ЗАДАНИЕ

№ вар.	**Задания**
Задание 1: выполнить ряд задач, используя функционал **CyberChef** для обработки и анализа различных типов данных и анализа их безопасности.	
1.	**Шифрование и дешифрование текста алгоритмом AES.** **Оценка эффективности и безопасности алгоритма шифрования AES.**
2.	**Анализ изображений:** - Загрузить изображение и извлечь из него метаданные с помощью операции Extract EXIF. - Проанализировать полученные метаданные на наличие конфиденциальной информации или потенциальных уязвимостей. - Оценить уровень безопасности обработанных изображений и предложить меры по защите метаданных. **Исследовать все инструменты анализа изображений**
3.	**Исследовать все инструменты анализа сетевого трафика:** - Например, анализировать HTTP-заголовок для извлечения информации о запросе. - Оценить уровень безопасности передаваемых данных и выявить потенциальные уязвимости или аномалии в сетевом трафике.
4.	**Шифрование и дешифрование текста алгоритмом шифрования RSA:** - Сгенерировать открытый и закрытый ключи RSA с помощью специальных инструментов (например, онлайн-генераторов или криптографических библиотек). - Используя открытый ключ RSA, зашифруйте текст с помощью алгоритма RSA Encrypt. Используя закрытый ключ RSA, дешифруйте текст с помощью алгоритма RSA Decrypt. - Сравните исходный текст с зашифрованным и дешифрованным текстами. - Убедитесь, что текст успешно зашифрован и дешифрован с использованием ключей RSA.
5.	**Исследование всех инструментов шифрования и дешифрования на платформе CyberChef**

Задание 2. Исследование вредоносного программного кода с использованием метода обратной разработки на платформе CyberDefenders.	
1.	**Выбор образца вредоносного кода:** - Выберите образец вредоносного программного кода для исследования. Это может быть образец известного вредоносного ПО или же образец, предоставленный на платформе CyberDefenders. https://cyberdefenders.org/blueteam-ctf-challenges/lespion/ https://cyberdefenders.org/walkthroughs/lespion/ https://cyberdefenders.org/blueteam-ctf-challenges/grabthephisher/ https://cyberdefenders.org/blueteam-ctf-challenges/amadey/ https://cyberdefenders.org/blueteam-ctf-challenges/fakegpt/ https://cyberdefenders.org/blueteam-ctf-challenges/oski/ https://cyberdefenders.org/blueteam-ctf-challenges/androidbreach/ https://cyberdefenders.org/blueteam-ctf-challenges/reveal/
2.	**Выполнение задания по инструкции**

КРАТКИЕ ТЕОРЕТИЧЕСКИЕ СВЕДЕНИЯ

Цель работы: изучить и применить инструменты CyberChef для анализа, обработки, защиты данных, а также получить навыки анализа вредоносного программного кода с использованием методов обратной разработки на платформе CyberDefenders для выявления угроз и разработки мер по их предотвращению.

1 Инструмент анализа, обработки и преобразования данных CyberChef

CyberChef — это мощный инструмент для анализа, обработки и преобразования данных в области информационной безопасности и защиты данных. Этот инструмент имеет простой и интуитивно понятный интерфейс, который позволяет выполнять различные операции над данными, такие как кодирование, декодирование, шифрование, дешифрование, анализ форматов файлов и многое другое. Он предоставляет набор различных операций и инструментов, которые можно использовать для обработки, анализа и преобразования данных, таких как текст, файлы, изображения и многое другое. Давайте разберем подробнее, как использовать CyberChef в контексте информационной безопасности и защиты данных.

1.1 Установка и запуск CyberChef

- CyberChef можно использовать как веб-приложение, открыв его в браузере, либо установив его локально.
- Для локальной установки, можно загрузить исходный код с GitHub и запустить на своем компьютере.
- Для использования в веб-браузере, достаточно открыть сайт CyberChef и начать работу.

1.2 Основные функции CyberChef

1) Операции с текстом: шифрование, дешифрование, кодирование, декодирование, поиск и замена текста и многое другое.
2) Операции с файлами: загрузка, обработка, анализ и экспорт файлов различных форматов.
3) Операции с изображениями: изменение формата, обработка, скрытие информации и др.
4) Работа с сетевыми данными: анализ HTTP-запросов, работа с URL и др.

