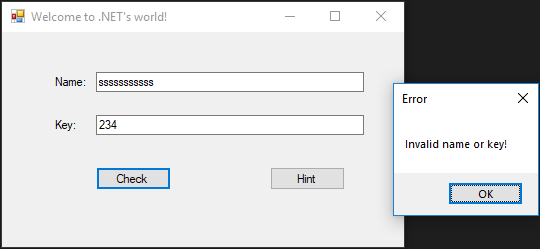
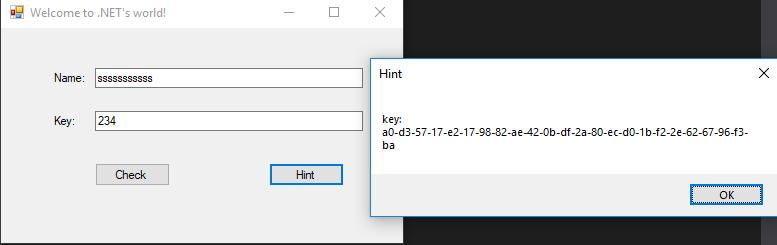
1. basic

chạy thử chương trình ta có

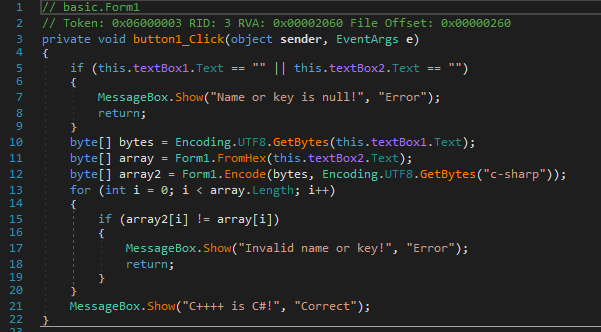


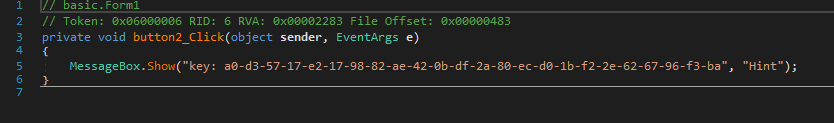
chương trình yêu cầu nhập vào Name và key nếu đúng sẽ hiện thị 1 cái gì đó. trong trường hợp sai sẽ hiện thông báo sai

