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\_\_\_\_\_\_\_\_\_\_\_ТРУСОВ І.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.

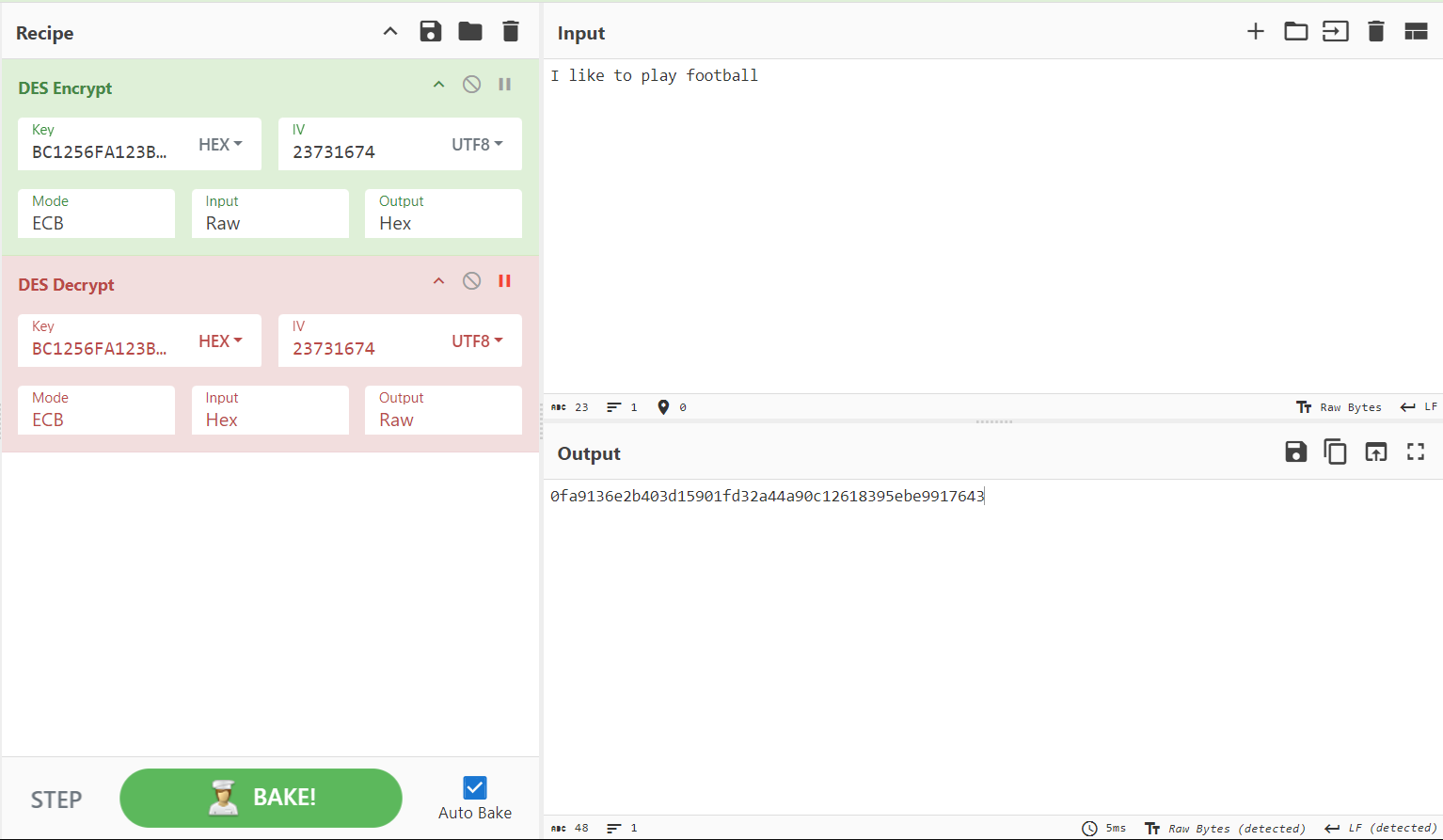
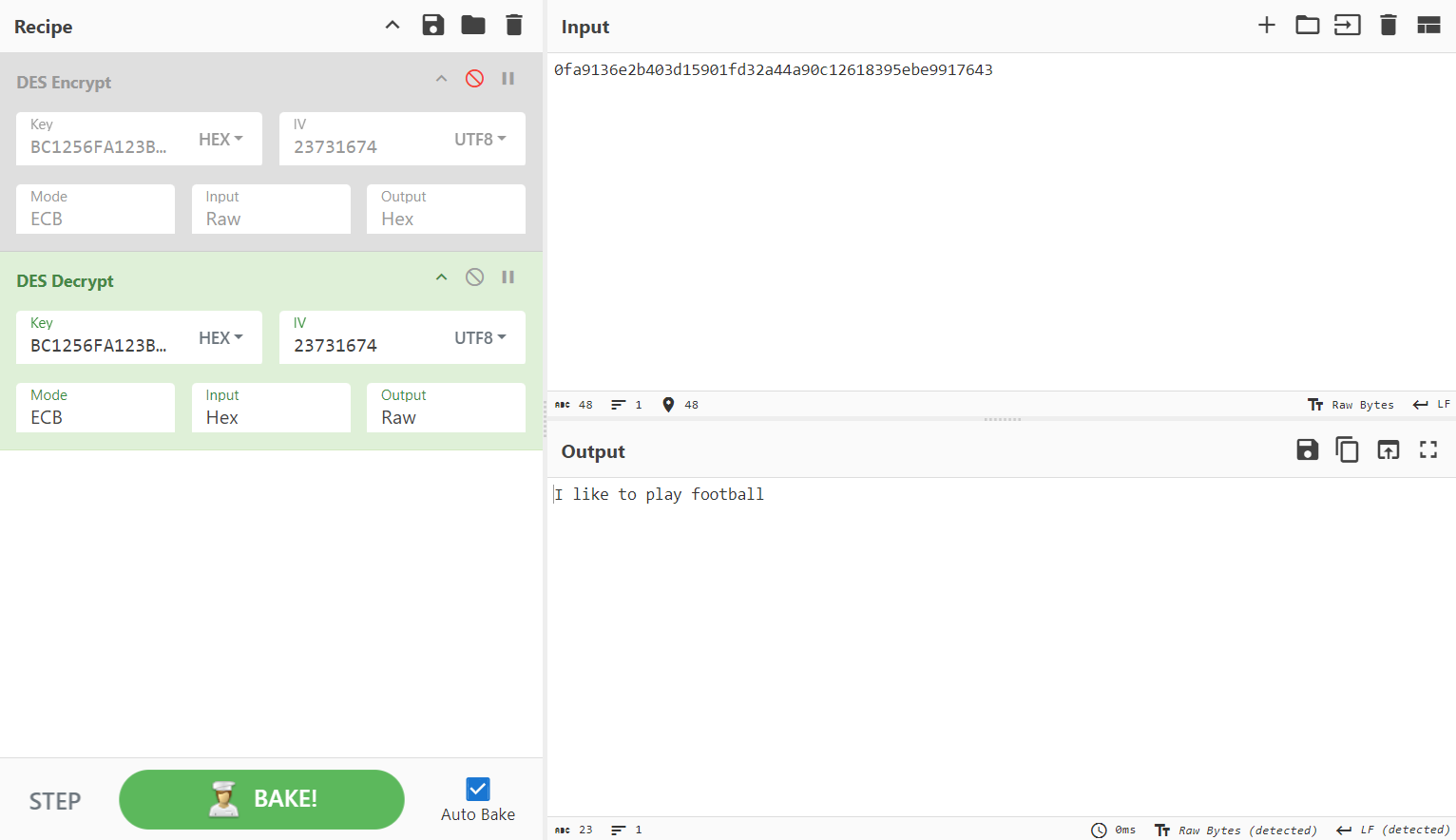
**1.MODE ECB**

