CHALLENGE : Secret Sharing

CATEGORY : Crypto

AUTHOR : 0xsakthi

LEVEL : EASY

Secret Sharing

295

Jo , Pj and Shamir communicating with each other in group, jo ask for a flag, Shamir send's junk of data, did you decrypt this data?

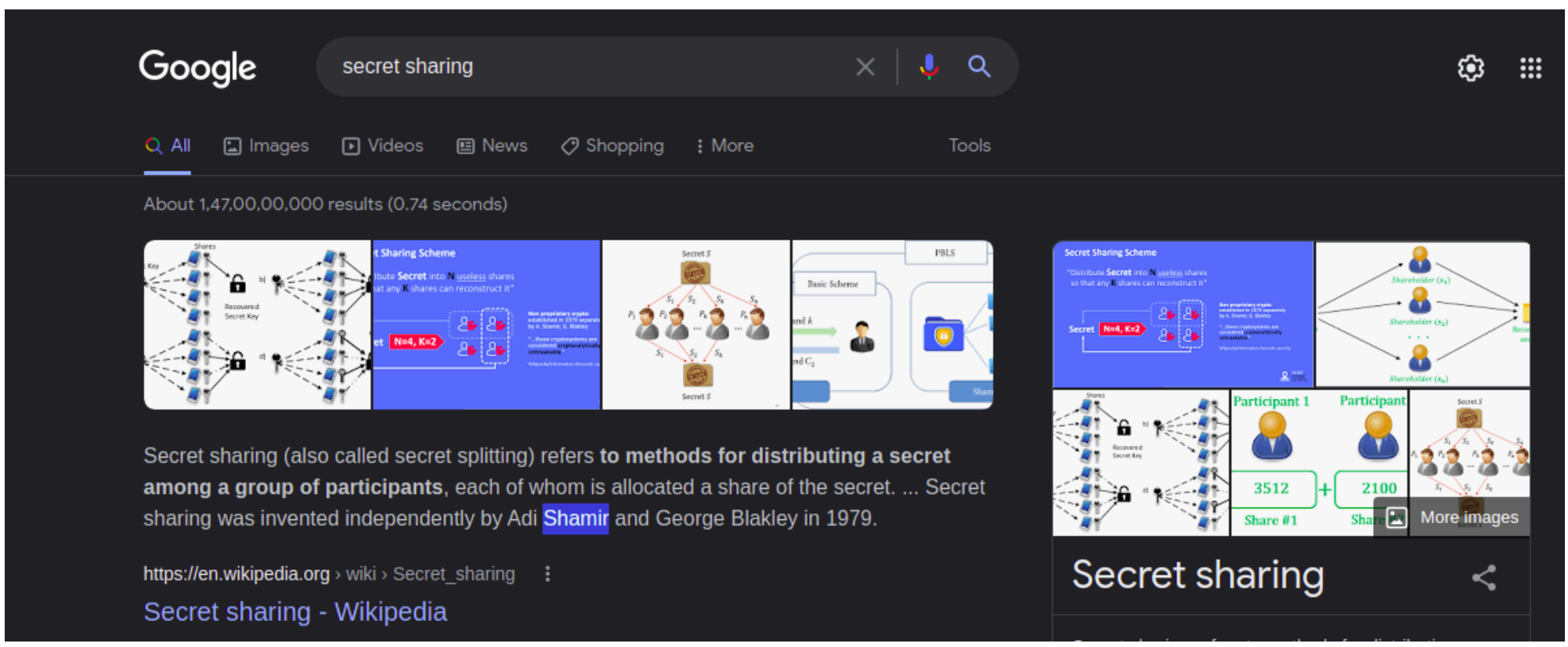
AUTHOR - 0xsakthi

Try to decipher this file

Flag

Submit

Secret sharing? something mysterious algorithm...mmm



Shamir? the name also mentioned in the description so the encrypted data is encrypted by **Shamir Secret Sharing Algorithm**

```
sakthi@debian:~/TamilCTF/Crypto-Writeups/secret-sharing$ ls
secretsharing.zip
sakthi@debian:~/TamilCTF/Crypto-Writeups/secret-sharing$ unzip secretsharing.zip
Archive:  secretsharing.zip
  inflating: file
sakthi@debian:~/TamilCTF/Crypto-Writeups/secret-sharing$ cat file
jo ,pj and Shamir communicating with each other in group, jo ask for a flag, Shamir send's junk of data, did you decrypt this
data?

#Decrypt the data Find The Flag

#DATA

required_shares : 2

prime_mod AQAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAEp'

shares
1-MEwx7cz+C01rL8H0Hhz2EIgHjWYXVcL81uITmRha674=
2-YJhj22+ntS1s80CT9b6Y7ayc52baTFGNRpPUyLxtaf8=
3-kOSVyRJRXw1utr8zzWA7ytEyQWedQuAdtkWV+GB/6EA=
4-wTDHtrT7CO1wej3TpQHep/XHm2hgOW6uJfdXKASSZoE=
5-8Xz5pFekss1yPbxzfKOBhRpc9WkjL/0+lakYV6ik5MI=
sakthi@debian:~/TamilCTF/Crypto-Writeups/secret-sharing$
```

this is the given data!

- python3 have a module, for decrypting Shamir's secret sharing algorithm

Steps To Decode

- pip install sslib

required_shares: the number of shares required for recovery;

prime_mod: the prime number P;

shares: a list containing n points of the polynomial Q

(we have these values, so we can decrypt this easily)

flag.py

```
#!/usr/bin/python3

from sslib import shamir

data = {'required_shares': 2,'prime_mod': 'AQAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAEp','shares':['1-
MEwx7cz+C01rL8H0Hhz2EIgHjWYXVcL81uITmRha674=','3-kOSVyRJRXw1utr8zzWA7ytEyQWedQuAdtkWV+GB/6EA=']}

print(shamir.recover_secret(shamir.from_base64(data)).decode('ascii'))
```

Result

```
sakthi@debian:~/TamilCTF/Crypto-Writeups/secret-sharing$ cat flag.py
#!/usr/bin/python3

from sslib import shamir

data = {'required_shares': 2,'prime_mod': 'AQAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAEp','shares':['1-MEwx7cz+C01rL8H0Hhz2EIgH
jWYXVcL81uITmRha674=','3-kOSVyRJRXw1utr8zzWA7ytEyQWedQuAdtkWV+GB/6EA=']}

print(shamir.recover_secret(shamir.from_base64(data)).decode('ascii'))sakthi@debian:~/TamilCTF/Crypto-Writeups/secret-sharing$
sakthi@debian:~/TamilCTF/Crypto-Writeups/secret-sharing$ python3 flag.py
TamilCTF{S3cr3eT_4lg0RitHm}
sakthi@debian:~/TamilCTF/Crypto-Writeups/secret-sharing$
```

for more about this module

FLAG

```
TamilCTF{S3cr3eT_4lg0RitHm}
```

First Blood : thehackerscrew