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

старший солдат\_\_\_\_\_\_\_\_\_\_\_СІДНЕНКО Д.В.

**Перевiрив:** старший 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.

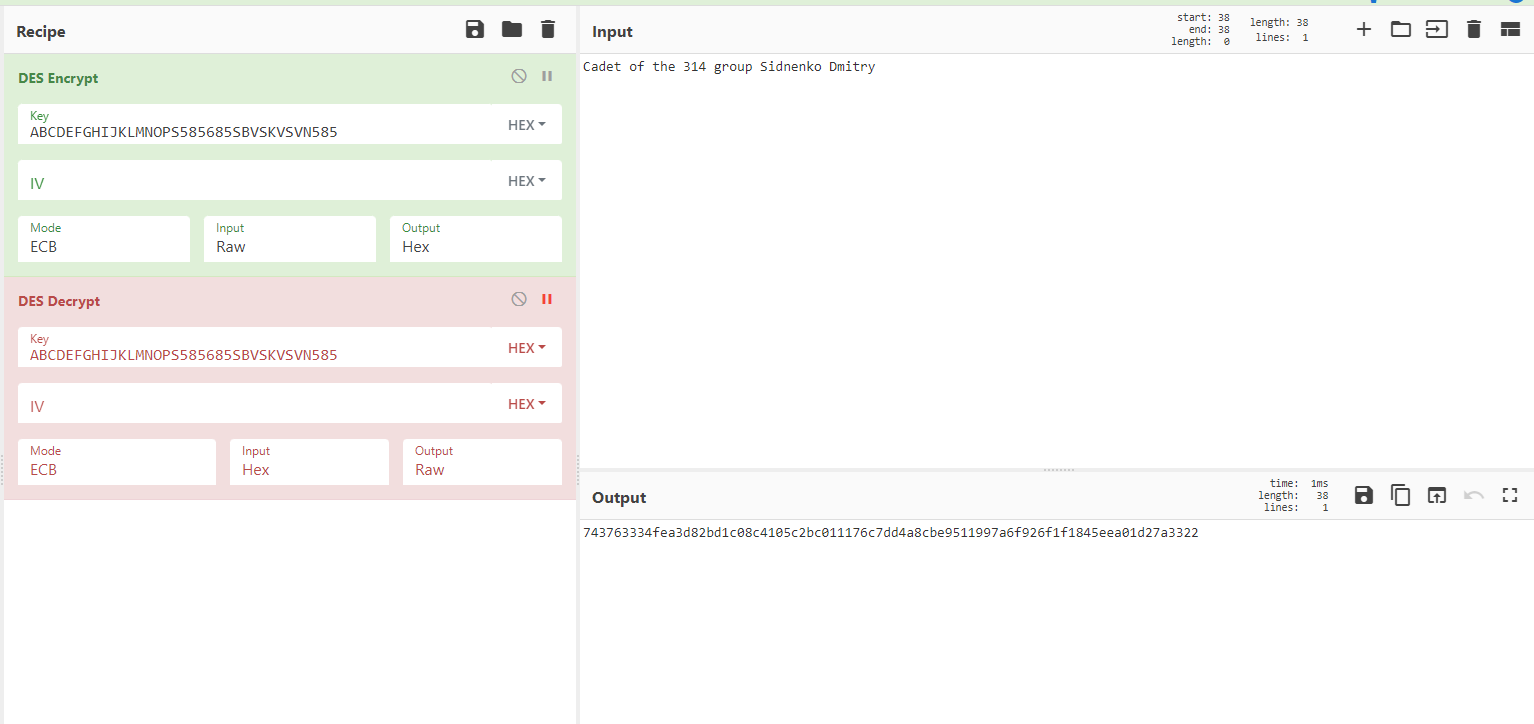
**1.MODE ECB**

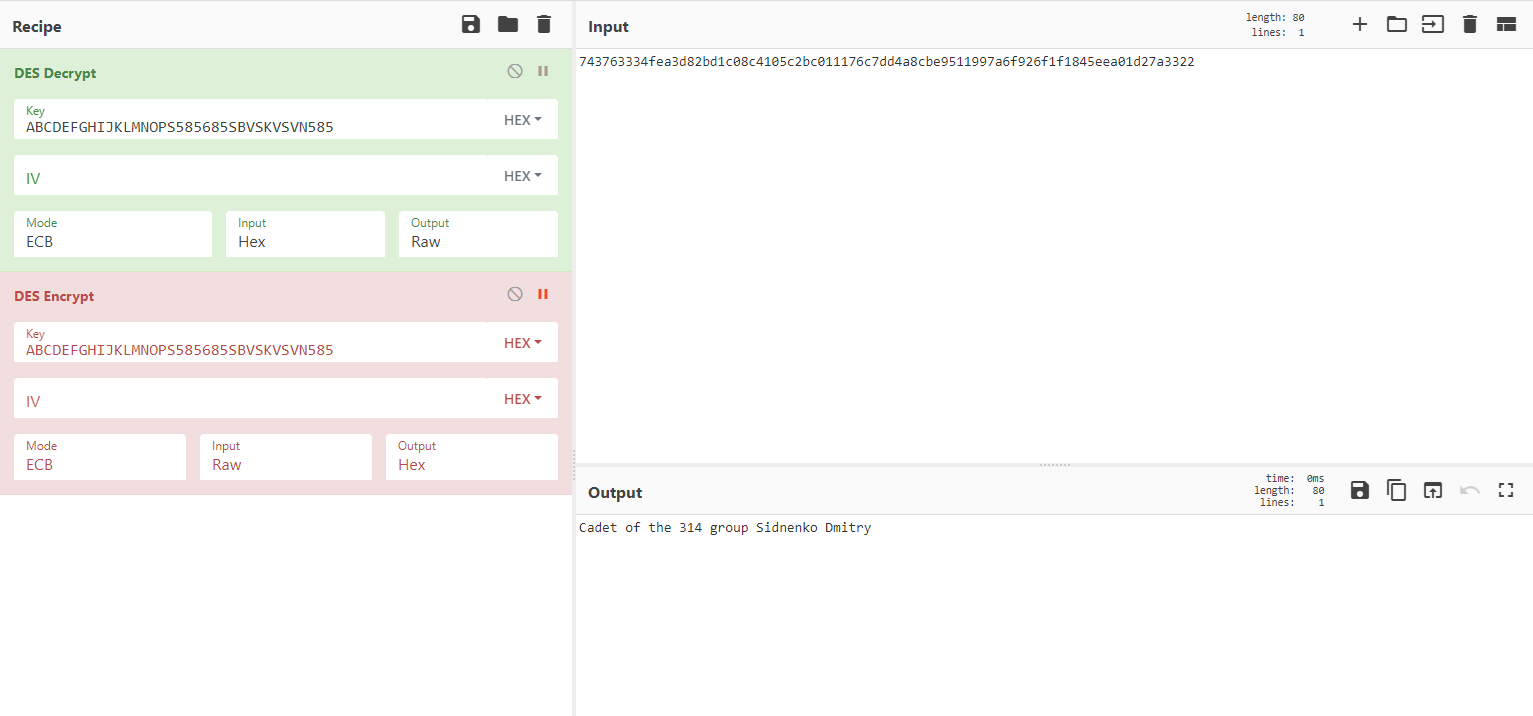
