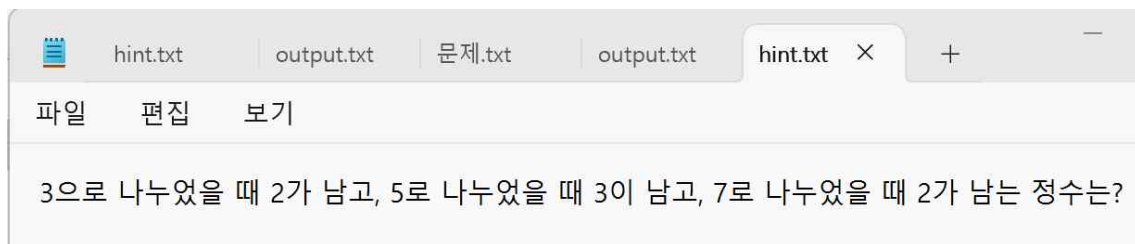


<Math - RSA>

파일을 열어 보았다.

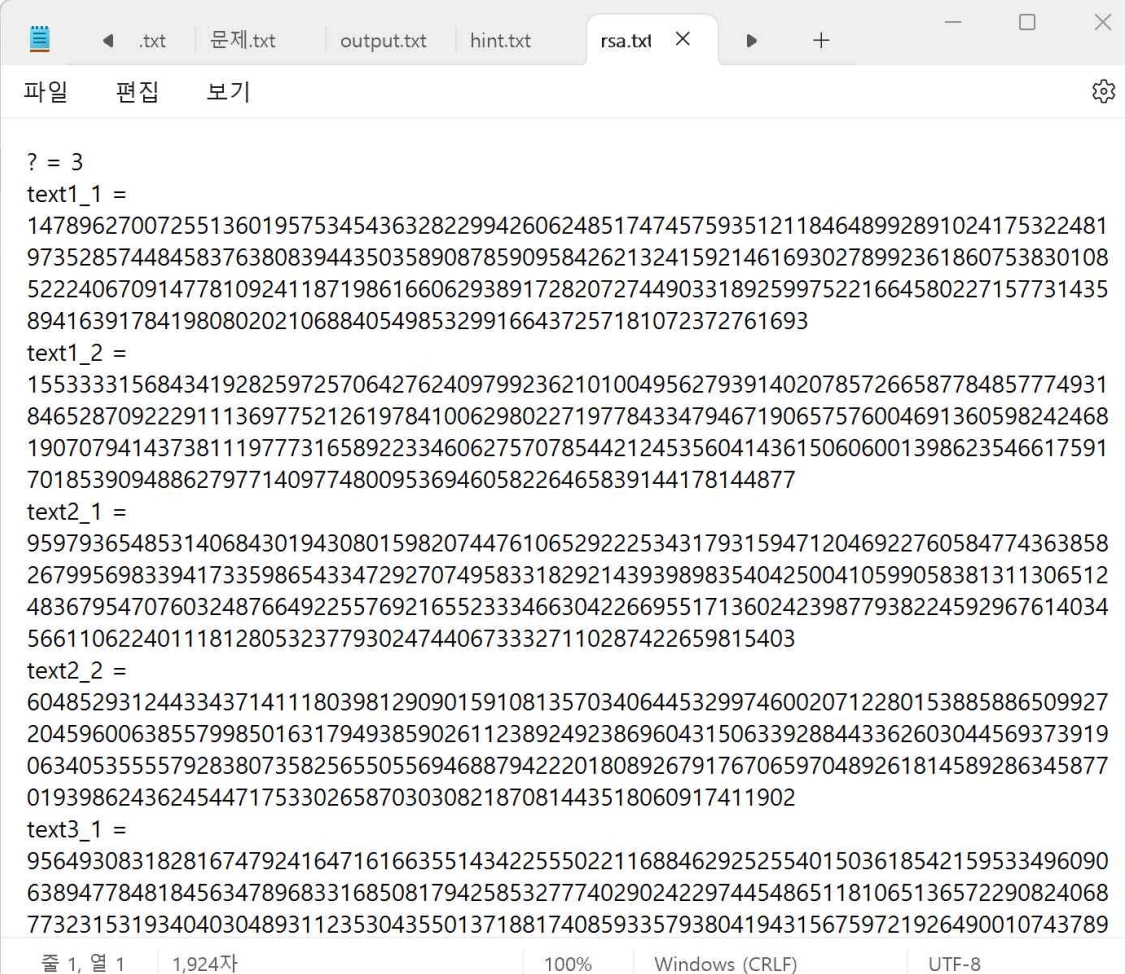
 hint		2024-07-24 오후 11:49	텍스트 문서	1KB
 rsa		2024-07-25 오전 12:12	텍스트 문서	2KB
 문제		2024-07-25 오전 12:14	텍스트 문서	1KB

존재하는 텍스트 파일을 순서대로 열어보았다.



3으로 나누었을 때 2가 남고, 5로 나누었을 때 3이 남고, 7로 나누었을 때 2가 남는 정수는 중국인의 나머지 정리를 통해서 찾을 수 있다. 주어진 조건을 만족하는 가장 작은 정수는 23이다.

RSA 텍스트 파일은 다음과 같았다.



