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\_\_\_\_\_\_\_\_\_\_\_КОНОНУЧЕНКО A.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.

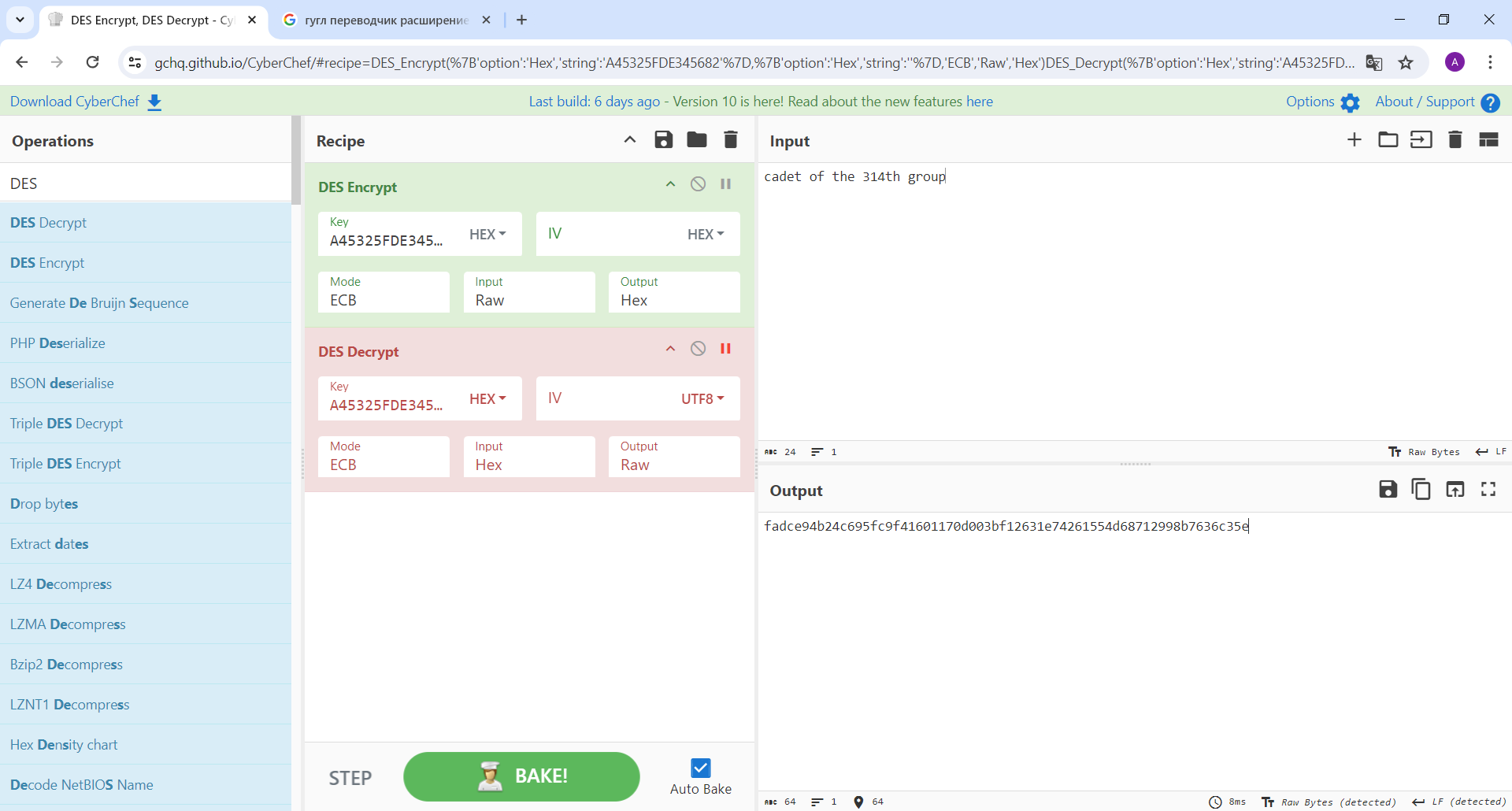
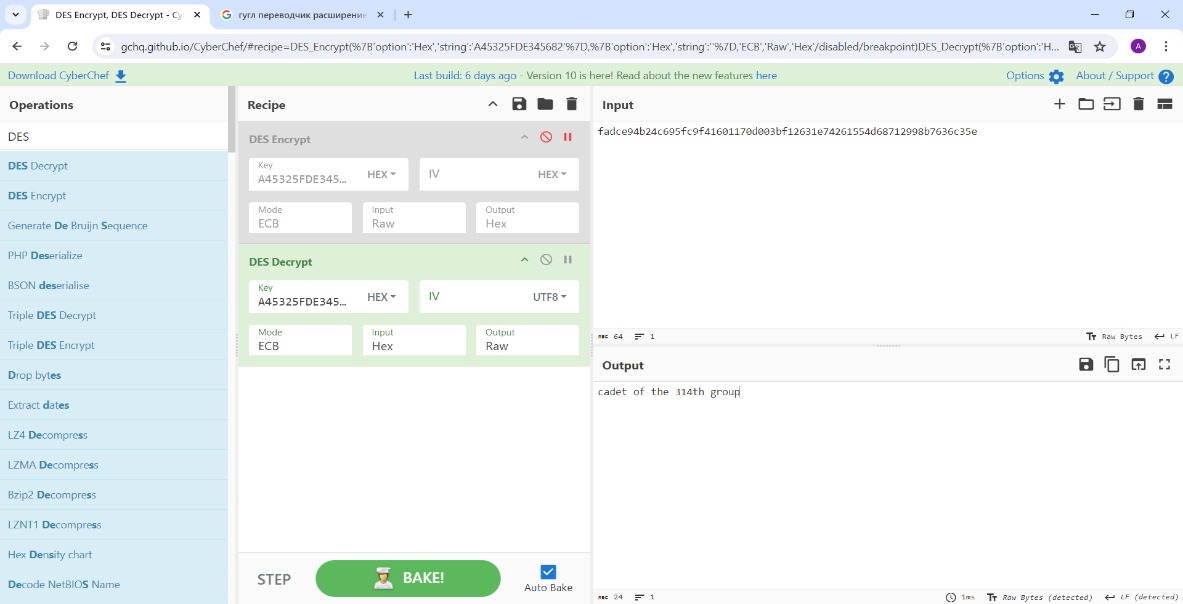
**1.MODE ECB**

