Computer Security HWA Write-Up

Student ID: B07902143
Account: soyccan
Name: 陳正康

Mandalorian

FLAG{Youg0tTH3Fl4GIHavesPoKEN}

RSA Chosen Ciphertext Oracle Attack

we can obtain public key (n, e) and a piece of ciphertext c
and we can send any chosen ciphertext cc to server,
server will respond: $decrypt(cc) \mod 16$

Limited Query Times

we are supposed to crack the plaintext with at most (1024 // 4 + 5) queries

Strategy: 16-ary search

similar to binary search in LSB Oracle Attack

we can let $cc = 16^e c$ and get oracle response $o(cc)$
let plaintext of c be m
since:
$c = encrypt(m) = m^e \mod n$
and:
$decrypt(16^e c)$
$\equiv (16^e c)^d \pmod n$
$\equiv 16^{ed} c^d \pmod n$
$\equiv 16^{ed} m^{ed} \pmod n$
$\equiv (16m)^{ed} \pmod n$
$\equiv decrypt(encrypt(16m)) \pmod n$
$\equiv 16m \pmod n$
thus:
$o(16^e c) = decrypt(16^e c) \mod 16$
$= 16m \mod n \mod 16$

then we can determine the range of m:

$$o(cc) = \begin{cases} 16m \mod 16 & \text{if } m \in [0, n/16) \\ (16m - n) \mod 16, & \text{if } m \in [n/16, 2n/16) \\ (16m - 2n) \mod 16, & \text{if } m \in [2n/16, 3n/16) \\ \ldots \\ (16m - 15n) \mod 16, & \text{if } m \in [15n/16, n) \end{cases}$$

in general:
$o(16^e c) = (-in) \mod 16, \quad \text{if } m \in [in/16, (i+1)n/16)$

similarly:
$o(32^e c) = (-in) \mod 16, \quad \text{if } m \in [in/32, (i+1)n/32) \cup [in/32 + n/2, (i+1)n/32 + n/2)$

and so on

we can reduce a 16-ary search on $[0, n)$ to find m

query times

this require $\log_{16} n$ queries
for an 1024-bit n
$\log_{16} n \leq \log_{16} 2^{1024} = 1024/4$
within the limit !

implementation issue

since dividing an integer interval into 16 partitions requires floating number calculation,
precision loss may cause last 3 bytes of the cracked plaintext uncertain
$\implies$ use **fraction** calucation

Reference

https://furutsuki.hatenablog.com/entry/2020/01/01/221936
(https://furutsuki.hatenablog.com/entry/2020/01/01/221936)