**KEY(HEX):** ABCDEFGHIJKLMNOPS585685SBVSKVSVN585

**ВТ:** *Cadet of the 314 group Sidnenko Dmitry*

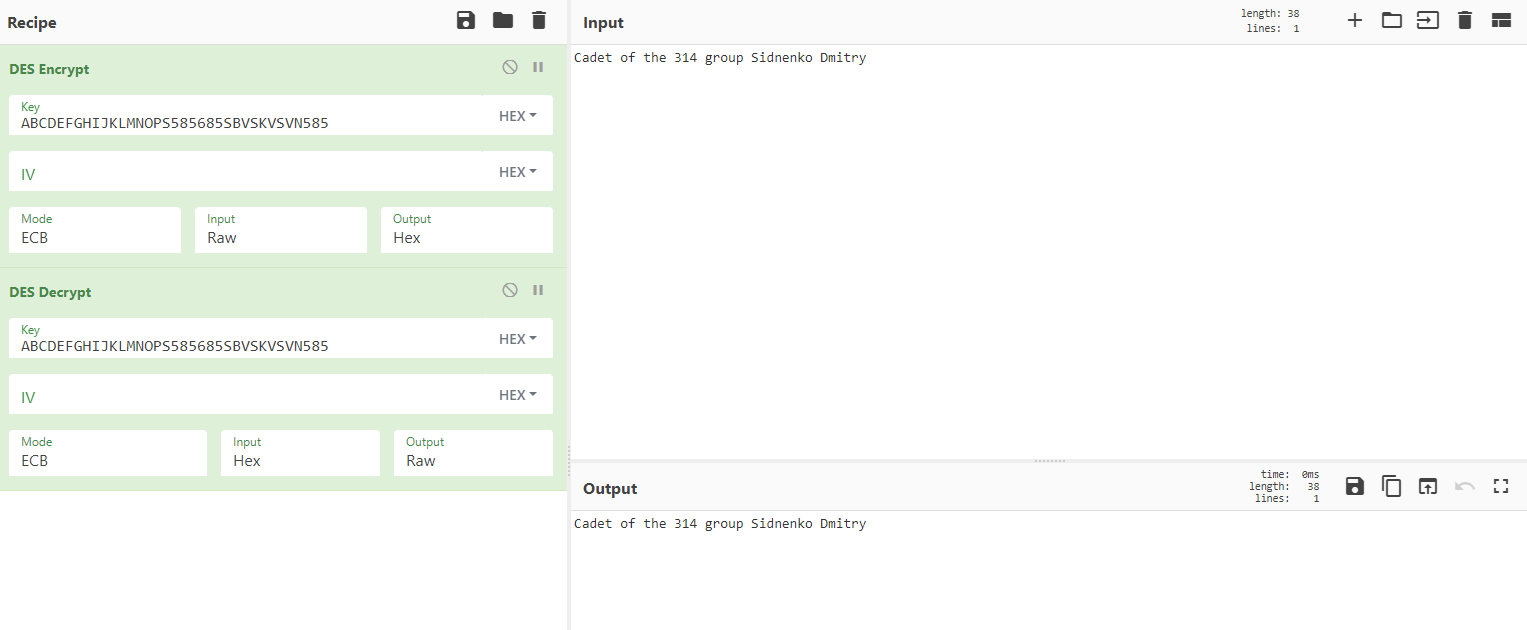
**ШТ:***743763334fea3d82bd1c08c4105c2bc011176c7dd4a8cbe9511997a6f926f1f1845eea01d27a3322*

