Новейшие технологии защиты информации

Список вопросов для зачета

Ревизия: 0.1

Последняя модификация: Vlad Kovtun

Дата последней модификации: 05.01.2010 12:29:00

История изменений

10.11.2009 – Версия 0.1. Первичный документ. Владислав Ковтун

Содержание

Список вопросов

Тема 1

Лекция 1

Разведка

Смысла разведки. Методы ведения разведки. Характеристики разведки. Виды информации по ограничению доступа. Виды разведки. Виды представления информации в терминах разведки.

Каналы распространения информации

Формальные и неформальные каналы распространения. Способы НСД к источникам. Комплексная защита информации включает меры … Принципы создания СЗИ. Источники утечки информации.

Каналы несанкционированного получения информации

Паразитная связь. Технические каналы утечки. Основные источники технических каналов утечки информации и их типы. Причины образования технических каналов утечки информации. Источники образования технических каналов утечки информации. Информационные характеристики канала.

Защита информации на уровне государства

Основные причины защиты информации в АСОИ. Основные руководящие документы в Украине. Информация. Защита информации. Безопасность АСОИ. Санкционированный и несанкционированный доступ. Разграничение доступа. Конфиденциальность данных. Субъект и объект АСОИ. Целостность. Угроза безопасности АСОИ. Случайные и преднамеренные угрозы. Уязвимость АСОИ. Атака. Безопасная (защищенная) система. Комплекс средств защиты. Политика безопасности. Подходы к обеспечению защиты информации в АСОИ. Система защита информации АСОИ. Мероприятия по обеспечению безопасности АСОИ. Безопасность информации. Обеспечение безопасности информации. Криптографическое преобразование информации. Криптографическая защита информации. Криптографическая система. Средства КЗИ. Ключевые данные. Услуги криптографической системы. Криптографический анализ. Информационная война. Информационная безопасность. Информационное оружие.

Криптография

Криптология. Криптография. Криптоанализ. Симметричные и ассиметричные криптосистемы. Направления в современной криптографии. Модель защищенной системы. Злоумышленник. Нарушитель. Угроза и ее виды. Угрозы криптоаналитика. Атаки криптоаналитика. Классификация систем защиты по Шеннону. Необходимое и достаточно условие теоретической недешифруемости. Расстояние единственности.

Лекция 2

Случайные числа и их генераторы

Основная сложность в реализации генератора случайных чисел. Генератор псевдослучайной последовательности. Криптографически надежная псевдослучайная последовательность. Генератор случайной последовательности. Структура генератора ключевой последовательности. Генераторы реализованные в компиляторах языков высокого уровня. Линейный конгруэнтный генератор. Линейный регистр с обратной связью. Модифицированный линейный регистр с обратной связью. Подходы к конструированию криптографически надежных генераторов. Примеры. Критерии, которым обязаны удовлетворять генераторы.

Статистические тесты

Пакет тестов NIST STS. Тесты Diehard.

Лекция 3.1

Симметричные криптосистемы

Гамма-шифра. Гаммирование. Стойкость шифра. Требования к псевдослучайным последовательностям. Рассеивание и перемешивание. Блочные и поточные криптосистемы. Режимы работы блочных шифров.

Шифр AES

Термины и определения: Переменные. Процедуры. Шифрование: SubBytes(), ShiftRows(), MixColumns(), AddRoundKey(), KeyExpansion(). Дешифрование. Особенности реализации.

Лекция 3.2

Шифр ГОСТ 28147-89

Термины и определения. Логика построения шифра и структура ключевой информации ГОСТа. Основной шаг криптопреобразования. Базовые циклы криптографических преобразований. Основные режимы шифрования. Замечания по архитектуре. Требования к качеству ключевой информации и источники ключей. Замечания по реализации.

Лекция 3.3

Поточные шифры

Одноразовый блокнот (шифр Вернама). Безопасность. Построение поточных шифров. Генератор потока ключей. Подходы к построению поточных шифров на основе линейных регистров сдвига с обратной связью. Синхронный поточный шифр. Положительные и отрицательные стороны синхронных шифров. Атака – вскрытие вставкой. Режим обратной связи по выходу блочного шифра. Распространение ошибки. Режим счетчика. Самосинхронизирующиеся шифры. Положительные и отрицательные стороны самосинхронизирующихся шифров. Атака – вскрытие повторной передачей. Режим обратной связи блочного шифра для реализации самосинхронизирующегося поточного шифра. Другие режимы блочных шифров: режим сцепления блоков, режим распространяющегося сцепления блоков, режим сцепления блоков с контрольной суммой, обратная связь по выходу с нелинейной функцией, прочие режимы.

Требования к поточным шифрам.

