает проблема, как аутентификации автора электронного документа, так и самого документа, т.е. установление подлинности автора и отсутствия изменений в полученном электронном сообщении.

В алгоритмах ЭЦП как и в асимметричных системах шифрования используются однонаправленные функции. ЭЦП используется для аутентификации текстов, передаваемых по телекоммуникационным каналам.

ЭЦП представляет собой относительно небольшой объём дополнительной цифровой информации, передаваемой вместе с подписанным текстом.

Концепция формирования ЭЦП основана на обратимости асимметричных шифров, а также на взаимосвязанности содержимого сообщения, самой подписи и пары ключей. Изменение хотя бы одного из этих элементов сделает невозможным подтверждение подлинности подписи, которая реализуется при помощи асимметричных алгоритмов шифрования и хэш-функций.

Система ЭЦП включает две процедуры:

- формирование цифровой подписи;
- проверку цифровой подписи.

В процедуре формирования подписи используется секретный ключ отправителя сообщения, в процедуре проверки подписи — открытый ключ отправителя.

Безопасность системы RSA определяется вычислительной трудностью разложения на множители больших целых чисел. Недостатком алгоритма цифровой подписи RSA является уязвимость её к мультипликативной атаке. Другими словами, алгоритм ЭЦП RSA позволяет хакеру без знания секретного ключа сформировать подписи под теми документами, в которых результат - хэширования можно вычислить как произведение результата хэширования уже подписанных документов.

Алгоритм электронной цифровой подписи (ЭЦП) RSA

1.Определение открытого «e» и секретного «d» ключей (действия отправителя)

1.1. Выбор двух взаимно простых больших чисел p и q

1.2. Определение их произведения $n = p*q$

1.3. Определение функции Эйлера: $\phi(n) = (p-1)(q-1)$

1.4. Выбор секретного ключа d с учетом условий: $1 < d < \phi(n)$,

$$НОД(n, \phi(n)) = 1$$

1.5. Определение значения открытого ключа e: $e < n$,

$$e*d \pmod{\phi(n)} = 1$$

2. Формирование ЭЦП

2.1. Вычисление хэш - значения сообщения M: $m = h(M)$

2.2. Для получения ЭЦП шифруем хэш – значение m с помощью секретного ключа d и отправляем получателю цифровую подпись $S = m^d \pmod{n}$ и открытый текст сообщения M

3.Аутентификация сообщения - проверка подлинности подписи

3.1. Расшифровка цифровой подписи S с помощью открытого ключа e и вычисление её хэш - значения $m' = S^e \pmod{n}$

3.2. Вычисление хэш - значения принятого открытого текста M и $m = h(M)$

3.3. Сравнение хэш - значений m и m', если $m = m'$, то цифровая подпись **S** — достоверна.

Процедуру формирования ЭЦП сообщения M рассмотрим на следующем простом примере:

3.4. Вычисление хэш - значения сообщения M: $m = h(M)$.

Хэшируемое сообщение M представим как последовательность целых чисел

3.5. В соответствии с приведённым выше алгоритмом формирования ЭЦП RSA выбираем два взаимно простых числа $p = 3$, $q = 11$, вычисляем значение $n = p*q = 3*11 = 33$, выбираем значение секретного ключа $d = 7$ и вычисляем значение открытого ключа $e = 3$. Вектор инициализации H_0 выбираем равным 6 (выбирается случайным образом).

Хэш - код сообщения **M =312** формируется следующим образом:

$$H_1 = (M_1 + H_0)^2 \pmod{n} = (3 + 6)^2 \pmod{33} = 81 \pmod{33} = 15;$$
$$H_2 = (M_2 + H_1)^2 \pmod{n} = (1 + 15)^2 \pmod{33} = 256 \pmod{33} = 25;$$

$H_3 = (M_3 + H_2)^2 \pmod n = (2+25)^2 \pmod{33} = 729 \pmod{33} = 3,\ m = 3$

3.6. Для получения ЭЦП шифруем хэш - значение ***m*** с помощью секретного ключа ***d*** и отправляем получателю цифровую подпись

$S = m^d \pmod n$ *и открытый текст сообщения M*
$S = 3^7 \pmod{33} = 2187 \pmod{33} = 9$

3.7. Проверка подлинности ЭЦП

Расшифровка ***S*** (т. е. вычисление её хэш - значения $\mathbf{m}^{/}$) производится с помощью открытого ключа **e**.

$$m' = S^e \pmod n = 9 \pmod{33} = 729 \pmod{33} = 3$$

3.8. Если сравнение хэш - значений ***m'***и ***m*** показывает их равенство, т.е. ***m =m'***, то подпись достоверна.

4.Содержание отчета

4.1. Составить блок-схему алгоритма и программу формирования ЭЦП RSA.
4.2. Листинг программы расчета ЭЦП RSA в соответствии с заданием.

Лабораторная работа №4 Технологии и методы реализации ИБ. Комплексная защита информационной инфраструктуры

Простой столбцевой перестановочный шифр

В данном виде шифра текст пишется на горизонтально разграфленном листе бумаги фиксированной ширины, а шифротекст считывается по вертикали. Дешифрование заключается в записи шифротекста вертикально на листе разграфленной бумаги фиксированной ширины и затем считывании открытого текста горизонтально.

