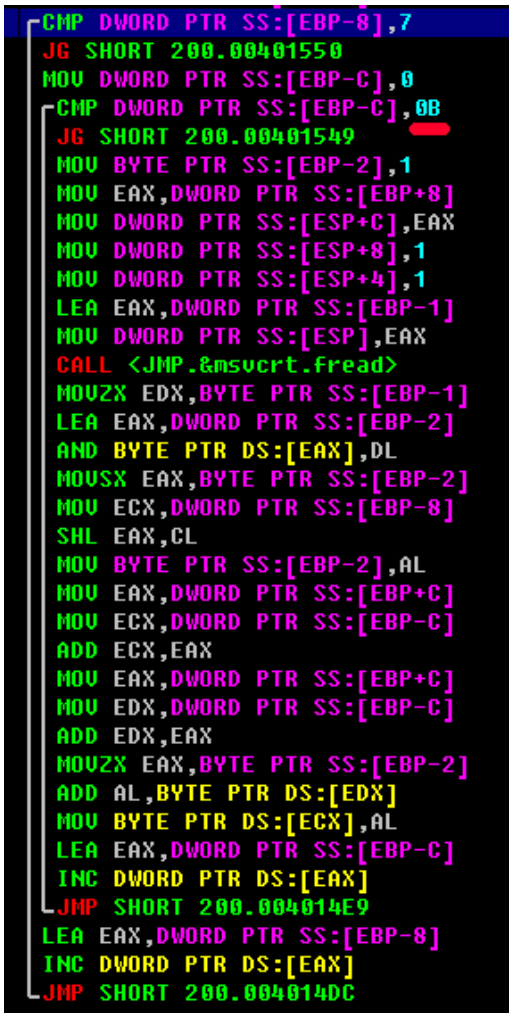
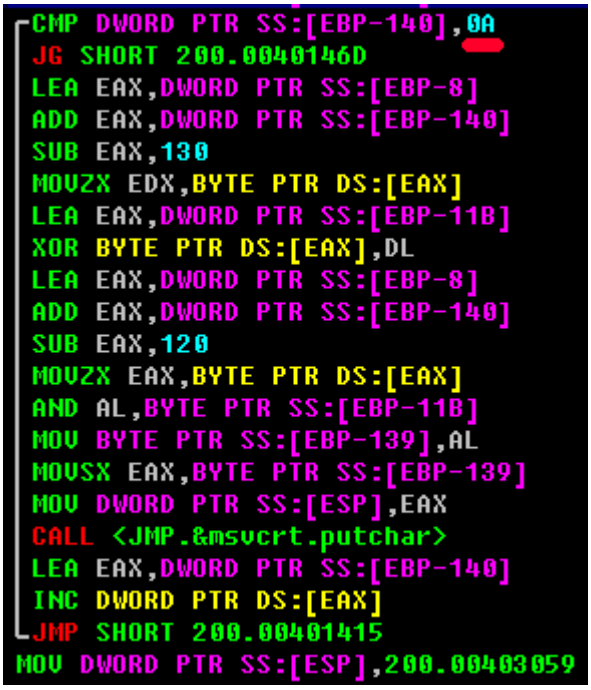
WriteUP Reverse 200. KrasCTF 2017

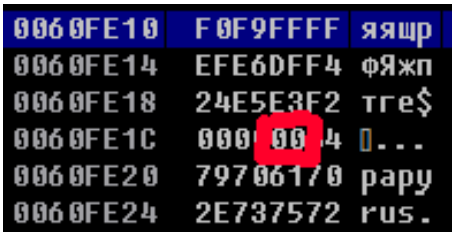
Программа достает из изображения массив данных длиной 12 элементов.



Но при расшифровке сообщения используются 11 элементов.



Двенадцатый элемент необходим именно для расшифровки, но вместо него используется значение, лежащее по адресу 0060FE1D.



Поэтому патчим цикл расшифровки и получаем флаг.