Computer Security Hw0x0A Writeup

- Realname: 胡安鳳
- ID on course web: alfons0329
- Student ID: R08922024

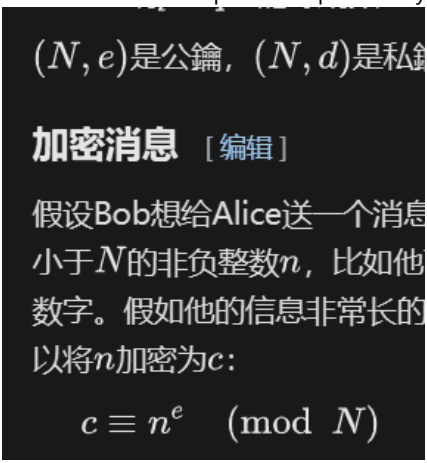
tags: Computer Security NTU CS CS CTF Writeup

Mandalorian (crypto)

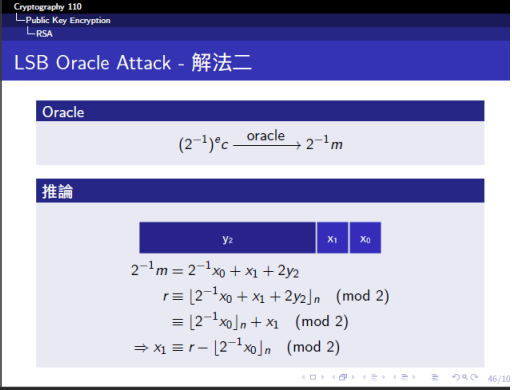
A classical RSA LSB attack.

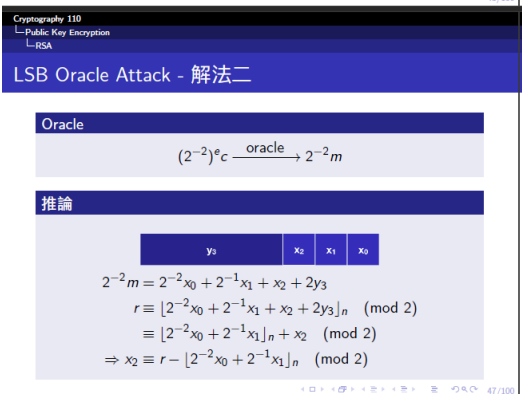
Step 1: Get c, e, n in RSA from the server.

The c e n are the cipher and public key pair (e, N) in RSA encryption.



Step 2: LSB attack as the Cryptography 110 ppt shown.





The flag will be $(xn, xn-1 \ldots\ldots, x1, x0)$, with $c \to m$, and MOD being 16.

So the overall exploitation will be.

$$((base^{-ie}))c \to (base^{-i})m$$

The i above is equivalent to `pow_cnt` shown below and the LSB message forging will be

```
multiplied_c = pow(base, pow_cnt * e, n) * c % n # ((base ^ {-ie}))c
rem.sendline(str(multiplied_c))
multiplied_m = int(rem.recvline().split()[-1]) # (base ^ {-i})m
```

So the overall LSB attack part

```python
pow_cnt = 0
try_cnt = 0
flag_res = 0
flag_list = []

while try_cnt < 1024 // 4:
    rem.sendlineafter('>', '2')

    # under the mod n cycle
    multiplied_c = pow(base, pow_cnt * e, n) * c % n
    rem.sendline(str(multiplied_c))
    multiplied_m = int(rem.recvline().split()[-1])
    r = multiplied_m % n % MOD

    tmp = 0
    start_pow = len(flag_list)
    for i in range(len(flag_list)):
        tmp += pow(base, start_pow, n) * flag_list[i]
        start_pow -= 1

    xi = (r - ((tmp) % n)) % MOD

    # check if the received bit(ot byte) is the padding zero
    # (continuously padding zero), break as the threshold meets
    if xi == 0:
        if continuous_padding >= 10:
            break
        else:
            continuous_padding += 1
    else:
        continuous_padding = 0

    flag_list.append(xi)
    # make flag_res grow bigger, ex:
    # x2x1x0 will be mod ** 2 * x2 + mod ** 1 * x1 + mod ** 0 8 x0
    # (just like naive method for turning 0x7FB to 2043)
    flag_res = (((MOD ** pow_cnt) % n * xi) %n + flag_res) % n
    print(hex(flag_res))
    pow_cnt += 1
    try_cnt += 1
```