Пример:

МОСКОВСКАЯ ФИНАНСОВО-ЮРИДИЧЕСКАЯ АКАДЕМИЯ

М	О	С	К	О	В
С	К	А	Я		Ф
И	Н	А	Н	С	О
В	О	-	Ю	Р	И
Д	И	Ч	Е	С	К
А	Я		А	К	А
Д	Е	М	И	Я	

Зашифрованный текст:
МСИВДАДОКНОИЯЕСАА-Ч МКЯНЮЕАИО СРСКЯВФОИКА

М	О	С	К	О	В
С	К	А	Я		Ф
И	Н	А	Н	С	О
В	О	-	Ю	Р	И
Д	И	Ч	Е	С	К
А	Я		А	К	А
Д	Е	М	И	Я	

Задание: Реализовать на любом языке программирования работу данного шифра

Перестановочный шифр с ключевым словом

Буквы открытого текста записываются в клетки прямоугольной таблицы по ее строчкам. Буквы ключевого слова пишутся над столбцами и указывают порядок этих столбцов (по возрастанию номеров букв в алфавите). Чтобы получить зашифрованный текст, надо выписывать буквы по столбцам с учетом их нумерации.

Открытый текст: Прикладная математика *Ключ*: Шифр

Ш	И	Ф	Р
4	1	3	2
П	р	и	к
л	а	д	н
а	я	м	а
т	е	м	а
т	и	к	а

Криптограмма: Раяеикнааидммкплатт

Ключевое слово (последовательность столбцов) известно адресату, который легко сможет расшифровать сообщение.

Так как символы криптотекста те же, что и в открытом тексте, то частотный анализ покажет, что каждая буква встречается приблизительно с той же частотой, что и обычно. Это дает криптоаналитику информацию о том, что перестановочный шифр. Применение к криптотексту второго перестановочного фильтра значительно повысит безопасность. Существуют и еще более сложные перестановочные шифры, но с применением компьютера можно раскрыть почти все из них.

Хотя многие современные алгоритмы используют перестановку, с этим связана проблема использования большого объема памяти, а также иногда требуется работа с сообщениями определенного размера.

Задание: Реализовать на любом языке программирования работу данного шифра

Шифр Полибия

Одной из наиболее древней из известных является система греческого историка Полибия. Его суть состоит в следующем: рассмотрим прямоугольник, что называется доской Полибия.

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

Каждая буква может быть представлена парой букв, указывающих строку и столбец, в которых расположена данная буква. Так представления букв В, Г, П, У будут АВ, АГ, ВГ, ГБ соответственно, а сообщение

ПРИКЛАДНАЯ МАТЕМАТИКА

зашифруется как

ВГВДБВБДБЕАААДВБААЕБЕЕВАААГААЕВАААГАБВБДААЕЕ

Задание: Реализовать на любом языке программирования работу данного шифра

Практическая работа №1 Применение информационных технологий для изучения вопросов организационно-правового обеспечения информационной безопасности

Работа с правовыми справочными системами Гарант и Консультант Плюс

Практическая работа №2 Использование криптографических средств защиты информации

Задание 1: Придумать акростих, в котором скрыто ваше имя.
Задание 2: Придумать послание, в котором каждое четвертое слово в посылаемом сообщении несет информацию (остальные слова ничего не значат).

Маршрутная транспозиция

Т - дополнительная буква.

В	О	С	К	Р	Е
А	М	Я	А	Н	С
Т	Е	М	А	Т	И
Я	А	К	С	Е	Ч
Ш	К	О	Л	А	Т

Фраза "Воскресная математическая школа" становится: "ЕСИЧТ АЕТНР КААСЛ ОКМЯС ОМЕАК ШЯТАВ".
Ключ - число 6.

Задание 3:

1. Зашифровать:
   a) Французский математик Пьер Ферма по образованию был юрист.
   b) Леонардо Пизанского математики знают под именем "сын добряка" или Фибоначчи.
2. Дешифровать (восстановить сообщение, зная ключ) Ключ 8.
   Чинои сечем лчгмс хыеоо еаитн ккыин лтсбч втрйы еоосс ееорс неомв бадер покп.
   Примечание: АБ-дополнительные буквы.
3. Расшифровать (восстановить сообщение, не зная ключа).
   Осуз уаан евем исчи тдьм одоа ьлвь рдво быи.
4. Расшифровать:
   Етгртуой дкмиуиав цлишлаег врныинис аяоплыдб аанполбр.

Постолбцовая транспозиция

К	А	Ш	А	Лшше ссис пссл шшао соак ааои ау.
З	1	4	2	Над столбцами записывается ключевое слово, затем в
Ш	Л	А	С	соответствии с порядком букв в алфавите столбцы
А	Ш	А	П	нумеруются, а затем выписываются подряд: первый
О	Ш	О	С	столбец, за ним второй и т.д.
С	Е	И	С	Ключ здесь - "каша".
О	С	А	Л	
А	С	У	Ш	
К	И			

Задание 4:

1. Зашифруйте фразу: Не плюй в колодец: вылетит - не поймаешь.

