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 по середине
   (b) Атака с повторной передачей
   (c) Атака подмены типа
   (d) Комбинированная атака
   (e) Атака с известным сеаносвым ключом
   (f) Атака с неизвестным общим ключом
   (g) Атака с использованием специально подобранных текстов
   (h) Атака на основе связывания

3 Вопрос 3

Управление ключами
Жизненый цикл ключей

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 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 симметричной кс

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