**KEY(HEX):** *BC1256FA123BC123*

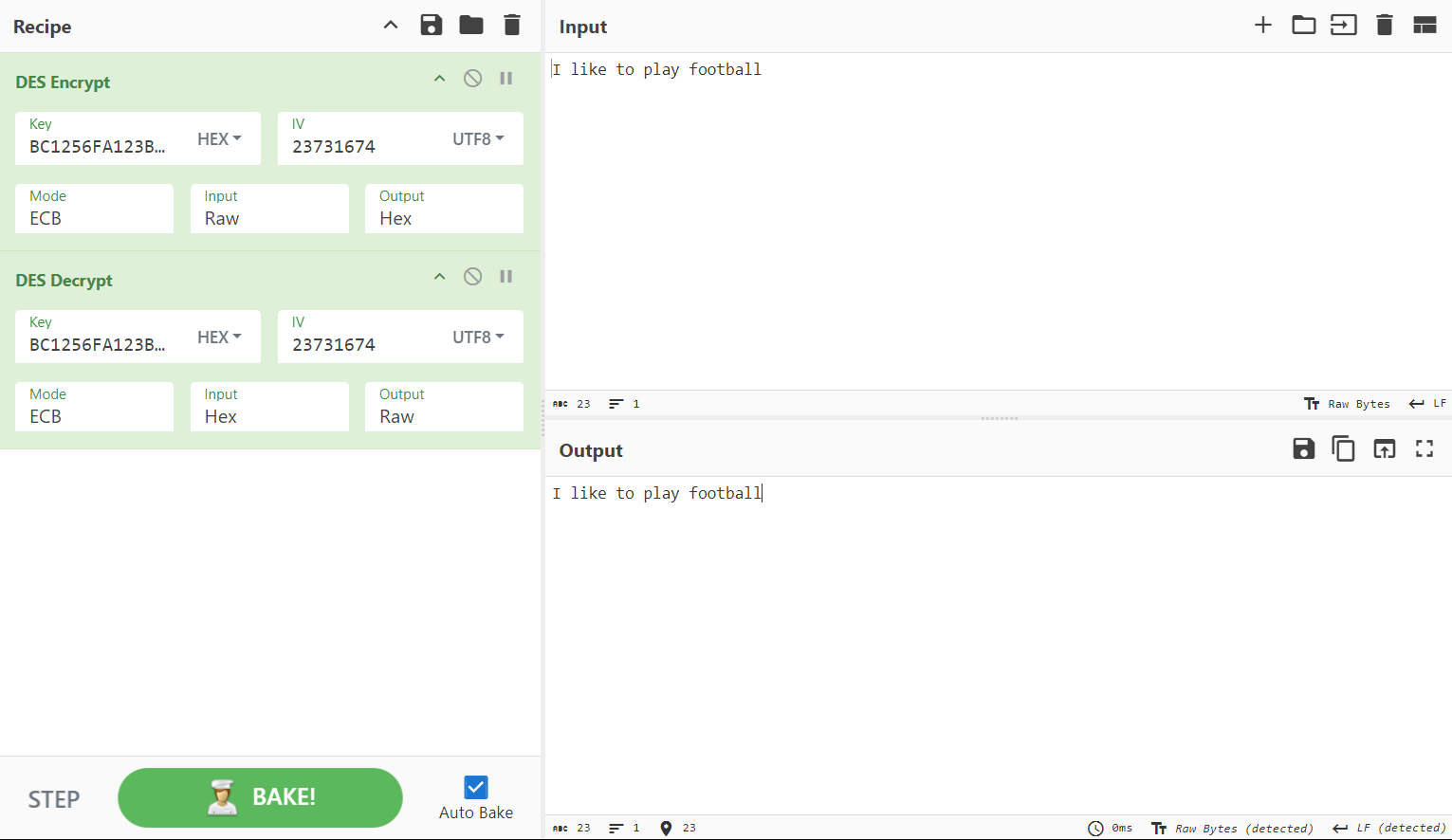
**ВТ:** *I like to play football*

**ШТ:** *0fa9136e2b403d15901fd32a44a90c12618395ebe9917643*

Encrypt Decrypt

** **

In block

****

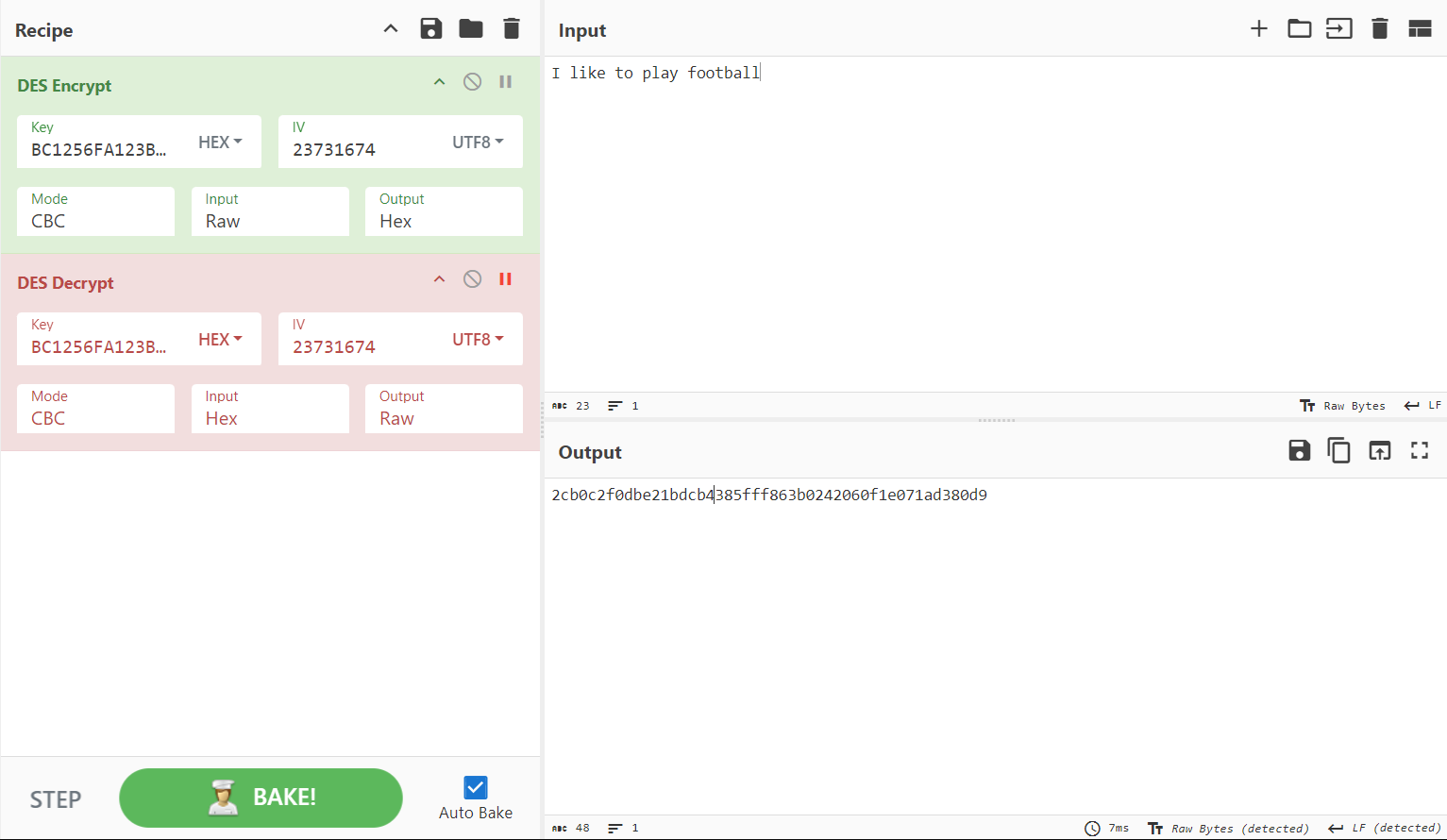
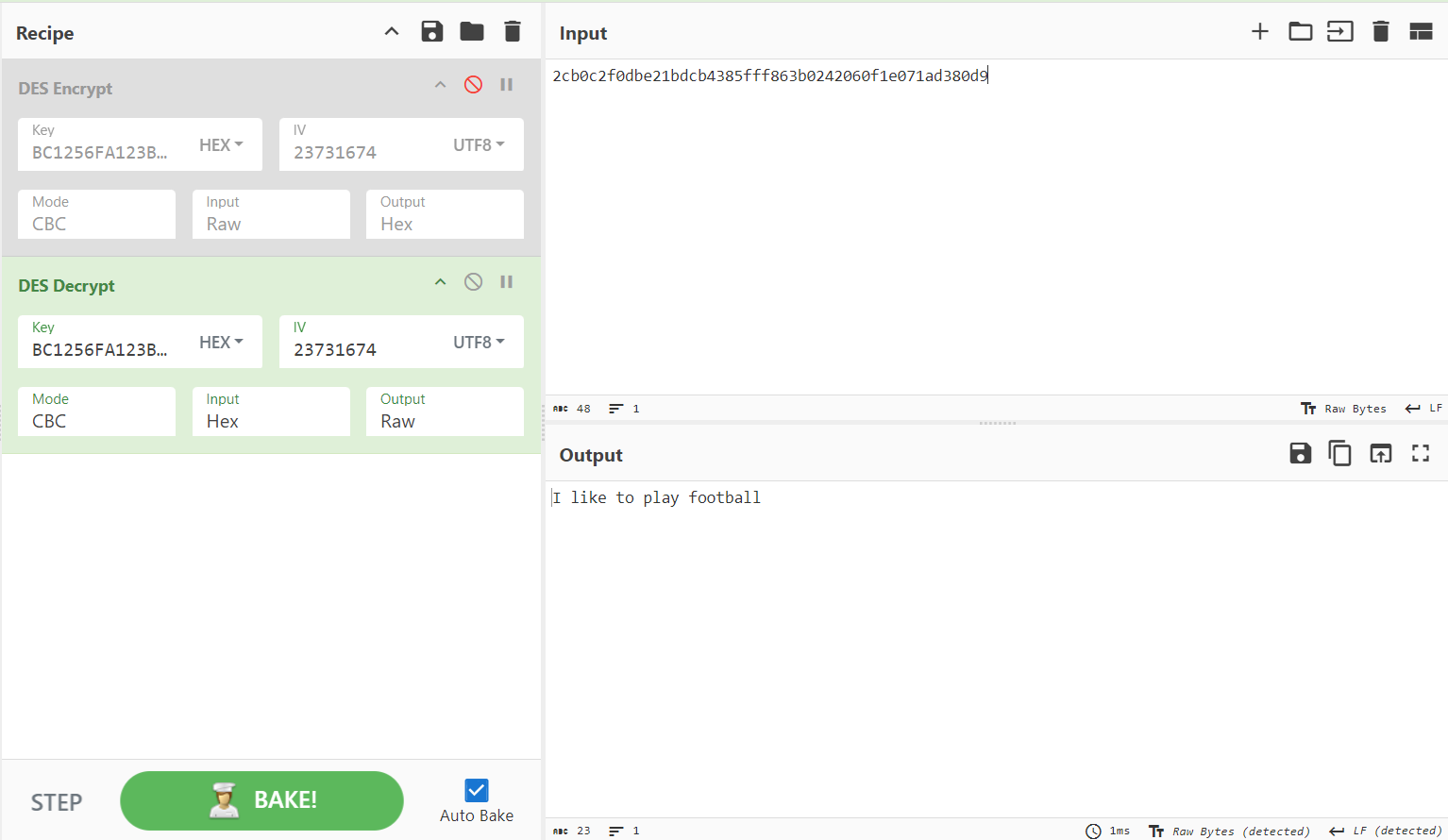
**2.MODE CBC**

