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
для обучающихся по освоению дисциплины

«Б.1.Б.17 Основы информационной безопасности»

Уровень высшего образования

БАКАЛАВРИАТ

Направление подготовки

09.03.01 Информатика вычислительной техники
(код и наименование направления подготовки)

Программное обеспечение средств вычислительной техники и автоматизированных систем
(наименование направленности (профиля) образовательной программы)

Тип образовательной программы

Программа академического бакалавриата

Квалификация

Бакалавр

Форма обучения

Очная

Год начала реализации программы (набора)

2014, 2015, 2016, 2017

г. Орск 2017

Методические указания для обучающихся по освоению дисциплины «Б.1.Б.17 Основы информационной безопасности» предназначены для обучающихся очной формы обучения направления подготовки 09.03.01 Информатика и вычислительная техника, профиля «Программное обеспечение средств вычислительной техники и автоматизированных систем»

Составитель _____ О.В. Подсобляева

Методические указания рассмотрены и одобрены на заседании кафедры программного обеспечения, протокол № 9 от «07» июня 2017 г.

Заведующий кафедрой программного обеспечения _____ Е.Е.Сурина

1 Методические указания по проведению лекционных занятий

Лекционные занятия в высшем учебном заведении являются основной формой организации учебного процесса и должны быть нацелены на выполнение ряда задач:

- ознакомить студентов со структурой дисциплины;
- изложить основной материал программы курса дисциплины;
- ознакомить с новейшими подходами и проблематикой в данной области;
- сформировать у студентов потребность к самостоятельной работе с учебной, нормативной и научной литературой.

Лекционное занятие представляет собой систематическое, последовательное, монологическое изложение преподавателем-лектором учебного материала, как правило, теоретического характера.

Цель лекции – организация целенаправленной познавательной деятельности студентов по овладению программным материалом учебной дисциплины.

Чтение курса лекций позволяет дать связанное, последовательное изложение материала в соответствии с новейшими данными науки, сообщить слушателям основное содержание предмета в целостном, систематизированном виде.

В ряде случаев лекция выполняет функцию основного источника информации, когда новые научные данные по той или иной теме не нашли отражения в учебниках.

Организационно-методической базой проведения лекционных занятий является рабочий учебный план направления подготовки. При подготовке лекционного материала преподаватель обязан руководствоваться учебными программами по дисциплинам кафедры, тематика и содержание лекционных занятий которых представлена в рабочих программах, учебно-методических комплексах.

При чтении лекций преподаватель имеет право самостоятельно выбирать формы и методы изложения материала, использовать различные технические средства обучения.

Рекомендации по работе студентов с конспектом лекций.

Изучение дисциплины студенту следует начинать с проработки рабочей программы, особое внимание, уделяя целям и задачам, структуре и содержанию курса.

При конспектировании лекций студентам необходимо излагать услышанный материал кратко, своими словами, обращая внимание, на логику изложения материла, аргументацию и приводимые примеры. Необходимо выделять важные места в своих записях. Если непонятны какие-либо моменты, необходимо записывать свои вопросы, постараться найти ответ на них самостоятельно. Если самостоятельно не удалось разобраться в материале, впоследствии необходимо либо на следующей лекции, либо на лабораторном занятии или консультации обратиться к ведущему преподавателю за разъяснениями.

Успешное освоение курса предполагает активное, творческое участие студента путем планомерной, повседневной работы. Лекционный материал следует просматривать в тот же день. Рекомендуемую дополнительную литературу следует прорабатывать после изучения данной темы по учебнику и материалам лекции.

Каждая тема имеет свои специфические термины и определения. Усвоение материала необходимо начинать с усвоения этих понятий. Если какое-либо понятие вызывает затруднения, необходимо посмотреть его суть и содержание в словаре (Интернете), выписать его значение в тетрадь для подготовки к занятиям.

При подготовке материала необходимо обращать внимание на точность определений, последовательность изучения материала, аргументацию, собственные примеры, анализ конкретных ситуаций. Каждую неделю рекомендуется отводить время для повторения пройденного материала, проверяя свои знания, умения и навыки по контрольным вопросам и тестам.