Лекция 4.1

Криптоанализ

Допущения криптоанализа. Классификация методов криптоанализа. Взлом. Условие взлома шифра. Атака на шифр. Известные атаки. Пассивные и активные атаки. Имитация и подмена. Классификация атак по необходимым ресурсам. Стойкость. Проблема современной криптографии. Относительное ожидаемое безопасное время. Стойкость ключа. Стойкость бесключевого чтения. Имитостойкость.

Теоретически стойкие криптосистемы. Доказуемо стойкие криптосистемы. Предположительно стойкие криптосистемы.

Метод полного перебора. Подходы к увеличению производительности. Ограничения применения. Атака по ключам. Частотный анализ. Методы подбора паролей.

Криптоанализ симметричных шифров

Криптоанализ блочных шифров.

Статистический метод. Реализация. Процедура статистической классификации. Расстояние единственности. Сравнение алгоритмов определения ключа.

Дифференциальный (разностный) метод. Слабое криптографическое преобразование. Дифференциал итерации цикла. Гипотеза о статической эквивалентности. Условие применения дифференциального анализа. Направления развития.

Линейный метод. Алгоритм 1 бита Мацуи.

Лекция 4.2

Методы криптоанализа поточных шифров

Методы криптоанализа поточных шифров. Уязвимые места. Направления криптоанализа поточных шифров. Подходы к анализу поточных шифров. Требования к стойким поточным шифрам. Задачи криптографических исследований (анализа) поточных шифров.

Методы криптоанализа по побочным каналам

…

Тема 2

Лекция 5.1

Ассиметричные криптосистемы

Особенности. Схема коммуникаций между множеством пользователей. Новая схема защищенной передачи информации. Шифрование, дешифрование и генерация ключей. Хранение и распределение ключей.

Криптосистема RSA

Трудноразрешимая задача, лежащая в основе криптосистемы. Генерация ключей. Шифрование. Дешифрование. Корректность. Эффективность.

Криптосистема Эль-Гамаля

Трудноразрешимая задача, лежащая в основе криптосистемы. Генерация ключей. Шифрование. Дешифрование. Корректность. Эффективность.

Однонаправленные хеш-функции

Определение. Назначение. Требования. Известные алгоритмы. Итеративная модель. Функция сжатия. Применение блочных алгоритмов симметричного шифрования для построения хеш-функций. Применение модулярной арифметики для построения хеш-функций. Алгоритмы: MD5, RIPEMD, SHA.

Лекция 5.2

Группы и конечные поля

Группа. Абелева группа. Конечное поле. Условие существования конечного поля. Классификация конечных полей применяемых в криптографии. Двоичные и простые поля (четной и нечетной характеристики). Представления полей для эффективной реализации. Арифметические операции над элементами полей.

Эллиптическая кривая

Определение. Сингулярность. Представление кривой в форме Вейерштрасса и Хассе. Основное свойство точек кривой. Групповой закон. Графическая интерпретация. Иерархия операций. Метрика операций ЭК: сложение и удвоение точек.

Лекция 5.3

Эллиптическая кривая

Аффинный и проективный базис. Основные представления кривых в аффинном базисе. Основные представления кривых в проективном базисе. Представления кривых: представление Doche-Icart-Kohel, представление Edwards, представление Hasse, представление Jacobi intersection, представление Jacobi quartics, представление Montgomery, представление Вейерштрасса.

Аффинное и проективное представление точек ЭК заданных над полями четной и нечетной характеристик: стандартное представление, представление Якоби, модифицированное представление Якоби, обобщенное представление Якоби, расширенное стандартное представление, представление Лопеса-Дахаба, расширенное представление Лопеса-Дахаба, модифицированное расширенное представление Лопеса-Дахаба, инвертирование проективное представление.

Аналогии между групповыми операциями в полях, кольцах и ЭК.

Лекция 6

Криптоанализ хеш-функций. Свойства хеш-функций. Метод коллизий. Метод встречи посредине (метод Шенкса либо метод «Больших и малых шагов») - парадокс о днях рождения. Метод Полларда.

Решение задачи факторизации. Описание. Существующие подходы. Метод Ферма: описание, сложность, положительные и отрицательные стороны. Метод Ленстры: описание, сложность, положительные и отрицательные стороны. Метод Диксона: описание, сложность, положительные и отрицательные стороны, стратегии. Метод Бриллхарта-Моррисона. Метод квадратичного решета Померанца.

Решение задачи дискретного логарифма. Описание. Сложность. Решение задачи в общем виде (для мультипликативной группы конечного поля). Метод Index-calculus: описание, сложность, положительные и отрицательные стороны. Метод Полларда: описание, сложность, положительные и отрицательные стороны.

Решение задачи дискретного логарифма в группе точек эллиптической кривой. Описание. Сложность.

Решение задачи дискретного логарифма в якобиане гиперэллиптической кривой. Описание. Сложность.

