Министерство образования Республики Беларусь

Учреждение образования “Белорусский государственный университет информатики и радиоэлектроники”

Факультет информационных технологий и управления

Кафедра интеллектуальных информационных технологий

Дисциплина: Средства и методы защиты информации в интеллектуальных системах

Отчёт к лабораторной работе №2

Выполнил: Потоцкий Д.А.

Группа: 221702

Проверила: Крищенович В.А.

Минск 2024

Лабораторная работа №2

Генерация паролей

**Задание:**

1) Реализовать в виде программы шифр (зашифрование и расшифрование) в соответствии с вариантом. Язык исходного текста русский или английский по выбору исполнителя.

2) Реализовать в виде программы атаку полным перебором ключа,

используя для оценки правильности выбора ключа визуальный метод или исходный текст для автоматического сравнения результата дешифрования.

3) Оценить криптографическую стойкость реализованного шифра.

4) Предложить варианты усложнения шифра. Предложенные варианты оформить в виде алгоритма.

**Вариант 4**

Вариант шифра: Шифр Цезаря.

**Описание шифра:**

Шифр Цезаря — это один из самых простых и известных методов шифрования. Он работает путем замены каждой буквы текста на другую букву, сдвинутую в алфавите на фиксированное количество позиций.

**Принцип работы:**

1)Алфавит: Для английского языка алфавит содержит 26 букв (A-Z).

2)Сдвиг (ключ): Шифр использует фиксированное число — ключ, который определяет, на сколько позиций в алфавите каждая буква должна быть сдвинута. Например, если ключ равен 3, каждая буква исходного текста будет заменена на третью букву после неё в алфавите.

3)Шифрование: Каждая буква исходного текста сдвигается на заданное количество позиций вправо (по алфавиту).

**Описание основных функций программы:**

**1)String encrypt(String text, int shift)**

Метод encrypt зашифровывает текст с заданным сдвигом

**2)String decrypt(String text, int shift)**

Метод decrypt расшифровывает текст, используя обратный сдвиг. **3)void bruteForceAttack(String encryptedText, String originalText)**

Метод bruteForceAttack пытается перебрать все возможные ключи от 0 до 25 и автоматически сравнивает результат с исходным текстом, чтобы найти правильный ключ.

**Криптографическая стойкость:** Шифр Цезаря обладает крайне низкой криптографической стойкостью по следующим причинам:

1. **Малое количество ключей**: Для английского алфавита есть только 26 возможных ключей (для сдвигов от 0 до 25). Это означает, что злоумышленнику достаточно перебрать все ключи, что можно сделать за очень короткое время. Такой метод называется атакой полным перебором, и он легко применим к шифру Цезаря.
2. **Отсутствие зависимости от статистики языка**: Поскольку шифр Цезаря не изменяет структуру текста, сохраняется частотность букв в языке. Например, наиболее частая буква в английском — "E". Это позволяет легко применить частотный анализ: проанализировав распределение букв в зашифрованном тексте, можно угадать ключ.
3. **Детерминированность**: Один и тот же символ всегда шифруется одинаково, что делает шифр уязвимым к простым шаблонным атакам. Если в тексте встречается повторяющийся символ, после шифрования он будет также повторяться, что может быть замечено злоумышленником.
4. **Известные уязвимости**: Шифр Цезаря — это классический метод, который изучался в криптографии сотни лет. Его слабости хорошо известны, и существуют стандартные методы его взлома.

Для повышения стойкости шифра можно предложить следующие усовершенствование: **Шифр Цезаря с двойной перестановкой (**добавление второго шифрования с другим сдвигом поверх первого, чтобы усложнить дешифровку методом полного перебора).

**Алгоритм двойного шифрования**:

1. Зафиксировать два ключа (сдвига).
2. Выполнить шифрование исходного текста с первым ключом.
3. Результат шифрования зашифровать еще раз с другим ключом.
4. Для расшифровки нужно выполнить две обратные операции с обоими ключами.