2. Дешифруйте старинное японское хайку: (ключом будет имя известного японского поэта "Басё") Тйдг адга лвис ыуы лояк пкшр ррув лшсс иеап пнву увет н.
3. Расшифруйте высказывание Козьмы Пруткова: Ако еаь дне дсц тан жод сск даг рео о.

Задание 5:

1. Придумать решетку и зашифровать фразу:
   "Евклид был древнегреческим математиком"

Задание 6:

Зашифровать слово используя шифр Цезаря. Обменяться шифровками с соседом по парте. Попытаться расшифровать чужую шифровку.

Практическая работа №3 Реализация работы инфраструктуры открытых ключей

Использование контрольных чисел и контрольных сумм в документах.

Контрольное число добавляется (обычно в конец) длинных номеров с целью первичной проверки их правильности. Применяется с целью уменьшения вероятности ошибки при обработке таких номеров: машинном считывании с упаковки товара, записи в документы, голосовой передаче от человека к человеку.

Наличие и правильность контрольного числа не гарантирует достоверность рассматриваемого номера (в том числе не спасает от действий злоумышленников), но на практике достаточно хорошо оберегает от случайных ошибок.

Контрольное число чаще всего это либо последняя цифра суммы всех чисел номера, либо результат другой математической операции над цифрами. В компьютерных программах понятие "контрольного числа" обобщено до CRC, бита чётности и кодов Рида-Соломона; а в некоторых архиваторах объём контрольных данных таков, что позволяет не только обнаружить ошибку, но и исправить её.

Контрольные числа, применяемые в документах, обычно позволяют восстановить 1 потерянную цифру при условиях, что известно, на какой позиции в номере она должна находиться и что остальные цифры в номере правильные. Если неизвестно, на какой позиции есть ошибка, нужно перебрать все возможные варианты (например, для 13-значного номера их будет 13), а из них выбрать наиболее правдоподобные (исходя из анализа *содержательной информации* в номере). Простое исправление контрольной цифры может привести только к большей ошибке, не связанной с математикой…

Примеры использования контрольных сумм.

В примерах обычно вычисляется некоторая функция (контрольная сумма) от цифр номера. Если она равна 0, то номер признаётся правильным. (В некоторых случаях удобнее вычислять контрольное число и сверять его с имеющимся. Формально контрольной суммой можно считать разность между имеющимся и вычисленным контрольными числами). Цифры номера нумеруются справа налево: $\ldots n_3 n_2 n_1$, так же, как и соответствующие им коэффициенты $\ldots k_3 k_2 k_1$. Обычно *содержательная информация* (код страны, товара, банка и т. п.) находится в левой части номера, а контрольное число (цифра) является завершающей (самой правой) и имеет номер 1 (n_1), однако с математической точки зрения все цифры кода, как правило, равноправны, и любая из них может считаться контрольной для остальных.

Контрольные суммы вычисляются по сходному алгоритму. Кроме того, тот же алгоритм, (таблица обрезается или продолжается влево по очевидному правилу) используется во многих других случаях, например для номеров товаров в магазинах.

	k_{13}	k_{12}	k_{11}	k_{10}	k_9	k_8	k_7	k_6	k_5	k_4	k_3	k_2	k_1
EAN-13	1	3	1	3	1	3	1	3	1	3	1	3	1
UPC-12													
EAN-8													

Контрольная сумма есть остаток от деления на 10 суммы из цифр номера, умноженных на соответствующие коэффициенты из таблицы. Если контрольная сумма есть 0, то номер признаётся правильным.

Если нужно подсчитать требуемое контрольное число для произвольного номера, нужно вначале поставить «0» на крайнюю правую позицию, посчитать контрольную сумму, а затем, если она не равна нулю, заменить этот «0» на «10 - контрольная сумма».

Примеры

1) Штрих – код товаров

4600051000057 (сигареты «Прима») — код EAN-13.
4×1 + 6×3 + 0×1 + 0×3 + 0×1 + 5×3 + 1×1 + 0×3 + 0×1 + 0×3 + 0×1 + 5×3 + 7×1 =
4 + 18 + 0 + 0 + 0 + 15 + 1 + 0 + 0 + 0 + 0 + 15 + 7 = 60.
Контрольная сумма = 0 — номер правильный.

46009333 (папиросы «Беломорканал») — код EAN-8.
4×3 + 6×1 + 0×3 + 0×1 + 9×3 + 3×1 + 3×3 + 3×1 =
12 + 6 + 0 + 0 + 27 + 3 + 9 + 3 = 60.
Контрольная сумма = 0 — номер правильный.

041689300494 (бензин для зажигалки «Zippo») — код UPC-12.
0×3 + 4×1 + 1×3 + 6×1 + 8×3 + 9×1 + 3×3 + 0×1 + 0×3 + 4×1 + 9×3 + 4×1 =
0 + 4 + 3 + 6 + 24 + 9 + 9 + 0 + 0 + 4 + 27 + 4 = 90.
Контрольная сумма = 0 — номер правильный.

Восстановление контрольного числа. Дан номер 460154602129?, EAN-13 с потерянной контрольной цифрой «?».

