МІНІСТЕРСТВО ОБОРОНИ УКРАЇНИ

ВІЙСЬКОВИЙ ІНСТИТУТ ТЕЛЕКОМУНІКАЦІЙ ТА ІНФОРМАТИЗАЦІЇ

КАФЕДРА КІБЕРЗБЕЗПЕКИ

**ЗВІТ**

про виконання практичної роботи:

з дисципліни «Прикладна криптологія»

Дата 20.04.2024

**Виконав:** курсант 314 навчальної групи

солдат\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_Мелехов Я.Р.

**Перевiрив:** викладач кафедри 33

капітан\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ПРИЙМА О.О.

**DES** (*Data Encryption Standard*) — це симетричний алгоритм шифрування певних даних, стандарт шифрування.

Для DES рекомендовано декілька режимів:

• ECB (electronic code book) – режим «електронної кодової книги» (проста заміна);

• CBC (cipher block chaining) – режим зчеплення блоків;

• CFB (cipher feed back) - режим зворотного зв'язку за шифротекстом;

• OFB (output feed back) – режим зворотного зв'язку по виходу;

• Counter Mode (CM) — режим лічильника.

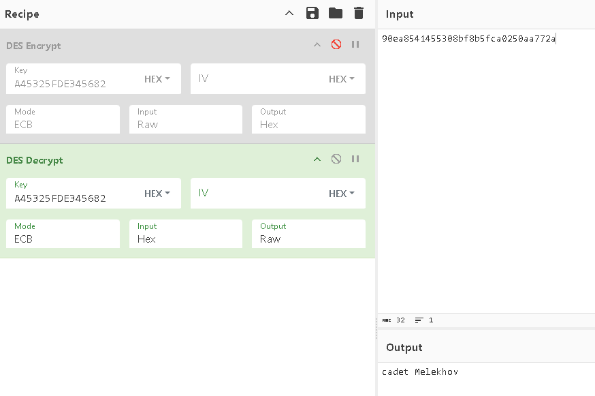
**1.MODE ECB**

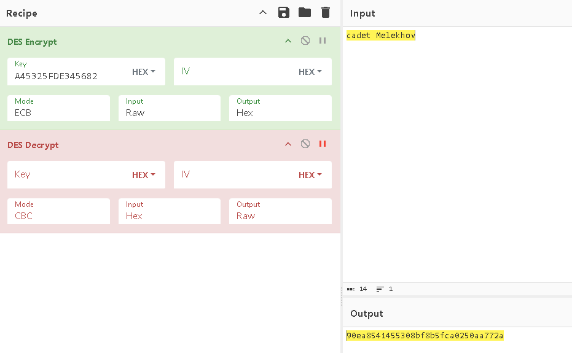
**KEY(HEX):** *A45325FDE345682*

**ВТ:** *cadet Melekhov*

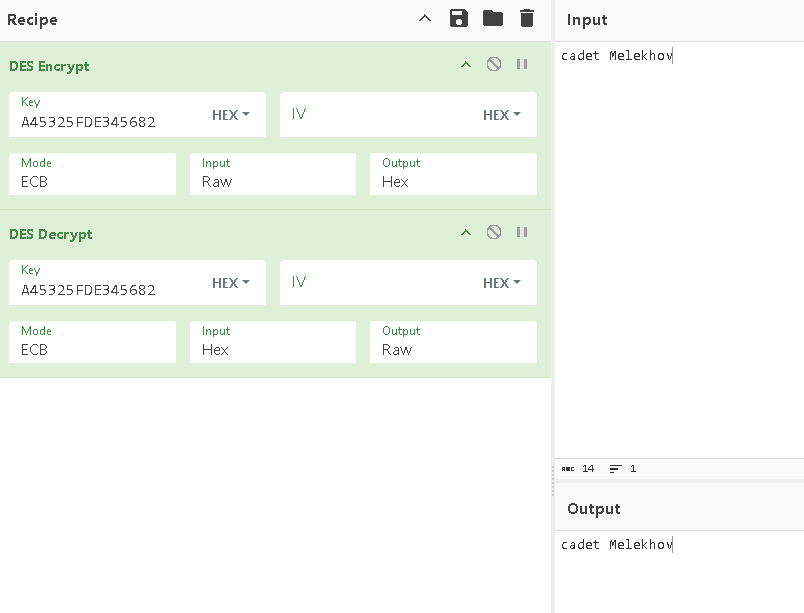
**ШТ:** *90ea8541455308bf8b5fca0250aa772a*