**KEY(HEX):** *BC1256FA123BC123* **IV(UTF-8):** *23731674*

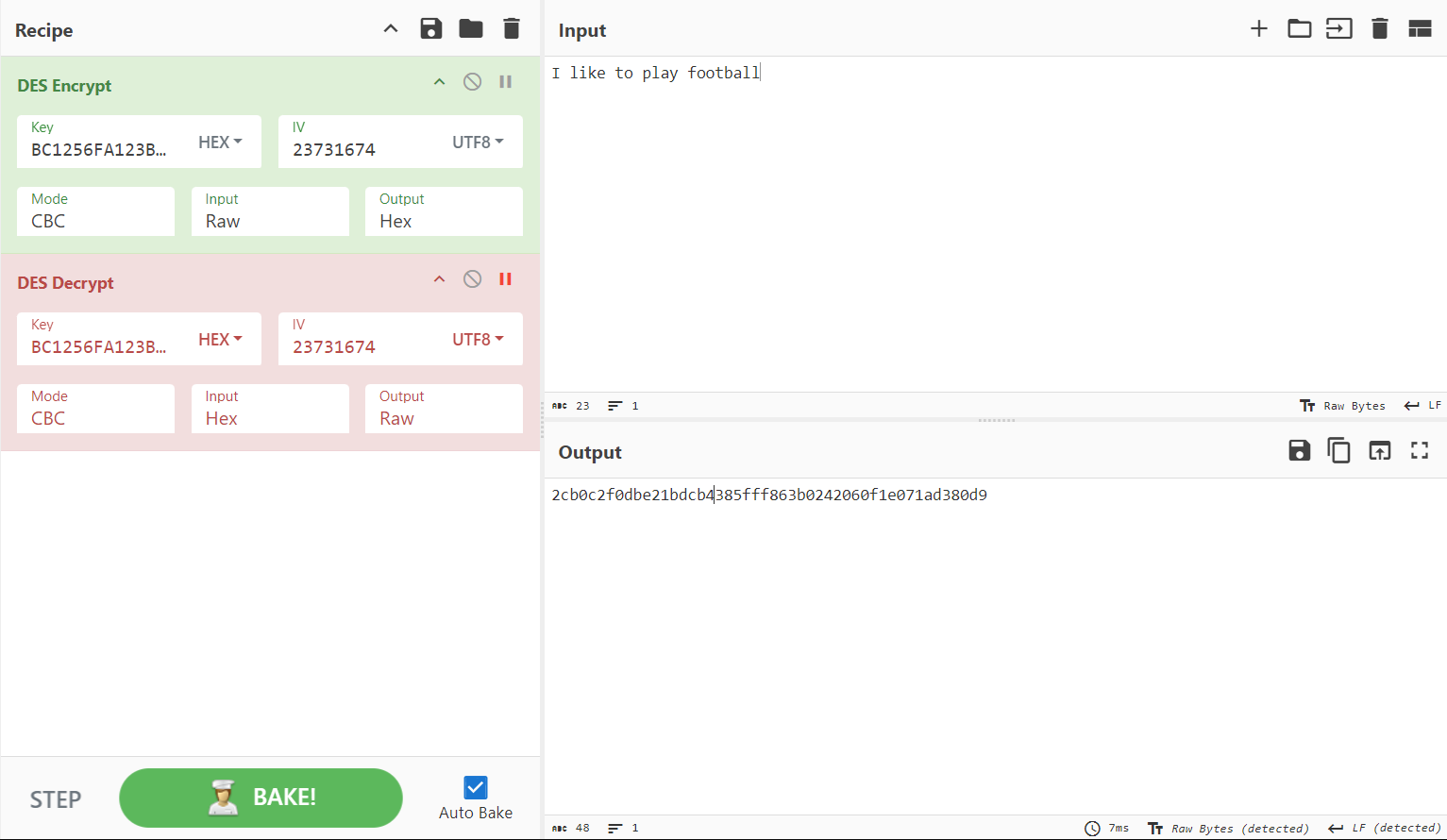
**ВТ:** *I like to play football*

**ШТ:** *2cb0c2f0dbe21bdcb4385