The screenshot shows a text editor window with the following content:

```
? = 3
text1_1 =
14789627007255136019575345436328229942606248517474575935121184648992891024175322481
97352857448458376380839443503589087859095842621324159214616930278992361860753830108
52224067091477810924118719861660629389172820727449033189259975221664580227157731435
894163917841980802021068840549853299166437257181072372761693
text1_2 =
15533331568434192825972570642762409799236210100495627939140207857266587784857774931
84652870922291113697752126197841006298022719778433479467190657576004691360598242468
19070794143738111977731658922334606275707854421245356041436150606001398623546617591
70185390948862797714097748009536946058226465839144178144877
text2_1 =
95979365485314068430194308015982074476106529222534317931594712046922760584774363858
26799569833941733598654334729270749583318292143939898354042500410599058381311306512
48367954707603248766492255769216552333466304226695517136024239877938224592967614034
56611062240111812805323779302474406733327110287422659815403
text2_2 =
60485293124433437141118039812909015910813570340644532997460020712280153885886509927
20459600638557998501631794938590261123892492386960431506339288443362603044569373919
0634053555792838073582565505569468879422201808926791767065970489261814589286345877
01939862436245447175330265870303082187081443518060917411902
text3_1 =
95649308318281674792416471616635514342255502211688462925255401503618542159533496090
63894778481845634789683316850817942585327774029024229744548651181065136572290824068
77323153193404030489311235304355013718817408593357938041943156759721926490010743789
```

줄 1, 열 1 | 1,924자 | 100% | Windows (CRLF) | UTF-8

RSA는 공개 키 암호화 방식 하나로, 해당 알고리즘은 두 개의 큰 소수를 기반으로 한다. 원지 전혀 모르겠어서 살짝 찾아봤다. 근데 그래도 어렵다.

RSA 알고리즘의 기본 개념

1. 키 생성:

- 두 개의 큰 소수 p 와 q 를 선택합니다.
- $n = p \times q$ 를 계산합니다. n 은 공개 키의 일부가 됩니다.
- $\phi(n) = (p - 1) \times (q - 1)$ 을 계산합니다.
- e 를 선택합니다. e 는 $1 < e < \phi(n)$ 을 만족하는 e 이며, e 와 $\phi(n)$ 은 서로소(즉, 최대공약수가 1)이어야 합니다.
- d 를 계산합니다. d 는 $d \times e \equiv 1 \pmod{\phi(n)}$ 을 만족하는 수입니다. 즉, d 는 e 의 모듈러 역원입니다.
- 공개 키는 (e, n) 이고, 개인 키는 (d, n) 입니다.

2. 암호화:

- 메시지 M 을 암호화하려면, $C = M^e \pmod{n}$ 를 계산합니다.
- C 는 암호문입니다.

3. 복호화:

- 암호문 C 를 복호화하려면, $M = C^d \pmod{n}$ 를 계산합니다.
- M 은 원래의 메시지입니다.

RSA 암호문을 복호화하려면 RSA의 개인 키를 알아야 한다고 한다.

HINT 값이 23이었으니까 개인 키 (d, n) 을 $(2, 3)$ 으로 설정해볼까?

약간의 구글링을 통해 파이썬으로 복호화 코드를 만들어보았다.

```
malware.py X decode.py rsadiscod.py X
C: > Users > kimye > OneDrive > 바탕 화면 > rsadiscod.py > ...
1 def rsa_decrypt(ciphertext, d, n):
2     """RSA 복호화 함수"""
3     # 복호화 과정
4     plaintext = pow(ciphertext, d, n)
5     return plaintext
6
7 # 개인 키와 모듈러스
8 d = 2
9 n = 3
10
11 # 복호화하려는 암호문
12 texts = [
13     14789627007255136019575345436328229942606248517474575935121184648992891024175322481973528574484583763808394435035890878590958426,
14     15533331568434192825972570642762409799236210100495627939140207857266587784857774931846528709222911136977521261978410062980227197,
15     95979365485314068430194308015982074476106529222534317931594712046922760584774363858267995698339417335986543347292707495833182921,
16     60485293124433437141118039812909015910813570340644532997460020712280153885886509927204596006385579985016317949385902611238924923,
17     9564930831828164792416471616635514342255502211688462925255401503618542159533496090638947784818456347896833168508179425853277740,
18     85737153723532791682986185847254831480032106939823543174113563634075907849864317401408162886710375511127052760055880351226323598,
19 ]
20
21 # 복호화 수행
22 for text in texts:
23     plaintext = rsa_decrypt(text, d, n)
24     print("Plaintext:", plaintext)
25
```

실행을 해보니까 아까와 마찬가지로 파일이 존재하지 않는다고 뜬다.

```
PS C:\Users\kimye> python rsadecode.py
C:\Users\kimye\AppData\Local\Programs\Python\Python312\python.exe: can't open file 'C:\\Users\\kimye\\rsadecode.py': [Errno 2] No such file or directory
```

코드가 잘못된 것 같지는 않은데 자꾸 같은 곳에서 막혀서 답답하다.

경로 설정이 잘못 된건가 싶다가도, 설정되어 있는 경로가 가장 포괄적인 경로라서 모든 파일을 포함하는데 파일이 존재하지 않는다는 건 파일이 저장되어 있지 않다는 것 밖에 의미하지 않는 것 같아서 뭐가 문제인지 모르겠다.