Files

main

Go to file t

.github
2023
0ByteCTF 2023
0xL4ugh CTF 2023
1337UP LIVE CTF
24h@CTF 2023
ASC Cyber Wargames Qualificat...
AmateursCTF 2023
BDSec CTF 2023
BYUCTF 2023
BlueHens CTF 2023

daffainfo feat: grouped the challs e6c48e5 · last month History

Name	Last commit message	Last commit date
..		
images	feat: grouped the challs	last month
README.md	feat: grouped the challs	last month
cursedctf.png	feat: grouped the challs	last month

README.md

find the paper

> here is a screenshot from a paper

Key Size	Bytes	*Encryption*	*Decryption*		
			Rem. tree	Cube root	CRT tree
1MB	2^{20}	0.3	0.2	4.8	25.0
10MB	$2^{23.3}$	5	6	18	262
100MB	$2^{26.6}$	77	261	177	2851
1GB	2^{30}	654	812	1765	33586
4GB	2^{32}	3123	2318	8931	101309
8GB	2^{33}	6689	7214	17266	212215
16GB	2^{34}	18183	20420	34376	476798
32GB	2^{35}	29464	62729	62567	N/A
128GB	2^{37}	150975	N/A	N/A	N/A
256GB	2^{38}	362015	N/A	N/A	N/A

Table 4.1. Encryption and decryption times—We measure wall clock time in seconds on `lattice0` for encryption and the three stages of decryption: reducing the ciphertext modulo each prime factor, computing a cube root modulo each prime, and reconstructing the plaintext modulo the product.

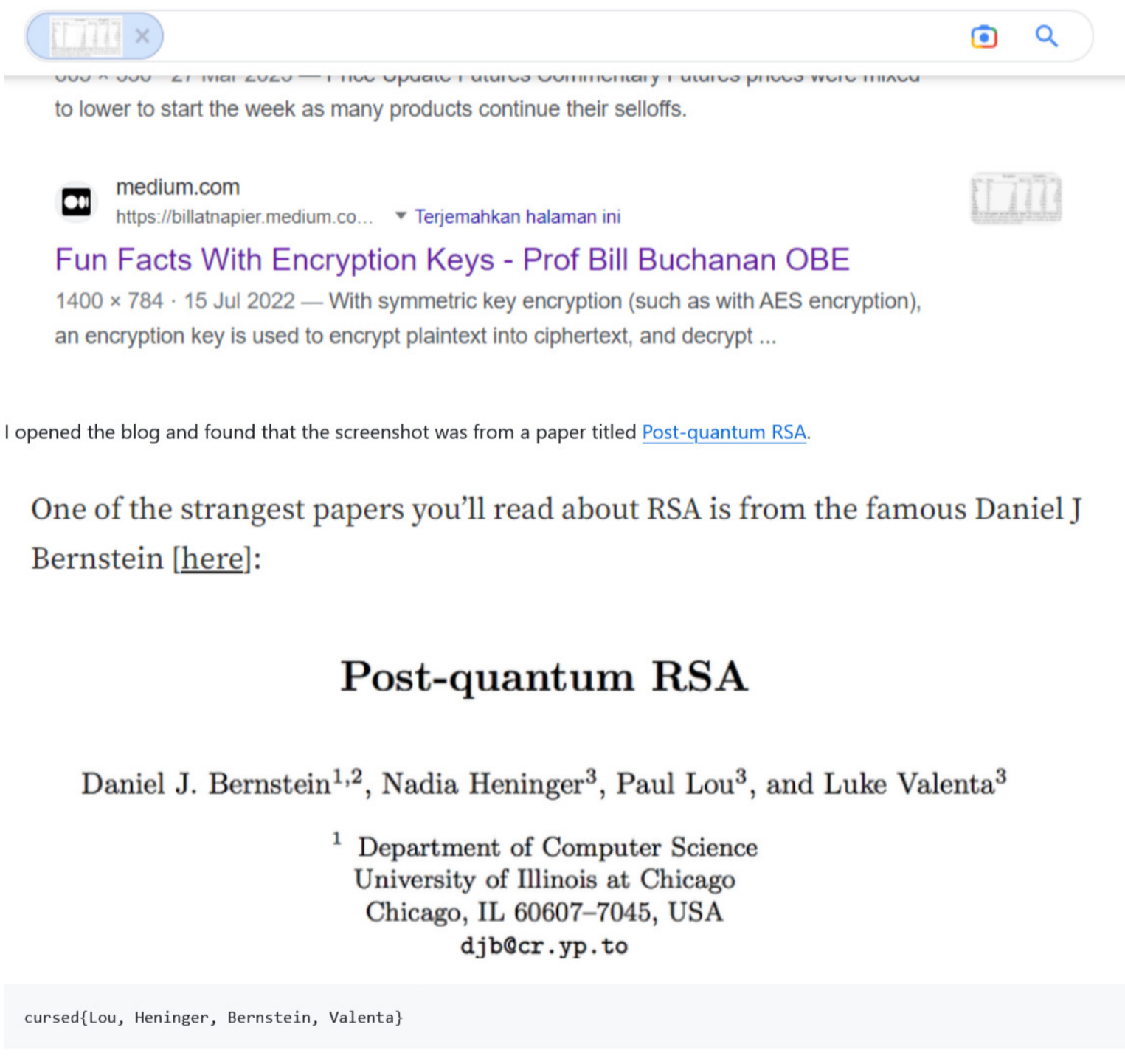
> here is a screenshot from a paper picture from a paper the flag format is cursed{last name 1, last name 2, ..., last name n}

About the Challenge

We need to find the author of the paper

How to Solve?

At first, im using google reverse image and I found this medium post



I opened the blog and found that the screenshot was from a paper titled Post-quantum RSA.

One of the strangest papers you'll read about RSA is from the famous Daniel J Bernstein [here]:

Post-quantum RSA

Daniel J. Bernstein[1,2], Nadia Heninger[3], Paul Lou[3], and Luke Valenta[3]

[1] Department of Computer Science
University of Illinois at Chicago
Chicago, IL 60607–7045, USA
djb@cr.yp.to

```
cursed{Lou, Heninger, Bernstein, Valenta}
```