fff863b0242060f1e071ad380d9*

Encrypt Decrypt

In block

****

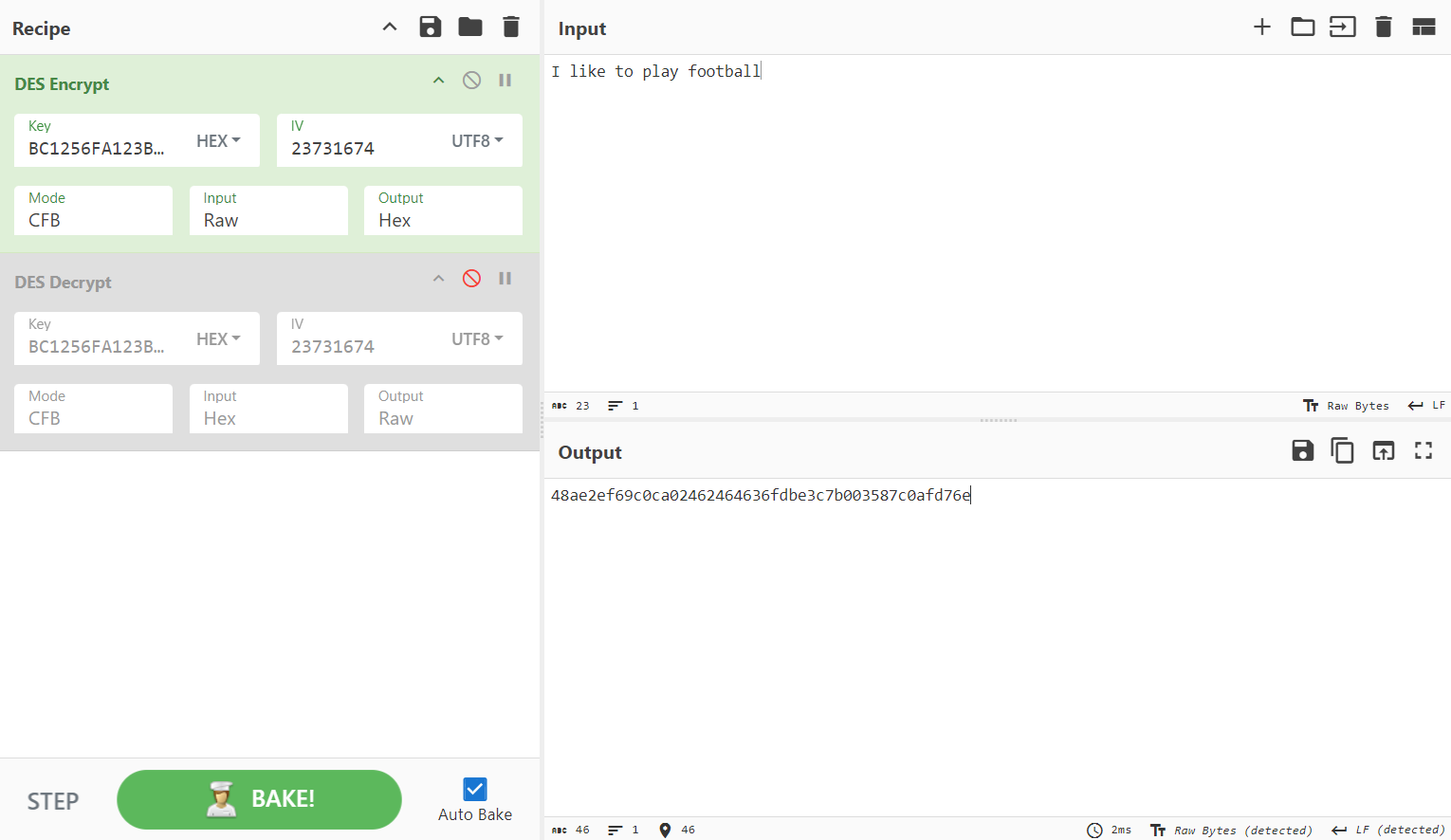
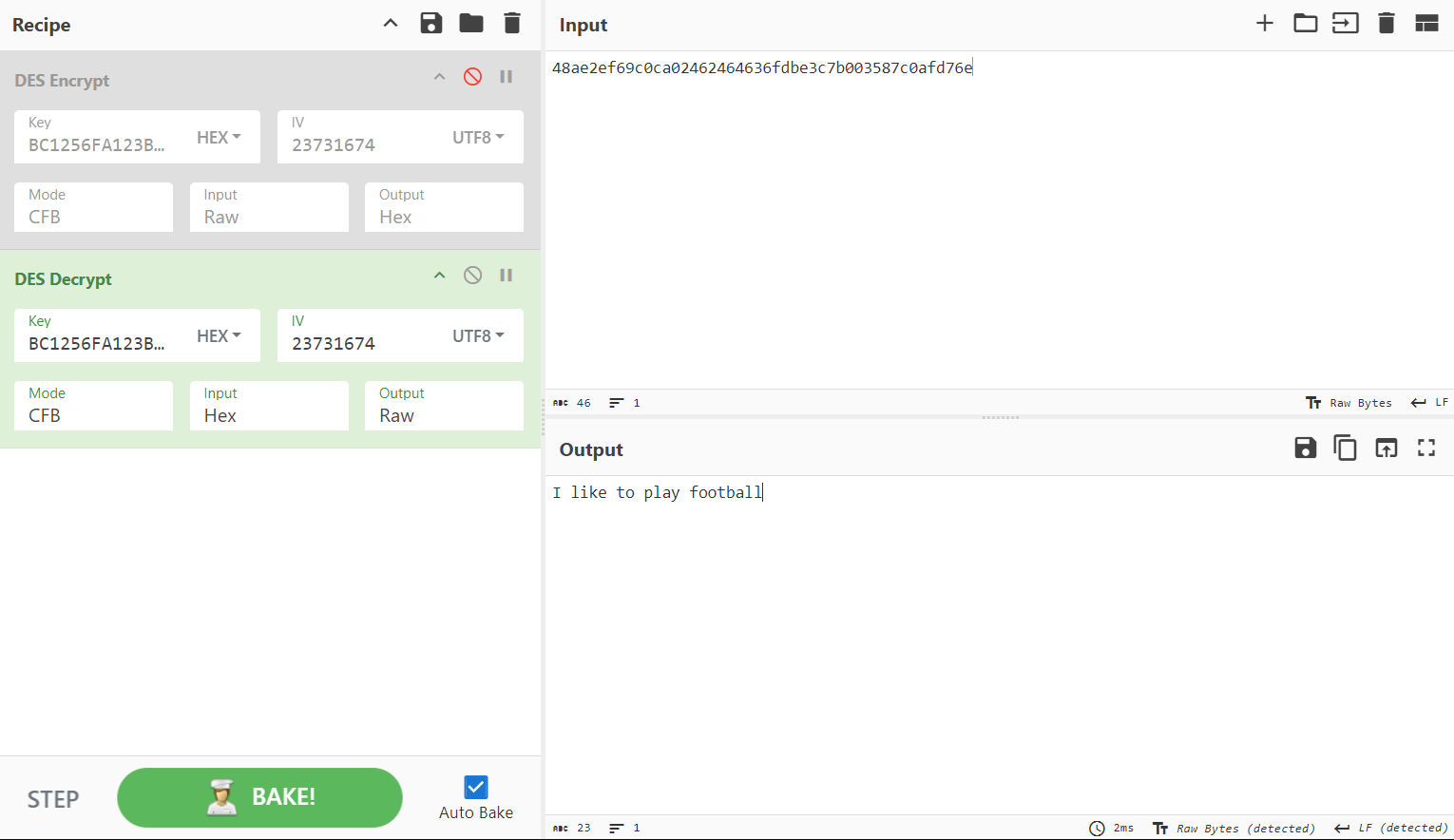
**3.MODE CFB**