Для 4601546021290:
4×1 + 6×3 + 0×1 + 1×3 + 5×1 + 4×3 + 6×1 + 0×3 + 2×1 + 1×3 + 2×1 + 9×3 + 0×1 =
4 + 18 + 0 + 3 + 5 + 12 + 6 + 0 + 2 + 3 + 2 + 27 + 0 = 82.
Контрольная сумма = 2 — номер неправильный, но если вместо «?» подставить «10 - 2» = «8», то номер станет правильным. Таким образом, контрольное число (цифра) есть «8».

2) Номера банковских карт

Номера кредитных карт American Express всегда начинаются на цифру 3, VISA начинается на 4, MasterCard на 5 и Maestro на 6.

Контрольные суммы вычисляются по сходному алгоритму. Правило продолжения таблицы влево (для длинных номеров) и усечения её для коротких номеров очевидно.

В случае наличия в номере (коде) ISIN английских букв, каждая из них заменяется на 2 цифры, представляющие собой порядковый номер буквы в латинском алфавите, увеличенный на 9 (т.е. A ~ 10, B ~ 11, …, Z ~ 35).

	k_{16}	k_{15}	k_{14}	k_{13}	k_{12}	k_{11}	k_{10}	k_9	k_8	k_7	k_6	k_5	k_4	k_3	k_2	k_1	
	банковские карты, 16 цифр	2	1	2	1	2	1	2	1	2	1	2	1	2	1	2	1
	ценные бумаги																
	банковские карты, 13 цифр																

Контрольная сумма. Цифры кода умножаются на коэффициенты из таблицы, если результат умножения превосходит 9, то вычитаем из него 9, получившиеся числа складываем. Берём остаток от деления суммы на 10.

Если контрольная сумма есть 0, то номер признаётся правильным.

Восстановление «контрольного числа» аналогично способу для штрих-кода.

4000-0000-0000-6 — 13-значная банковская карта Visa.

```
Произведения: 4x1, 0x2, 0x1, 0x2, 0x1, 0x2, 0x1, 0x2, 0x1, 0x2, 0x1, 0x2, 6x1;
После вычитания 9:  4,  0,  0,  0,  0,  0,  0,  0,  0,  0,  0,  0,  6;
Их сумма: 10;
```

Контрольная сумма = 0 — номер правильный.

5610-0000-0000-0001 — 16-значная банковская карта Australian Bankcard.

```
Произведения: 5x1, 6x2, 1x1, 0x2, 0x1, 0x2, 0x1, 0x2, 0x1, 0x2, 0x1, 0x2, 1x1;
После вычитания 9:  5,  3,  1,  0,  0,  0,  0,  0,  0,  0,  0,  0,  1;
Их сумма: 10;
```

Контрольная сумма = 0 — номер правильный.

RU0007661625 — ISIN акции Газпрома номиналом 5 руб.

Буквы RU заменяем на 2730 и получаем 14-значный номер 27300007661625, который и будем проверять.

```
Произведения: 2x2, 7x1, 3x2, 0x1, 0x2, 0x1, 0x2, 7x1, 6x2, 6x1, 1x2, 6x1, 2x2, 5x1;
После вычитания 9:  4,  7,  6,  0,  0,  0,  0,  7,  3,  6,  2,  6,  4,  5;
Их сумма: 50;
```

Контрольная сумма = 0 — номер правильный.

DE0001136927 — пример ISIN с сайта Банка Эстонии.

Буквы DE заменяем на 1314 и получаем 14-значный номер 13140001136927.

```
Произведения: 1x2, 3x1, 1x2, 4x1, 0x2, 0x1, 0x2, 1x1, 1x2, 3x1, 6x2, 9x1, 2x2, 7x1;
После вычитания 9:  2,  3,  2,  4,  0,  0,  0,  1,  2,  3,  3,  9(!),  4,  7;
Их сумма: 40;
```

Контрольная сумма = 0 — номер правильный.

3) Номер карточки медицинского страхования

Номер карточки медицинского страхования (он же СНИЛС) проверяется на валидность контрольным числом. СНИЛС имеет вид: "XXX-XXX-XXX YY", где XXX-XXX-XXX - собственно номер, а YY - контрольное число. Алгоритм формирования контрольного числа СНИЛС таков:

1) Проверка контрольного числа Страхового номера проводится только для номеров больше номера 001-001-998

2) Контрольное число СНИЛС рассчитывается следующим образом:

2.1) Каждая цифра СНИЛС умножается на номер своей позиции (позиции отсчитываются с конца)

2.2) Полученные произведения суммируются

2.3) Если сумма меньше 100, то контрольное число равно самой сумме

2.4) Если сумма равна 100 или 101, то контрольное число равно 00

2.5) Если сумма больше 101, то сумма делится нацело на 101 и контрольное число определяется остатком от деления аналогично пунктам 2.3 и 2.4

```
ПРИМЕР: Указан СНИЛС 112-233-445 95
Проверяем правильность контрольного числа:
цифры номера        1 1 2 2 3 3 4 4 5
```

```
номер позиции        9 8 7 6 5 4 3 2 1
Сумма = 1x9 + 1x8 + 2x7 + 2x6 + 3x5 + 3x4 + 4x3 + 4x2 + 5x1 = 95
Контрольное число 95 – указано верно
```