2 Методические указания по лабораторным и практическим работам

Изучение дисциплины «Основы информационной безопасности» предполагает посещение обучающимися не только лекций, но и лабораторных работ. Лабораторные работы со студентами предназначены для проверки усвоения ими теоретического материала дисциплины.

Основные цели лабораторных работ:

- закрепить основные положения дисциплины;
- проверить уровень усвоения и понимания студентами вопросов, рассмотренных на лекциях и самостоятельно изученных по учебной литературе;
- научить пользоваться нормативной и справочной литературой для получения необходимой информации о конкретных технологиях;
- оказать помощь в приобретении навыков расчета точностных характеристик;
- восполнить пробелы в пройденной теоретической части курса и оказать помощь в его усвоении.

Для контроля знаний, полученных в процессе освоения дисциплины на лабораторных занятиях обучающиеся выполняют задания реконструктивного уровня и комплексное практическое задание.

Целью выполнения задания реконструктивного уровня и комплексного задания студентами является систематизация, закрепление и расширение теоретических знаний, полученных в ходе изучения дисциплины.

Ниже приводятся общие методические указания, которые относятся к занятиям по всем темам:

- в начале каждого лабораторного занятия необходимо сформулировать цель, поставить задачи;
- далее необходимо проверить знания студентами лекционного материала по теме занятий;
- в процессе занятия необходимо добиваться индивидуальной самостоятельной работы студентов;
- знания студентов периодически контролируются путем проведения текущей аттестации (рубежного контроля), сведения о результатах которой доводятся до студентов и подаются в деканат;
- время, выделенное на отдельные этапы занятий, указанное в рабочей программе, является ориентировочным; преподаватель может перераспределить его, но должна быть обеспечена проработка в полном объеме приведенного в рабочей программе материала;
- на первом занятии преподаватель должен ознакомить студентов с правилами поведения в лаборатории и провести инструктаж по охране труда и по пожарной безопасности на рабочем месте;
- преподаватель должен ознакомить студентов со всем объемом лабораторных работ и требованиями, изложенными выше;
- преподаватель уделяет внимание оценке активности работы студентов на занятиях, определению уровня их знаний на каждом занятии.

На лабораторных работах решаются задачи из всех разделов изучаемой дисциплины.

Задания на лабораторные практикумы по дисциплине
«Безопасность информационных систем и баз данных».

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 №1

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

ВГВДБВБДБЕАААДВБААЕБЕЕВАААГАААЕВАААГАБВБДААЕЕ

Задание: Реализовать на любом языке программирования работу данного шифра

ЛАБОРАТОРНАЯ РАБОТА №2

Исследование криптоалгоритма шифрования RSA

Цель работы: Исследование структуры алгоритма и методики практической реализации криптосистемы шифрования RSA.

Основные теоретические положения:

Как известно, алгоритмы симметричного шифрования используют ключи относительно небольшой длины и поэтому могут быстро шифровать большие объёмы данных.

При использовании алгоритма симметричного шифрования отправитель и получатель применяют для шифрования и расшифрования данных один и тот же секретный ключ. Таким образом, алгоритмы симметричного шифрования основываются на предположении о том, что зашифрованное сообщение не сможет прочитать никто, кроме того кто обладает ключом для его расшифрования. При этом если ключ не скомпрометирован, то при расшифровании автоматически выполняется аутентификация отправителя, т.к. только он имеет ключ, с помощью
которого можно зашифровать сообщение. Таким образом, для симметричных криптосистем актуальна проблема безопасного распределения симметричных секретных ключей. В связи с этим без эффективной организации защищённого распределения ключей использование обычной системы симметричного шифрования в вычислительных сетях практически невозможно.

Решением данной проблемы является использование асимметричных алгоритмов шифрования, называемых криптосистемами с открытым ключом. В них для зашифрования данных используется один ключ, называемый «открытым» а для расшифрования — другой называемый «закрытым или секретным». Следует иметь в виду, что ключ расшифрования не может быть определён из ключа зашифрования.