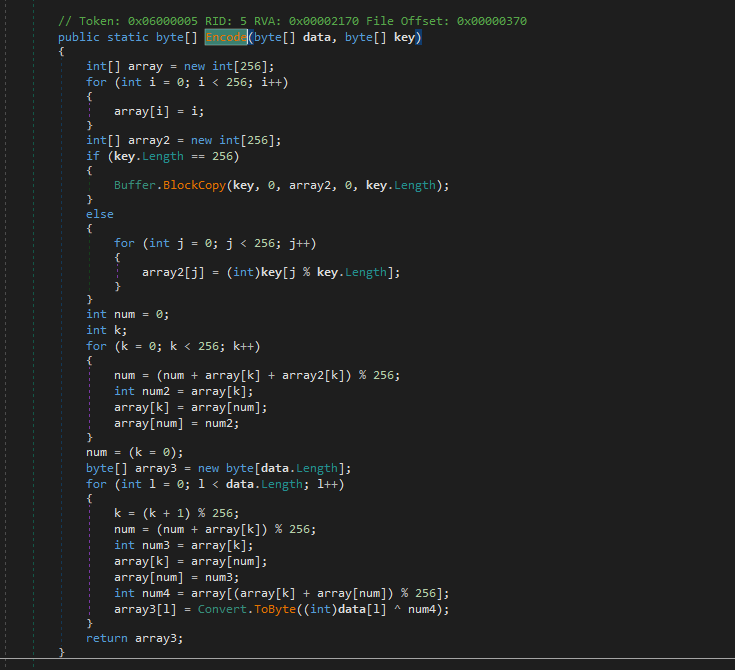


có buttom Hint nhấn thử thì có

dùng DnSpy để phân tích chương trình

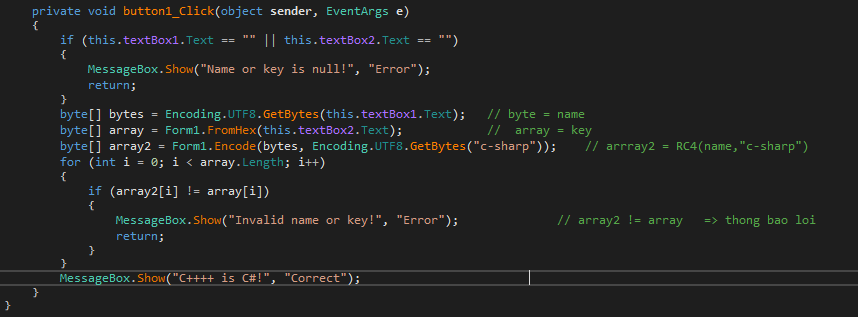






1. Hàm Encode ta thấy đây chính là thuật toán của  mã RC4
2. 2 button (button1 và button 2 ) ta đã phân tích sơ qua ở trên bây giờ sẽ phân tích chi tiết.

* Button2 chỉ đơn giản là show ra key dưới dạng đã được mã hóa a0-d3-57-17-e2-17-98-82-ae-42-0b-df-2a-80-ec-d0-1b-f2-2e-62-67-96-f3-ba
* Button1

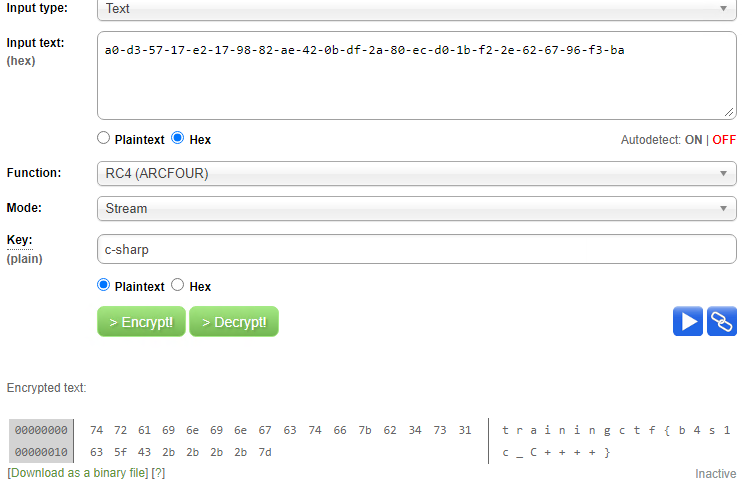


array2 có được bằng cách mã hóa chuỗi nhập vào ở textBox **name** với key\_RC4 là “c-sharp” sau đó tiến hành so sánh với array là chuỗi nhập vào ở textBox **key**

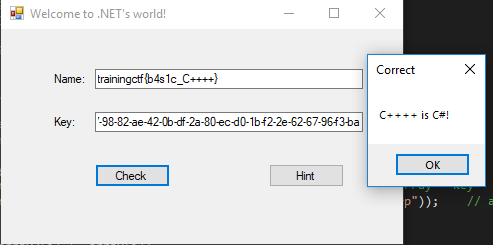
ta đã biết mảng **array (a0-d3-57-17-e2-17-98-82-ae-42-0b-df-2a-80-ec-d0-1b-f2-2e-62-67-96-f3-ba)**

tức biết được mảng **array2** biết được key của mã RC4 là **c-sharp** từ đó có thể tìm ra