4) Номера ИНН

Бывают 10-значные (1 контрольная цифра в конце) и 12-значные (2 контрольные цифры в конце).

	k_{12}	k_{11}	k_{10}	k_9	k_8	k_7	k_6	k_5	k_4	k_3	k_2	k_1	
	вычисление контрольного числа n_2 для 12-значного ИНН	7	2	4	10	3	5	9	4	6	8		
	вычисление контрольного числа n_1 для 12-значного ИНН	3	7	2	4	10	3	5	9	4	6	8	
	вычисление контрольного числа n_1 для 10-значного ИНН												

Проверку ИНН удобнее проводить, вычисляя контрольные числа:

Шаг 1 (только для 12-значного ИНН). Контрольное число n_2 есть остаток от деления на 11 суммы из цифр номера, умноженных на соответствующие коэффициенты из таблицы (из строки «вычисление контрольного числа n_2»). Если остаток есть 10, то $n_2 = 0$.

Шаг 2. Контрольное число n_1 есть остаток от деления на 11 суммы из цифр номера, умноженных на соответствующие коэффициенты из таблицы (из строки «вычисление контрольного числа n_1»). Если остаток есть 10, то $n_1 = 0$.

ИНН 500100732259 — 12 цифр (первый попавшийся в Интернете ИНН).

```
Шаг   1:   5*7+   0*2+   0*4+   1*10+   0*3+   0*5+   7*9+   3*4+   2*6+   2*8=   148
148= 11*13 + 5(остаток); совпадает
Шаг   2:   5*3+   0*7+   0*2+   1*4+   0*10+   0*3+   7*5+   3*9+   2*4+   2*6+   5*8=   141
141= 11*12 +9(остаток); совпадает
```

Оба контрольных числа совпадают, номер правильный.

ИНН 7830002293 — 10 цифр (Санкт-Петербургская бумажная фабрика Гознака).

```
Шаг    2:    7*2+    8*4+    3*10+    0*3+    0*5+    0*9+    2*4+    2*6+    9*8=    168
168= 11*15 +3(остаток)
```

Контрольное число совпадает, номер правильный.

Задание: Написать программы проверки контрольного числа или контрольной суммы на любом языке программирования.

Практическая работа №4 Средства стеганографии для защиты информации

Методы кодирования

Как уже отмечалось выше, под кодированием понимается замена элементов открытого текста (букв, слов, фраз и т.п.) кодами. Различают символьное и смысловое кодирование.

При символьном кодировании каждый знак алфавита открытого текста заменяется соответствующим символом. Примером символьного кодирования служит азбука Морзе, а также методы шифрования заменой и перестановкой. Рассмотрим метод символьного кодирования, который использует предыдущие символы открытого текста. Этот метод, называемый метод стопки книг, был предложен Б.Я. Рябко.

Предположим, что нужно передать сообщение X из алфавита A, в котором буквы алфавита отождествлены с числами 1,2,..L, где L - число элементов алфавита A. Каждой букве алфавита

соответствует код ki, i=1..L. При появлении в сообщении X очередной буквы xj ее код представляется кодом номера позиции j, занимаемой в данный момент буквой xj в списке. Это дает возможность на приемном конце по коду номера позиции j определить букву xj. После кодирования буквы xj одновременно на приемном и передающих концах перемещают букву xj в начало списка, увеличивая тем самым на единицу номера букв, стоявших на позициях от 1 до j-1. Номера букв, стоявших на позициях от j+1 до L, остаются без изменений. В результате кодирования открытого текста в начале списка будут находиться буквы, которые наиболее часто встречались в открытом тексте.

Пример 1. Открытый текст: "АБРАКАДАБРА". Алфавит:{А,Б,Д,К,Р}.

Начальный список соответствует последовательности букв в алфавите и ему соответствует список кодов {К1,К2,К3,К4,К5}. Схема кодирования показана на рис. 9 (коды, которыми кодируется открытый текст, выделены).

К1 *А* А Б Р А К А Д А Б Р А
К2 Б *Б* А Б Р *А* К А Д А Б Р
К3 Д Д Д *А* Б Р Р К К Д *А* Б
К4 К К К Д Д Б Б Р Р К Д Д
К5 Р Р *Р* К *К* Д *Д* Б *Б* *Р* К К
¦ ¦
¦ L начальный список
список кодов

Закодированное сообщение: "К1 К2 К5 К3 К5 К2 К5 К2 К5 К5 К3".

Интересный метод кодирования в 1992 году предложил С.П. Савчук. В отличие от метода стопки книг перемещению подвергается список кодов. Пусть алфавит A={a1,a2,...,an}. Данному порядку расположения букв соответствует начальный список кодов K0={k1,k2,..,kn}. При появлении в кодируемом сообщении буквы ai в качестве кода выбирается соответствующий ее местоположению код ki. После этого осуществляется сдвиг списка кодов:

{k1,k2,...,ki,...,kn}->{k2,k3,...,kn,k1}

Таким образом, список кодов образует замкнутое кольцо.