Использования CyberChef в информационной безопасности:

1) **Шифрование и дешифрование:** CyberChef поддерживает множество алгоритмов шифрования, таких как AES, RSA, XOR и другие. Вы можете использовать его для шифрования и дешифрования текста или файлов.
2) **Анализ и обработка файлов:** CyberChef позволяет анализировать и обрабатывать различные типы файлов, включая архивы, изображения, аудио и видео файлы. Например, вы можете извлечь метаданные из изображений или анализировать содержимое файлов на наличие вредоносного кода.

3) **Работа с сетевыми данными:** CyberChef может быть полезен при анализе сетевого трафика. Вы можете декодировать и анализировать HTTP-заголовки, параметры запросов, а также осуществлять манипуляции с данными, например, изменять значения параметров.

1.3 Некоторые примеры использования CyberChef

1. **Шифрование и дешифрование текста:**

Пример задачи: У вас есть текст, который нужно зашифровать алгоритмом AES с ключом "mysecretkey".

Шаги в CyberChef:

- В CyberChef выберите операцию "AES Encrypt".
- Введите текст, который нужно зашифровать, и ключ "mysecretkey".
- Получите зашифрованный текст.

2. **Анализ изображений:**

Пример задачи: Вам нужно извлечь метаданные из изображения для получения информации о его источнике и параметрах.

Шаги в CyberChef:

- Загрузите изображение в CyberChef.
- Используйте операцию "Extract EXIF" для извлечения метаданных.
- Проанализируйте полученную информацию, такую как камера, дата съемки и т.д.

3. **Дешифрование текста с помощью XOR:**

Пример задачи: У вас есть зашифрованный текст, который был зашифрован с использованием операции XOR с ключом "secretkey".

Шаги в CyberChef:

- Выберите операцию "XOR Brute Force".
- Введите зашифрованный текст и диапазон возможных ключей для перебора (например, от 0 до 255).
- CyberChef попробует различные ключи и выдаст дешифрованный текст, когда найдет правильный ключ.

4. **Анализ трафика:**

Пример задачи: Вам нужно проанализировать HTTP-заголовки запроса для выявления потенциально вредоносных параметров.

Шаги в CyberChef:

- Скопируйте HTTP-заголовок запроса в CyberChef.
- Используйте операцию "Parse HTTP Header" для анализа заголовка и извлечения параметров.
- Проанализируйте извлеченные параметры на предмет аномалий или подозрительных значений.

5. **Шифрование и дешифрование с использованием RSA:**

Пример задачи: Вы хотите зашифровать текст с помощью алгоритма RSA с открытым и закрытым ключом.

Шаги в CyberChef:

- Создайте пару ключей RSA с помощью операции "RSA key generation".
- Используйте операцию "RSA Encrypt" для шифрования текста с использованием открытого ключа.
- Для дешифрования можно использовать операцию "RSA Decrypt" с закрытым ключом.

Каждый из этих примеров показывает, как CyberChef может быть эффективным инструментом для шифрования и дешифрования текста, анализа изображений и сетевого трафика, а также работы с различными форматами файлов в контексте информационной безопасности и защиты данных.

1.4 Оценка эффективности и безопасности алгоритмов шифрования

1.4.1 Оценка эффективности и безопасности алгоритма шифрования AES

Оценка эффективности и безопасности алгоритма шифрования AES (Advanced Encryption Standard) может быть выполнена на основе нескольких критериев и методов анализа.

1. **Криптографическая стойкость:**

- Оценка стойкости AES к криптоанализу и атакам на основе известных методов атак, таких как атаки посредством известных открытых текстов (Known-plaintext attack) или атаки посредством выбранных открытых текстов (Chosen-plaintext attack).
- Использование инструментов для криптографического анализа, таких как Cryptool, для проверки стойкости AES к известным типам атак.

2. **Скорость и производительность:**

- Измерение скорости шифрования и дешифрования данных с использованием AES на различных типах данных и размерах блоков.
- Сравнение производительности AES с другими алгоритмами шифрования для определения его эффективности в реальном времени.