**Encrypt**



**Decryp**

**In block**

****

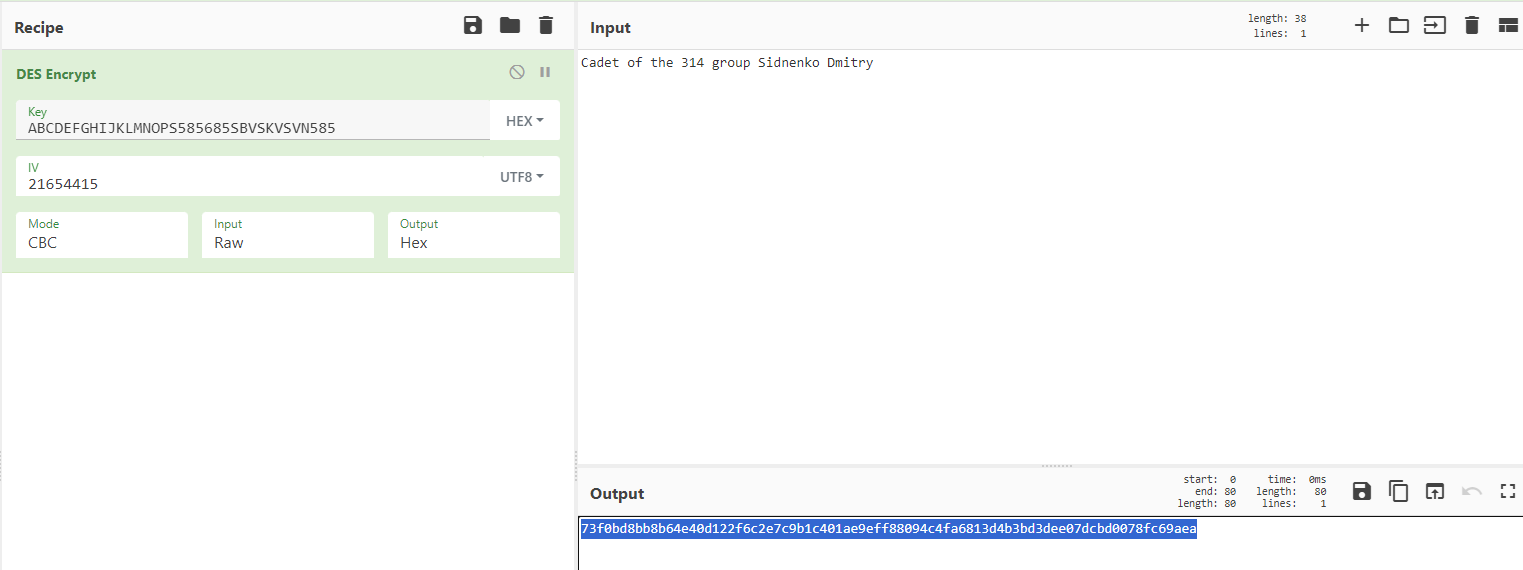
**2.MODE CBC**

**KEY(HEX):** *ABCDEFGHIJKLMNOPS585685SBVSKVSVN585* **IV(UTF-8):** *21654415*

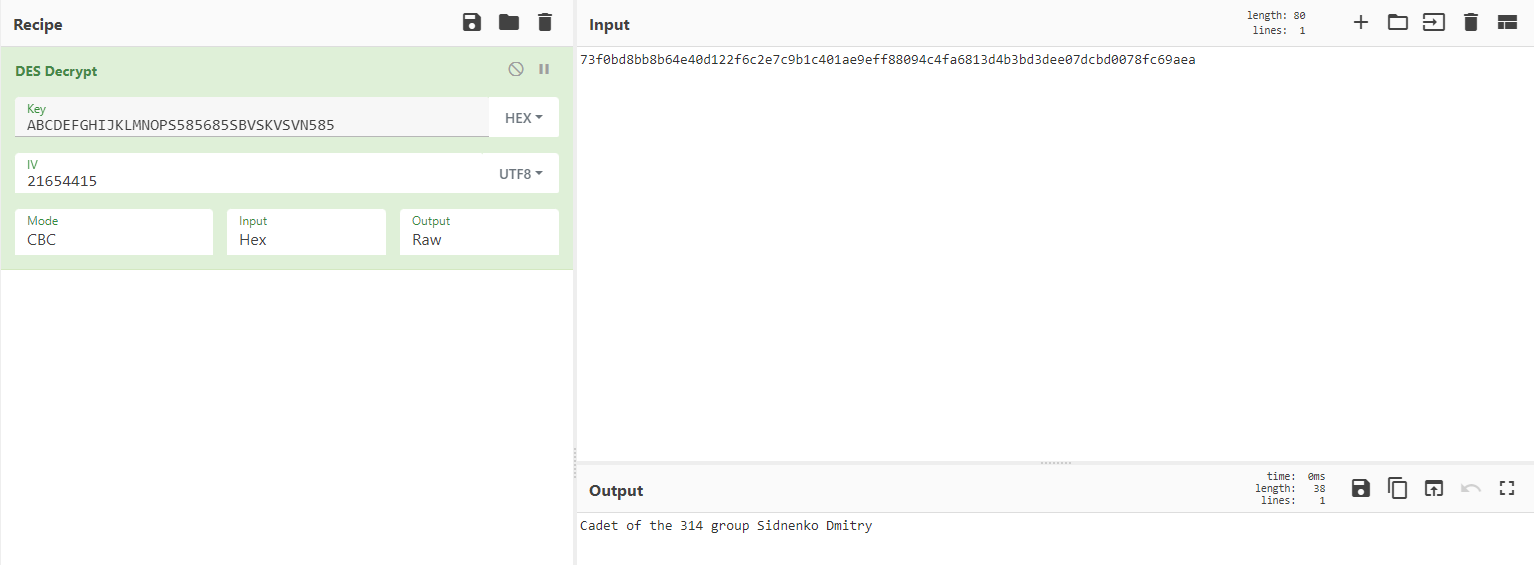
**ВТ:** *Cadet of the 314 group Sidnenko Dmitry*