Лекция 7

Основные принципы построения системы защиты: простота, постоянство, контроль, открытость, идентификация, разделение полномочий, минимальность полномочий, надежность, обособленность, защита памяти, удобство, контроль доступа, авторизация, отчетность, доступность к исполнению, системность, наращиваемость, комплексность, адекватность, минимизация привилегий, наказуемость нарушений, экономичность, специализация, неформальность, гибкость, непрерывность.

Периоды развития системы защиты информации. Трудности реализации СЗИ. Основные правила.

Защищенность информационной системы, СЗИ. Представления защищенности.

Основные правила при организации работ по защите информации.

Требования к СЗИ. Общие требования: анализ и проектирование метода защиты, идентификация объектов, ограничение доступа, привилегии пользователей. Требования к техническому обеспечению: физические, аппаратурные, связь. Требования к документированию: протоколирование, тестирование, обработка угроз. Организационные требования: организационные, административные, процедурные. Требования к программному обеспечению: контроль доступа, безопасность данных, защита системы защиты.

Распределение тем по модулям

Модуль 1

Тема 1.

Модуль 2

Тема 2.

Билеты к модулям

Модуль 1

Вариант 1

1. Классифицируйте каналы распространения информации.

2. Дайте определения следующим терминам: криптография, криптология, криптоанализ.

3. Укажите основные сложности в реализации генератора случайных и псевдослучайных последовательностей.

4. Поясните назначение следующих функций: SubBytes(), ShiftRows(), MixColumns(), AddRoundKey(), KeyExpansion(), которые используются при реализации алгоритма шифрования AES, при выполнении шифрования.

5. Перечислите и поясните основные режимы шифрования.

6. Охарактеризуйте и опишите самосинхронизирующиеся поточные шифры. Укажите их назначение, положительные и отрицательные стороны.

7. Сформулируйте требования к стойким поточным шифрам.

8. Поясните суть пассивных и активных криптоаналитических атак.

Вариант 2

1. Классифицируйте основные способы НСД.

2. Дайте определение следующим терминам: нарушитель, угроза и ее виды.

3. Что такое генератор псевдослучайной и случайной последовательности?

4. Сформулируйте требования к псевдослучайным последовательностям.

5. Сформулируйте требования к качеству ключевой информации и источники ключей для шифра ГОСТ 28147-89.

6. Сформулируйте подходы к построению поточных шифров.

7. Опишите статистический метод криптоанализа. Дайте рекомендации для реализации.

8. Сформулируйте основные направления криптоанализа поточных шифров.

Вариант 3

1. Дайте определение АСОИ. Сформулируйте мероприятия по обеспечению безопасности АСОИ.

2. Опишите симметричные и ассиметричные криптосистемы. Их положительные и отрицательные стороны.

3. Линейный конгруэнтный генератор. Особенности реализации, положительные и отрицательные стороны.

4. Охарактеризуйте блочные и поточные криптосистемы. Их положительные и отрицательные стороны.

5. Опишите основной шаг криптопреобразования в алгоритме шифрования ГОСТ 28147-89.

6. Сформулируйте требования к поточным шифрам.

7. Опишите особенности теоретически, доказуемо и предположительно стойких криптосистем. Их положительные и отрицательные стороны.

8. Опишите основные методы криптоанализа поточных шифров.

Модуль 2

Вариант 1

1. Криптосистема RSA: трудноразрешимая задача, лежащая в основе криптосистемы; генерация ключей, шифрование/дешифрование; корректность; эффективность.

2. Определение эллиптической кривой. Метрика операций ЭК: сложение и удвоение точек.

3. Аффинный базис. Представление Дочи-Икарт-Кохеля (Doche-Ikart-Kohel), представление Хассе (Hasse), представление Вейерштрасса (Weierstrass) для полей нечетной характеристики.

4. Метод криптоанализа Index-calculus: описание, сложность, положительные и отрицательные стороны.

5. Требования к программному обеспечению: контроль доступа, безопасность данных, защита системы защиты.

Вариант 2

1. Криптосистема Эль-Гамаля: трудноразрешимая задача, лежащая в основе криптосистемы; генерация ключей; шифрование; дешифрование; корректность; эффективность.

2. Дайте следующие определения: группа; Абелева группа; конечное поле; условие существования конечного поля.

3. Проведите аналогии между групповыми операциями: в полях, кольцах и ЭК.

4. Метод криптоанализа Полларда: описание, сложность, положительные и отрицательные стороны.

5. Основные принципы построения системы защиты: простота, надежность, адекватность, неформальность, непрерывность.

Вариант 3

1. Ассиметричные криптосистемы: условия появления; особенности; преимущества и недостатки.

2. Определение эллиптической кривой. Основное свойство точек кривой. Графическая интерпретация основного свойства.

3. Представление точек эллиптической кривой в проективном базисе, для поля нечетной характеристики: уравнение в форме Вейерштраса; уравнение в форме скрещивания Якоби; уравнение в форме Хассе.

4. Метод криптоанализа: «встреча посредине».

5. Трудности реализации СЗИ. Основные правила.