Encrypt Decrypt





In block



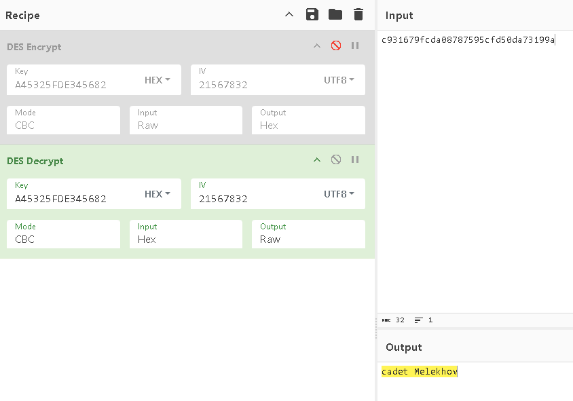
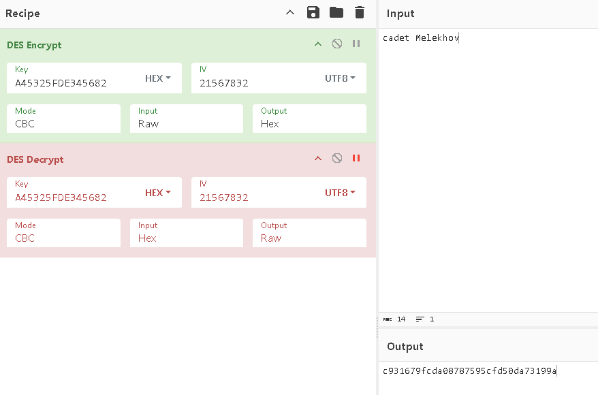
**2.MODE CBC**

**KEY(HEX):** *A45325FDE345682* **IV(UTF-8):** *21567832*

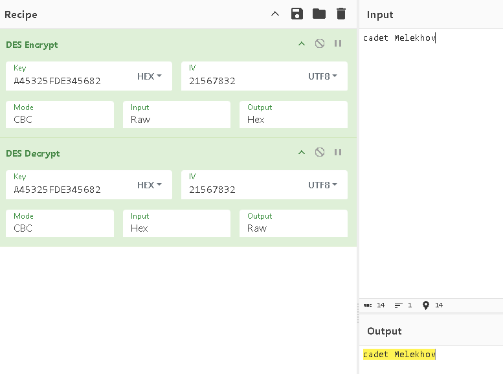
**ВТ:** *cadet Melekhov*

**ШТ:** *c931679fcda08787595cfd50da73199a*

Encrypt Decrypt



In block



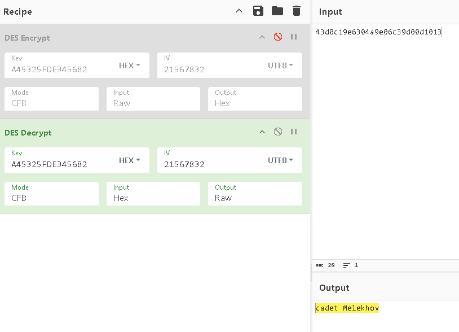
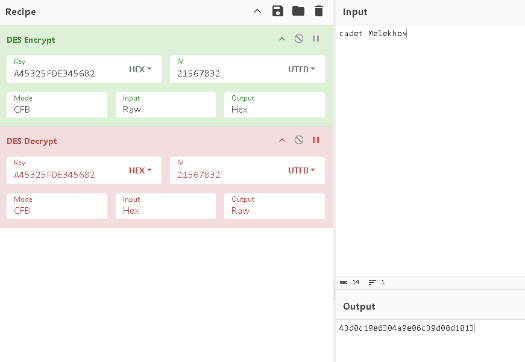
**3.MODE CFB**