В асимметричных криптосистемах отрытый ключ и криптограмма могут быть отправлены по незащищённым каналам. Концепция таких систем основана на применении однонаправленных функций.

В качестве примера однонаправленной функции может служить целочисленное умножение.

Прямая задача — вычисление произведения двух больших целых чисел p и q, $n = p*q$. Это относительно несложная задача для ЭВМ.

Обратная задача — факторизация или разложение на множители большого целого числа практически неразрешима при достаточно больших значениях n.

Например, если $p \sim q$, а их произведение $n \sim 2^{664}$, то для разложения этого числа на множители потребуется 2^{23} операций, что практически невозможно выполнить за приемлемое время на современных ЭВМ.

Другим примером однонаправленной функции является модульная экспонента с фиксированным основанием и модулем.

Например, если $y=a^x$, то естественно можно записать, что $x = \log_a (y)$.

Задача дискретного логарифмирования формулируется следующим образом. Для известных целых a, n, y следует найти такое число x, при котором

$$a^x (mod\ n) = y$$

Например, если $a=2^{664}$ и $n=2^{664}$ нахождение показателя степени x для известного y потребует около 10^{26} операций, что также невозможно выполнить на современных ЭВМ .

В связи с тем, что в настоящее время не удалось доказать, что не существует эффективного алгоритма вычисления дискретного логарифма за приемлемое время, то модульная экспонента также условно отнесена к однонаправленным функциям.

Другим важным классом функций, используемых при построении криптосистем с открытым ключом являются, так называемые, однонаправленные функции с секретом. Функция относится к данному классу при условии, что она является однонаправленной и, кроме того, возможно эффективное вычисление обратной функции, если известен секрет.

В данной лабораторной работе исследуется криптосистема RSA, использующая модульную экспоненту с фиксированным модулем и показателем степени (т.е. однонаправленную функцию с секретом).

Схема алгоритма шифрования данных RSA

1. Определение открытого «e» и секретного «d» ключей

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 открытого ключа ***e*** с учётом условий:

$$1 < e < \phi(n), \text{ НОД}(e, \phi(n)) = 1$$

1.5. Определение секретного ключа ***d***, удовлетворяющего условию

$$e*d \pmod{\phi(n)} = 1, \text{ где } d < n$$

2. Алгоритм шифрования сообщения M (действия отправителя)

2.1. Разбивает исходный текст сообщения на блоки $M_1, M_2, ..., Mn$,

$$(M_i = 0, 1, 2, ..., n)$$

2.2. Шифрует текст сообщения в виде последовательности блоков:

$$C_i = M_i^e \pmod{n}$$

2.3. Отправляет получателю криптограмму: $C_1, C_2, ... C_n$
2.4. Получатель расшифровывает криптограмму с помощью секретного ключа ***d*** по формуле:

$$M_i = C_i^d \pmod{n}$$

3. Процедуру шифрования данных рассмотрим на следующем примере (для простоты и удобства расчётов в данном примере использованы числа малой разрядности):

3.1. Выбираем два простых числа ***p*** и ***q***, $p = 3, q = 11;$
3.2. Определяем их произведение (модуль) $n = p*q = 33;$
3.3. Вычисляем значение функции Эйлера $\phi(n) = (p-1)(q-1)$

$$\phi(n) = 2*10 = 20$$

3.4. Выбираем случайным образом открытый ключ с учётом выполнения условий

$$1 < e < \phi(n) \text{ и НОД } (e, \phi(n)) = 1, e = 7;$$

3.5. Вычисляем значение секретного ключа ***d***, удовлетворяющего условию

$$e*d(\bmod \phi(n)) = 1, 7*d \pmod{20} = 1; d = 3;$$

3.6. Отправляем получателю пару чисел $(n = 33, e = 7);$
Представляем шифруемое сообщение M как последовательность целых чисел **312.**
3.7. Разбиваем исходное сообщение на блоки $M_1 = 3, M_2 = 1, M_3 = 2;$
3.8. Шифруем текст сообщения, представленный в виде последовательности , блоков: $C_i = M_i^e \pmod{n}$

$$C_1 = 3^7 \pmod{33} = 2187 (\text{mod} 33) = 9,$$
$$C_2 = 1^7 \pmod{33} = 1 (\text{mod} 33) = 1,$$
$$C_3 = 2^7 \pmod{33} = 128 \pmod{33} = 29.$$