**ШТ:** *73f0bd8bb8b64e40d122f6c2e7c9b1c401ae9eff88094c4fa6813d4b3bd3dee07dcbd0078fc69aea*

Encrypt

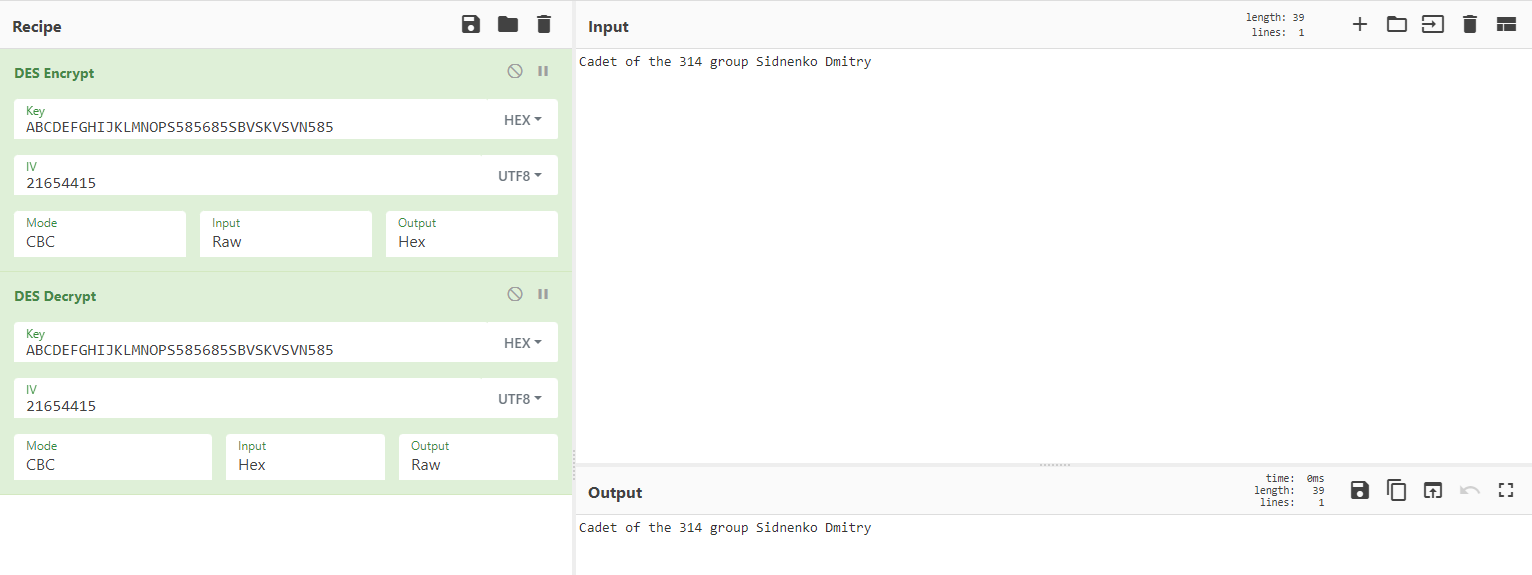


Decrypt



Inblock

In block



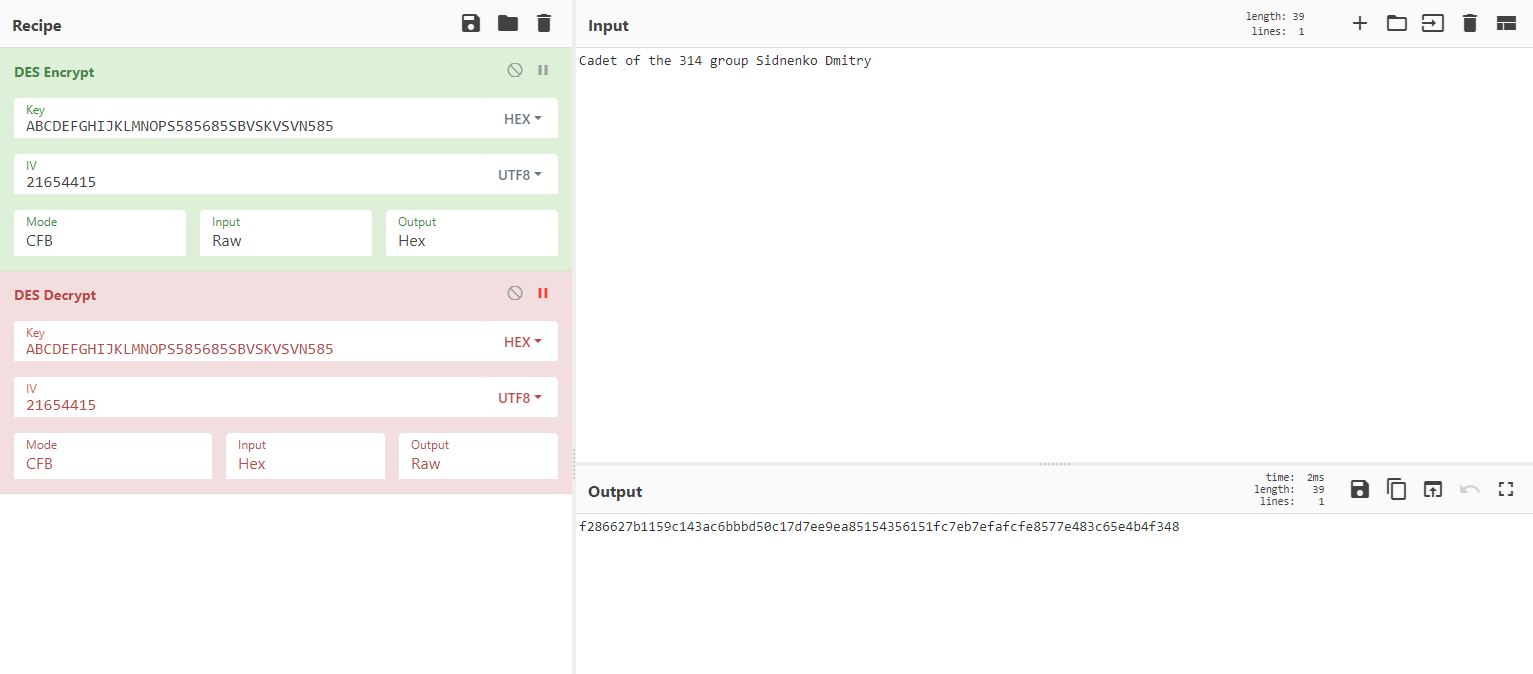
**3.MODE CFC**

**KEY(HEX):** *ABCDEFGHIJKLMNOPS585685SBVSKVSVN585* **IV(UTF-8):** *21654415*

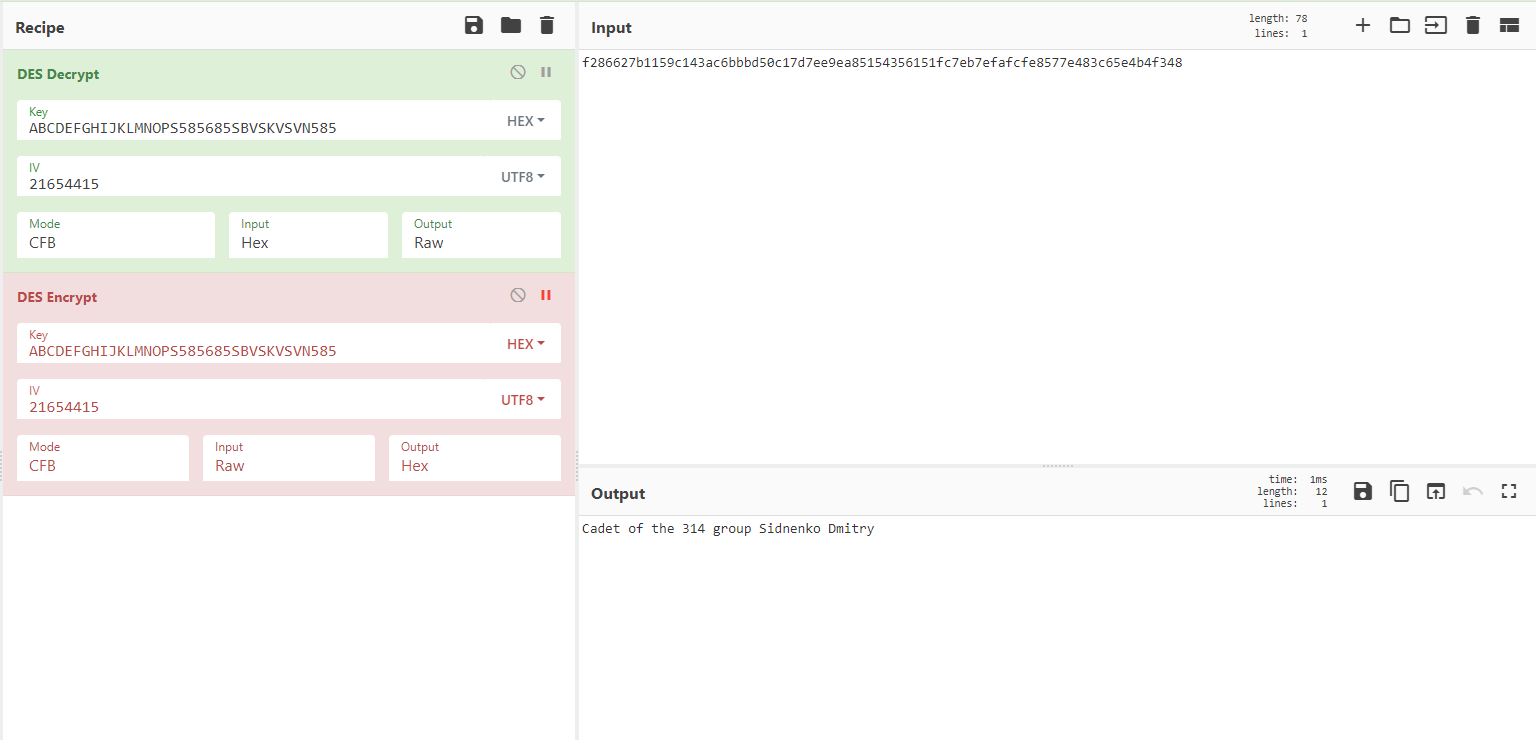
**ВТ:** *Cadet of the 314 group Sidnenko Dmitry*

