Бауманский учебный центр «Специалист»

Программа курса Этичный хакинг. Специалист по шифрованию

Код курса: **СЕНШ**

Тема	Ак. часов

Модуль 1. Введение и история криптографии
 	
• Что такое криптография?
• История криптографии
• Моно-алфавитные подстановочные шифры
  ◦ Шифр Цезаря
  ◦ Шифрование Atbash
  ◦ Аффинный шифр
  ◦ Шифр ROT 13
  ◦ Шифр Scytale
  ◦ Отдельные недостатки подстановки
• Мульти-алфавитные подстановочные шифры
  ◦ Шифрование диска
  ◦ Шифр Виженера
  ▪ Шифр Виженера: Пример
  ▪ Шифр Виженера: Взлом
  ◦ Шифр Плейфера
  ◦ Шифр ADFGVX
• Гомофонная замена
• Нулевые шифры
• Книжные шифры
• Шифры Rail Fence
• Машина Enigma
 	
Практическая работа. Знакомство с инструментом CrypTool
	2

Модуль 2. Симметричная криптография и хэши
 	
• Симметричная криптография
• Теория информации
  ◦ Теоретические основы криптографии
• Принцип Керкхоффса
• Подстановка
• Транспозиция
• Бинарная математика
  ◦ Двоичное И (AND)
  ◦ Двоичное ИЛИ (OR)
  ◦ Двоичное исключающее ИЛИ (XOR)
• Блочный шифр и потоковый шифр
• Алгоритмы симметричного блочного шифрования
  ◦ Структура Фейстеля
  ◦ Несбалансированный шифр Фейстеля
  ◦ Стандарт шифрования данных (DES)
  ◦ 3DES
  ◦ Стандарт расширенного шифрования (AES)
  ▪ Общий обзор AES
  ▪ Особенности AES
  ◦ Blowfish
  ◦ Serpent
  ◦ Twofish
  ◦ Skipjack
  ◦ Международный алгоритм шифрования данных (IDEA)
  ◦ CAST
  ◦ TEA
  ◦ SHARK
• Симметричные алгоритмические методы
  ◦ Электронная кодовая книга (EBC)
  ◦ Cipher-Block Chaining (CBC)
  ◦ Распространение цепочек шифрованных блоков (PCBC)
  ◦ Обратная связь с шифрованием (CFB)
  ◦ Обратная связь вывода (OFB)
  ◦ Счетчик (CTR)
  ◦ Вектор инициализации (IV)
• Симметричные поточные шифры
  ◦ Пример симметричных поточных шифров: RC 4
  ◦ Пример симметричных потоков: FISH
  ◦ Пример симметричных поточных шифров: PIKE
• Функция хеширования
  ◦ Хэш и Соль
  ◦ Алгоритм MD5
  ◦ MD 6
  ◦ Алгоритм безопасного хэша (SHA)
  ◦ FORK-256
  ◦ RIPEMD-160
  ◦ ГОСТ
  ◦ Tiger
  ◦ MAC и HMAC
 	
Практическая работа
Использование CrypTool для изучения симметричного шифрования
Использование инструмента CryptoBench
	6

Модуль 3. Теория чисел и асимметричная криптография
 	
• Асимметричное шифрование
• Основы теории чисел
  ◦ Простые числа
  ◦ Относительно простые числа
  ◦ Функция Эйлера
  ◦ Модульные операторы
  ◦ Числа Фибоначчи
• Парадокс дней рождений
  ◦ Вероятность
  ◦ Атака
• Генерация случайных чисел
  ◦ Классификация генераторов случайных чисел
  ◦ Признаки хорошего генератора случайных чисел
  ◦ Псевдослучайная функция Наора-Рейнгольда и Вихрь Мерсенна
  ◦ Линейный конгруэнтный генератор
  ◦ Генератор случайных чисел Лемера
  ◦ Метод Фибоначчи с запаздываниями
  ◦ Алгоритм Блюм — Блюма — Шуба
  ◦ Алгоритм Yarrow
  ◦ Алгоритм Fortuna
• Диффи-Хеллман
• Rivest Shamir Adleman (RSA)
  ◦ RSA - Как это работает
  ◦ Пример RSA
• Протокол Менезес-Кью-Ванстоун (MQV)
• Алгоритм цифровой подписи
  ◦ Цифровая подпись DSA
• Эллиптические кривые
  ◦ Вариации эллиптической кривой
• Схема Эль-Гамаля
 	