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

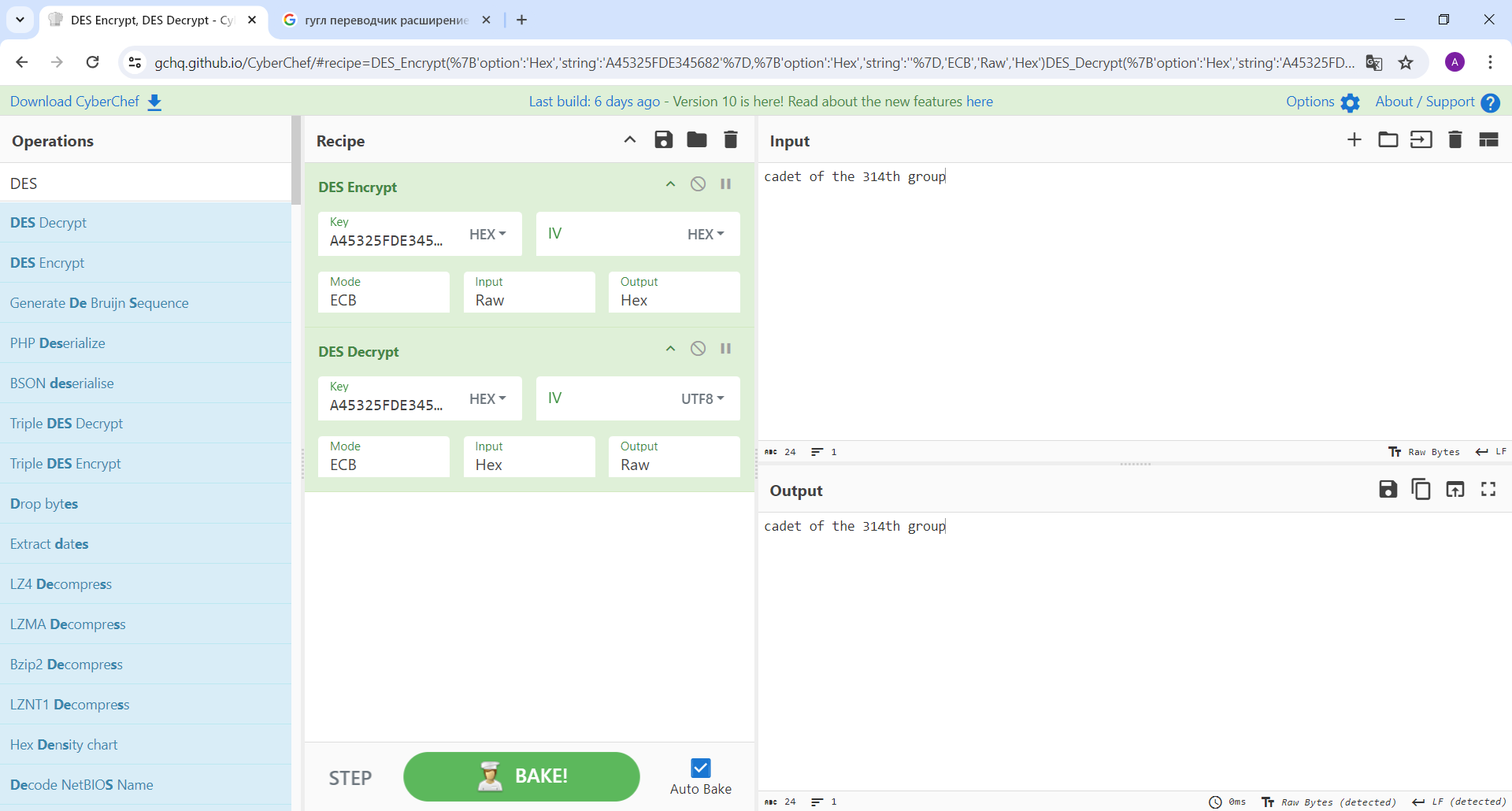
**ВТ:** *cadet of the 314th group*

**ШТ:***fadce94b24c695fc9f41601170d003