ما متغیرهای ورودی و خروجی رو u8\* انتخاب کردیم.

اما cbc\_mac متغیرهای u32\* می خواد برای ورودی اش. که ما مجبوریم cast کنیم: (خط 241)

cbc\_mac((u32\*)msg,msgSize\*8,(u32\*)IV,(u32\*)output,key,128);

درون تابع cbc\_mac از یک blockcipher باید استفاده بشه که این جا AES خواهد بود. اما مشکل اینه که این سایفر خودش متغیرهای u8\* می خواد که مجبوریم دوباره u32\* رو به u8\* cast بکنیم: ( خطوط 166 و 183)

blockcipher((u8\*)out,(u8\*)out,key,keySize);