Пример 2. Открытый текст: "АБРАКАДАБРА".

Алфавит: {А,Б,Д,К,Р}.

Список кодов: К0={К1,К2,К3,К4,К5}.

Динамика изменения списка кодов представлена на рис.10 (коды, которыми кодируется открытый текст, выделены квадратами).

А [К1] К2 К3 [К4] К5 [К1] К2 [К3] К4 К5 [К1]
Б К2 [К3] К4 К5 К1 К2 К3 К4 [К5] К1 К2
Д К3 К4 К5 К1 К2 К3 [К4] К5 К1 К2 К3
К К4 К5 К1 К2 [К3] К4 К5 К1 К2 К3 К4
Р К5 К1 [К2] К3 К4 К5 К2 К2 К3 [К4] К5
¦ ¦
¦ L начальный список
L алфавит

Закодированное сообщение:
"К1 К3 К2 К4 К3 К1 К4 К3 К5 К4 К1".

Особенность данного метода состоит в том, что кодированный текст обеспечивает равномерную частоту появления кодов. Обычно криптоаналитики при наличии доступа к системе шифрования (кодирования) используют шифрование своих сообщений из одинаковых символов для анализа получаемых криптограмм и раскрытия ключа. Рассмотрим пример с кодированием по методу С.П. Савчука .

Пример 3. Открытый текст: "АААААААААА"
Алфавит: {А,Б,Д,К,Р}.
Список кодов: К0={К1,К2,К3,К4,К5}.
Закодированное сообщение
"К1 К2 К3 К4 К5 К1 К2 К3 К4 К5" содержит одинаковое число всех кодов.
Таким образом, если число символов открытого текста кратно длине алфавита, то этот метод дает одинаковое число появления различных кодов при использовании в качестве открытого текста одинаковых символов.
Смысловое кодирование - это кодирование, в котором в качестве исходного алфавита используются не только отдельные символы (буквы), но и слова и даже наиболее часто встречающиеся фразы.
Рассмотрим пример одноалфавитного и многоалфавитного смыслового кодирования.
Пример 4. Открытый текст: "19.9.1992 ГОДА".
Таблица кодирования представлена в таблице 13.

элементы открытого текста	коды
1	089 146 214 417
2	187 226 145 361
_	_
9	289 023 194 635
ГОД	031 155 217 473
_	786 432 319 157

Таблица 13

Закодированное сообщение при одноалфавитном кодировании: "089 289 786 289 786 089 289 289 187 031".
Закодированное сообщение при многоалфавитном кодировании: "089 289 786 023 432 146 194 635 187 031" (при многоалфавитном кодировании одинаковые символы заменяются кодами из следующего столбца).
Среди различных кодов, применяемых для кодирования естественных языков, особый интерес вызывает КОД ХАФФМЕНА, который позволяет сжимать открытый текст. Суть его состоит в присваивании наиболее часто встречающимся буквам наиболее коротких кодов.
Строка двоичных символов кодов Хаффмена единственным образом разлагается на коды символов (такие коды называются префиксными).
Пример 5. Закодированное кодом Хаффмена сообщение имеет вид: "O11O1OOO1OOOOOO1O1O1111OOO1OOOOO".
Пользуясь деревом для английского языка, получаем 0110=S. Далее снова начинаем движение из вершины: 100=E; 01000=C; 00010=U; 1011=R; 1010=I; 001=T; 00000=Y. Открытый текст: "SECURITY".
УПРАЖНЕНИЯ.

1. В чем смысл символьного кодирования?
2. Символьным кодированием закодировать открытый текст: "Лаванда".
3. На основе примера 2 закодировать открытый текст: "Лаванда".
4. На чем основывается смысловое кодирование?
5. Предложите метод кодирования, опираясь на примеры 1, 2 и 3.

Рассмотрим более подробно примеры, отражающие логику развития представляемой предметной области.

Шифр «Сцитала». Этот шифр известен со времен войны Спарты против Афин в V веке до н. э. [7] Для его реализации использовалась сцитала – жезл, имеющий форму цилиндра. На сциталу виток к витку наматывалась узкая папирусная лента (без просветов и нахлестов), а затем на этой ленте вдоль оси сциталы записывался открытый текст. Лента разматывалась и получалось (для непосвященных), что поперек ленты в беспорядке написаны какие-то буквы. Затем лента отправлялась адресату. Адресат брал такую же сциталу, таким же образом наматывал на нее полученную ленту и читал сообщение вдоль оси сциталы.

Отметим, что в этом шифре преобразование открытого текста в шифрованный заключается в определенной перестановке букв открытого текста.

Поэтому класс шифров, к которым относится и шифр «Сцитала», называется шифрами перестановки.

Шифр подобного класса можно получить иным путем. Пусть необходимо зашифровать фразу: «Это слово будет зашифровано». В такой простой фразе просматривается закономерность относительно частости повторения отдельных букв языка (см. таблицу 2.5).