bf12631e74261554d68712998b7636c35e*

Encrypt Decrypt



In block



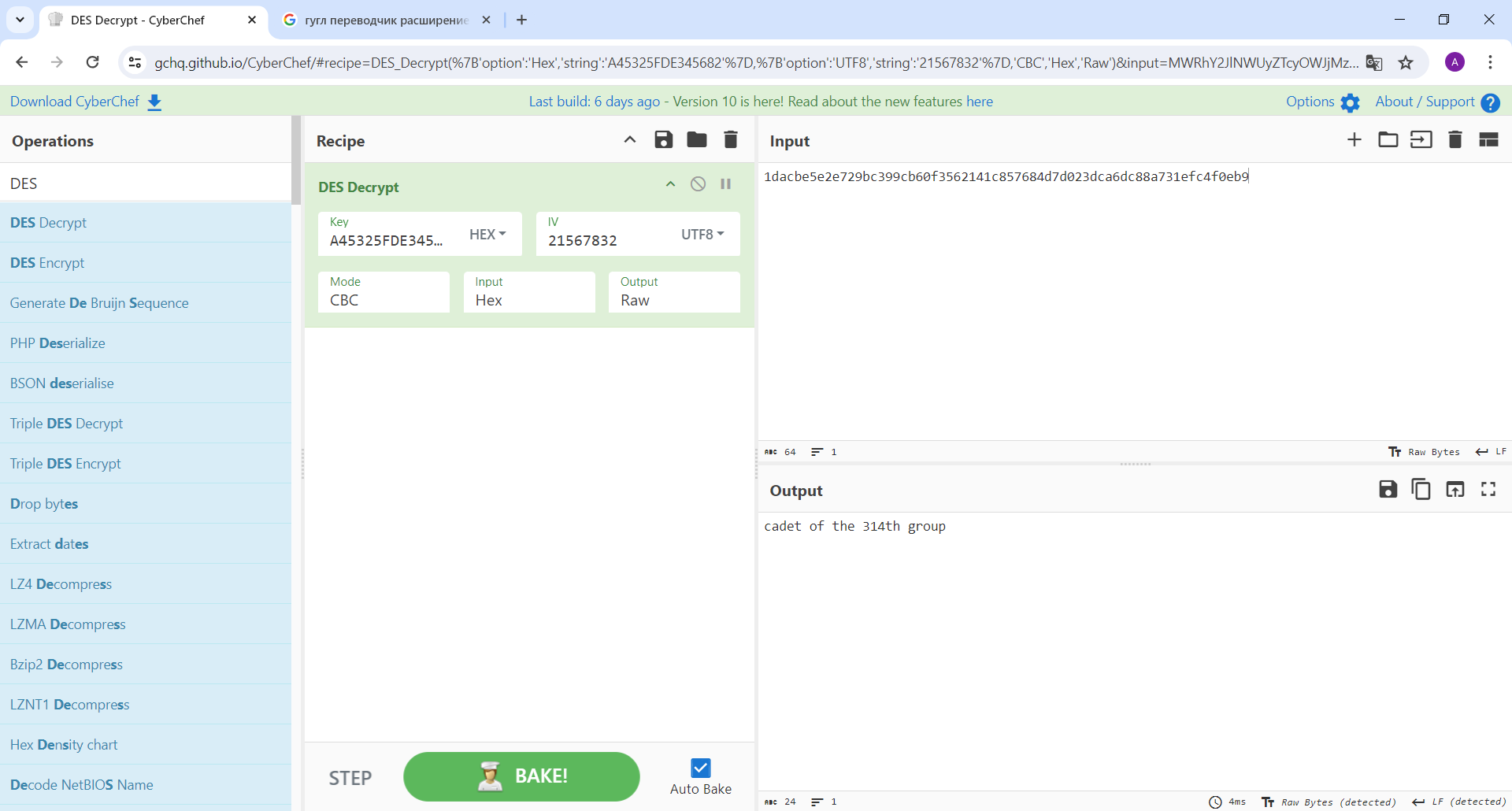
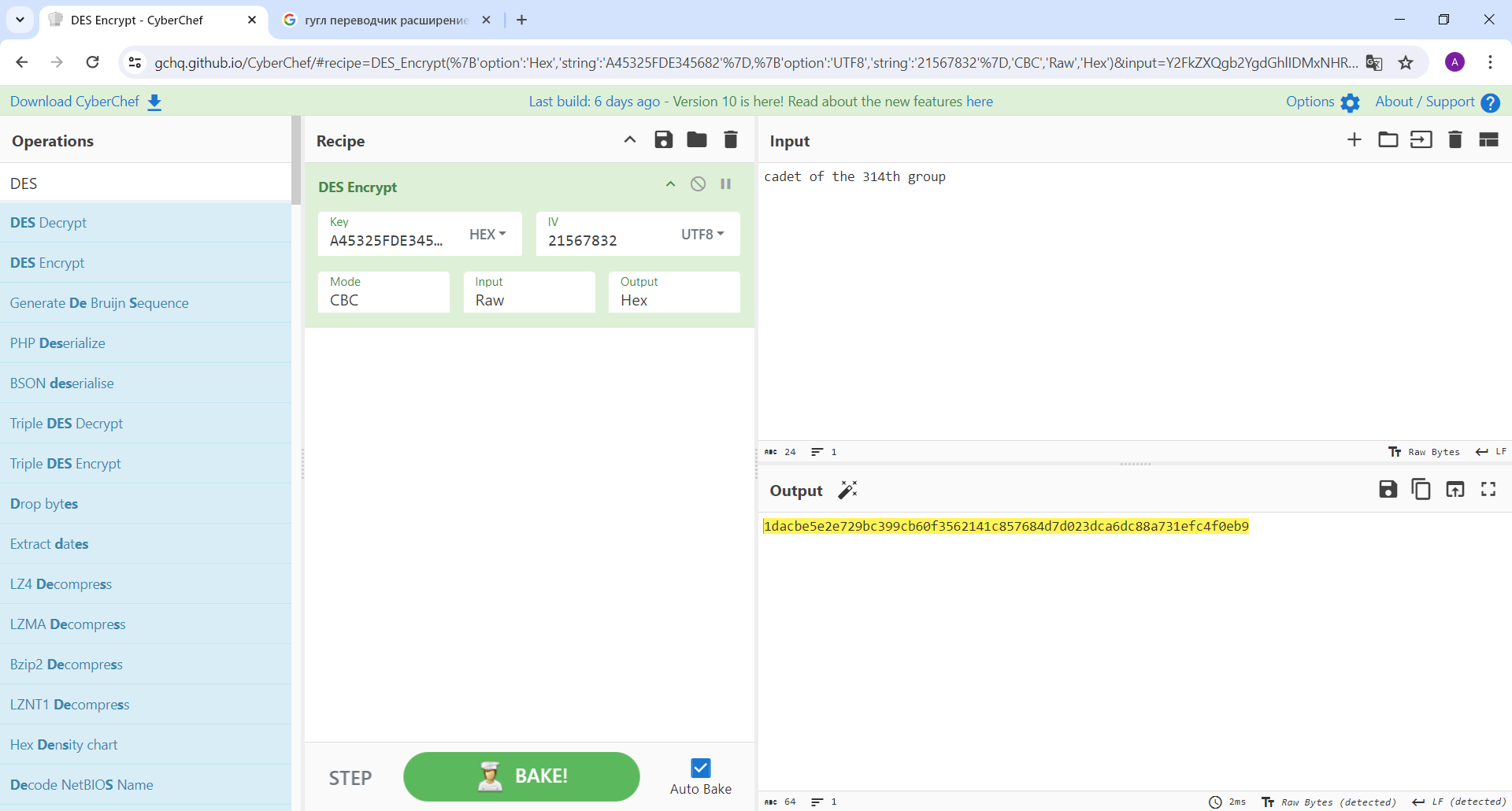
**2.MODE CBC**

