2022 부채널정보분석 경진대회

7번 문제 : Fault Attack

- 문제 요약

- RSA 복호화 과정($c^d \bmod N$)에서 지수승 연산을 하기 위해 Square-and-multiply 지수승 알고리즘을 사용한다 가정한다. 악의적인 공격자는 Square-and-multiply 지수승 알고리즘의 3번 줄 연산이 일어나지 않게 조절할 수 있는 능력이 있다. 악의적인 공격자는 각 i에 대해 3번 줄 연산을 한 번만 skip하여 2046개의 새로운 메시지를 얻었다.
그런데 공격자의 부주의로 2046개의 메시지가 어떠한 i를 skip한 메시지인지 알 수 없게 되었다.
비밀키 d를 복구하라.

Square-and-multiply 지수승 알고리즘 [ref1]
입력 : $x \in (\mathbb{Z}/N\mathbb{Z})^{\times}$, $d = (d_{t-1}, \dots, d_0)_2$
출력 : $y = x^d$
1. $R_0 \leftarrow 1, R_1 \leftarrow x$
2. for $i = t-1$ down to 0 do
3. $\quad R_0 \leftarrow R_0^2$
4. $\quad$ if $d_i = 1$ then
5. $\quad\quad R_0 \leftarrow R_0 \cdot R_1$
6. return R_0

- 제공 파일

  - CTF-7-Fault-message.txt : 공격자가 가진 오류가 발생된 메시지 (2046개)

- 참고 사항

  - 평문 m, 암호문 c, 비밀키 d, 공개키 <N, e>,

  - N = 0xbec9b02a8a91abbf5b67885bfcb3b9692044030e17e8fce85177faea815a7b35e1beadbe90725308c2d76c7ca656ef35a677a70c5015e0efbd13c2171419e9148317c2e5b66a8b7d3e209c836c8d1987fb736f29fcc4e588aa2a00762c6297ac4f7fba7f241e3b49ae806898d49cf7027b20b049bc03939b5a651bbd9afceed431f2214b739083bae5c21475966f1a4aa3137006bb6b26a779ae0b9a584151001406ba024c689c018794cbcc4f237532461514a21e1a57aa56504b436e0939acaedfddafabac08e3a575207d6ab274c066674732362ad78925ef646414f038bbbb2b6f754e57f5ed0ab8aff1b541679e16aa959a40785bb748214d5a24a87b29

  - C = 0x1f549e6512a3a24c86b6dfaa159faca736c56ab6114ea2abcf16fe1bbf09469dfadba49f46bc16a96ecf0c0c46cd3eb4051ce70b720a9d92c6983900efef2d7d3337a0f2397554e6957fda21f860f8731822fa520dbe6f4d7f8ec8a207514e532b13f5e22a59bd3ccd0b6a437a175c2cc0528ea0

fcf064d2f8b9a8ba88768010549143950d54451ced3799fa39eb14c8afed652c9fee36872984a7a1a42d800aaa5657ef3e9a3ef530e3745021a76286548f381bbc583f65008d117cd5f4791644c1aa38246e7397811bbca171920689a291b6228c9cf1a08b5ec9c46850dd2f76207d961590ca364dca203379afcd033e47370750f991dc84f27ea2d48b6290

- e = 0x275a37b7d3bbfe4bf119fd22438c44c223e58d0c882fcd37d4e18126d7b0e34b2820b0caa1e35895ef736125a76df23b46f847011e24af4bf613fa753219a8020390b5ef2c5eead63d382786c8b2eae2e7a2c05660c7a0626e7c58d587b499a6529b85058c7a4b207c95e2d88935a70f2c2e894c39c305467bebb4d8d66106539fac24b114635e668b8ddf56e77d8033d7ec92c50e4fa8250ff441c8ff60dbecb2ea7702fa667eede86fa3784cd98e30adc9d3651c1ba551c410826c89267f81db23d9953c1c845e8416b13ef7553b18dad13d1bb92ff2de5f78dfbd5677c09849ddc1663369472cf9924575a64f2f99aecab654a8737d5d77bda684b48a2819

- m = 0x4661554c7441547461434b40725341

- 플래그

- 복구한 d를 이용해 (d * 123) mod 2^{128}을 계산한 후 MSB 부터 차례로 hex 값으로 삽입

- 참고 문헌

- Ref.-1 : Joye, Marc. A Method for Preventing “Skipping” Attacks