**ШТ:** *f286627b1159c143ac6bbbd50c17d7ee9ea85154356151fc7eb7efafcfe8577e483c65e4b4f348*

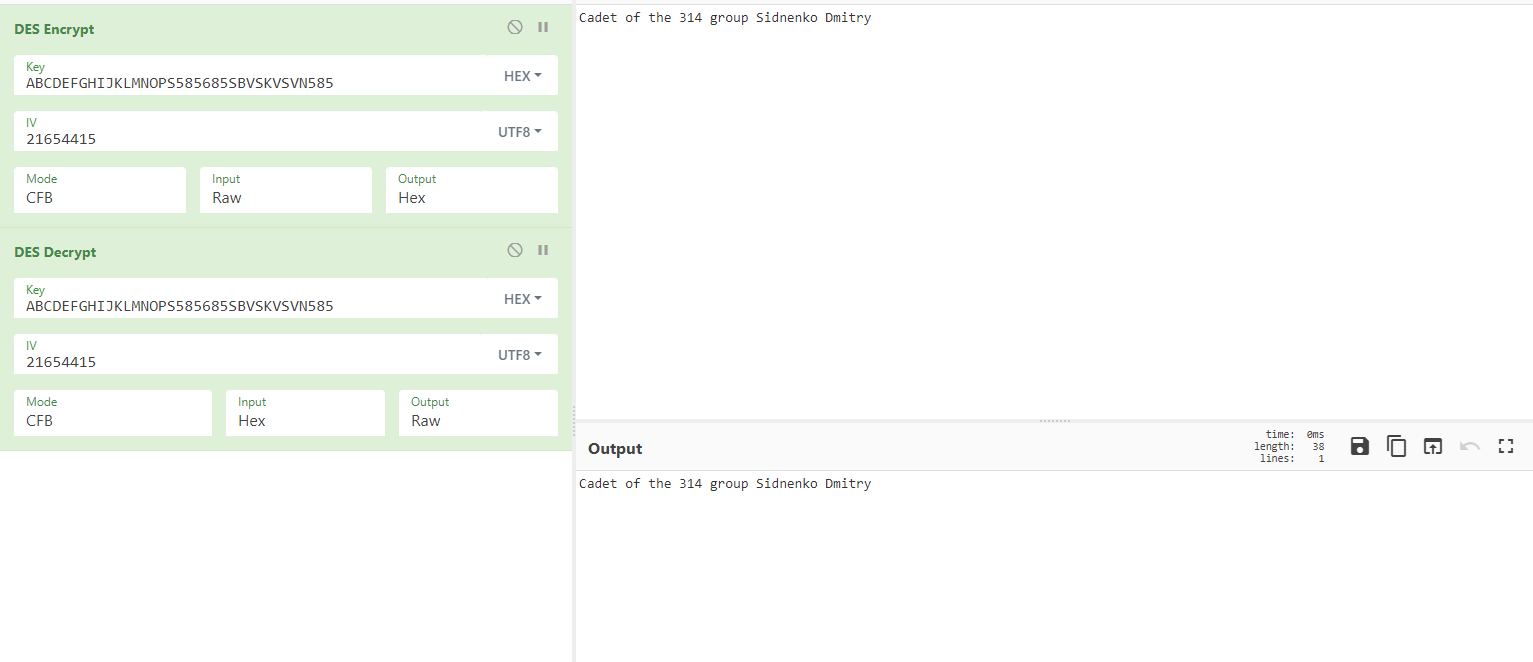
Encrypt



Decrypt



In block



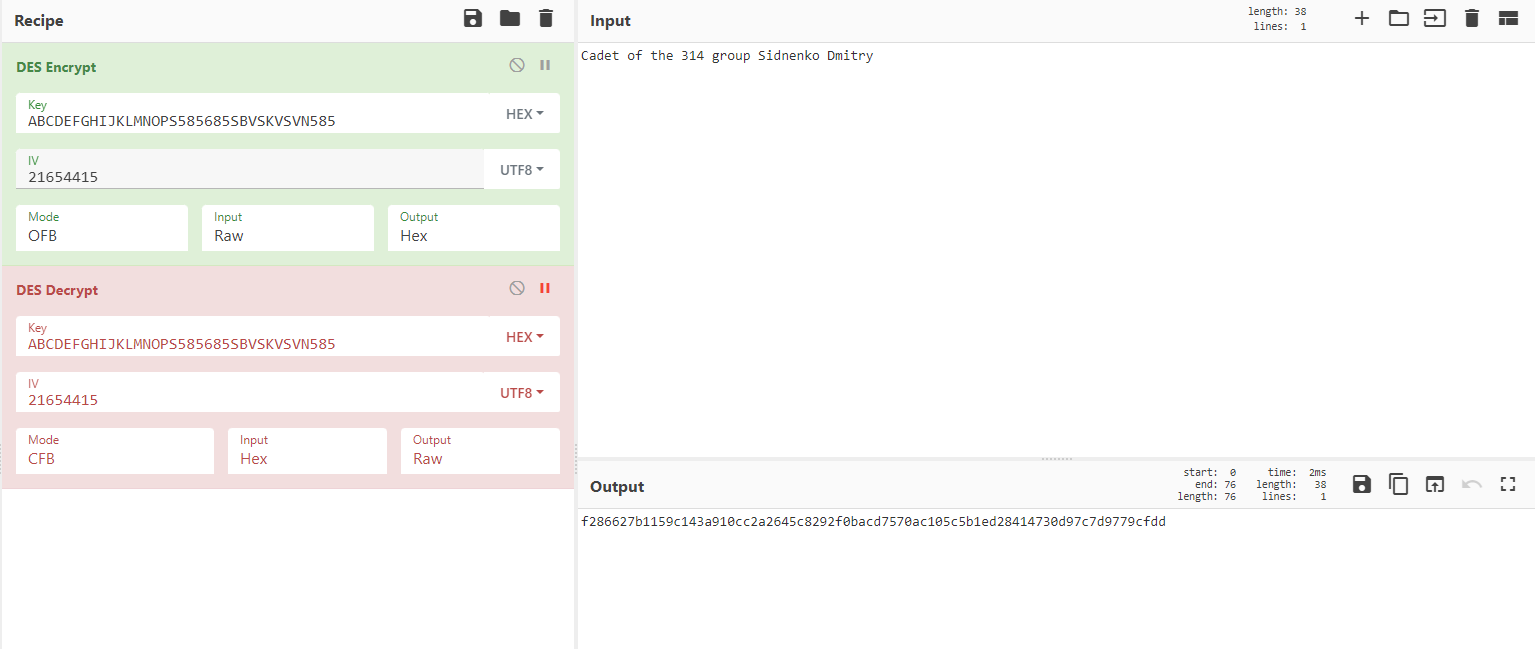