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

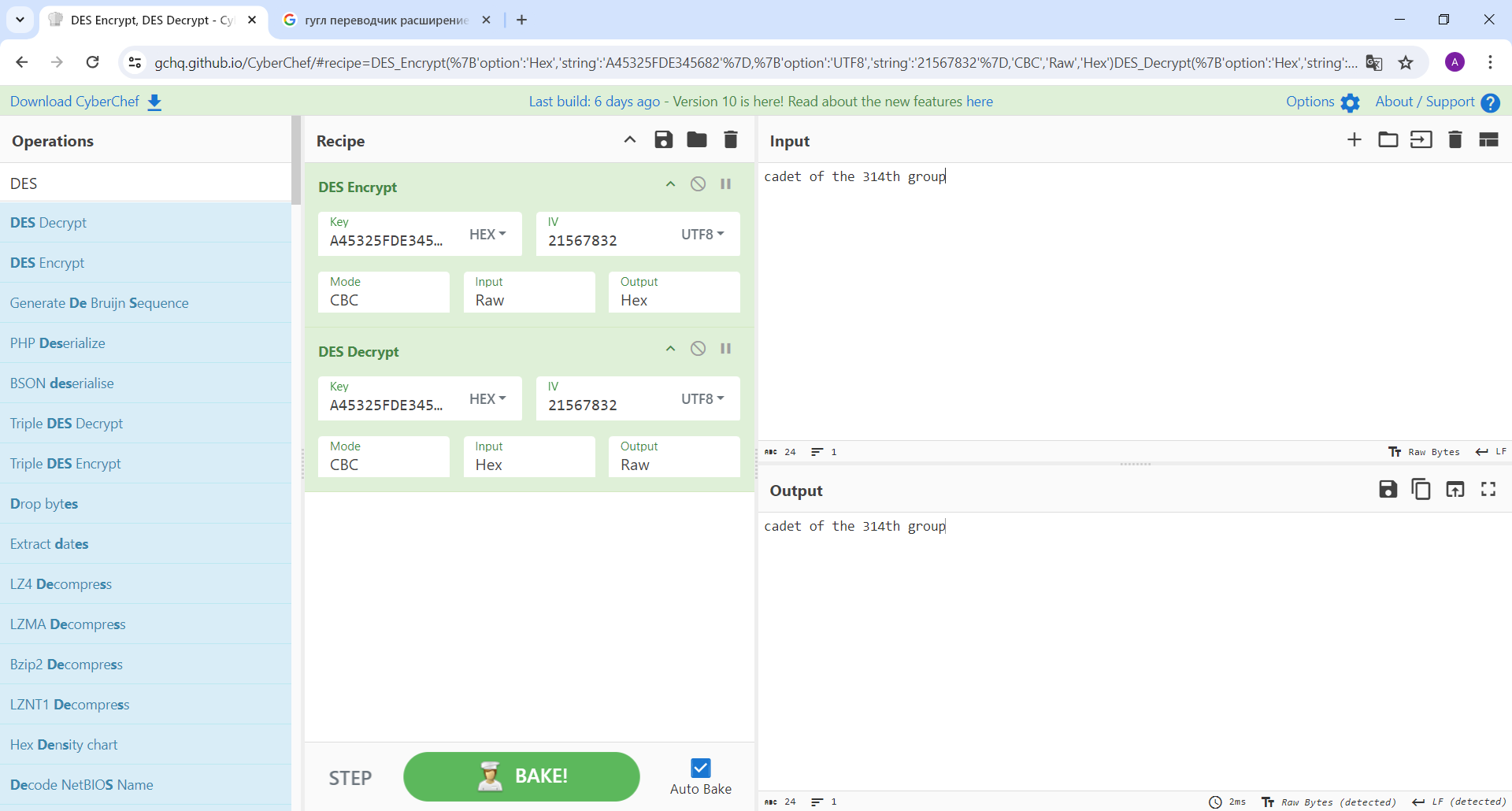
**ВТ:** *cadet of the 314th group*

**ШТ:** *1dacbe5e2e729bc399cb60f3562