**Міністерство освіти і науки України**

**Національний технічний університет України**

**«Київський політехнічний інститут імені Ігоря Сікорського»**

**Факультет інформатики та обчислювальної техніки**

**Кафедра обчислювальної техніки**

**Лабораторна робота №2**

з дисципліни

«Системне програмування»

на тему

«Дослідження структури програм формату COM»

Виконала: Перевірив:

студент групи ІП-93 доц. кафедри ОТ

Узунлу Гамзенур Павлов В. Г.

номер залікової книжки: 9822

Київ 2021

Код програми

.model tiny

.data

pwd db "qwerty"

start db "Insert password: ", "$"

bad db "Wrong password", "$"

good db "Узунлу Гамзенур, 9882, IP-93", "$"

inserted db 64 dup(0)

.code

.startup

mov ax, 3

int 10h

mov ah, 9

mov dx, offset start

int 21h

mov cx, 64

mov ah, 3fh

mov bx, 0

mov dx, offset inserted

int 21h

cmp ax, 8

jne \_bad

mov bp, 0

cmpSymb:

mov bl, pwd[bp]

mov bh, inserted[bp]

cmp bl, bh

jne \_bad

inc bp

cmp bp, 6

jne cmpSymb

jmp \_good

\_good:

mov ah, 9

mov dx, offset good

int 21h

ret

\_bad:

mov ah, 9

mov dx, offset bad

int 21h

ret

end

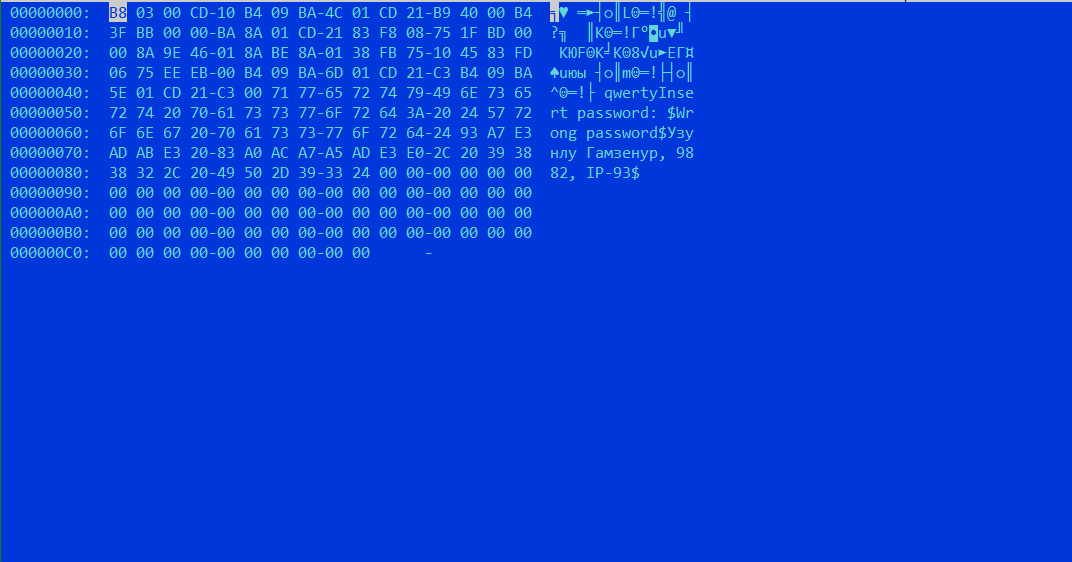
Скриншот програми

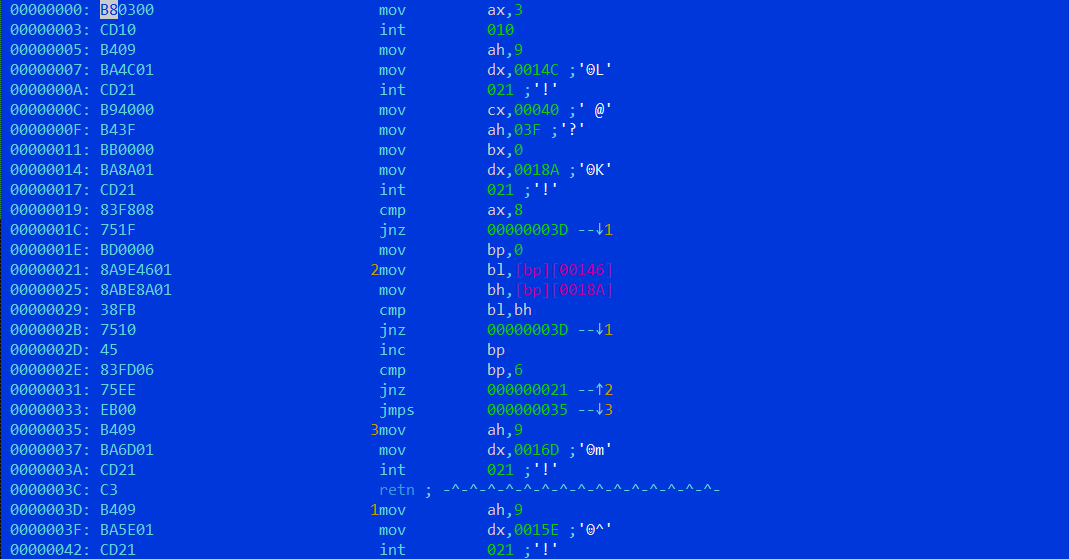




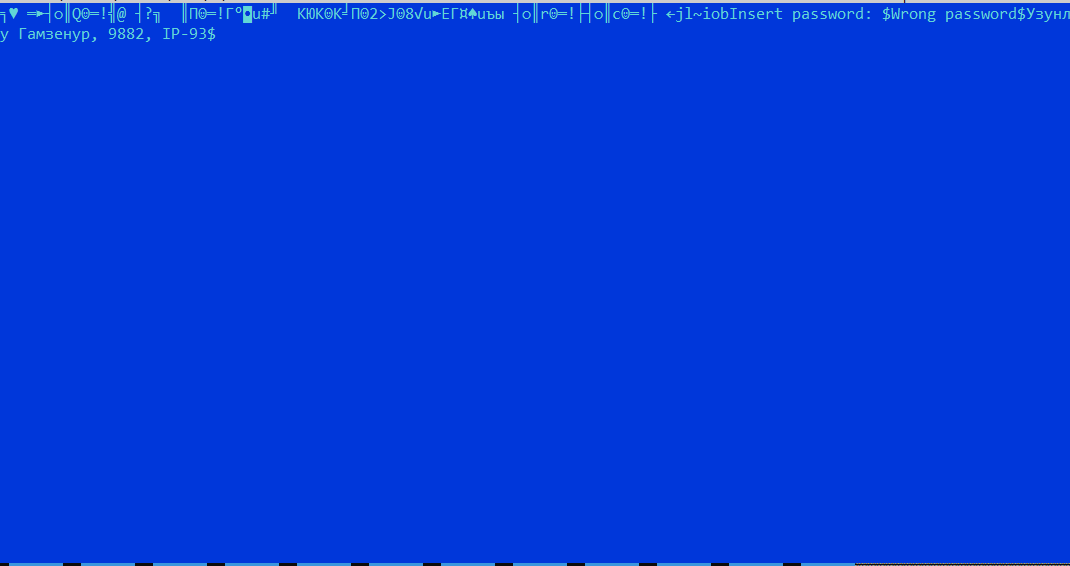
HIEW32

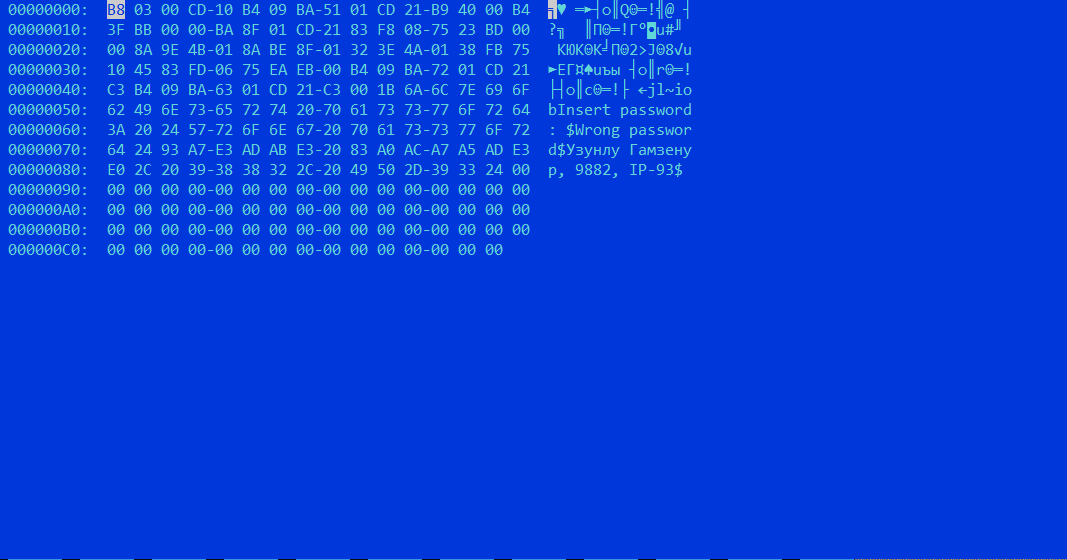


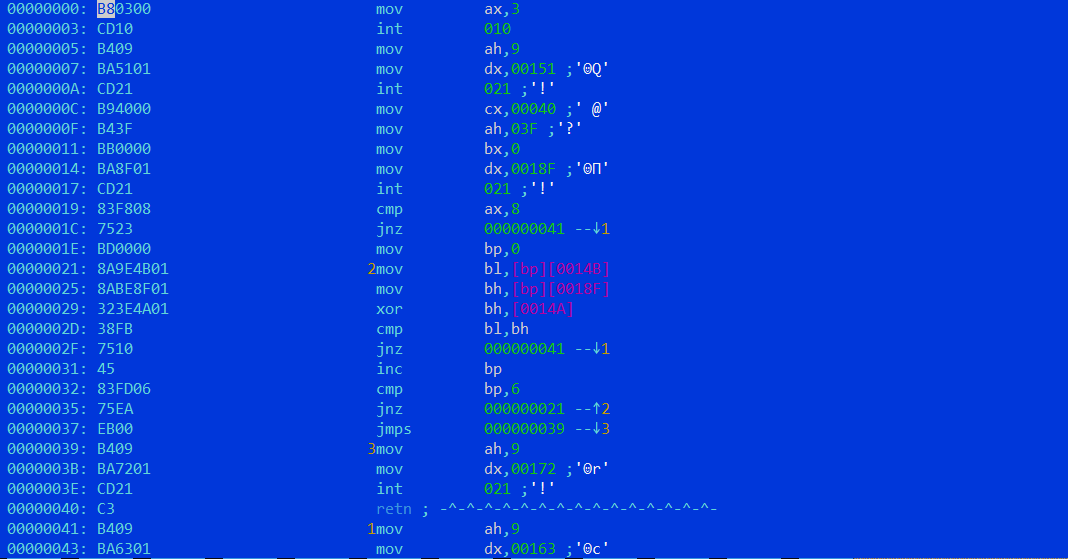




2 версія програми







Бачимо, що в першій версій програми пароль видно у вкладках TEXT та HEX. А у другій версії - він зашифрований.

Команди mov

B80300 mov ax,3

B8 - код операції

0300 - операнд

B409 mov ah,9

B4 - код операції

09 - операнд

BA5101 mov dx,00151

BA - код операції

5101 - операнд

B94000 mov cx,00040

B9 - код операції

4000 - операнд

B43F mov ah,03F

B4 - код операції

3F - операнд

BB0000 mov bx,0

BB - код операції

0000 - операнд

BA8F01 mov dx,0018F

BA - код операції

8F01 - операнд

8A9E4B01 mov bl,[bp][0014B]

8A - код операції

9E - MOD R/M

4B01 - зсув

8ABE8F01 mov bh,[bp][0018F]

8A - код операції

BE - MOD R/M

8F01 - зсув

BA7201 mov dx,00172

BA - код операції

7201 - операнд

BA6301 mov dx,00163

BA - код операції

6301 - операнд

Висновки

Було розроблено 2 програми на мові асемблер. В обох ми виводили дані при вводі правильного пароля. В другій програмі ми застосували XOR-шифрування, щоб пароль не було видно у лістингу програми.

При розробці програми було використано команди mov мови асемблеру. Їх коди було знайдено у редакторі HIEW32 у вкладці DECODE. Коди команд були виписані та розібрані по полям.