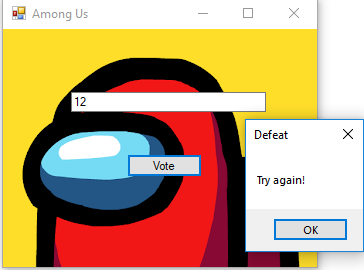
**name**



tìm được giá trị cần nhập vào ở textBox name là: **trainingctf{b4s1c\_C++++}**



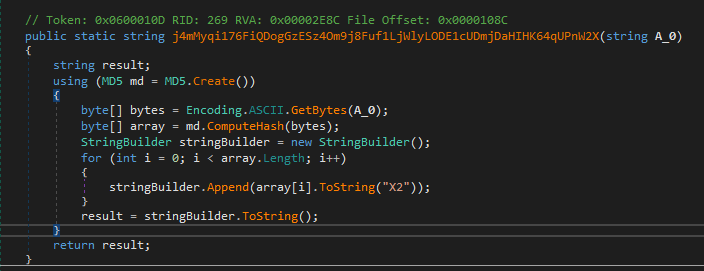
Find\_Imposter



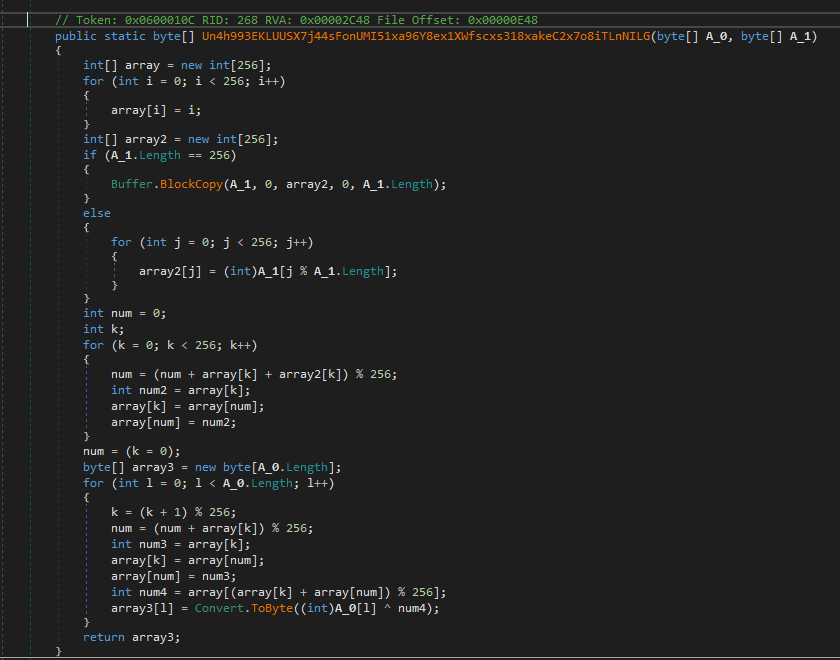
Chương trình yêu cầu nhập vào textBox sau khi click vào button Vote thì sẽ hiện thông báo



button 1



hàm băm MD5



thuật toán RC4



hàm Encoding chỉ là convert từ string sang kiểu byte

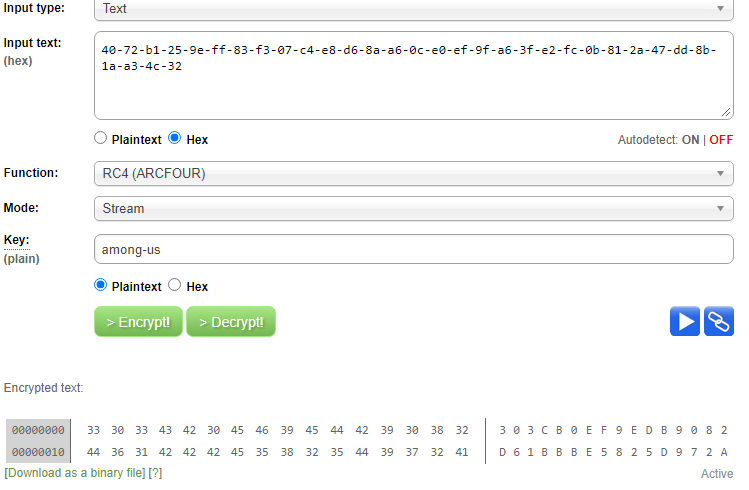
chuỗi s chính là input sau khi băm bằng hàm băm MD5

byte chính là chuỗi “among-us”

array  được mã hóa bằng hàm RC4 với key là “among-us”

array2 là chuỗi có sẵn

vì array = array2 chương trình mới hiện thị ra flag nên từ đây là có được giá trị của mảng byte

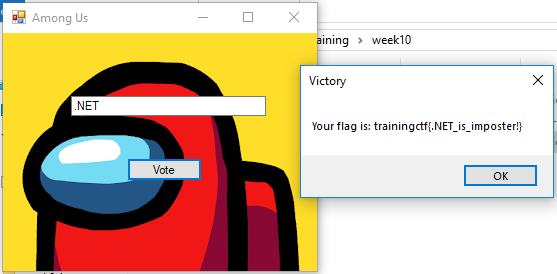


bytes=[ 0x33,0x30,0x33,0x63,0x62,0x30,0x65,0x66,0x39,0x65,0x64,0x62,0x39,0x30,0x38,0x32,0x64,0x36,0x31,0x62,0x62,0x62,0x65,0x35,0x38,0x32,0x35,0x64,0x39,0x37,0x32,0x61 ]

=> s = “303cb0ef9edb9082d61bbbe5825d972a”

hàm băm MD5 không thể giải mã ngược nhưng nhờ vào cơ sở dữ liệu có sẵn ta  tìm được chuỗi s la “.NET”

=> input  là .NET



flag là : traningctf{.NET\_is\_imposter!}