141c857684d7d023dca6dc88a731efc4f0eb9*

Encrypt Decrypt



In block



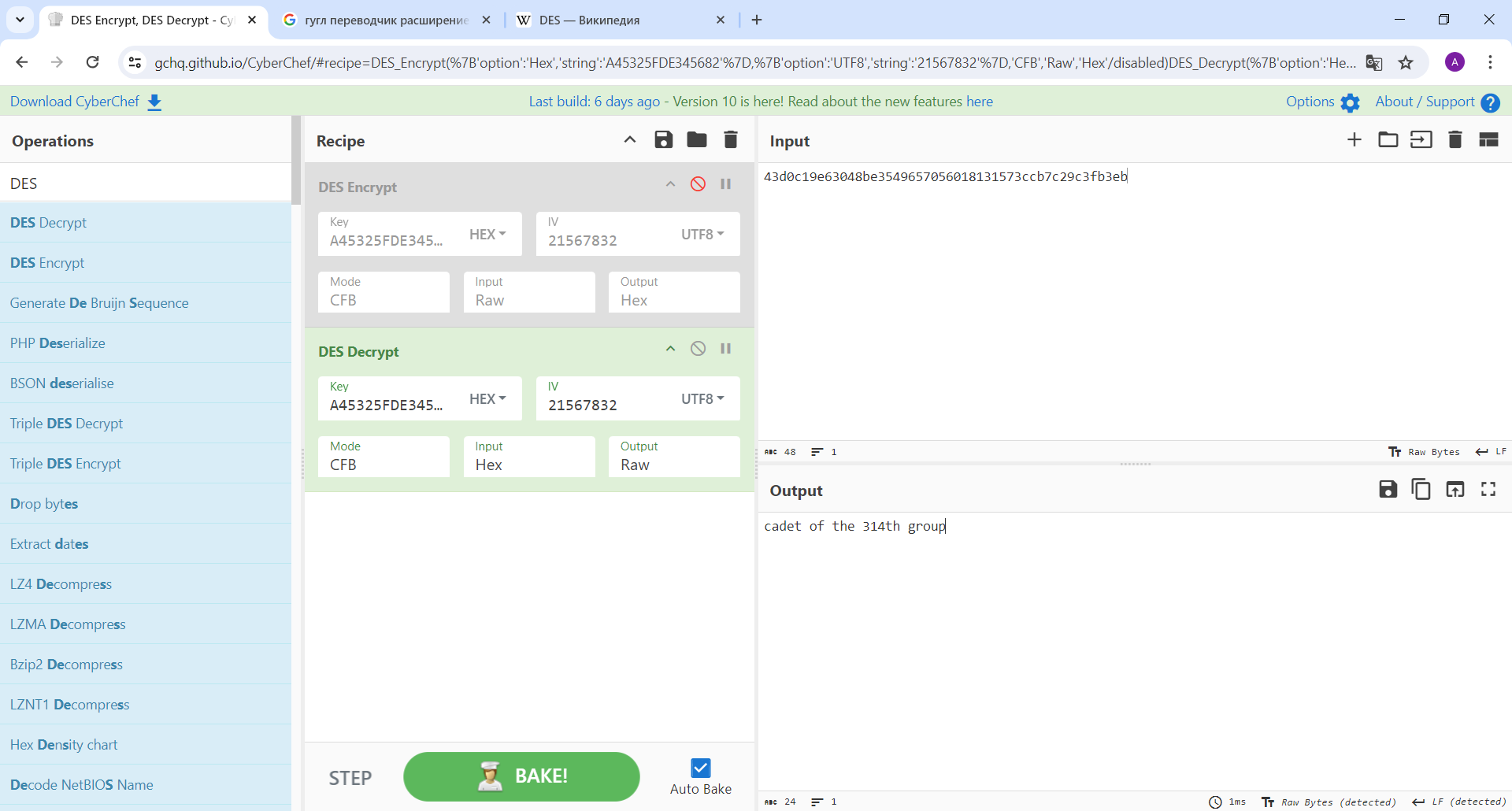
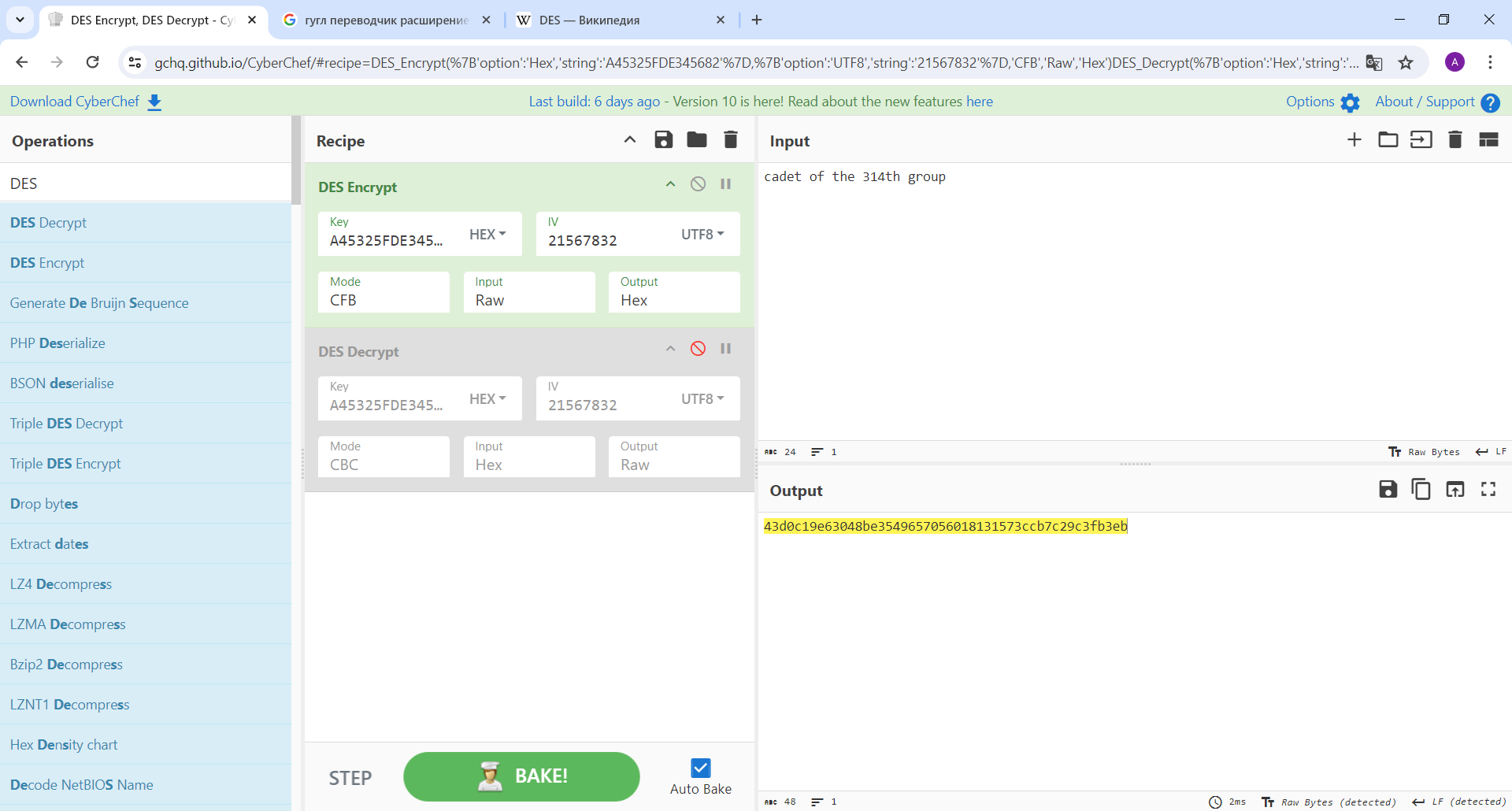
**3.MODE CFC**

