All Topics

Add a Post

Search all posts Search

[OFFICIAL] Final Challenge (Answer, Spoiler Alert!)

discussion posted 6 days ago by **mako9999** (Staff)

Pinned

Please post a decrypted message in this thread when you have succeeded in decrypting the encrypted message from Prof. Ito.

If you don't want to see the decrypted message, please go to another thread to discuss the way to decrypt it.

This post is visible to everyone.

Add a Response

3 responses

tetsushiito (Staff)
6 days ago

Dear all, I hope you are enjoyed the course!

[Spoiler Alert!] Note that this is the place to discuss about the answers of Final Challenge. **If you don't want to see answers, please leave, and try to calculate by yourself!** There is another thread "[OFFICIAL] Final Challenge", where you are welcome to discuss about Final Challenge (without answers).

Add a comment

rvatalaro
6 days ago

ENJOYPRIMENUMBERS

(Please delete ASAP if I wasn't supposed to post the answer.)

P.S. Yes, thank you, I enjoyed the course very much. I made it a point to learn how RSA worked. I beefed up my understanding of Euclidean Algorithm and computing the multiplicative inverse, and I have a rudimentary knowledge of what's going on with ECC. I would look forward to a third installment of the course! :)

@rvatalaro , can you share the value of 'D' that you obtained by solving E*D = 1 (mod N)

I have written a C++ code for calculating multiplicative inverses and wish to verify my answer

posted 6 days ago by **Vrund_AS**

correction : E*D = 1 (mod (P-1)(Q-1))

posted 6 days ago by **Vrund_AS**

Here's a table of my results. (If you get "Math processing error," what works for me is just right-clicking and re-choosing the Math renderer.)

[Math Processing Error]

posted 5 days ago by **rvatalaro**

Vrund_AS in case you cant get past the "Math Processing Error" from above

D = 340593660390353558263687297330403 3

posted 5 days ago by **kraDen**

Add a comment

kraDen
5 days ago

Mathematica

In[1]:= LCM[659865899771032, 51410152252116118102]

Out[1]= 16961903186604174717509999235210632

In[2]:= PowerMod[1001, -1, 16961903186604174717509999235210632]

Out[2]= 340593660390353558263687297330403 3

In[3]:= PowerMod[84639267257953000521855196145672 84, 340593660390353558263687297330403 3, 33923806373208400845832116486310399]

Out[3]= 5141015251618091305142113020518l9

Note the missing leading 0

So decrypted message is

05141015251618091305142113020518l9

E N J O Y P R I M E N U M B E R S

Cheers from Oz

and thanks for a great course

Ken

Add a comment

Showing all responses

Add a response:

Preview

Submit

filter topics

All Discussions

★ Posts I'm Following

Announcements

General

Introduce Yourself

Technical Problems

English

edX

About
edX for Business
Open edX
Careers
News

More Information

Terms of Service & Honor Code
Privacy Policy
Accessibility Policy
Sitemap

Connect

Blog
Contact Us
Help Center
Media Kit
Donate

Download on the App Store
ANDROID APP ON Google play