3.9. Отправляем криптограмму $C_1 = 9, C_2 = 1, C_3 = 29.$
3.10. Получатель расшифровывает криптограмму с помощью секретного ключа ***d*** по формуле: $M_i = C_i^d \pmod{n}$

$$M_1 = 9^3 \pmod{33} = 729 (\text{mod } 33) = 3$$
$$M_2 = 1^3 \pmod{33} = 1 \pmod{33} = 1$$
$$M_3 = 29^3 \pmod{33} = 24389 \pmod{33} = 2.$$

Полученная последовательность чисел 312 представляет собой исходное сообщение M.

4. Содержание отчёта

4.1. Составить блок-схему и программу алгоритма шифрования RSA.
4.2. Листинг программы шифрования заданного сообщения M с использованием алгоритма RSA.

ЛАБОРАТОРНАЯ РАБОТА №3

Исследование электронной цифровой подписи (ЭЦП)

RSA

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: $e < n$,

$$e*d(mod\ \phi(n))=1$$

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

Исследование криптоалгоритма шифрования Эль - Гамаля

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:

$$y=q^x \pmod p$$

2. Алгоритм шифрования сообщения M

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: $a = q^k \pmod p$

2.3. Определение значения ***b*** из выражения: $b = y^k M \pmod p$

2.4. Криптограмма ***C***, состоящая из ***a*** и ***b***, отправляется получателю

2.5. Получатель расшифровывает криптограмму с помощью выражениями:

$$Ma^x = b \pmod p$$

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

$$y=q^x \pmod p = 2^8 \pmod{11} = 256 \pmod{11} = 3$$

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:

$$a = q^k \pmod p = 2^9 \pmod{11} = 512 \pmod{11} = 6;$$

3.7. Определяем значение ***b*** из выражения:

$$b = y^k M \pmod p = 3^9 * 5 \pmod{11} = 98415 \pmod{11} = 9.$$

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:

$$M*a^x = b \pmod p = 5*6^8 = 9 \pmod{11} = 8398080 = 9 \pmod{11}$$

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.

3 Методические указания по самостоятельной работе

Для успешного освоения курса «Основы информационной безопасности» необходима самостоятельная работа. В настоящее время актуальными становятся требования к личным качествам современного студента – умению самостоятельно пополнять и обновлять знания, вести самостоятельный поиск необходимого материала, быть творческой личностью.

Самостоятельную работу по освоению дисциплины обучающимся следует начинать с изучения содержания рабочей учебной программы дисциплины, цели и задач, структуры и содержания курса, основной и дополнительной литературы, рекомендованной для самостоятельной работы.

Самостоятельная учебная деятельность является необходимым условием успешного обучения. Многие профессиональные навыки, способность мыслить и обобщать, делать выводы и строить суждения, выступать и слушать других, – все это развивается в процессе самостоятельной работы студентов.

Самостоятельная работа по освоению дисциплины включает:

- самостоятельное изучение разделов;
- самоподготовку (проработку и повторение лекционного материала и материала учебников и учебных пособий);
- подготовку к лабораторным работам;
- подготовку к рубежному и итоговому контролю.

Самостоятельная учебная работа – условие успешного окончания высшего учебного заведения. Она является равноправной формой учебных занятий, наряду с лекциями, семинарами, экзаменами и зачетами, но реализуемая во внеаудиторное время.

Эффективность аудиторных занятий во многом зависит от того, насколько умело студенты организуют в ходе них свою самостоятельную учебную познавательную деятельность. Такая работа также способствует самообразованию и самовоспитанию, осуществляемому в интересах повышения профессиональных компетенций, общей эрудиции и формировании личностных качеств.