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

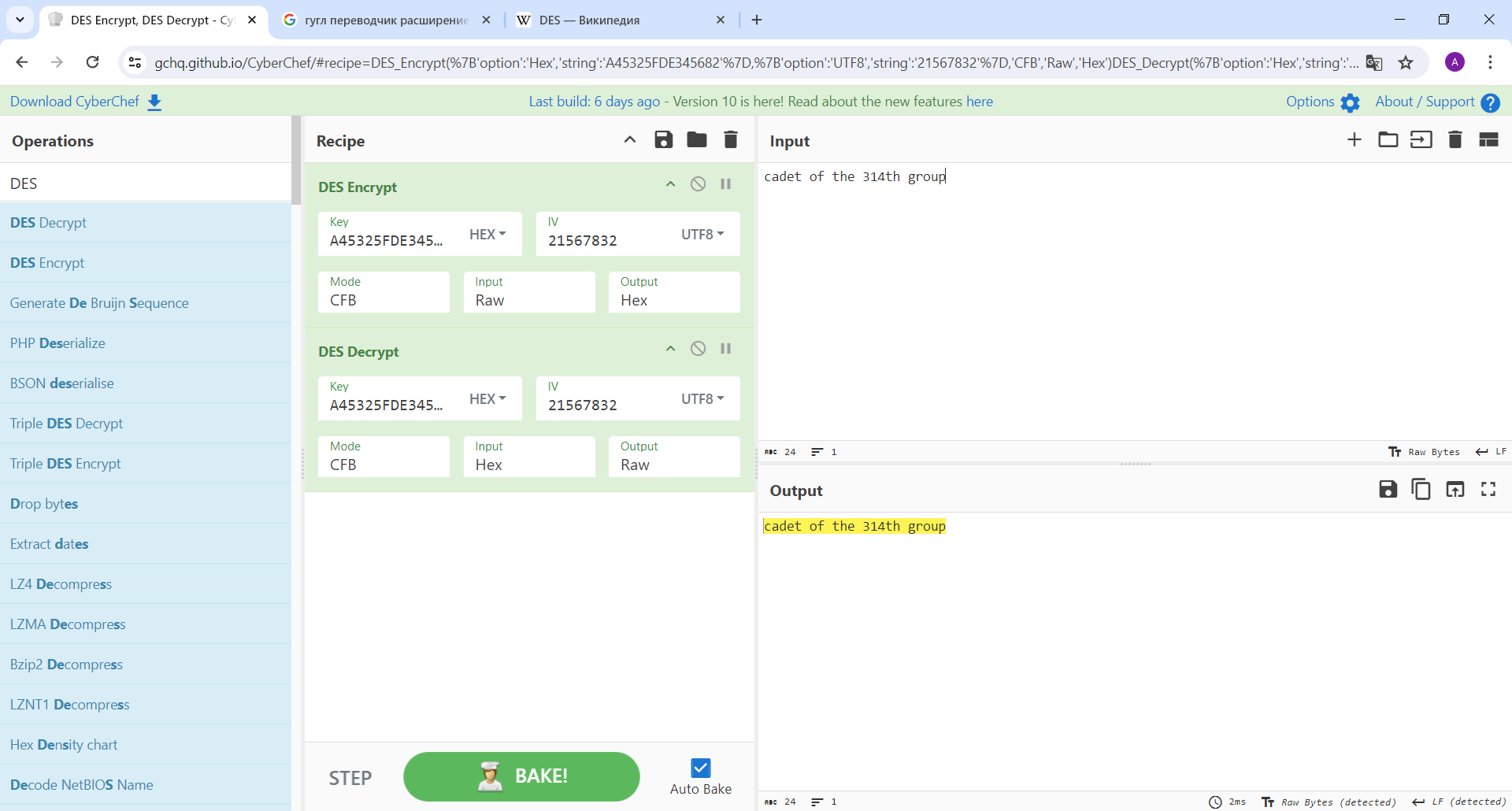
**ВТ:** *cadet of the 314th group*

**ШТ:** *43d0c19e63048be3549657056018131573ccb7c29c3fb3eb*

Encrypt Decrypt



In block



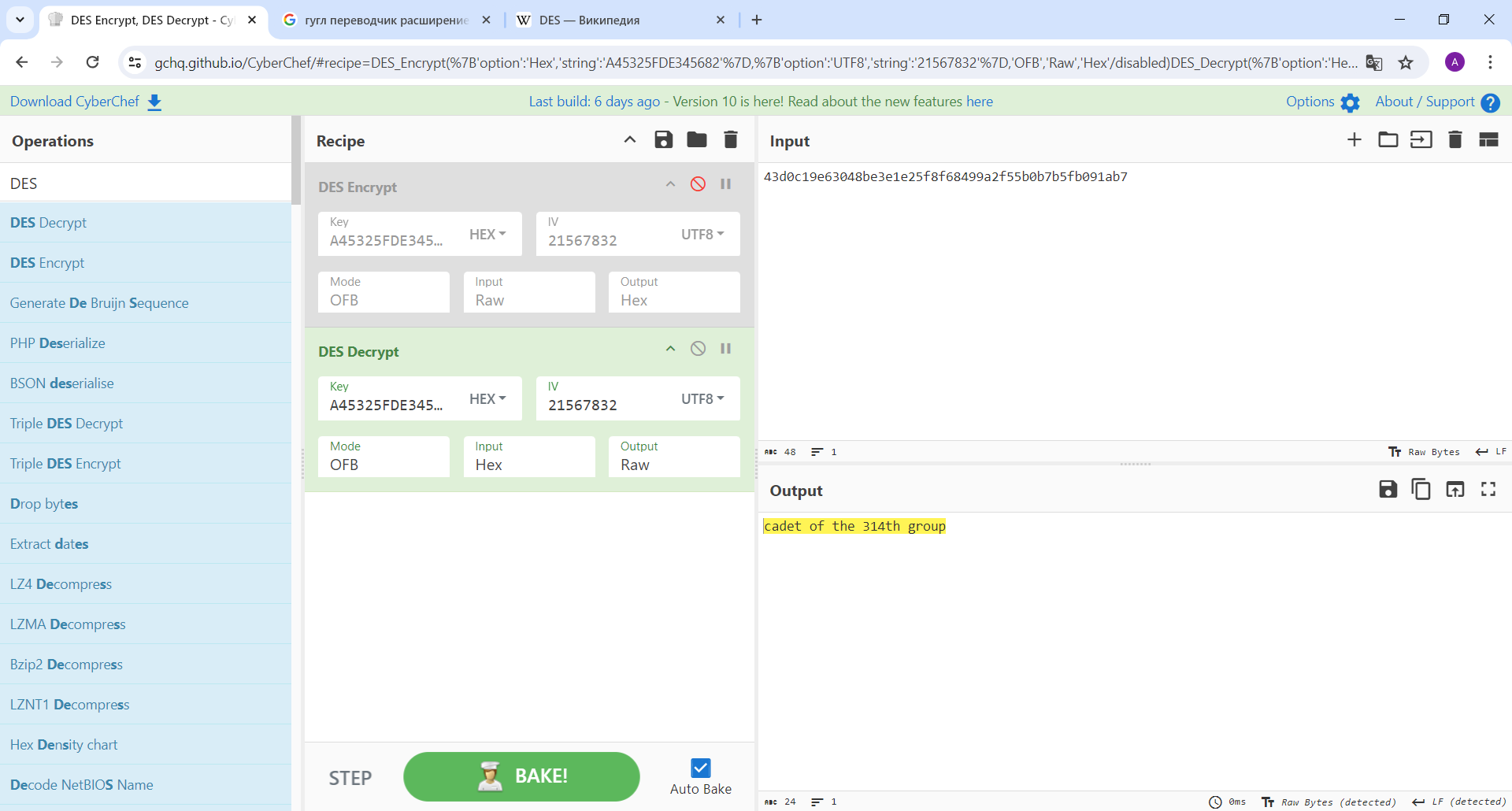
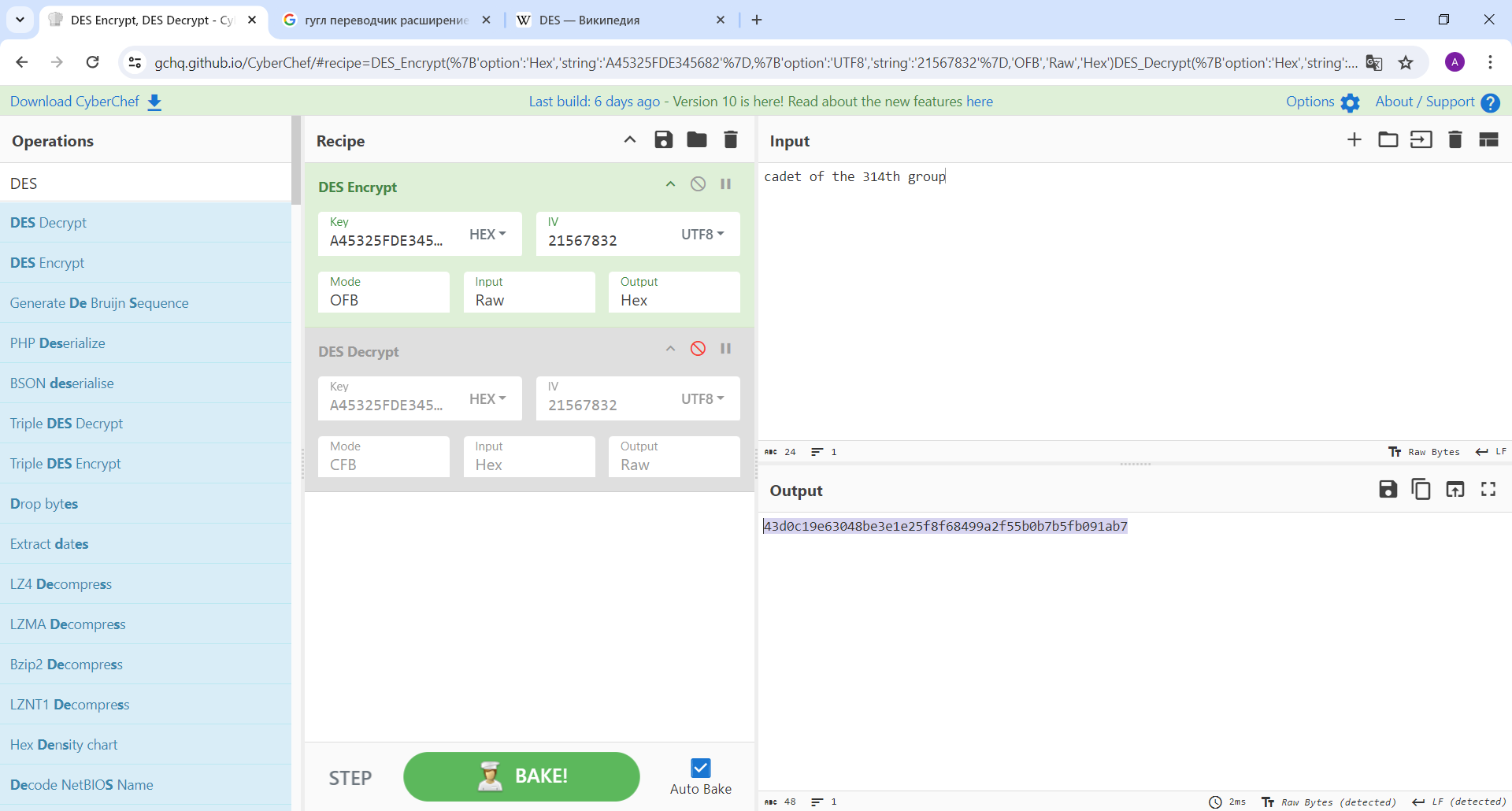
**4.MODE OFB**

