ВОПРОСЫ
по программе курса “КРИПТОГРАФИЧЕСКИЕ ПРОТОКОЛЫ”
ДЛЯ СТУДЕНТОВ Y КУРСА, ФАК-ТА КНиИТ,

I.

1) Понятие протокола, понятие криптографического протокола, понятие шага протокола, понятие прохода протокола.
2) Понятие сеанса протокола, понятие роли и число ролей, основные действующие лица криптографических протоколов.
3) Основные характеристики (3) и основные задачи (3) криптографического протокола и основное требование.

II.

1) Классификация криптографических протоколов по степени их развития.
2) Классификация по степени участия незаинтересованных сторон.
3) Классификация по числу проходов, по числу участников, по типу используемой криптографической системы.

III.

1) Обмен ключами средствами симметричной криптографии, протокол Ньюмана-Стабблбайна.
2) Протоколы открытого распределения ключей: протокол Диффи и Хельмана, протокол Хьюза.
3) Протокол «Станция-станция». Протокол передачи секретного ключа по открытому каналу – Трехпроходный (трехэтапный) протокол Шамира и пример криптосистемы для его реализации.

IV.

1) Понятия идентификации, аутентификации и авторизации.
2) Понятие аутентификатора и его конкретные формы.
3) Блок-схема типичной процедуры идентификации, аутентификации и авторизации.

V.

1) Парольные системы аутентификации с помощью однонаправленных функций.
2) Программа аутентификации SKEY и протокол с её применением.
3) Простейшая система аутентификации средствами криптографии с открытым ключом. Взаимная аутентификация по протоколу «взаимоблокировки» или «держась за руки» («рукопожатия»).

VI.

1) Вручение битов средствами симметричной криптографии.
2) Вручение битов с использованием однонаправленных функций.
3) Вручение битов с помощью генераторов псевдослучайных последовательностей.

VII.

1) Пояснение Кискате-Гилу сути нулевого разглашения на примере «Пещеры с нулевым разглашением».
2) Доказательство изоморфизма графов с нулевым разглашением (Блюм).
3) Доказательство гамильтоновости графа с нулевым разглашением (Блюм).

VIII.

1) Классический протокол честного дележа «разделяй и выбирай».
2) Формализация понятия интерактивного протокола и нулевого разглашения.
3) Неинтерактивное доказательство с нулевым разглашением.

IX.

1) Подбрасывание монеты по телефону с помощью вручения бита.
2) Подбрасывание монеты по телефону с помощью однонаправленных функций.
3) Подбрасывание монеты по телефону с помощью криптографии с открытым ключом.

X.

1) Доказательство знания дискретного логарифма с нулевым разглашением.
2) Доказательство способности вскрытия RSA с нулевым разглашением.
3) Доказательство с нулевым разглашением того, что *n* является числом Блюма.

XI.

1) Схема аутентификации Фейге-Фиата-Шамира
2) Схема аутентификации Гиллу-Кискате.
3) Схема аутентификации Шнорра.

XII.

1) Схема подписи Фиата-Шамира.
2) Схема подписи Гиллу-Кискате.
3) Протокол цифровой подписи (Схема подписи Шнорра).

XIII.

1) Преобразование схем аутентификации в схемы подписи.
2) Многократная подпись Гиллу-Кискате.
3) Подписи, подтверждаемые доверенным лицом.

XIV.

1) Неоспоримые цифровые подписи, протокол1 (Д. Чаум) и протокол2 (Д. Чаум).
2) Преобразуемая неоспоримая цифровая подпись на основе схемы Эль-Гамаля.
3) Подписи «вслепую» (протокол Д. Чаум).

XV.

1) Понятие схемы, разделяющей секрет (СРС), понятие пороговых (n, k) – СРС.
2) Пример простейшей СРС. Векторная схема разделения секрета Блэкли.
3) Схема интерполяционных полиномов Лагранжа.

XVI.

1) Схема разделения секрета Асмута-Блума.
2) Схема разделения секрета Карнина-Грина-Хеллмана.
3) Более сложные схемы разделения секрета, пример коалиционной схемы.

XVII.

1) Базовый протокол скрытого канала.
2) Скрытый канал на основе схемы Эль-Гамаля.
3) Скрытый канал на основе DSA и его уничтожение.

XVIII.

1) Мысленный покер с тремя игроками.
2) Однонаправленные Сумматоры: основная функция и алгоритм суммирования.
3) Раскрытие секретов «всё или ничего» с помощью RSA.

Максимальный балл 40. Ниже приведена таблица перевода оценок в пятибалльную систему.

0-20	21-27	28-34	35-40
2	3	4	5

Литература

1. Баричев С.Г., Серов Р.Е. Основы современной криптографии. М: Горячая Линия - Телеком, 2002. — 153 с.
2. Ростовцев А.Г., Маховенко Е.Б. Теоретическая криптография. Санкт-Петербург: НПО «Профессионал», 2005. — 486 с.
3. Рябко Б.Я., Фионов А.Н. Криптографические методы защиты информации: Учебное пособие для вузов. — М.: Горячая линия–Телеком, 2005. — 229 с.
4. Смарт Н. Криптография. М.: Техносфера, 2005. — 528 с.
5. Фомичев В.М. Дискретная математика и криптология. Курс лекций // Под общ. ред. д-ра физ.-мат. н. Подуфалова Н.Д. — М.: ДИАЛОГ-МИФИ, 2003. — 400 с.

Составил: Новиков В.Е.