Таблица 2.5 Простой перестановочный шифр

Э	Т	О	С	Л	О
В	О	Б	У	Д	Е
Т	З	А	Ш	И	Ф
Р	О	В	А	Н	О

Передадим в канал связи криптограмму, разбив ее для удобства представления на пятизначные группы:

ЭВТРТ ОЗООБ АВСУШ АЛДИН ОЕФОФ.

Заметно, что криптограмма совершенно не стойкая относительно частного анализа. Данный шифр с позиций современной криптографии наивен. Шифр можно усилить за счет перестановки столбцов по ключевому слову.

Другим простым типом шифра является шифр замены (трансформационный шифр). Каждый символ в сообщении заменяется в зашифрованном тексте другим символом. Символы для зашифрованного текста обычно берутся из того же алфавита, что и для сообщения, но это не обязательно. Система называется моноалфавитной из-за того, что каждый символ сообщения всегда преобразуется в один и тот же символ зашифрованного текста (статистика языка сохраняется) [17].

Рассмотрим шифр Цезаря. Этот шифр реализует следующее преобразование открытого текста: каждая буква открытого текста заменяется третьей после нее буквой в алфавите, который считается написанным по кругу, т. е. после буквы «я» следует буква «а». Отметим, что Цезарь заменял букву третьей после нее буквой, но можно заменять и какой-нибудь другой. Главное, чтобы тот, кому посылается шифрованное сообщение, знал эту величину сдвига. Класс шифров, к которым относится и шифр Цезаря, называется шифрами замены.

Для иллюстрации такого шифра создадим таблицу замены, получившей название таблицы Веженера. Таблица приведена в Приложении. Поступим по правилу Цезаря и зашифруем ранее приведенную фразу. Для этого в первом столбце будем брать буквы открытого текста, а в качестве ключа возьмем букву «Г». Получим криптограмму вида

АХСФО СЕСДЦ ЗИХЛГ ЬМЧУС ЕГРСД.

В этой криптограмме подозрительно часто употребляется буква «С», т. е. сохраняется признак открытого текста, исходя из частости повторения букв. Вскрыть такой шифр способен даже не опытный в вопросах криптоанализа человек. Покажем это на примере. Выпишем в одну строку

криптограмму и разворачивая столбцы вниз под каждой буквой напишем продолжение алфавита таким образом, чтобы в столбце оказались буквы всего алфавита с некоторым циклическим сдвигом.

В выделенной строке таблицы криптоанализа появляется сообщение, которое среди других строк таблицы имеет выраженную семантику. Более безопасной (но лишь незначительно) является произвольная подстановка, когда изменяется порядок подстановочных символов. Однако, хотя такая система имеет больше возможных ключей (30! вместо 30 возможных в системе Цезаря, один из которых тривиален), проблема со всеми шифрами замены состоит в том, что их очень просто атаковать с использованием частотного анализа.

Например, избыточность, свойственная английскому языку, такова, что только около 25 символов зашифрованного текста требуются для того, чтобы дешифровать сообщение. Если в зашифрованном тексте остаются пробелы, расшифровка его даже упрощается. Через эти прорехи может просачиваться и другая информация сообщения.

Применяя в качестве ключа не одну букву, а несколько, например, в виде слова, можно получить более стойкую криптограмму. Читателю представляется возможность самостоятельно изучить данную проблему, применяя в качестве ключа двухбуквенный ключ, трехбуквенный и т. д. Ключ в форме кодового слова легко запомнить, но шифр очень беден. Одним из способов преодоления атаки частотного анализа является использование разных алфавитов преобразования, зависящих от позиции символа в сообщении (рис. 2.6).