Практическая работа. Использование CrypTool для изучения асимметричного шифрования
	4

Модуль 4. Применение криптографии
 	
• Стандарты FIPS
• Цифровые подписи
• Что такое цифровой сертификат?
• Цифровые сертификаты
  ◦ X.509
  ◦ Сертификаты X.509
  ◦ Содержание сертификата X.509
  ◦ Расширения сертификата X.509
• Центр сертификации (CA)
  ◦ Центр сертификации – Verisign
• Центр регистрации (RA)
• Инфраструктура открытых ключей (PKI)
• Терминология цифровых сертификатов
• Протокол серверной проверки сертификатов (SCVP)
• Управление цифровыми сертификатами
• Модели доверия
• Сертификаты и веб-серверы
• Microsoft Certificate Services
• Управление сертификатами в Windows
• Проверка подлинности (Аутентификация)
  ◦ Протокол аутентификации по паролю (PAP)
  ◦ Протокол аутентификации Shiva (S-PAP)
  ◦ Протокол аутентификации оклик-ответ (CHAP)
  ◦ Kerberos
  ▪ Компоненты системы Kerberos
  ▪ Процесс аутентификации Kerberos
• Pretty Good Privacy (PGP)
  ◦ Сертификаты PGP
• Шифрование Wi-Fi	

◦ Wired Equivalent Privacy (WEP) ◦ WPA - защищенный доступ к Wi-Fi ◦ WPA 2 • Уровень защищённых сокетов (SSL) • Протокол защиты транспортного уровня (TLS) • Виртуальные частные сети (VPN) ◦ Протокол туннелирования «точка-точка» (PPTP) ◦ Протокол туннелирования второго уровня (L2TP) ◦ VPN и IPSec ◦ VPN и SSL / TLS • Шифрующая файловая система (EFS) ◦ Принцип работы EFS ◦ Резервное копирование ключа EFS ◦ Восстановление ключа EFS • BitLocker • VeraCrypt • Типичные криптографические ошибки • Стеганография ◦ Термины стеганографии ◦ Историческая стеганография ◦ Стеганографические данные ◦ Формы стеганографии ◦ Как работает стеганография ◦ Стеганографические файловые системы ◦ Применение стеганографии • Стеганализ ◦ Стеганализ - Быстрая пара ◦ Стеганализ - Анализ Чи-Квадрата ◦ Стеганализ - Аудио Steganalysis • Средства обнаружения стеганографии • Агентство национальной безопасности и криптография ◦ Алгоритмы шифрования NSA Suite A ◦ Алгоритмы шифрования NSA Suite B ◦ Алгоритмы типа 1 ◦ Алгоритмы типа 2 ◦ Алгоритмы типа 3 ◦ Алгоритмы типа 4 • Невзламываемое шифрование **Практическая работа** Использование прикладных криптографических инструментов Использование инструментов стеганографии Обнаружение стеганографии	**8**
Модуль 5. Криптоанализ • Взлом шифров • Криптоанализ • Частотный анализ • Метод Касиски • Взлом современной криптографии ◦ Атака на основе подобранного открытого текста ◦ Атака на основе шифротекста ◦ Атака на основе связанных ключей • Линейный криптоанализ • Дифференциальный криптоанализ • Интегральный криптоанализ • Ресурсы для криптоанализа • Успехи криптоанализа • Радужные таблицы • Взлом паролей **Практическая работа.** Использование инструментов для взлома шифрования	**4**
Аудиторная нагрузка в классе с преподавателем	**24 ак.ч. + 24 ак.ч. самостоятельно**

По окончании обучения на курсе проводится итоговая аттестация. Аттестация проводится в виде теста на последнем занятии или на основании оценок практических работ, выполняемых во время обучения на курсе.

Контакты центра

Для частных лиц
+7 (495) 232-32-16

Для организаций
+7 (495) 780-48-44

E-mail
info@specialist.ru