СПбГЭТУ «ЛЭТИ»
ПЕРВЫЙ ЭЛЕКТРОТЕХНИЧЕСКИЙ

А.Б. Левина

Криптография и криптографические протоколы

Методические материалы по практическим работам

СПбГЭТУ «ЛЭТИ», 2022 г.

1 ПРАКТИЧЕСКИЕ РАБОТЫ

1.1 Общие положения и методика оценивания результатов

В процессе обучения по дисциплине «Криптография и криптографические протоколы» студент обязан выполнить 7 практических работ. Под выполнением практических работ подразумевается подготовка к работе, проведение экспериментальных исследований, подготовка отчета и его защита на практическом занятии. Выполнение практических работ студентами осуществляется в бригадах до 2 человек. Оформление отчета студентами осуществляется индивидуально в соответствии с принятыми в СПбГЭТУ правилами оформления студенческих работ. Отчет оформляется после выполнения экспериментальных исследований и представляется преподавателю на проверку. После проверки отчет либо возвращается (при наличии замечаний) на доработку, либо подписывается к защите. Практические работы защищаются студентами индивидуально. Каждый студент получает вопрос по теоретической и практической части, после чего ему предоставляется время для подготовки ответа. На защите практической работы студент должен показать: понимание и умение объяснять особенности применяемых методов, возможные области их применения и т.д., прогнозировать реакции исследуемого объекта на различные воздействия, навыки и умения, приобретенные при выполнении практических работы. При обсуждении ответа преподаватель может задать несколько уточняющих вопросов. В случае если студент демонстрирует достаточное знание вопроса, работа считается зачтенной. Текущий контроль включает в себя выполнение, сдачу в срок отчетов и их защиту по всем практическим работам, по результатам которой студент получает допуск к экзамену. Критерием оценки работы на практическом занятии является оценка, выставляемая по 5-ти балльной шкале в соответствии со следующими критериями: оценка в 5 баллов выставляется при отличном выполнении задания, то есть при наличии полных (с детальными пояснениями и выкладками), оригинальных и правильных решений задач, дополненных при необходимости документами, полученными в результате реализации (проверки) решения, верных ответов и высококачественного оформления работы. Оценка в 4 балла выставляется при правильном выполнении задания, то есть при наличии полных (с пояснениями и выкладками), оригинальных и правильных решений задач, дополненных при

необходимости документами, полученными в результате реализации (проверки) решения, верных ответов. Оценка в 3 балла выставляется при наличии отдельных неточностей в ответах (включая грамматические ошибки) или неточностях в решении задач непринципиального характера (описки и случайные ошибки арифметического характера). Оценка в 2 и ниже баллов выставляется в случаях, когда в ответах и в решениях задач имеются неточности и ошибки, свидетельствующие о недостаточном понимании вопросов и требующие дополнительного обращения к тематическим материалам.

1.2 Содержание отчетов

- Титульный лист
- Цель работы
- Формулировка задания
- Краткое описание выполнения основных этапов работы
- Выводы по работе

1.3 Практические работы

1.3.1 Симметричное шифрование

Цель работы: изучение алгоритмов симметричного шифрования.

Задание:

Реализовать программно алгоритмы симметричного шифрования, осуществить процесс шифрования и дешифрования. Язык программирования выбирается любой, на усмотрение студента.

Контрольные вопросы:

1. **Реализовать алгоритм Вижнера и Тест Касиского;**
2. **Реализовать алгоритм DES;**
3. **Реализовать алгоритм Rijndael;**
4. **Реализовать алгоритм поточного шифрования, на пример алгоритма A5 стандарта GSM.**

1.3.2 Асимметричное шифрование

Цель работы: изучение алгоритмов асимметричного шифрования.

Задание:

Реализовать программно алгоритмы асимметричного шифрования, осуществить процесс шифрования и дешифрования. Язык программирования выбирается любой, на усмотрение студента.

Контрольные вопросы:

1. **Реализовать алгоритм RSA;**
2. **Реализовать алгоритм передачи ключей Диффи-Хэллмана;**
3. **Реализовать алгоритм на выбор (Эль-Гамаль, криптосистема Рабина).**

1.3.3 Протоколы гибридного шифрования

Цель работы: изучение подходов к построению гибридных криптосистем, основные принципы их построения, принципы работы.

Задание:

На основе запрограммированных ранее алгоритмов построить гибридную криптосистему. Язык программирования выбирается любой, на усмотрение студента.

1. **Реализовать гибридную криптосистему;**
2. **Обеспечить передачу ключей с помощью алгоритма RSA или Дифии-Хэллмана;**
3. **Обеспечить шифрование с помощью любого алгоритма симметричного шифрования.**

1.3.4 Протоколы аутентификации

Цель работы: изучить работу алгоритмов аутентификации.

Задание: реализовать программно алгоритм аутентификации, используя алгоритм построения ЭЦП и хэш-функцию. Язык программирования выбирается любой, на усмотрение студента.

1. Реализовать алгоритм хэширования, используя любую из существующих хэш-функций;
2. Реализовать алгоритм ЭЦП, применяя запрограммированную ранее хэш-функцию и любой из известных алгоритмов постановки ЭЦН.

1.3.5 Протоколы индивидуальной и коллективной цифровой подписи

Цель работы: изучение работы алгоритмов индивидуальной и коллективной ЭЦП.

Задание:

Реализовать программно алгоритм коллективной ЭЦП, внедрить его в разработанный ранее протокол гибридной криптосистемы. Язык программирования выбирается любой, на усмотрение студента.

1. Реализовать любой алгоритм коллективной ЭЦП;
2. Добавить реализованный алгоритм в разработанную ранее гибридную криптосистему.

1.3.6 Криптоанализ и криптостойкость

Цель работы: изучить основные принципы проведения криптоатак.

Задание: выбрать любую систему и проанализировать ее уязвимости, описать детально найденные уязвимости и предложить методы защиты.

1. **Выбрать систему для проведения криптоатаки;**
2. **Найти все возможные уязвимости;**
3. **Реализовать найденные уязвимости;**
4. **Разработать и предложить методы защиты от выявленных уязвимостей.**