Перспективные технологии защиты информации

Типовые контрольные задания на проверку сформированности компетенций

ПК-8 – Способность проектировать распределенные информационные системы, их компоненты и протоколы их взаимодействия

- В чем состоит назначение протокола генерации ключей?
- Какой объем данных необходимо передать по сети в протоколе MQV?
- Как реализуется атака посредника в протоколе Диффи–Хеллмана?
- Какова роль асимметричных криптографических алгоритмов в протоколах взаимодействия информационных систем?
- Какова роль криптографических хэш-функций в протоколах взаимодействия информационных систем?

ПК-13 – Способность к программной реализации распределенных информационных систем

- Раскрыть суть подхода оптимизации по памяти программной реализации шифра Кузнечик.
- Раскрыть суть подхода оптимизации по времени программной реализации шифра Кузнечик.
- Как интегрируются при построении распределенных информационных систем алгоритмы генерации ключей и блочные шифры?
- Как интегрируются при построении распределенных информационных систем алгоритмы генерации ключей и хэш-функции?
- Назовите средства измерения времени выполнения программ, доступных на платформах x86.

Типовые задания на РГР:

1. Разработать программу обмена зашифрованными файлами по сети между двумя пользователями. Использовать протокол Диффи-Хеллмана для генерации ключа и блочный шифр.
2. Разработать программу обмена зашифрованными файлами по сети между двумя пользователями. Использовать протокол MQV для генерации ключа и потоковый шифр.
3. Разработать программу передачи управляющих команд по сети между двумя узлами. Использовать протокол Диффи-Хеллмана для генерации ключа и блочный шифр. Предусмотреть защиту от атаки повторения.
4. Разработать программу передачи управляющих команд по сети между двумя узлами. Использовать протокол MQV для генерации ключа и хэш-функцию. Предусмотреть защиту от атаки повторения.
5. Провести сравнительный анализ по быстродействию для выбранных блочных и потоковых шифров.

Экзаменационный билет содержит 4 вопроса (задачи) – 2 вопроса по компетенции ПК-8 и 2 вопроса по компетенции ПК-13. Примеры вопросов приведены в разд. 4.1.

Темы для подготовки к экзамену:

- Понятие мультипликативной группы в простом поле. Генератор группы. Примеры криптографических алгоритмов в мультипликативной группе.
- Понятие циклической подгруппы в простом поле. Построение циклических подгрупп простого порядка. Примеры криптографических алгоритмов в циклической подгруппе.
- Протокол Диффи-Хеллмана в циклической подгруппе.
- Протокол MQV.
- Бинарные поля. Понятия неприводимых и примитивных многочленов.
- Операции сложения и умножения в бинарных полях.
- Шифр "Кузнечик". Преобразования
- Шифр "Кузнечик". Оптимизация скорости зашифрования с помощью таблиц.
- Шифр "Кузнечик". Оптимизация скорости расшифрования с помощью таблиц.
- Криптографическая функция Стрибог. Общая характеристика и используемые элементарные операции.
- Криптографическая функция Стрибог. Линейные и нелинейные преобразования.
- Криптографическая функция Стрибог. Процедура вычисления.
- Криптографическая функция Keccak. Общая характеристика и используемые элементарные операции.
- Криптографическая функция Keccak. Конструкция "губка".
- Потоковый шифр HC-218. Общая характеристика, основные операции и внутренние структуры.
- Потоковый шифр HC-218. Алгоритм.
- Потоковый шифр Salsa. Общая характеристика, основные операции и внутренние структуры.
- Потоковый шифр Salsa. . Алгоритм.
- Потоковый шифр Rabbit. Общая характеристика, основные операции и внутренние структуры.
- Потоковый шифр Rabbit. Алгоритм.
- Потоковый шифр Sosemanuk. Общая характеристика, основные операции и внутренние структуры.
- Общая характеристика библиотеки GMP: целочисленные функции.

Задачи:

- С помощью функций библиотеки GMP сгенерировать два простых числа p (1024 бита) и q (256 бит), таких что $p = bq + 1$.
- С помощью функций библиотеки GMP вычислить $y = g^x b^k \bmod p$.
- С помощью функций библиотеки GMP сформировать случайное число заданного размера.
- С помощью функций библиотеки GMP вывести в файл в двоичном виде заданное большое число.