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

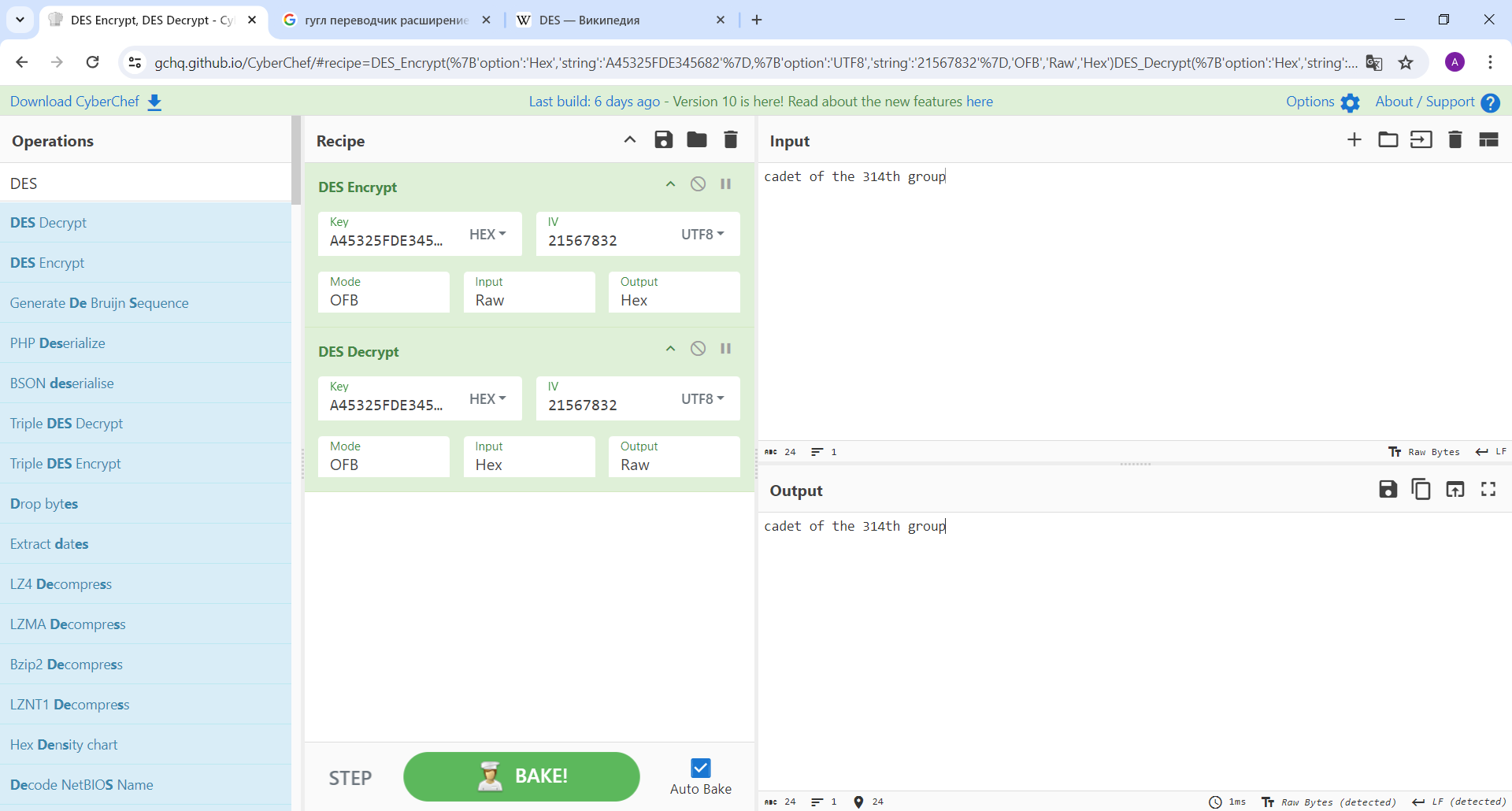
**ВТ:** *cadet of the 314th group*

**ШТ:** *43d0c19e63048be3e1e25f8f68499a2f55b0b7b5fb091ab7*

Encrypt Decrypt



In block



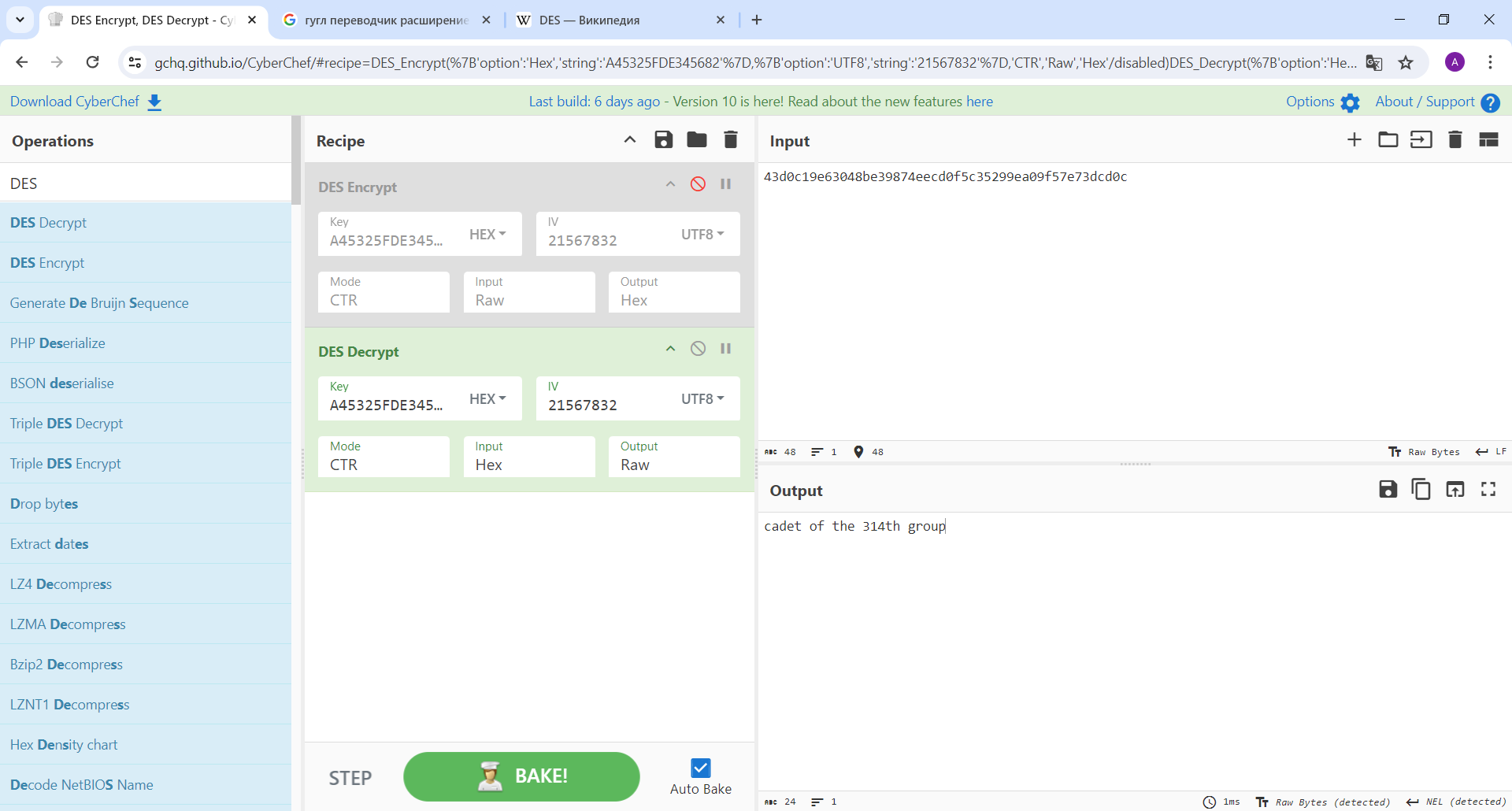