Самостоятельная работа реализуется:

1. непосредственно в процессе аудиторных занятий – на лекциях, лабораторных занятиях, при проведении рубежного контроля;
2. в контакте с преподавателем вне рамок расписания – на консультациях по учебным вопросам, при ликвидации задолженностей, при выполнении индивидуальных заданий;
3. в библиотеке, дома, в общежитии, на кафедре при выполнении студентом учебных задач.

В процессе проведения самостоятельной работы необходимо производить подбор литературных источников, научной периодической печати и т.д

4 Методические указания по итоговому контролю

Итоговый контроль знаний по дисциплине «Основы информационной безопасности» проводится в форме дифференцированного зачета. Для подготовки к

итоговому контролю знаний по дисциплине «Основы информационной безопасности» обучающиеся используют перечень вопросов, приведенный в фонде оценочных средств. Дифференцированный зачет проводится в устной форме. В экзаменационный билет включен один теоретический вопрос. На подготовку студенту отводится 20-25 минут. На дифференцированном зачете ответы обучающегося оцениваются с учетом их полноты, правильности и аргументированности с учетом шкалы оценивания.

Оценка «отлично» выставляется студенту, если он глубоко и прочно усвоил программный материал, исчерпывающе, последовательно, четко и логически его излагает, умеет тесно увязывать теорию с практикой, свободно справляется с вопросами и другими видами применения знаний, причем не затрудняется с ответом при видоизменении заданий, использует в ответе профессиональные термины, правильно обосновывает принятое решение.

Оценка «хорошо» выставляется студенту, если он твердо знает материал, грамотно и по существу излагает его, не допуская существенных неточностей в ответе на вопрос, правильно применяет теоретические положения при решении практических вопросов, владеет необходимыми навыками и приемами их выполнения.

Оценка «удовлетворительно» выставляется студенту, если он имеет знания только основного материала, но не усвоил его деталей, допускает неточности, недостаточно правильные формулировки, нарушения логической последовательности в изложении программного материала.

Оценка «неудовлетворительно» выставляется студенту за отсутствие знаний по дисциплине, представления по вопрос, непонимание материала по дисциплине, наличие коммуникативных «барьеров» в общении, отсутствие ответа на предложенный вопрос.

5.1 Основная литература

1. Информационные системы и их безопасность [Текст] : учебное пособие / А. В. Васильков, А. А. Васильков, И. А. Васильков. - Москва : Форум, 2012. - 528 с. - Библиогр. : с. 513-514. - ISBN 978-5-91134-289-0. (ОГТИ ч/з N4-1; аб.ТБ-18), коэффициент книгообеспеченности 1

5.2 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.

5.3 Периодические издания

1. Журнал «Вестник компьютерных и информационных технологий »
2. Журнал «Информационные технологии и вычислительные системы»
3. Журнал «Стандарты и качество»
4. Журнал «Прикладная информатика»

5.4 Интернет-ресурсы

5.4.1 Современные профессиональные базы данных и информационные справочные системы:

1. Информационная система «Единое окно доступа к образовательным ресурсам» - http://window.edu.ru/
2. КиберЛенинка - https://cyberleninka.ru/
3. Университетская информационная система Россия – uisrussia.msu.ru
4. Бесплатная база данных ГОСТ – https://docplan.ru/

5.4.2 Тематические профессиональные базы данных и информационные справочные системы:

1. Портал искусственного интеллекта – AIPortal
2. Web-технологии – Web-технологии
3. Электронная библиотека Института прикладной математики им. М.В. Келдыша – Электронная библиотека публикаций Института прикладной математики им. М.В. Келдыша РАН

5.4.3 Электронные библиотечные системы

1. ЭБС «Университетская библиотека онлайн» – http://www.biblioclub.ru/
2. ЭБС Znanium.com – https://znanium.com/

5.4.4 Дополнительные Интернет-ресурсы

1. https://www.ixbt.com - Интернет-издание о компьютерной технике, информационных технологиях и программных продуктах. На сайте публикуются новости IT, статьи с обзорами и тестами компьютерных комплектующих и программного обеспечения.
2. http://www.intuit.ru – ИНТУИТ – Национальный открытый университет.
3. http://cppstudio.com/ - Основы программирования на языках Си и C++.
4. https://www.anti-malware.ru/ - Информационно-аналитический центр, посвященный информационной безопасности.

