Лабораторная работа № 4
Тема: Исследование симметричных криптоалгоритмов

Цель работы: Формировать навыки шифрования данных современными блочными шифрами.
Длительность: 4 часа

Подготовка к работе

Изучить теоретический материал по конспекту лекций. Обратить особое внимание на принципы построения и характерные особенности симметричных криптографических систем; современные алгоритмыы криптографического преобразования с секретным ключом DES, ГОСТ 28147-89.

Изучить порядок выполнения лабораторной работы.

Порядок выполнения работы

1. Исследование алгоритма шифрования DES (Data Encryption Standard)

1. Использовать обучающую программу DESTutor.
2. Выполнить шифрование и дешифрование двух вариантов открытого текста (сообщений) на различных криптографических ключах по алгоритму DES в режиме "Электронной кодовой книги" (ECB –Electronic Code Book):

   а) ввести в режиме ручного ввода открытый текст для шифрования длиной 8 символов;

   б) ввести в режиме ручного ввода 64-битовый криптографический ключ для шифрования;

   в) выполнить процесс формирования раундовых 48-битовых криптографических ключей, вывести на экран дисплея исходный 64-битовый криптографический ключ и полученные раундовые 48-битовые криптографические ключи;

   г) выполнить процесс шифрования и дешифрования введенного открытого текста, получить результаты по всем этапам шифрования на экране дисплея;

   д) убедиться в корректности работы программы, правильности проведенных перестановок, замен, расширений и преобразований, сравнить первичный открытый текст с результатом дешифрования его криптограммы;

   е) повторить пункты а –д для другого открытого текста и нового криптографического ключа;

   ж) сохранить в документе отчёта по лабораторной работе открытый текст, криптографические ключи и полученные результаты по всем этапам шифрования (копии экранов).

2. Исследование стандарта шифрования ГОСТ 28147–89

1. Использовать программу Tutorial в обучающем режиме.
2. Выполнить шифрование и дешифрование двух вариантов текста на различных криптографических ключах по алгоритму ГОСТ 28147–89 в режиме простой замены:

   а) ввести в режиме ручного ввода текст для шифрования длиной не более 240 символов;

б) ввести в режиме ручного ввода 256-битовый криптографический ключ для шифрования;

в) выполнить выборку из исходного 256-битового ключа 32-х раундовых 32-битовых криптографических ключей, вывести их на экран дисплея;

г) выбрать и вывести на экран дисплея таблицу подстановки, используемую в функции шифрования;

д) выполнить процесс шифрования и дешифрования введенного открытого текста, получить результаты по всем этапам шифрования на экране дисплея;

е) убедиться в корректности работы программы и правильности проведенных преобразований, сравнить первичный открытый текст с результатом дешифрования его криптограммы;

ж) повторить пункты а –д для другого открытого текста и нового криптографического ключа;

з) сохранить в документе отчёта по лабораторной работе открытый текст, криптографические ключи и полученные результаты по всем этапам шифрования (копии экранов).