**KEY(HEX):** *BC1256FA123BC123* **IV(UTF-8):** *23731674*

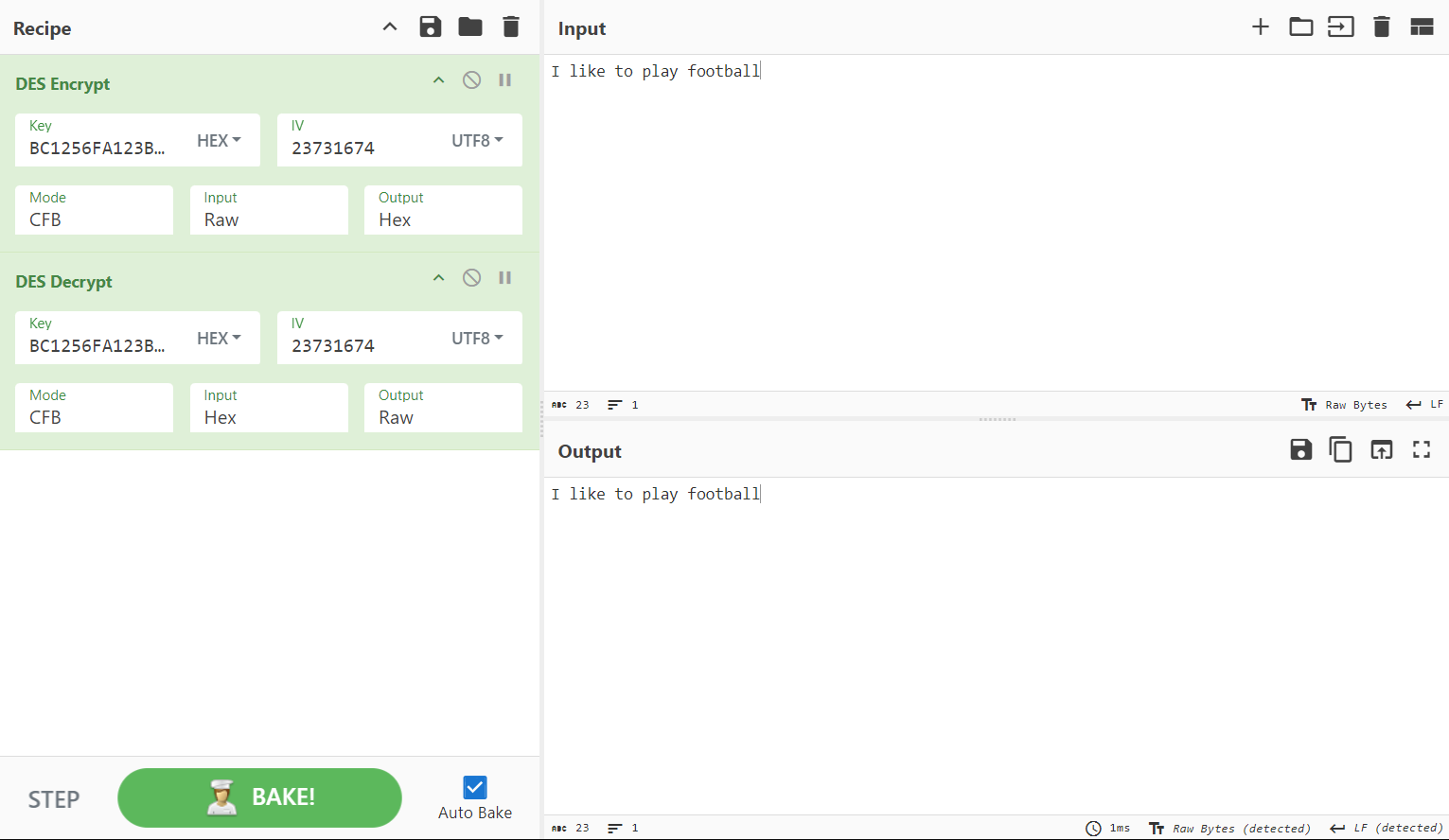
**ВТ:** *I like to play football*

**ШТ:** *48ae2ef69c0ca02