**Практические задания**

**по дисциплине «Криптографические протоколы»**

**(2023/2024 учебный год, 9 семестр)**

## Задание 1. Протоколы открытого распределения ключей

- Базовый протокол (алгоритм Диффи-Хеллмана)
- Алгоритм Хьюза (Hughes)
- Протокол «станция-станция»

## Задание 2. Протоколы обмена ключами

- Протокол Нидхема-Шрёдера
- Протокол Kerberos
- Протокол Ньюмана-Стабблбайна

## Задание 3. Протоколы передачи секретного ключа по открытому каналу

- Трехпроходный (трехэтапный) протокол Шамира
- Алгоритм Мэсси-Омура
- Протокол Encrypted Key Exchange (EKE) на базе алгоритма RSA
- Протокол Encrypted Key Exchange (EKE) на базе алгоритма Эль-Гамаля
- Протокол Encrypted Key Exchange (EKE) на базе алгоритма Диффи-Хеллмана

## Задание 4. Схемы аутентификации

- Упрощенная схема идентификации Фейге-Фиата-Шамира
- Схема идентификации Гиллу-Кискате
- Протокол аутентификации Шнорра

## Задание 5. Схемы ЭЦП

- Схема подписи Фиата-Шамира
- Схема подписи Гиллу-Кискате
- Схема подписи Шнорра
- Схема подписи Эль-Гамаля
- Схема подписи DSA

## Задание 6. Разделение секрета

- Схема Шамира (интерполяционные полиномы Лагранжа)
- Схема Блэкли (деление по гиперплоскостям)
- Схема Асмута-Блума (греко-римская теорема об остатках)
- Схема Миньотта (китайская теорема об остатках)
- Схема Карнина-Грина-Хеллмана (теория матриц)

## Задание 7. Скрытый канал связи

- На основе схемы Онга-Шнорра-Шамира
- На основе схемы Эль-Гамаля

- На основе ESIGN
- На основе DSA

**Задание 8. Протоколы анонимности**

- Протокол двух агентств Нурми-Саломаа-Сантин
- Протокол двух агентств Фудзиока-Окамото-Ота
- Протокол Sensus
- Протокол Хэ-Су
- Протокол голосования с одной Центральной комиссией на базе протокола ANDOS

ЛИТЕРАТУРА

- Б. Шнайер. Прикладная криптография. Протоколы, алгоритмы и исходный код на С (можно скачать по ссылке https://vk.com/wall-54530371_172816)

ТРЕБОВАНИЯ

Для каждого задания должен быть написан отчет, включающий в себя:

1) Теоретическую часть (постановка задачи, описание алгоритма)
2) Описание программы
3) Листинг кода

Помимо этого, код задачи должен быть залит на GitHub (создайте один публичный репозиторий, каждую задачу заливайте как подмодуль).

Желательно покрыть код юнит-тестами.

Отчеты присылать на почту renatfara@mail.ru с темой письма «[Криптопротоколы] Фамилия – Задача_N»