1 Вопрос 1

Криптографические протоколы: основные понятия.Модель угроз Долева-Яо.

1. Основные определения.
2. Свойства криптографических протоколов.
3. Классификация криптографических протоколов.
4. Модель Долева-Яою

2 Вопрос 2

Атаки на криптографические протоколы.

1. Основные определения.
2. Классификация атак на криптографические протоколы.
3. Дать определение, перечислить подтипы и привести пример для следующих классов атак:
   (a) Атака посередине
   (b) Атака с повторной передачей
   (c) Атака подмены типа
   (d) Комбинированная атака
   (e) Атака с известным сеансовым ключом
   (f) Атака с неизвестным общим ключом
   (g) Атака с использованием специально подобранных текстов
   (h) Атака на основе связывания

3 Вопрос 3

Управление ключами. Классификация ключей. Жизненный цикл ключей. Особенности управления ключами в симметричных и асимметричных криптосистемах

1. Основные определения
2. Классификация ключей
3. Жизненный цикл ключей
4. Особенности управления ключами

4 Вопрос 4

Протоколы аутентификации: классификация, атаки. Протоколы слабой аутентификации

1. Основные определения
2. Классификация аутентификации
3. Фиксированные пароли, HTTP authentication
4. Одноразовые пароли, Схема Лэмпорта

5 Вопрос 5

Протоколы сильной аутентификации

1. Основные определения
2. Классификация протоколов сильной аутентификации
3. Напишите протоколы ISO/ IEC 9798 - 2
4. Напишите протокол Ву-Лама и атаку к данному протоколу
5. Напишите протокол NSPK и атаку к данному протоколу
6. Напишите протокол сильной аутентификации с использованием ЭЦП

6 Вопрос 6

Протоколы аутентификации на основе техники доказательства знания

1. Основные определения
2. Схема протокола
3. Напишите протокол Фиата-Шамира
4. Напишите протокол Шнора
5. Напишите протокол GQ

7 Вопрос 7

Протоколы распределения ключей на основе симметричных криптосистем

1. Основные определения
2. Классификация протоколов распределения ключей
3. Напишите протоколы ISO/IEC 11770-2
4. Определение "Коммутирующее шифрующее преобразование", Трёхпроходный протокол Шамира
5. Напишите протокол Wide-Mouth-Frog и атаку к данному протоколу
6. Напишите протокол Needham-Schroeder (NSSK) и атаку к данному протоколу
7. Напишите протокол Отвея - Рисса и атаку к данному протоколу

8 Вопрос 8

Протоколы распределения ключей на основе асимметричных криптосистем

1. Основные определения
2. Классификация протоколов распределения ключей
3. Напишите протокол Needham-Schroeder Public Key (NSPK)
4. Напишите протокол NSPK без 3-ей стороны
5. Напишите протокол EKE(Encrypted Key Exchange)
6. Напишите протокол распределения ключей с использованием ЭЦП
7. Напишите протокол MTI

9 Вопрос 9

Предварительное распределение ключей. Протоколы голосования

1. Основные определения
2. Классификация протоколов распределения ключей
3. Напишите схему Шамира
4. Напишите схему разделения секрета Блома
5. Напишите протоколы голосования с ЦИК и ЦУР
6. Напишите улучшенный протокол голосования
7. Опишите гомоморфное шифрование в протоколах голосования

10 Вопрос 10

Протоколы SSL/TLS, СТБ 34.101.65

1. Описание протокола(ов): функционал, версии
2. Описание шагов протокола
3. Алгоритмы формирования общего ключа
4. Методы аутентификации

11 Вопрос 11

Протокол IPSEC

1. Описание протокола(ов): функционал, версии
2. Описание шагов протокола
3. Архитектура протокола
4. Security Association

12 Вопрос 12

Протоколы ESP, AH

1. Описание протокола(ов): функционал, версии
2. Описание структуры пакетов

13 Вопрос 13

Протокол SSH

1. Описание протокола(ов): функционал, версии
2. Описание шагов протокола
3. Архитектура протокола
4. SSH-TRANS
5. SSH-USERAUTH

14 Вопрос 14

Сравнение протоколов SSH, IPSEC, SSL. AEAD-режим шифрования

1. Сравнение протоколов SSH, IPSEC, SSL
2. Описание AE-, AEAD-режимов
3. Определение "Неразличимость шифротекста"
4. Определение "Неизменяемость шифротекста"
5. Определение "Целостность открытого текста"

15 Вопрос 15

Протокол WEP, атаки

1. Описание протокола(ов): функционал, версии
2. Описание шагов протокола
3. Архитектура протокола
4. Атаки на протокол

16 Вопрос 16

Протоколы WPA, WPA2, WPA3 и атаки

1. Описание протокола(ов): функционал, версии
2. Различие WEP и WPA, WPA и WPA2
3. Описание шагов протокола
4. Архитектура протокола
5. Атаки на протокол

17 Вопрос 17

СТБ 34.101.66-2014 "Информационные технологии и безопасность. Протоколы формирования общего ключа на основе эллиптических кривых".

1. Описание протокола(ов): функционал, версии
2. Шаги протокола и входные/выходные данные (один из BMQV, BSTS, BPACE)