5. https://developer.mozilla.org/ru/docs/Tools — Открытые уроки по веб-технологиям и инструментам разработчика.
6. https://frontender.info – Электронный журнал по фронтенд-разработке

5.5 Программное обеспечение, профессиональные базы данных и информационные справочные системы современных информационных технологий

Тип программного обеспечения	Наименование	Схема лицензирования, режим доступа
Операционная система	Microsoft Windows	Подписка Enrollment for Education Solutions (EES) по государственному контракту: № 2К/17 от 02.06.2017 г.;
Текстовый редактор	Notepad++	Свободное ПО, https://notepad-plus-plus.org/
Интернет-браузер	Google Chrome	Бесплатное ПО, http://www.google.com/intl/ru/policies/terms/
Векторный графический редактор, редактор диаграмм и блок-схем	Microsoft Visio Standard 2007	Сертификат Microsoft Open License № 46284547 от 18.12.2009 г., академическая лицензия на рабочее место
Интегрированная среда разработки программного обеспечения	Microsoft Visual Studio Professional 2008	Сертификат Microsoft Open License № 46284547 от 18.12.2009 г., академическая лицензия на рабочее место
	Embarcadero RAD Studio 2010 Professional	Образовательная лицензия по государственному контракту № 32/09 от 17.12.2009 г., сетевой конкурентный доступ
	Turbo Pascal 7.0 for DOS	Образовательная лицензия по государственному контракту № 34/10 от 10.12.2010 г., лицензия на рабочее место
	Borland C++ 3.1 for DOS	Образовательная лицензия по государственному контракту № 34/10 от 10.12.2010 г., лицензия на рабочее место
	Dev-C++	Свободное ПО, http://www.gnu.org/licenses/gpl.html

6 Материально-техническое обеспечение дисциплины

Учебные аудитории для проведения занятий лекционного типа, семинарского типа, для проведения групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации. Для проведения лабораторных и практических работ используются компьютерный класс (ауд. № 4-113, 4-116, 4-117), оборудованный средствами оргтехники, программным обеспечением, персональными компьютерами, объединенными в сеть с выходом в Интернет.

Аудитории оснащены комплектами ученической мебели, техническими средствами обучения, служащими для представления учебной информации большой аудитории.

Помещения для самостоятельной работы обучающихся оснащены компьютерной техникой, подключенной к сети «Интернет», и обеспечением доступа в электронную информационно-образовательную среду Орского гуманитарно-технологического института (филиала) ОГУ (ауд. № 4-307).

Наименование помещения	Материальное-техническое обеспечение
Учебные аудитории: - для проведения занятий лекционного типа, семинарского типа, - для групповых и индивидуальных консультаций; - для текущего контроля и промежуточной аттестации	Учебная мебель, классная доска, мультимедийное оборудование (проектор, экран, ноутбук с выходом в сеть «Интернет»)
Компьютерные классы № 4-113, 4-116, 4-117	Учебная мебель, компьютеры (29) с выходом в сеть «Интернет», проектор, экран, лицензионное программное обеспечение
Помещение для самостоятельной работы обучающихся, для курсового проектирования (выполнения курсовых работ)	Учебная мебель, компьютеры (3) с выходом в сеть «Интернет» и обеспечением доступа в электронную информационно-образовательную среду Орского гуманитарно-технологического института (филиала) ОГУ, программное обеспечение

Для проведения занятий лекционного типа используются следующе наборы демонстрационного оборудования и учебно-наглядные пособия:

- презентации к курсу лекций