462464636fdbe3c7b003587c0afd76e*

Encrypt Decrypt

In block



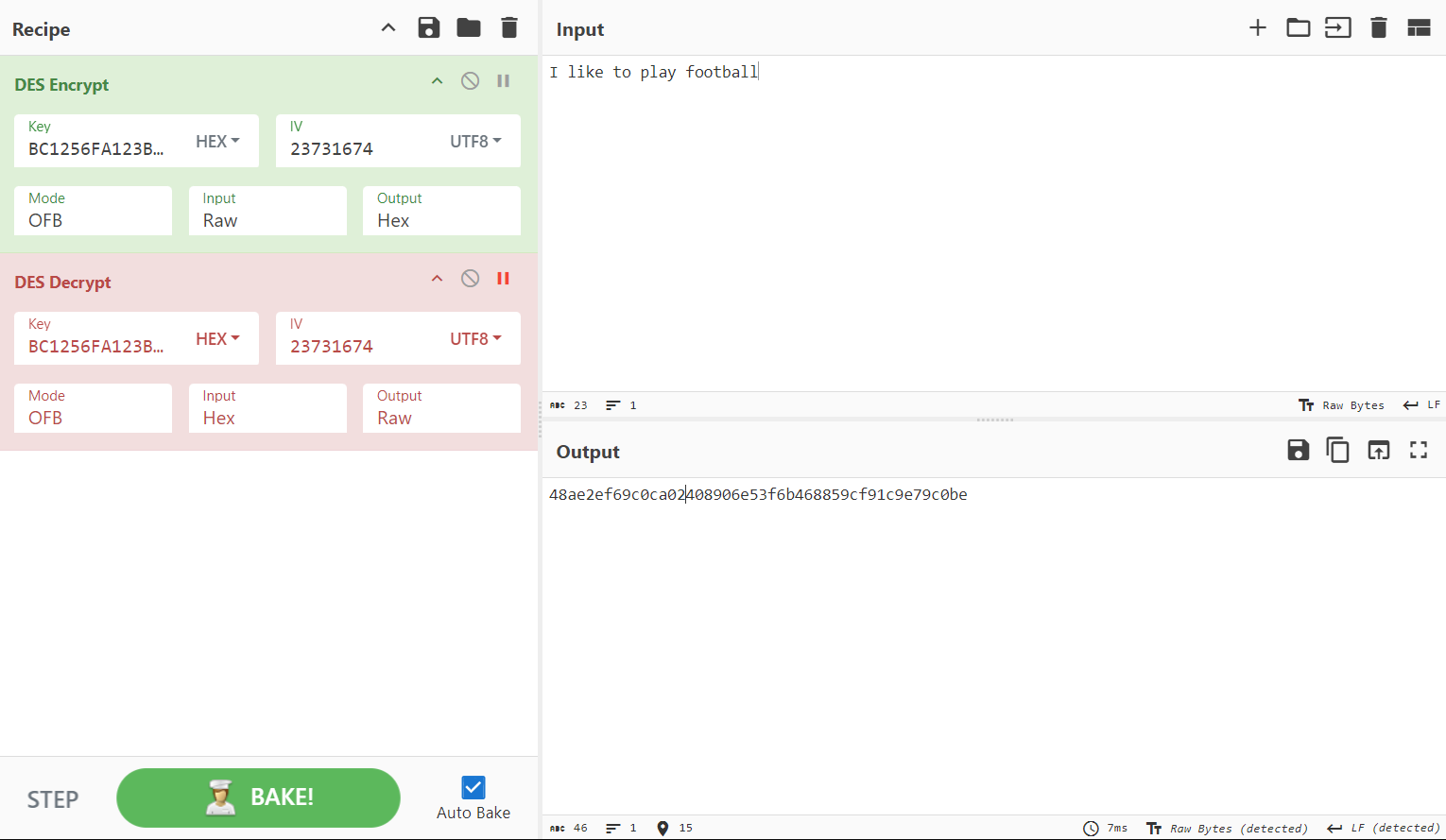
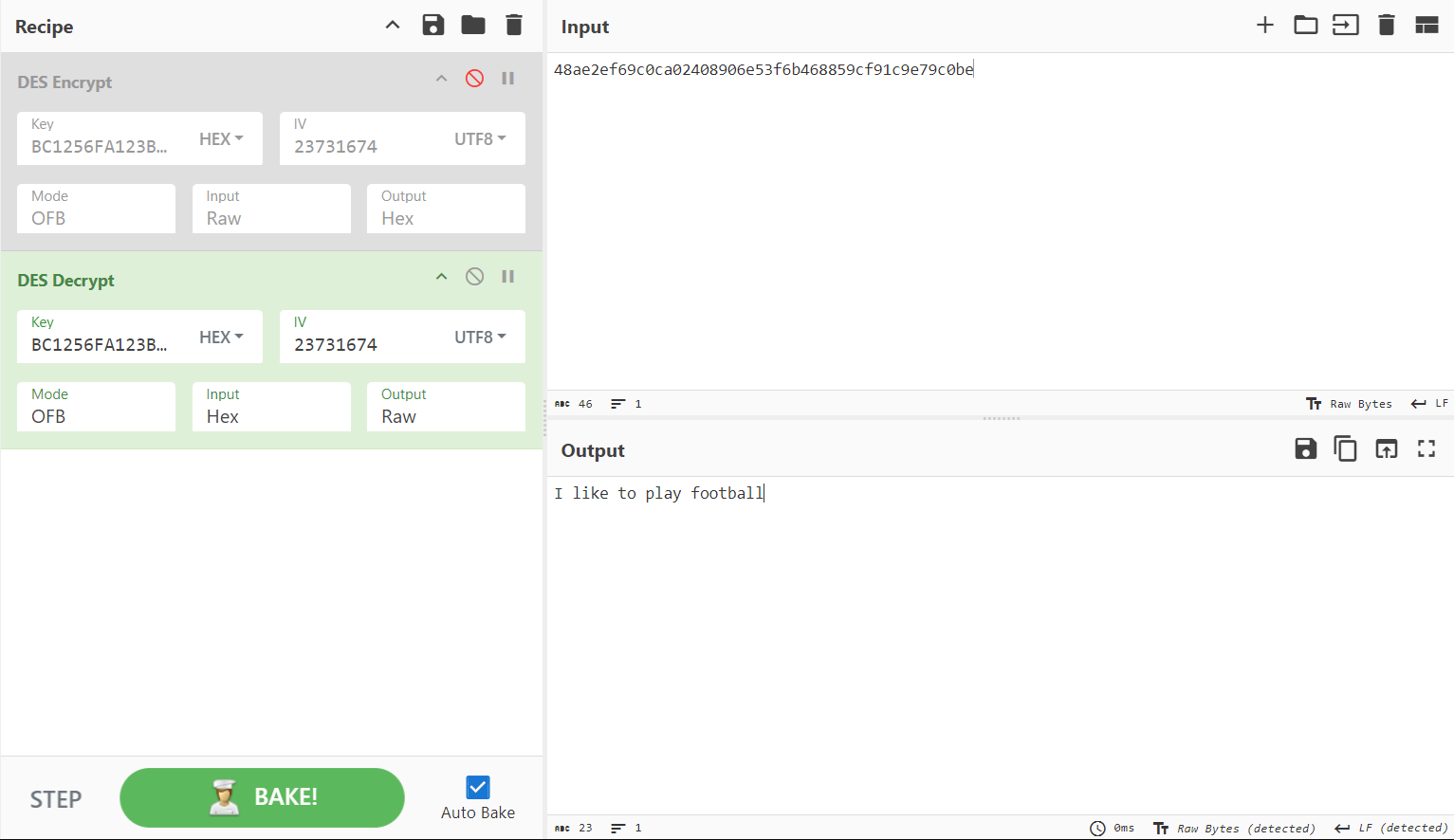
**4.MODE OFB**

