Computer Security Homework 0x0A

Real name: 涂世昱

Nick name: R07922115

Student ID: R07922115

Mandalorian

Explaination

這題直接使用助教上課所提的方法, `LSB Oracle Attack`, 我這邊是用方法二, 然後將`mod 2`改為`mod 16`, 其中每個loop會將`c`(cipher)乘上16^{-ie}, 就會收到對應的4bits的text, 再根據公式就可以得到x_i, 所以當所有x_i都找出來之後, 則必須兩兩合併為8 bits的數所構成的list, 再reverse過後再將它印出來, 就可以看到flag了。

i.e. 方式如下,

1. 取得 `n`, `cipher`
2. x = [], for each iteration i:
   (1) send $(16^{-i})^e c$
   (2) 得到 r
   (3) $x_i = (r - (\sum_{j=0}^{len(x)} x_j \times 16^{-(len(x)-j)}) mod\ n) mod\ 16$
   (4) x.append(x_i)
3. 將`x`兩兩合併為byte構成的array, 然後將它reverse再印出來就可以得到答案。