**Лабораторна робота № 1.2.**

**Лабораторна робота №2. Блочні криптосистеми типу DES**

**Мета роботи.**  Вивчити принципи роботи програм DESX та DES100. Дослідити вплив зміни паролю, розміру ключа та типу шифрованого файла.

Хiд  роботи

Програми DES100 та DESX призначені для шифрування та дешифруванння файлів.

DESlOO.exe   –   шифрувальник  –  дешифрувальник на основі DES (Data Encryption Standard). Довжина ключа змінна, обмежена ресурсами пам’яті, проте може бути задана жорстко через опцію —k. Можна спочатку на фіксовану довжину ключа запросити дамп таблиць ( – td) (таблиці \*\_s.dmp ), а потім підставити свої таблиці ( – tl). Таблиці генеруються генератором псевдовипадкових чисел з використанням заданого пароля (якщо пароль заданий – h’aaa.exe’, то паролем вважають файл ааа.ехе).

Опції:

 – *с* кодування,

 – *d* розкодовування,

 – *k* встановлення ключа фіксованої довжини,

 – *р* введення паролю,

 – *td* запитуємо дамп таблиць,

 – *tl* підставляємо свої таблиці.

Для того щоб зашифрувати файл  DES100, потрібно ввести у командну стрічку:

deslOO  – *с*  – *р*[пароль] [назва файла, що шифруватиметься (з розширенням)] [назва шифрованого файла (також з розширенням)].

**Наприклад:** deslOO  – *с*  – ppass myfile.txt myfile.cod.

Для того щоб зашифрувати файл в DESX, потрібно ввести у командний рядок:

desx  – *е* "пароль" [назва файла, що шифруватиметься (з розширенням)] [назва шифрованого файла (також з розширенням)].

**Наприклад:** desx  – e "parol" myfile.txt myfile.cod.

Для розшифрування: desx  – *e* "parol" myfile.cod myfile.txt

Система DES ґрунтується на 16 – кратному застосуванні одного і того ж самого алгоритму. Ця система є блочним алгоритмом шифрування з довжиною ключа 64 біти .

Кожну букву в алфавіті, починаючи з нуля, зіставляємо з числом. Своєю чергою, кожну цифру у двійковій системі числення подаємо у вигляді шестирозрядної послідовності нулів та одиничок.

Шифрування інформації ґрунтується на цифровому вираженні інформації і відбувається у двійковій формі. Воно являє собою операцію додавання символів за модулем числа *2*. Відкритий текст подаємо у вигляді співвідношення:  М=М 1М2МЗ...

У результаті певного перетворення за формулою С=:С1С2СЗ...одержуємо криптотекст. Загалом  для одержання блоку зашифрованого тексту необхідно 16 раундів.