**KEY(HEX):** *BC1256FA123BC123* **IV(UTF-8):** *23731674*

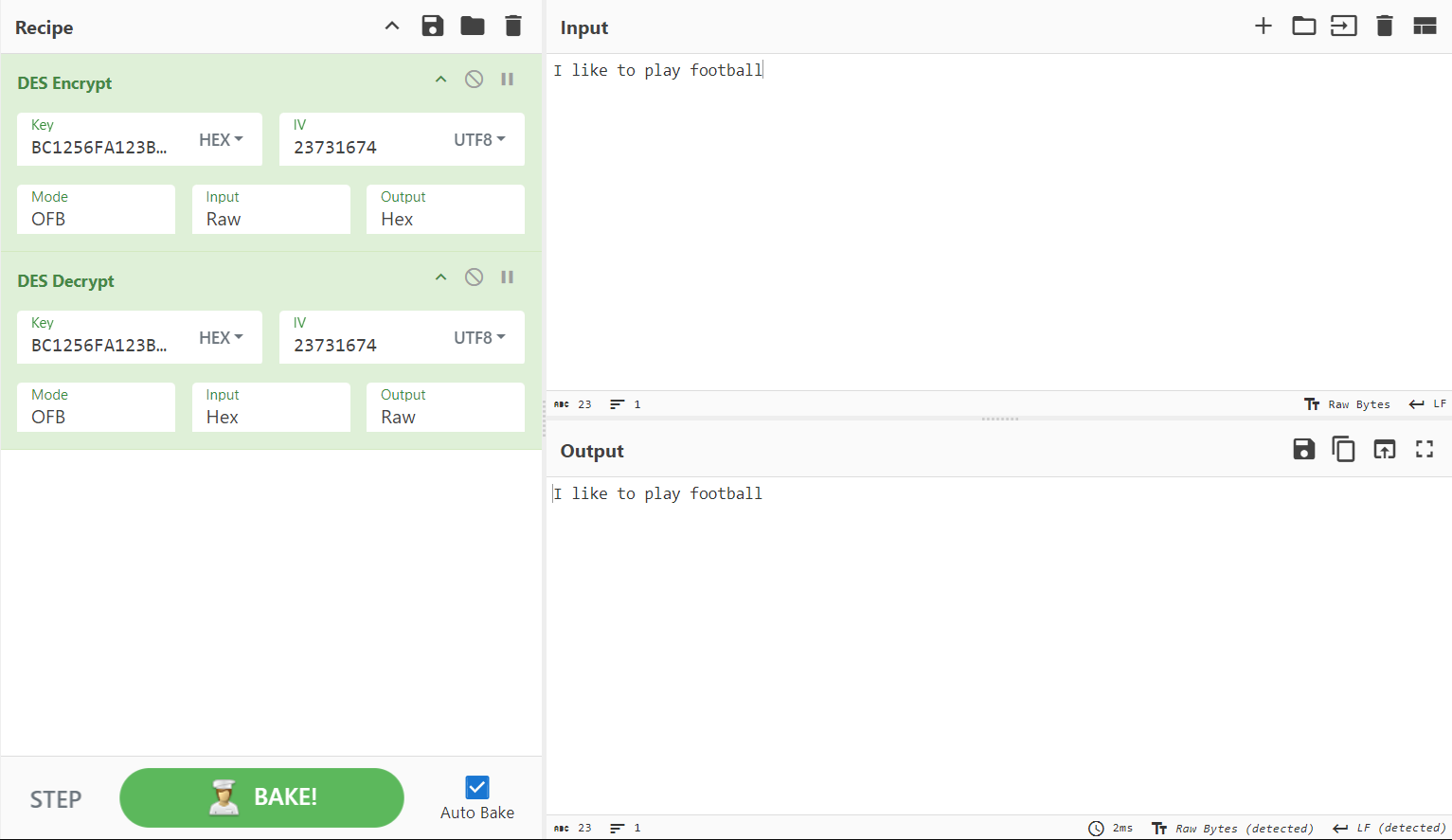
**ВТ:** *I like to play football*

**ШТ:** *48ae2ef69c0ca02408906e53f6b468859cf91c9e79c0be*

Encrypt Decrypt

In block



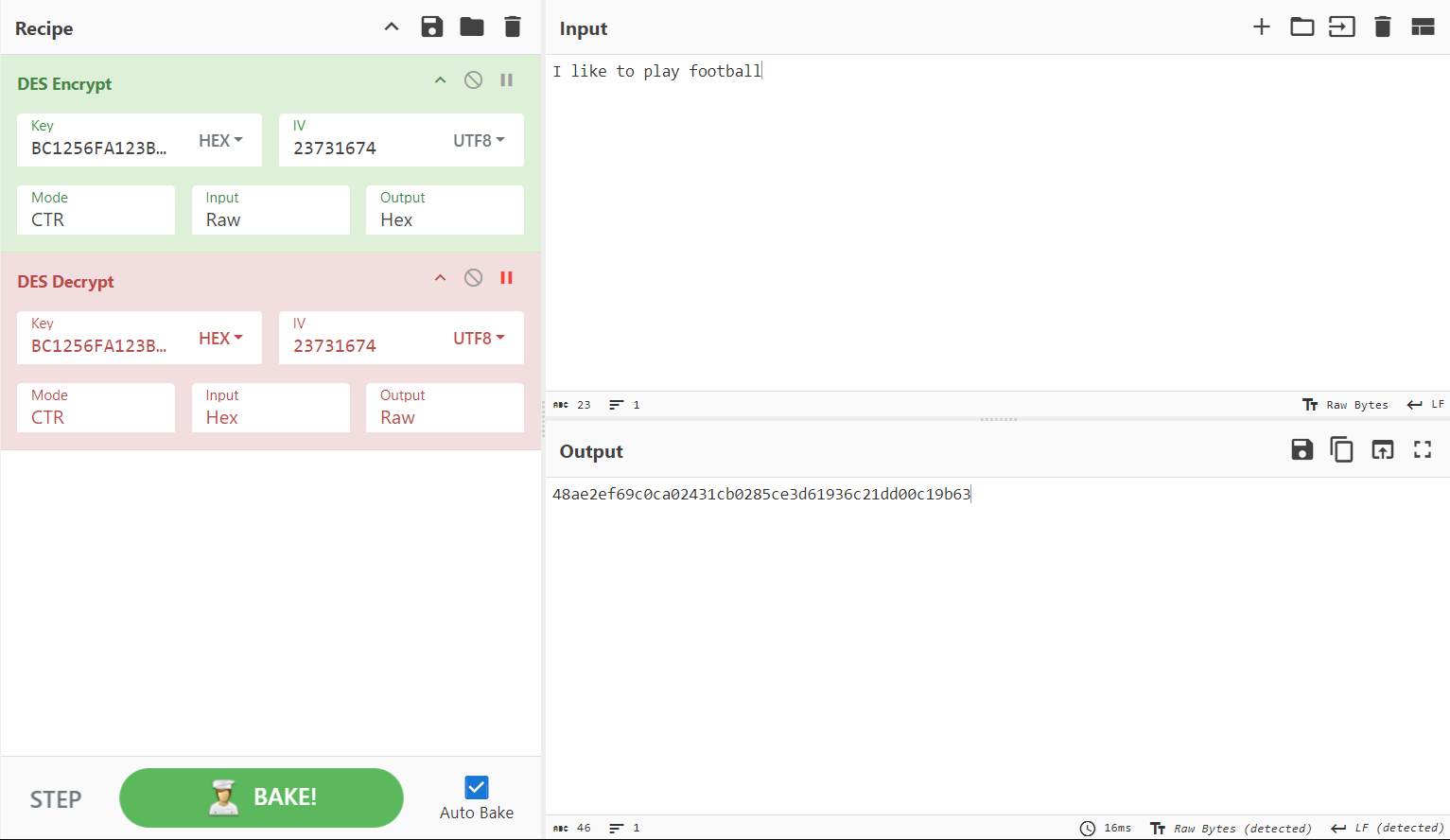
