

(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: $E*D = 1 \pmod{(P-1)(Q-1)}$

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 = 3405936603903535582636872973304033

posted 5 days ago by kraDen

Add a comment

kraDen 5 days ago Mathematica In[1]:= LCM[659865899771032, 51410152252116118102] Out[1]= 16961903186604174717509999235210632

Out[2]= 3405936603903535582636872973304033

In[3]:= PowerMod[8463926725795300052185519614567284, 3405936603903535582636872973304033, 33923806373208400845832116486310399]

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

•••

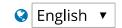
•••

•••

Out[3]= 514101525161809130514211302051819 Note the missing leading 0 So decrypted message is 0514101525161809130514211302051819 ENJOYPRIMENUMBERS 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





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

















© 2012-2017 edX Inc.

EdX, Open edX, and MicroMasters are trademarks of edX Inc., registered in the U.S. and other