3. **Уровень безопасности ключей:**

- Оценка длины ключа AES и его эффективности для защиты данных от перебора ключей методом "грубой силы" (brute force attack).
- Анализ уязвимостей и возможностей взлома ключей AES на основе известных методов криптоанализа.

4. **Распространенность использования:**

- Изучение практического применения AES в различных областях информационной безопасности и защиты данных.

- Оценка уровня поддержки и распространенности использования AES в различных криптографических библиотеках и системах безопасности.

5. **Стандартизация и нормативное регулирование:**

- Изучение стандартов и рекомендаций по использованию AES, таких как FIPS PUB 197 (Federal Information Processing Standards) и рекомендации NIST (National Institute of Standards and Technology).
- Оценка соответствия использования AES криптографическим стандартам и требованиям безопасности.

6. **Обзор исследований и анализа уязвимостей:**

- Изучение научных исследований и публикаций, посвященных анализу безопасности AES и выявлению возможных уязвимостей.
- Оценка актуальности исследований и применяемости их результатов к практической безопасности при использовании AES.

В целом, оценка эффективности и безопасности алгоритма шифрования AES требует комплексного подхода, включающего как теоретические аспекты (стойкость к криптоанализу, длина ключа), так и практические аспекты (производительность, распространенность использования, стандартизация и аудит безопасности).

1.4.2 Оценка эффективности и безопасности алгоритма шифрования RSA

Оценка эффективности и безопасности алгоритма шифрования RSA (Rivest-Shamir-Adleman) включает в себя несколько аспектов, которые можно рассмотреть для понимания его работы и надежности. Вот основные критерии, по которым можно оценить RSA:

1. **Длина ключа:**

- Оценка безопасности RSA начинается с выбора длины ключа. Обычно для RSA используются ключи длиной 2048 бит и выше. Более длинные ключи обеспечивают большую стойкость к атакам методом перебора (brute force).
- Можно провести сравнение эффективности шифрования с различными длинами ключей RSA для определения оптимальной длины ключа в конкретной ситуации.

2. **Атаки и уязвимости:**

- Оценка безопасности RSA также включает анализ известных атак на этот алгоритм, таких как атаки посредством подделанных сообщений (chosen-ciphertext attack) или атаки на основе факторизации чисел (factorization-based attacks).
- Изучение и анализ новых методов криптоанализа, направленных на обнаружение уязвимостей в алгоритме RSA.

3. **Производительность:**

- Оценка эффективности RSA также включает анализ скорости шифрования и дешифрования на различных устройствах и с разными размерами ключей.
- Сравнение производительности RSA с другими алгоритмами шифрования для определения его эффективности в различных сценариях использования.

4. **Стандартизация и поддержка:**

- Оценка степени стандартизации и поддержки RSA в криптографических библиотеках, протоколах и системах безопасности.
- Проверка соответствия использования RSA криптографическим стандартам, таким как FIPS 140-2.

5. **Исследования и практическое применение:**

- Изучение научных исследований и публикаций, посвященных анализу безопасности RSA и выявлению возможных уязвимостей.
- Анализ практического применения RSA в различных областях, таких как шифрование данных, аутентификация и цифровые подписи.

6. **Обзор стандартов и рекомендаций:**

- Изучение стандартов и рекомендаций по использованию RSA, таких как NIST SP 800-56A и PKCS #1.
- Оценка соответствия использования RSA рекомендациям по безопасности и стандартам криптографии.

7. **Комплексный анализ:**

- Наиболее полная оценка эффективности и безопасности RSA достигается путем комплексного анализа вышеописанных аспектов, а также учета специфических требований и контекста использования алгоритма.

Общий вывод о безопасности и эффективности RSA можно сделать на основе анализа вышеописанных критериев и сравнения с другими алгоритмами шифрования и криптографическими методами.

2 О платформе CyberDefenders

CyberDefenders — это платформа для обучения и соревнований в области кибербезопасности, которая предоставляет студентам и профессионалам возможность учиться и развиваться в сфере информационной безопасности.

1. **Образовательная платформа:**

CyberDefenders предоставляет образовательные материалы, курсы и тренировки, позволяющие изучать различные аспекты кибербезопасности. Эти материалы могут включать в себя видеоуроки, интерактивные задания, лабораторные работы и практические кейсы.

