Отчет по выполненной работе по дисциплине “Технологии и методы программирования”

1. Введение

В современном цифровом мире безопасность информации приобретает всё большую значимость. Методы шифрования, хеширования, численные методы и стеганография играют ключевую роль в обеспечении конфиденциальности, целостности и доступности данных.

1. **Шифрование** позволяет преобразовать информацию в форму, недоступную для неавторизованных лиц, обеспечивая конфиденциальность данных.
2. **Хеширование** используется для проверки целостности данных и хранения паролей, создавая уникальные отпечатки информации.
3. **Численные методы**, такие как метод хорд, применяются для решения уравнений, что важно в различных инженерных и научных задачах.
4. **Стеганография** предоставляет возможность скрытого обмена информацией, встраивая сообщения в медиафайлы без заметных изменений.

В данном отчете рассматриваются следующие технологии:

1. **DES (Data Encryption Standard)** — симметричный блочный шифр.
2. **SHA-384** — криптографическая хеш-функция из семейства SHA-2.
3. **Метод хорд** — численный метод для решения нелинейных уравнений.
4. **Внедрение сообщений в изображения** — метод стеганографии, основанный на модификации наименее значимых битов (LSB).

Актуальность темы обусловлена необходимостью защиты данных при передаче и хранении, а также потребностью в скрытом обмене информацией в условиях растущих угроз кибербезопасности.

2. Теоретическая часть

2.1. DES (Data Encryption Standard)

Описание:

DES — симметричный блочный шифр, разработанный в 1970-х годах компанией IBM и принятый в качестве стандарта шифрования данных. Он обрабатывает данные блоками по 64 бита, используя ключ длиной 56 бит.

Принцип работы:

1. **Начальная перестановка (Initial Permutation):** входной 64-битный блок подвергается перестановке битов.
2. **16 раундов шифрования:** каждый раунд включает разделение блока на две половины, применение функции Feistel, использование подключей и перестановок.
3. **Конечная перестановка (Final Permutation):** обратная начальной перестановке, применяется к объединённому блоку после всех раундов.

DES обеспечивает базовый уровень безопасности, однако в современных условиях считается устаревшим из-за ограниченной длины ключа, что делает его уязвимым для атак методом полного перебора .

2.2. SHA-384

Описание:

SHA-384 — криптографическая хеш-функция из семейства SHA-2, разработанная Национальным агентством безопасности США (NSA). Она генерирует 384-битный хеш из входных данных произвольной длины.

Принцип работы:

1. **Предобработка:** включает добавление битов для выравнивания длины сообщения и добавление длины исходного сообщения.
2. **Инициализация:** установка начальных значений хеш-регистров.
3. **Основной цикл:** обработка сообщения блоками по 1024 бита с использованием функций побитовых операций, сложения и логических функций.
4. **Вывод:** объединение конечных значений регистров для получения итогового хеша.

SHA-384 обеспечивает высокий уровень безопасности и широко используется для проверки целостности данных и цифровых подписей .

2.3. Метод хорд

Описание:

Метод хорд — численный метод для нахождения корней нелинейных уравнений. Он основан на приближении функции прямой линией (хордой) между двумя точками и нахождении её пересечения с осью абсцисс.

Принцип работы:

1. Выбираются две начальные точки x_0 и x_1, такие что f(x_0) и f(x_1) имеют противоположные знаки.
2. Вычисляется новая точка x_2 по формуле:
   x_2 = x_1 - \frac{f(x_1)(x_1 - x_0)}{f(x_1) - f(x_0)}
3. Процесс повторяется, заменяя одну из точек на x_2, до достижения заданной точности.

Метод хорд является простым в реализации и эффективным при наличии хороших начальных приближений .

2.4. Внедрение сообщений в изображения (LSB-стеганография)

Описание:

LSB-стеганография — метод скрытия информации в цифровых изображениях путём замены наименее значимых битов пикселей на биты сообщения.

Принцип работы:

1. Каждому пикселю изображения соответствует набор битов, определяющих его цвет.
2. Наименее значимый бит (LSB) каждого пикселя заменяется битом скрытого сообщения.
3. Изменения минимальны и не воспринимаются человеческим глазом, что обеспечивает скрытность передачи информации.

Этот метод широко используется для скрытой передачи данных и может быть реализован с помощью различных инструментов и языков программирования .

3. Заключение

В ходе работы были рассмотрены и реализованы ключевые методы обеспечения информационной безопасности:

1. **DES** продемонстрировал основы симметричного шифрования, несмотря на устаревание в современных условиях.
2. **SHA-384** показал эффективность хеширования для проверки целостности данных.
3. **Метод хорд** подтвердил свою применимость в решении нелинейных уравнений.
4. **Стеганография** продемонстрировала возможности скрытой передачи информации без заметных изменений в изображениях.

Эти методы находят широкое применение в различных областях: от защиты персональных данных и обеспечения безопасности коммуникаций до решения инженерных задач и создания скрытых каналов связи. Изучение и реализация данных технологий способствуют повышению уровня знаний в области информационной безопасности и программирования.