

Міністерство освіти і науки України  
Львівський національний університет імені Івана Франка  
Кафедра радіоелектронного матеріалознавства

Звіт  
про виконання  
лабораторної роботи №2  
**Блочні криптосистеми типу DES**

Виконала:  
студентка групи ФЕІ - 41  
Литвин Віра

Перевірив:  
доц. Монастирський Л. С.

Львів, 2014

**Мета роботи:** вивчити принципи роботи програм DESX та DES100. Дослідити вплив зміни паролю, розміру ключа та типу шифрованого файлу.

### Хід роботи:

Створюємо і зберігаємо на диску довільного змісту текстовий файл (lab\_1.txt). Копіюємо у власну директорію файли des100.exe та desx.exe.

d:\Vira\Nowadays\!!Технології_захисту_інформації\Zvity\Lab_1\*.*			
↑Ім'я	Тип	Розмір	Дата
[..]		<Тека>	16.03.2014 17:00
des100	exe	103 086	15.01.1999 16:32
desx	exe	48 128	22.07.1999 16:32
lab_1	txt	130	16.03.2014 17:04

#### 1. Шифрування за алгоритмом des100.

Запускаємо відповідну програму і вводимо в командній стрічці наступне:

```
des100 -c -psunny lab_1.txt lab_1zs.cod
```

Отримаємо вхідний файл, зашифрований з паролем sunny. При цьому довжина ключа фіксована і становить 64 біти.

Щоб дешифрувати файл, пишемо команду

```
des100 -d -psunny lab_1zs.cod lab_1rs.txt
```

```
d:\Vira\Nowadays\!!Технології_захисту_інформації\Zvity\Lab_1>des100 -c -psunny lab_1.txt lab_1zs.cod
Encrypt launched.
Table initialized.
Key generated.

d:\Vira\Nowadays\!!Технології_захисту_інформації\Zvity\Lab_1>des100 -d -psunny lab_1zs.cod lab_1rs.txt
Encrypt launched.
Table initialized.
Key generated.
Encrypt 00%
```

DES є блочним шифратором, тобто він шифрує дані 64-бітними блоками. DES працює симетрично: для шифрування і дешифрування використовується однаковий алгоритм і ключ. Довжина ключа рівна 56 бітам. Ключ зазвичай представляється 64-бітним числом, але кожен восьмий біт використовується для перевірки парності й ігнорується. Безпека системи повністю визначається ключем.

На найпростішому рівні алгоритм є комбінацією двох основних методів шифрування: зміщення і дифузії. Фундаментальним блоком DES є застосування до тексту одиничної комбінації цих методів (підстановка, за нею - перестановка), які залежать від ключа. Такий блок називається етапом.

DES складається з 16 етапів. Після початкової перестановки 64-бітний блок розбивається на праву й ліву половини довжиною по 32 біти. Після цього виконуються 16 етапів однакових дій, в яких дані об'єднуються з ключем. Після 16-го етапу права і ліва половини об'єднуються і алгоритм завершується кінцевою перестановкою (оберненою по відношенню до початкової). На кожному етапі біти

ключа зсуваються, а потім із 56 бітів вибираються 48. Права половина даних збільшується до 48 бітів за допомогою перестановки з розширенням, об'єднується з допомогою XOR із 48 бітами зміщеного і переставленого ключа, проходить через 8 S-блоків, утворюючи 32 нових біти, і переставляється знову. Потім результат об'єднується з лівою половиною за допомогою іншого XOR. У результаті цих дій з'являється нова права половина, а стара права половина стає новою лівою. Такі дії повторюються 16 разів.

Якщо  $B_i$ - це результат і-тої ітерації,  $L_i$  і  $R_i$ - ліва і права половини ,  
 $K_i = C_i + D_i$  - 48-бітний ключ для етапу , а  $F$  - це функція, яка виконує усі  
 підстановки, перестановки і XOR із ключем, то етап можна зобразити, як

$$L_i = R_{i-1} \quad R_i = L_{i-1} \oplus F(R_{i-1}, K_i).$$

## 2. Шифрування з використанням алгоритму desx.

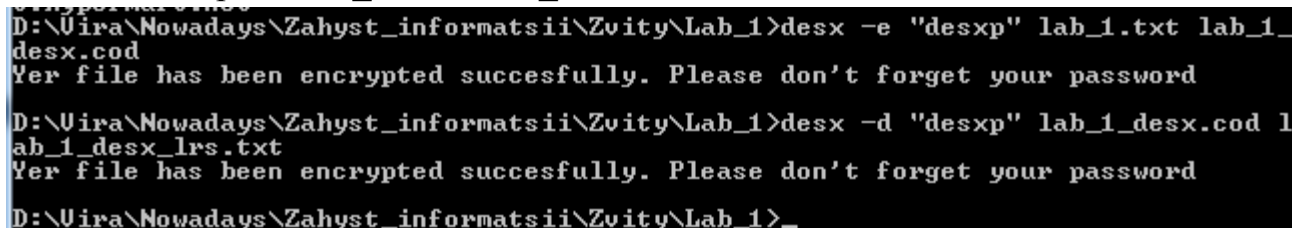
Щоб зашифрувати вхідний файл за цим алгоритмом, слід запустити відповідну програму і в консолі ввести команду:

```
desx -e "desxpass" lab_1.txt lab_1zs.cod
```

Ми зашифрували файл з паролем desxpass.

Для дешифрування вводимо у командній стрічці

```
desx -d "desxpass" lab_1zs.cod lab_1rs.txt
```



```
D:\Uira\Nowadays\Zahyst_informatsii\Zvity\Lab_1>desx -e "desxp" lab_1.txt lab_1_
desx.cod
Your file has been encrypted succesfully. Please don't forget your password
D:\Uira\Nowadays\Zahyst_informatsii\Zvity\Lab_1>desx -d "desxp" lab_1_desx.cod 1
ab_1_desx_lrs.txt
Your file has been encrypted succesfully. Please don't forget your password
D:\Uira\Nowadays\Zahyst_informatsii\Zvity\Lab_1>_
```

DESX можна визначити так

$$C = DESX_{KK_1K_2} = K_2 \oplus DES_K(K_1 \oplus M)$$

64-бітний блок повідомлення  $M$  підсумовується за mod 2 з першим «зашумлюючим» ключем  $K_1$  і потім обробляється DES-машиною з ключем  $K$ , після чого підсумовується за mod 2 з другим «зашумлюючим» ключем  $K_2$ . Загальна довжина ключа рівна  $K + K_1 + K_2 = 56 + 64 + 64 = 184$  біти.

**Висновки.** В результаті виконання роботи було досліджено алгоритми desx та des100 для шифрування текстової інформації. Розмір вхідного файлу становить 130 байт. Розмір файлу, зашифрованого за алгоритмом desx, становить 136 байти, за алгоритмом des100 – 4128 байт. При цьому обидва алгоритми застосовувались з фіксованими ключами. Для des100 це становить 64 біти, для desx – 184 біти. Алгоритм desx є значно стійкішим порівняно з des100 і майже не поступається йому у швидкодії, оскільки має всього на 2 операції XOR більше за оригінальний алгоритм. Обидва алгоритми працюють з блоками тексту розміром 64 біти.