2. **Соревнования и практические задания:**

Платформа предлагает соревнования и практические задания, включающие в себя различные кейсы и сценарии атак, которые студенты и профессионалы могут решать для проверки своих знаний и навыков в реальных условиях.

3. **Обучение в реальном времени:**

CyberDefenders предоставляет возможность обучаться и тренироваться в реальном времени, имитируя ситуации, которые могут возникнуть в реальных кибератаках или в работе киберспециалиста.

Парная работа

4. **Разнообразные темы:**

Платформа охватывает широкий спектр тем в области кибербезопасности, таких как криптография, сетевая безопасность, анализ уязвимостей, цифровая криминалистика, машинное обучение для кибербезопасности и многое другое.

CyberDefenders также способствует формированию сообщества студентов и профессионалов в области кибербезопасности, обмену знаниями и опытом, а также сотрудничеству при решении сложных задач и кейсов.

5. **Сертификация и признание:**

Успешное прохождение курсов и соревнований на платформе может быть подтверждено сертификатами, которые признаются в индустрии кибербезопасности и могут улучшить карьерные перспективы.

Итак, CyberDefenders — это интегрированная платформа, объединяющая образование, практику, соревнования и сообщество в области кибербезопасности, предоставляющая участникам возможность изучать, тренироваться и совершенствоваться в сфере информационной безопасности.

2.1 Инструменты платформы CyberDefenders для анализа вредоносного программного кода

На платформе CyberDefenders доступно множество инструментов для анализа вредоносного программного кода.

1. IDA Pro: IDA Pro является мощным инструментом для обратной разработки и анализа бинарного кода. Он позволяет анализировать и модифицировать исполняемые файлы, разбирать бинарный код на ассемблер и исследовать его структуру.

Пример использования:

- Загрузка вредоносного исполняемого файла в IDA Pro.
- Анализ функций, структур данных и потока выполнения программы.
- Выявление вредоносных операций, обход защит и скрытых функций.

2. Ghidra: Ghidra — это бесплатный инструмент для обратной разработки, разработанный NSA. Он предоставляет возможности для анализа исполняемого кода, дизассемблирования и декомпиляции программ.

Пример использования:

- Загрузка вредоносного исполняемого файла в Ghidra.
- Анализ функций и структур программы через дизассемблирование и декомпиляцию.
- Поиск вредоносных функций, алгоритмов шифрования, внедрения в систему.

3. Wireshark: **Wireshark** — это инструмент для анализа сетевого трафика, который может быть полезен для выявления вредоносных операций связанных с сетью, таких как атаки межсетевого экрана (firewall) или утечки данных.

Парная работа

Пример использования:

- Захват сетевого трафика с помощью Wireshark во время анализа вредоносного кода.
- Анализ пакетов данных, поиск необычных или подозрительных запросов к удаленным серверам.
- Выявление атак на сетевые службы, утечки информации или аномального поведения сети.

4. YARA: YARA — это мощный инструмент для поиска и идентификации вредоносных паттернов и сигнатур в файловой системе. Он позволяет создавать правила для обнаружения вредоносных файлов на основе их характеристик.

Пример использования:

- Создание YARA-правил для обнаружения вредоносных файлов по их характеристикам, например, хеш-суммам, строкам кода, метаданным и другим параметрам.
- Применение YARA-правил к файловой системе для обнаружения подозрительных файлов.
- Анализ и классификация вредоносных файлов на основе YARA-правил.

Эти инструменты являются лишь некоторыми из множества доступных на платформе CyberDefenders и предоставляют разнообразные возможности для анализа и исследования вредоносного программного кода.

Список литературы

1. Омассон Ж.-Ф. О криптографии всерьез / пер. с англ. А. А. Слинкина. – М.: ДМК Пресс, 2021. – 328 с.: ил.
2. Розенбаум Калле, Грокаем технологию Биткоин. — СПб.: Питер, 2020. — 496 с.: ил. — (Серия «IT для бизнеса»).
3. Свейгарт, Эл Криптография и взлом шифров на Python. : Пер. с англ. - СПб. : ООО" Диалектика", 2020. - 512 с. - Парал. тит. англ.