**4.MODE OFB**

**KEY(HEX):** *ABCDEFGHIJKLMNOPS585685SBVSKVSVN585* **IV(UTF-8):** *21654415*

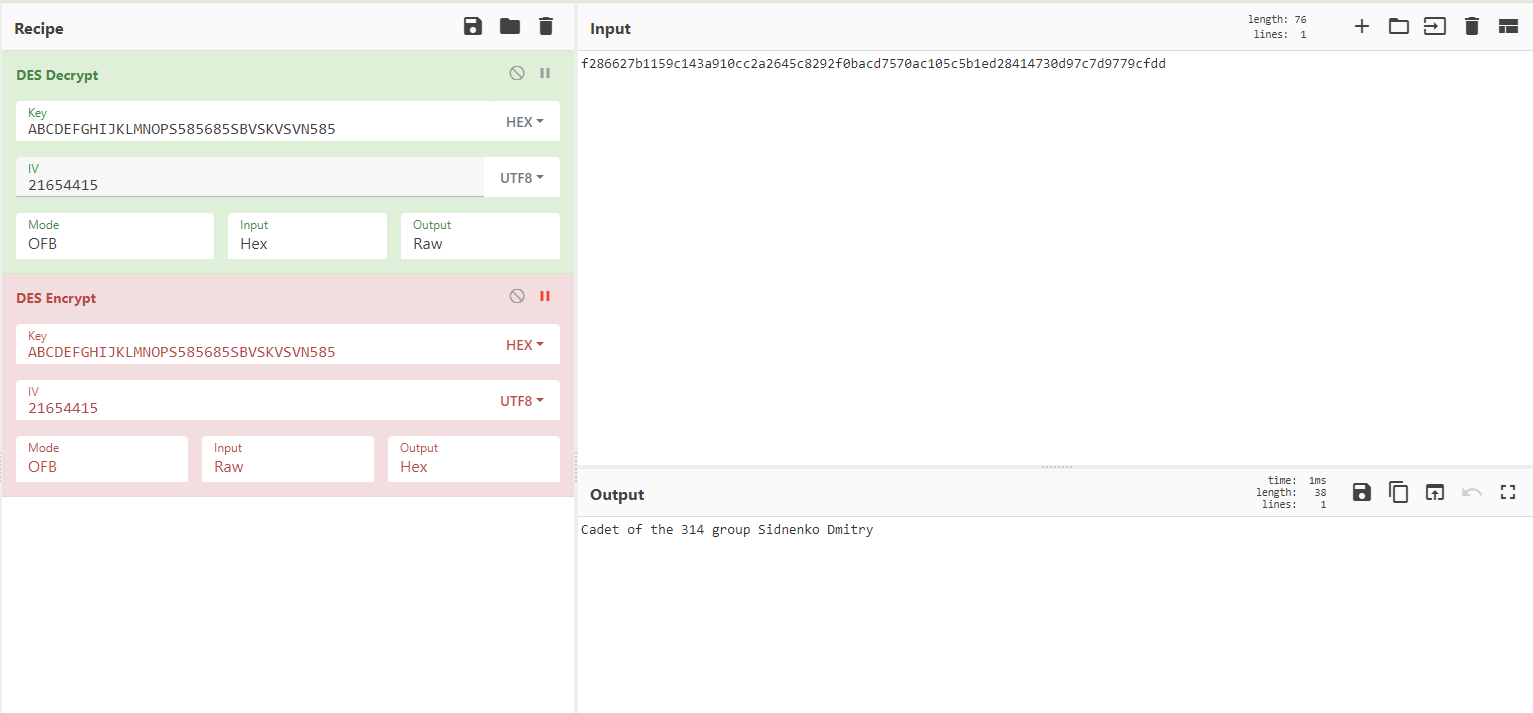
**ВТ:** *Cadet of the 314 group Sidnenko Dmitry*