Gradually decrypting to have a flag.

```
0x6f4b454e7d
0x506f4b454e7d
0x3506f4b454e7d
0x73506f4b454e7d
0x573506f4b454e7d
0x6573506f4b454e7d
0x66573506f4b454e7d
0x766573506f4b454e7d
0x1766573506f4b454e7d
0x61766573506f4b454e7d
0x861766573506f4b454e7d
0x4861766573506f4b454e7d
0x94861766573506f4b454e7d
```

```
0x494861766573506f4b454e7d
0x7494861766573506f4b454e7d
0x47494861766573506f4b454e7d
0x447494861766573506f4b454e7d
0x3447494861766573506f4b454e7d
0xc3447494861766573506f4b454e7d
0x6c3447494861766573506f4b454e7d
0x66c3447494861766573506f4b454e7d
0x466c3447494861766573506f4b454e7d
0x3466c3447494861766573506f4b454e7d
0x33466c3447494861766573506f4b454e7d
0x833466c3447494861766573506f4b454e7d
0x4833466c3447494861766573506f4b454e7d
0x44833466c3447494861766573506f4b454e7d
0x544833466c3447494861766573506f4b454e7d
0x4544833466c3447494861766573506f4b454e7d
0x74544833466c3447494861766573506f4b454e7d
0x74544833466c3447494861766573506f4b454e7d
0x3074544833466c3447494861766573506f4b454e7d
0x73074544833466c3447494861766573506f4b454e7d
0x673074544833466c3447494861766573506f4b454e7d
0x5673074544833466c3447494861766573506f4b454e7d
0x75673074544833466c3447494861766573506f4b454e7d
0xf75673074544833466c3447494861766573506f4b454e7d
0x6f75673074544833466c3447494861766573506f4b454e7d
0x96f75673074544833466c3447494861766573506f4b454e7d
0x596f75673074544833466c3447494861766573506f4b454e7d
0xb596f75673074544833466c3447494861766573506f4b454e7d
0x7b596f75673074544833466c3447494861766573506f4b454e7d
0x77b596f75673074544833466c3447494861766573506f4b454e7d
0x477b596f75673074544833466c3447494861766573506f4b454e7d
0x1477b596f75673074544833466c3447494861766573506f4b454e7d
0x41477b596f75673074544833466c3447494861766573506f4b454e7d
0xc41477b596f75673074544833466c3447494861766573506f4b454e7d
0x4c41477b596f75673074544833466c3447494861766573506f4b454e7d
0x64c41477b596f75673074544833466c3447494861766573506f4b454e7d
0x464c41477b596f75673074544833466c3447494861766573506f4b454e7d
0x464c41477b596f75673074544833466c3447494861766573506f4b454e7d
0x464c41477b596f75673074544833466c3447494861766573506f4b454e7d
0x464c41477b596f75673074544833466c3447494861766573506f4b454e7d
0x464c41477b596f75673074544833466c3447494861766573506f4b454e7d
0x464c41477b596f75673074544833466c3447494861766573506f4b454e7d
0x464c41477b596f75673074544833466c3447494861766573506f4b454e7d
0x464c41477b596f75673074544833466c3447494861766573506f4b454e7d
0x464c41477b596f75673074544833466c3447494861766573506f4b454e7d
0x464c41477b596f75673074544833466c3447494861766573506f4b454e7d
0x464c41477b596f75673074544833466c3447494861766573506f4b454e7d
0x464c41477b596f75673074544833466c3447494861766573506f4b454e7d
FLAG{Youg0tTH3Fl4GIHavesPoKEN}[*] Closed connection to edu-ctf.csie.org port 10192
```
]