

daffainfo / ctf-writeup

<> Code

Issues

Pull requests

Actions

Projects

Security

Insights

Files

main

Go to file

.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

ctf-writeup / 2023 / cursedCTF 2023 / find the paper

Add file

...

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

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

000 × 000 · 27 Mar 2020 — Price Update Futures Commentary Futures prices were mixed to lower to start the week as many products continue their selloffs.

medium.comhttps://billatnapier.medium.co...Terjemahkan halaman ini

Fun Facts With Encryption Keys - Prof Bill Buchanan OBE

1400 × 784 · 15 Jul 2022 — With symmetric key encryption (such as with AES encryption), an encryption key is used to encrypt plaintext into ciphertext, and decrypt ...

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 Heninger³, Paul Lou³, and Luke Valenta³

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

cursed{Lou, Heninger, Bernstein, Valenta}