Лабораторная работа № 4
РЕЖИМЫ РАБОТЫ БЛОЧНЫХ ШИФРОВ

Цель работы

Изучить режимы работы блочных шифров и их применение.

Методические указания

Режим шифрования - это алгоритм применения блочного шифра, который позволяет преобразовывать открытый текст произвольной длины в шифротекст, а затем выполнить обратное преобразование. Сам блочный шифр при этом является частью другого алгоритма – алгоритма режима шифрования. Это обусловлено тем, что блочный шифр работает только с отдельным *блоком* данных, в то время как алгоритм *режима шифрования* имеет дело уже с целым *сообщением*, которое может иметь произвольную длину и состоять из любого числа блоков.

Основные режимы шифрования:

1) ECB (Electronic Code Book) – электронная кодовая книга;
2) CBC (Cipher Block Chaining) – сцепление шифрованных блоков;
3) CFB (Cipher Feed Back) – шифрованная обратная связь;
4) OFB (Output Feed Back) – обратная связь по выходу алгоритма шифрования;
5) CTR (Counter) – шифрование со счётчиком.

Режимы работы блочных шифров были разработаны для стандарта DES.

В настоящее время эти режимы применяются для любых симметричных блочных шифров.

Существуют международные стандарты ИСО/МЭК 10116:2006 «Информационные технологии. Методы обеспечения безопасности. Режимы работы для n-битовых блочных шифров» (ISO/IEC 10116:2006 Information technology - Security techniques - Modes of operation for an n-bit block cipher).

Режимы, в которых функция шифрования применяется в алгоритме режима после суммирования с блоком открытого текста называют блочными.

К блочным относятся режимы:

1) ECB;
2) CBC.

Режимы, в которых функция шифрования применяется до суммирования с блоком открытого текста называют поточными.

К поточным относятся режимы:

1) CFB;
2) OFB;
3) CTR.

Задания на лабораторную работу

1. Привести схему и уравнения процессов шифрования и расшифрования для своего варианта задания (Взять из лекции 4).
2. Выполнить контрольный пример для своего варианта задания.

3. Написать программу шифрования и расшифрования открытого текста, состоящего из произвольного количества символов, в одном из режимов согласно варианту.

Открытый текст и ключ, а также дополнительные параметры, необходимые для режима (вектор инициализации, счетчики), вводит пользователь. Результат шифрования должен выводиться в десятичном или двоичном виде.

Варианты заданий:

1) электронной шифровальной книги;
2) сцепления шифрованных блоков;
3) шифрованной обратной связи;
4) обратной связи по выходу алгоритма шифрования;
5) шифрования со счетчиком.

Содержание отчета по лабораторной работе

1. Цель работы.
2. Схема и уравнения процессов шифрования и расшифрования для своего варианта задания
3. Описание контрольного примера для своего варианта (шифрование и расшифрование трех ASCII-символов).
4. Описание программы.
5. Листинг программы.
6. Результаты работы программы.
7. Выводы.

Контрольные вопросы

1. Что такое режим шифрования?
2. Перечислите режимы работы блочных шифров.
3. Для чего были разработаны различные режимы работы блочных шифров?
4. Какие из режимов являются блочными, какие поточными?
5. В каких случаях применяется тот или иной режим работы? Выберите из предложенных вариантов заданий те, которые могут быть использованы на практике для

а) обеспечения конфиденциальности передаваемой по сети информации произвольного размера;

б) обеспечения защиты секретных ключей;

в) обеспечения конфиденциальности поточных приложений;

г) получения криптографической контрольной суммы.

6. Охарактеризуйте преимущества и недостатки каждого из режимов работы блочных шифров.
7. В каких режимах шифрования используется вектор инициализации? Какие требования предъявляются к вектору инициализации в разных режимах? Должно ли его значение быть секретным?

8. Как ошибка в бите шифртекста или ошибка в векторе инициализации может повлиять на результат в различных режимах шифрования?