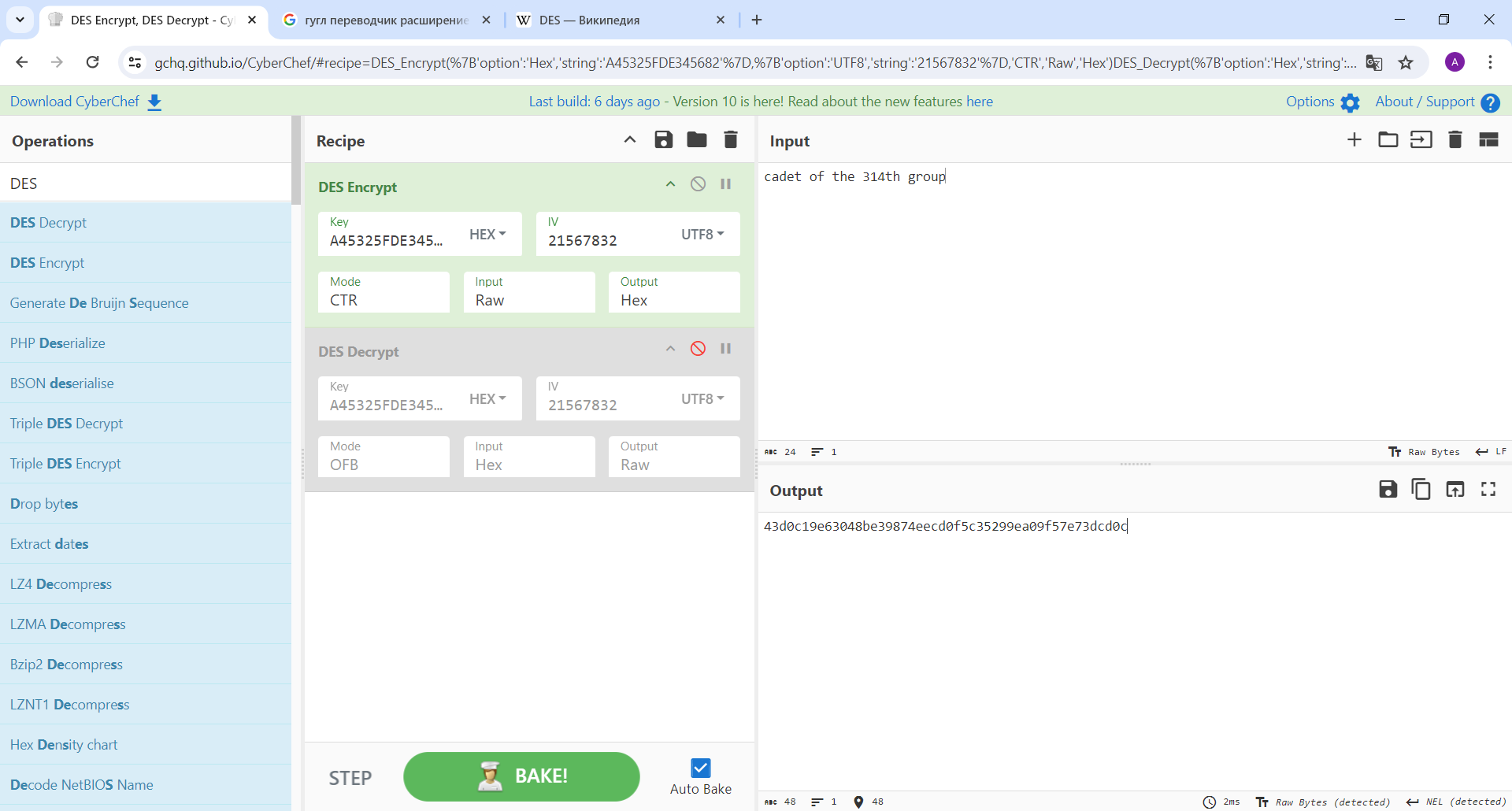
**5.MODE CTR**

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

**ВТ:** *cadet of the 314th group*

**ШТ:** *43d0c19e63048be39874eecd0f5c35299ea09f57e73dcd0c*

Encrypt Decrypt



In block