**KEY(HEX):** *A45325FDE345682* **IV(UTF-8):** *21567832*

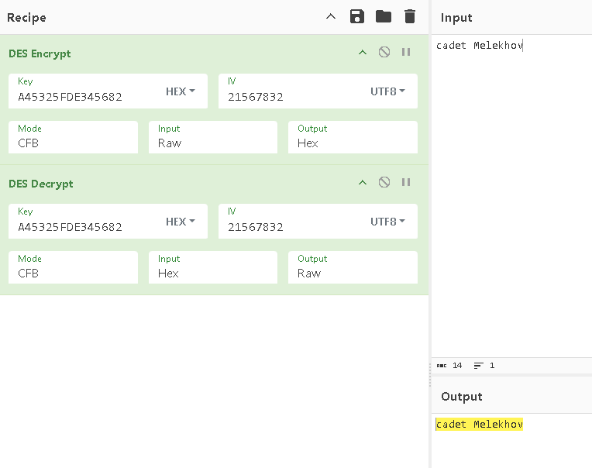
**ВТ:** *cadet Melekhov*

**ШТ:** *43d0c19e6304a9e06c39d00d1013*

Encrypt Decrypt



In block



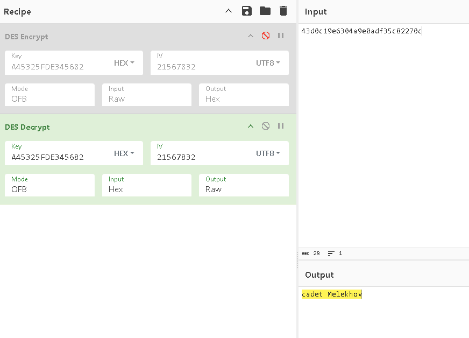
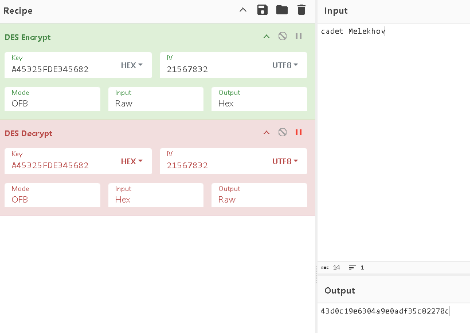
**4.MODE OFB**

**KEY(HEX):** *A45325FDE345682* **IV(UTF-8):** *21567832*

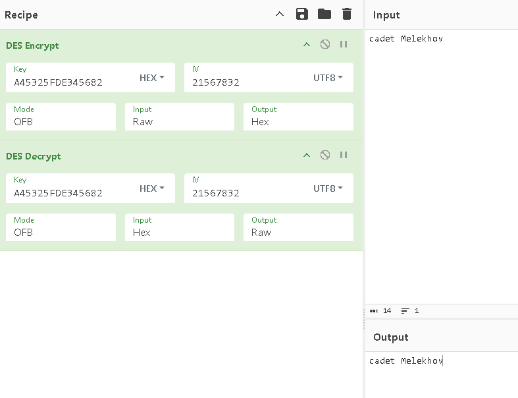
**ВТ:** *cadet Melekhov*

**ШТ:** *43d0c19e6304a9e0adf35c82270c*

Encrypt Decrypt



In block



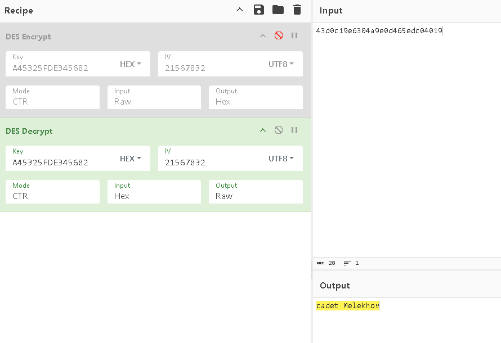
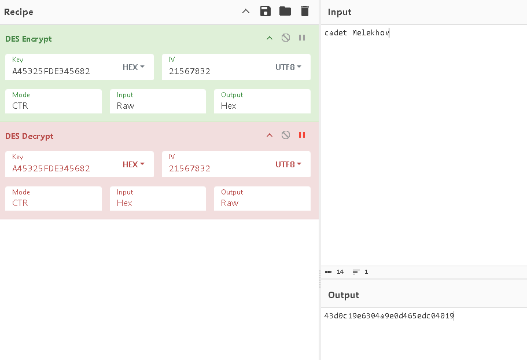
**5.MODE CTR**

**KEY(HEX):** *A45325FDE345682* **IV(UTF-8):** *21567832*

**ВТ:** *cadet Melekhov*

**ШТ:** *43d0c19e6304a9e0d465edc04019*

Encrypt Decrypt



In block

