Задачи по курсу «Основы криптографии»

1. **Шифр Цезаря**:
   - Реализовать алгоритм шифрования и расшифровки с использованием сдвига символов в алфавите.
   - Модифицировать шифр Цезаря с ключом, который меняется на основе текста.
2. **Шифр Виженера**:
   - Реализовать алгоритм шифрования и расшифровки с использованием ключевого слова для полиалфавитного шифрования.
   - Реализовать анализ частоты для взлома шифра Виженера.
3. **Метод Эль-Гамаля**:
   - Реализовать алгоритм шифрования и расшифровки на основе алгебры конечных полей.
   - Исследовать безопасность метода Эль-Гамаля, используя атаки на малые значения ключей.
4. **RSA-шифрование**:
   - Реализовать генерацию открытого и закрытого ключей с использованием простых чисел.
   - Реализовать шифрование и расшифровку с использованием алгоритма RSA.
   - Изучить безопасность RSA и провести атаки, такие как факторизация простых чисел.
5. **Алгоритм Диффи-Хеллмана для обмена ключами**:
   - Реализовать алгоритм для безопасного обмена ключами через небезопасный канал связи.
   - Исследовать проблемы, связанные с криптоанализом и уязвимостями алгоритма.
6. **Цифровые подписи**:
   - Реализовать алгоритм для создания и проверки цифровых подписей с использованием хеширования и алгоритмов, таких как RSA.
   - Исследовать методы проверки подлинности сообщений с использованием подписей.
7. **Хеш-функции (SHA, MD5)**:
   - Реализовать и сравнить различные хеш-функции для проверки целостности данных.
   - Изучить уязвимости, связанные с хеш-функциями (например, коллизии).
8. **Алгоритм Шенона-Фано для сжатия данных**:
   - Реализовать алгоритм Шенона-Фано для эффективного сжатия данных.
   - Изучить методы, такие как кодирование Хаффмана, для сжатия и защиты данных.
9. **Алгоритм Эдвардса для эллиптической криптографии (ECC)**:
   - Реализовать криптографические операции с эллиптическими кривыми.
   - Исследовать преимущества и безопасность ECC по сравнению с RSA.
10. **Атака на криптосистемы**:
    - Реализовать различные методы криптоанализа (например, атаки с полным перебором, атаки на основе анализа частоты).
    - Провести атаку на простые шифры, такие как шифр Цезаря и шифр Виженера.
11. **Протоколы аутентификации**:
    - Реализовать алгоритмы аутентификации и защиты сообщений с использованием симметричного и асимметричного шифрования.
    - Изучить и реализовать протоколы, такие как протокол аутентификации с использованием цифровых подписей и публичных ключей.