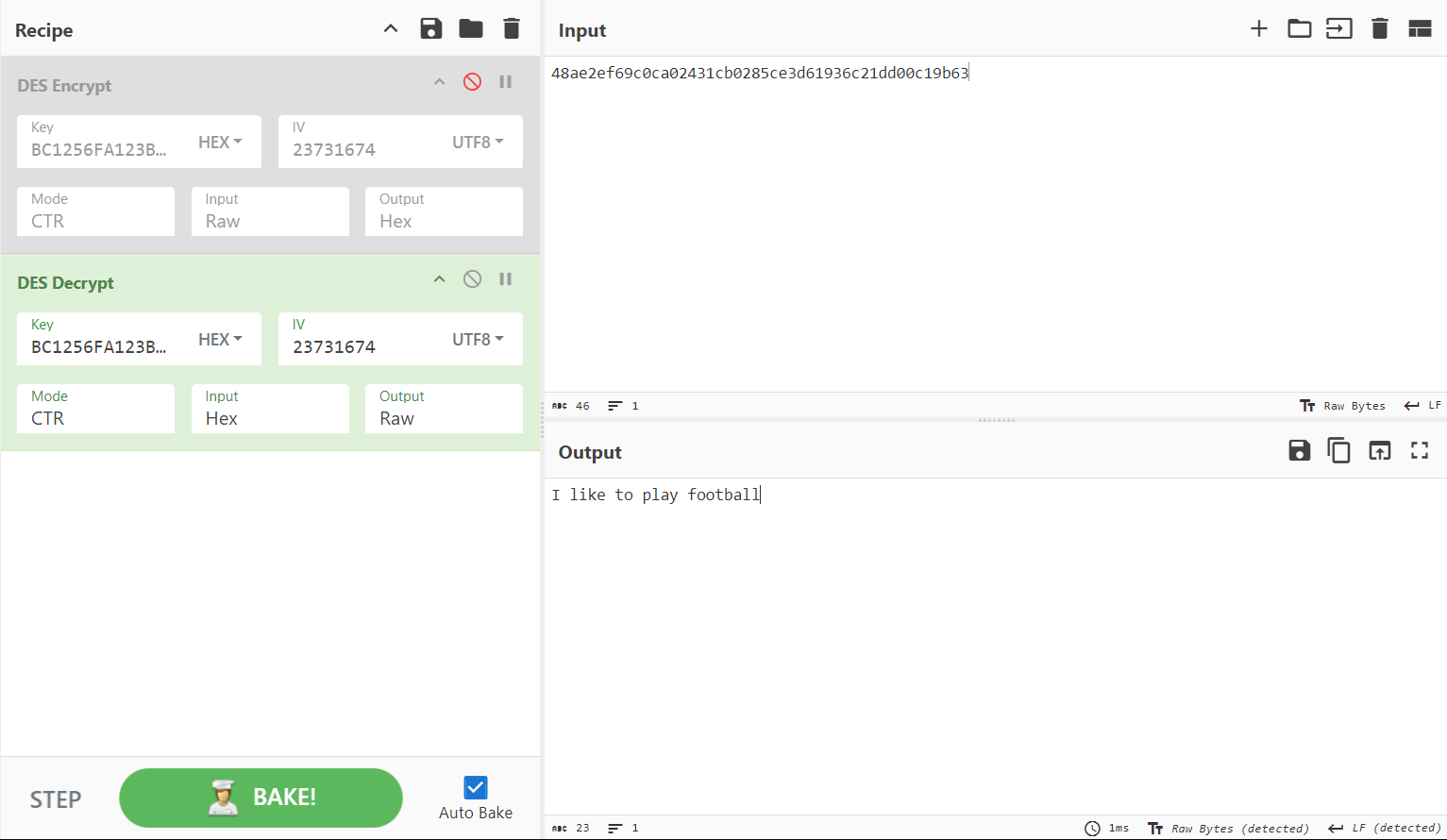
**5.MODE CTR**

**KEY(HEX):** *BC1256FA123BC123* **IV(UTF-8):** *23731674*

**ВТ:** *I like to play football*

**ШТ:** *48ae2ef69c0ca02431cb0285ce3d61936c21dd00c19b63*

Encrypt Decrypt

In block