**ШТ:** *f286627b1159c143a910cc2a2645c8292f0bacd7570ac105c5b1ed28414730d97c7d9779cfdd*

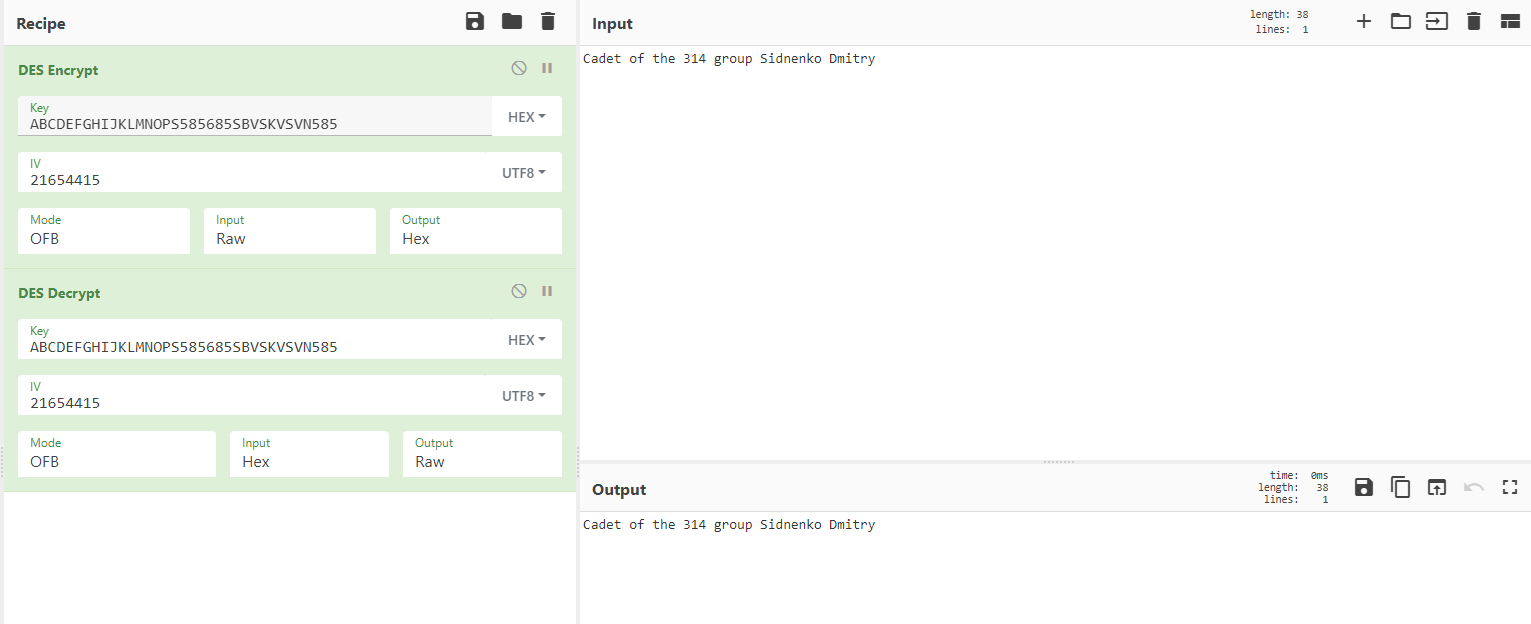
Encrypt



Decrypt



In block



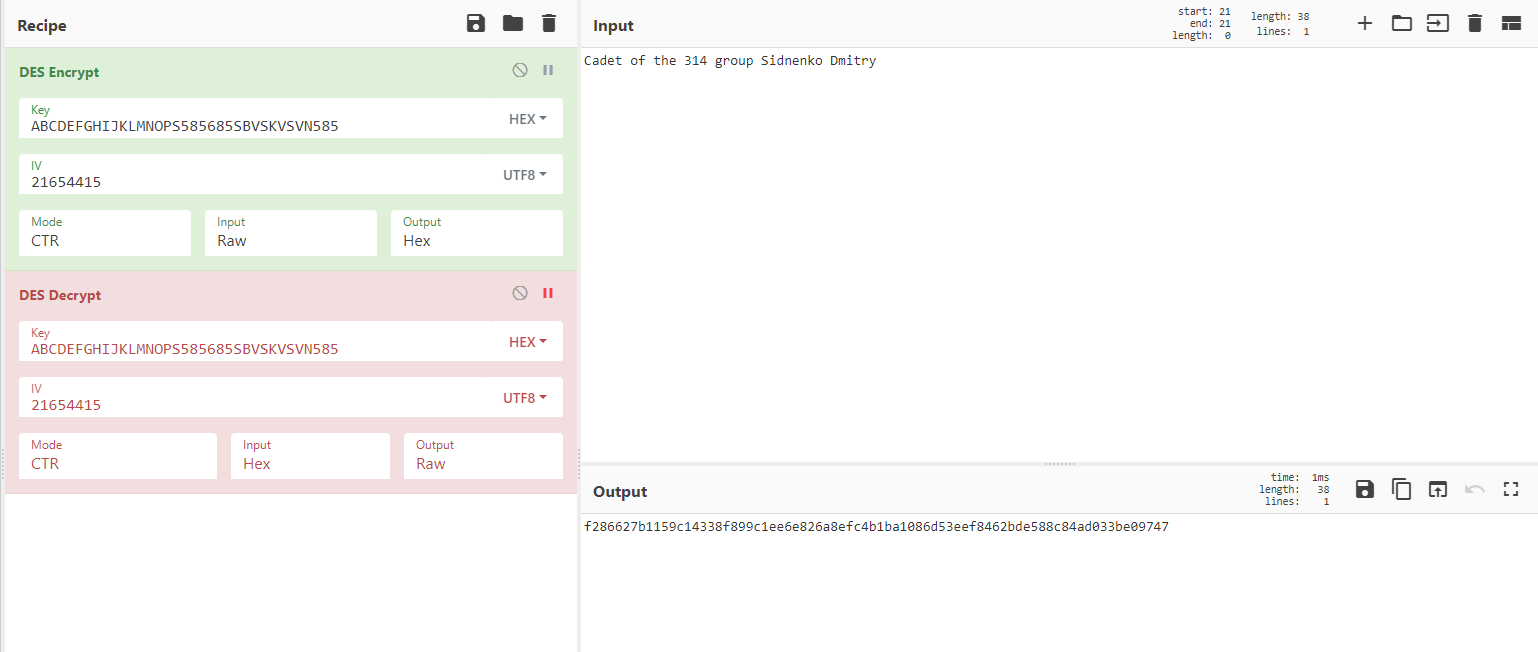
**5.MODE CTR**

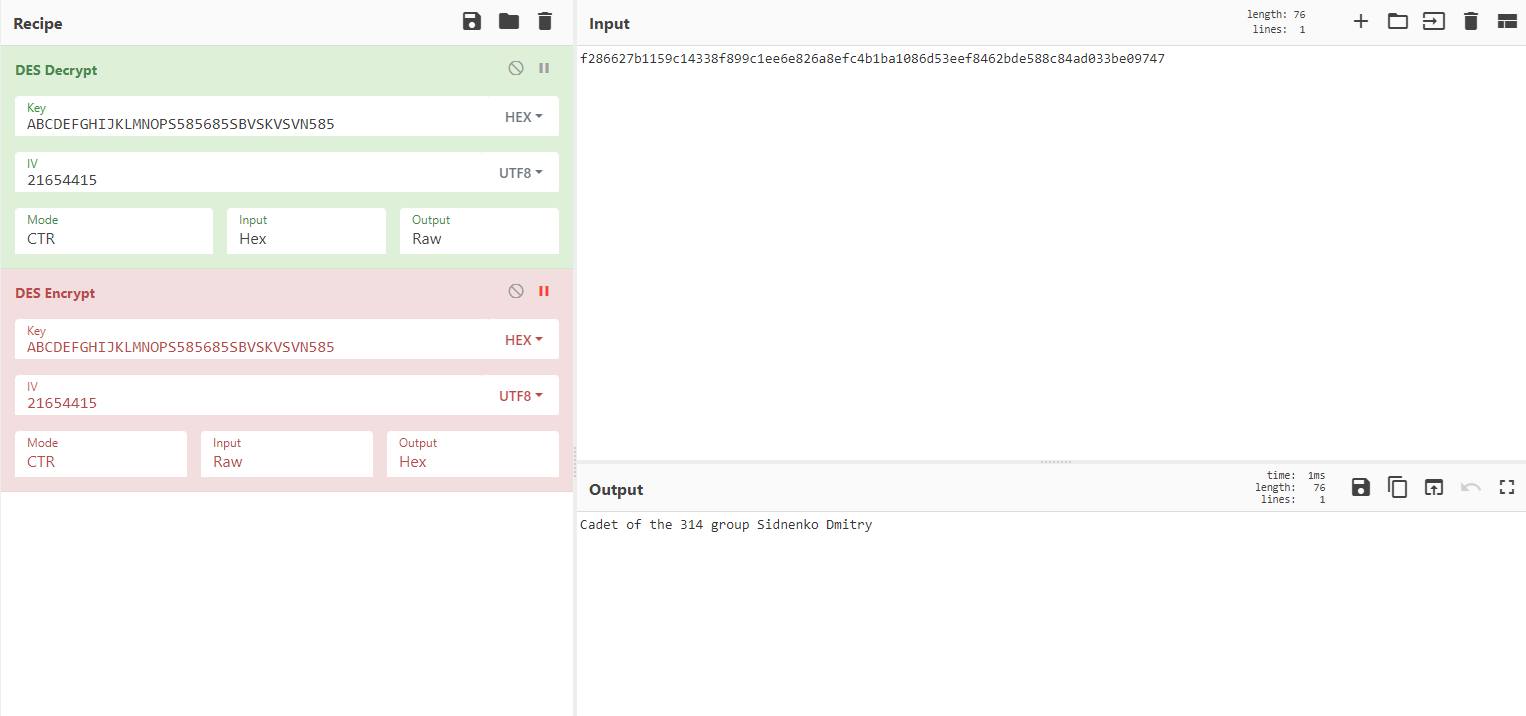
**KEY(HEX):** *ABCDEFGHIJKLMNOPS585685SBVSKVSVN585* **IV(UTF-8):** *21654415*

**ВТ:** Cadet of the 314 group Sidnenko Dmitry

**ШТ:** *f286627b1159c14338f899c1ee6e826a8efc4b1ba1086d53eef8462bde588c84ad033be09747*

Encrypt



Decrypt

In block