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

Рис. 2.6. Пример взлома шифра Цезаря без знания ключа

Такие полиалфавитные шифры лучше, чем моноалфавитные, но они все еще уязвимы для нападения, использующего частотный анализ, когда нападающий вычисляет длину повторения кодового слова и может затем выполнить частотный анализ для каждого алфавита индивидуально.
Важнейшим для развития криптографии был вывод К. Шеннона о существовании и единственности абсолютно стойкого шифра. Единственным таким шифром является какая-нибудь форма так называемой «ленты однократного использования», в которой открытый текст «объединяется» с полностью случайным ключом такой же длины. Этот результат был доказан К. Шенноном с помощью разработанного им теоретико-информационного метода исследования шифров.
Подчеркнем, что для абсолютной стойкости существенным является каждое из следующих требований к «ленте однократного использования»:
1) полная случайность (равновероятность) ключа (это, в частности, означает, что ключ нельзя вырабатывать с помощью какого-либо детерминированного устройства);
2) равенство длины ключа и длины открытого текста;
3) однократность использования ключа.
В случае нарушения хотя бы одного из этих условий шифр, перестает быть абсолютно стойким, и появляются принципиальные возможности для его вскрытия (хотя они могут быть трудно реализуемыми).
Но, оказывается, именно эти условия и делают абсолютно стойкий шифр очень дорогим и непрактичным. Прежде чем пользоваться таким шифром, необходимо обеспечить всех абонентов достаточным запасом случайных ключей и исключить возможность их повторного применения. А это сделать необычайно трудно и дорого.
В силу указанных причин, абсолютно стойкие шифры применяются только в сетях связи с небольшим объемом передаваемой информации, обычно это сети для передачи особо важной государственной информации.
Теперь уже понятно, что чаще всего для защиты своей информации законные пользователи вынуждены применять неабсолютно стойкие шифры. Такие шифры, по крайней мере, теоретически могут быть вскрыты. Вопрос только в том, хватит ли у противника сил, средств и времени для разработки и реализации соответствующих алгоритмов. Обычно эту мысль выражают так: противник с неограниченными ресурсами может вскрыть любой неабсолютно стойкий шифр.
Как же должен действовать в этой ситуации законный пользователь, выбирая для себя шифр? Лучше всего, конечно, было бы доказать, что никакой противник не может вскрыть выбранный шифр, скажем, за 10 лет и тем самым получить теоретическую оценку стойкости. К сожалению, математическая теория еще не дает нужных теорем – они относятся к нерешенной проблеме нижних оценок вычислительной сложности задач.
Поэтому у пользователя остается единственный путь – получение практических оценок стойкости. Этот путь состоит из следующих этапов:
- понять и четко сформулировать, от какого противника мы собираемся защищать информацию; необходимо уяснить, что именно противник знает или сможет узнать о системе шифра, а также какие силы и средства он сможет применить для его вскрытия;
- мысленно стать в положение противника и пытаться с его позиций атаковать шифр, т. е. разрабатывать различные алгоритмы вскрытия шифра; при этом необходимо в максимальной мере обеспечить моделирование сил, средств и возможностей противника;
- наилучший из разработанных алгоритмов использовать для практической оценки стойкости шифра.
Здесь полезно для иллюстрации упомянуть о двух простейших методах вскрытия шифра: случайное угадывание ключа (он срабатывает с маленькой вероятностью, зато имеет маленькую сложность) и перебор всех подряд ключей вплоть до нахождения истинного (он срабатывает всегда, зато имеет очень большую сложность). Отметим также, что не всегда нужна атака на ключ: для некоторых шифров можно сразу, даже не зная ключа, восстанавливать открытый текст по шифрованному.

Из приведенных примеров следует, что основное внимание разработчик шифра должен уделять именно системе ключей, а исполнитель обязан строго следовать правилам применения ключей в конкретной системе шифрования.

Рекомендуемая литература

Основная литература

1. Информационные системы и их безопасность [Текст] : учебное пособие / А. В. Васильков, А. А. Васильков, И. А. Васильков. - Москва : Форум, 2015. - 528 с. - Библиогр. : с. 513-514. - ISBN 978-5-91134-289-0. (ОГТИ ч/з N4-1; аб.ТБ-18), коэфициент книгообеспеченности 1

Дополнительная литература

1. Системы защиты информации в ведущих зарубежных странах : учебное пособие для вузов / В.И. Аверченков, М.Ю. Рытов, Г.В. Кондрашин, М.В. Рудановский. - 3-е изд., стер. - М. : Флинта, 2011. - 224 с. - (Организация и технология защиты информации). - ISBN 978-5-9765-1274-0 ; То же [Электронный ресурс]. – URL: //biblioclub.ru/index.php?page=book_red&id=93351, коэффициент книгообеспеченности 1.

2. Основы информационной безопасности. Учебно-практическое пособие [Электронный ресурс] / Сычев Ю. Н. - Евразийский открытый институт, 2010.]. - URL: //biblioclub.ru/index.php?page=book&id=93351, коэффициент книгообеспеченности 1.

3. Основы информационной безопасности при работе на компьютере [Электронный ресурс] / Фаронов А. Е. - Интернет-Университет Информационных Технологий, 2011.- .URL://biblioclub.ru/index.php?page=book_red&id=233763&sr=1, коэффициент книгообеспеченности 1.

4. Правовые основы информатики. Учебно-практическое пособие [Электронный ресурс] / Ефимова Л. Л. - Евразийский открытый институт, 2011. - URL://biblioclub.ru/index.php?page=book_red&id=93155&sr=1, коэффициент книгообеспеченности 1.

5. Организация безопасной работы информационных систем : учебное пособие / Ю.Ю. Громов, Ю.Ф. Мартемьянов, Ю.К. Букурако и др. ; Министерство образования и науки Российской Федерации, Федеральное государственное бюджетное образовательное учреждение высшего профессионального образования «Тамбовский государственный технический университет». - Тамбов : Издательство ФГБОУ ВПО «ТГТУ», 2014. - 132 с. : ил. - Библиогр. в кн. ; То же [Электронный ресурс]. - URL: //biblioclub.ru/index.php?page=book&id=277794, коэффициент книгообеспеченности 1.

6. Креопалов, В.В. Технические средства и методы защиты информации : учебно-практическое пособие / В.В. Креопалов. - М. : Евразийский открытый институт, 2011. - 278 с. - ISBN 978-5-374-00507-3 ; То же [Электронный ресурс]. - URL: //biblioclub.ru/index.php?page=book&id=90753, коэффициент книгообеспеченности 1.

Периодические издания

1. Журнал «Вестник компьютерных и информационных технологий »
2. Журнал «Информационные технологии и вычислительные системы»
3. Журнал «Стандарты и качество»
4. Журнал «Информатика и вычислительная техника»