help with Montgomery Reduction, Quiz 3, last question

You are subscribed. Unsubscribe

UNRESOLVED

helpMontgomeryReduction × + Add Tag

Sort replies by: Oldest first Newest first Most popular

 Karen West . a day ago

I re-read the notes, looked up "modulo multiplicative inverse" on the web, and made 4 attempts at the quiz3, but I guess I'm just not getting Montgomery Reduction's algorithm. If someone can help with this, tomorrow after the deadline has passed, I would greatly appreciate it! ;-) That was the only one I had trouble with.

1 · flag

Michael Myers . 12 hours ago

The problem with this question is that professor Qu didn't sufficiently warn us of the math pre-requisite here, modular arithmetic. His explanation of the Montgomery Reduction algorithm in lecture 3-07 requires one to understand the use of **modular multiplicative inverse,** which is what is happening to N in the equation. Modular arithmetic is not something that most people have encountered. So symbolically, his slide is very ambiguous, and I got hung up for a long time on this question because I was computing -N^-1 with N=109 as -(1/109), which is incorrect because N is not a scalar number (?), it is *N (mod 128)*.

In modular arithmetic, the *modular multiplicative inverse* of a number is the number that you multiply with N to get a modulus of 1 using some modulo. We are given that N = 109 mod 128, so you would multiply N by 101, to evenly divide by 128 and get 1. There

is a way to compute this, but for confirmation I used Wolfram Alpha.

In modular arithmetic, the negative of a number N (so, -N) is the difference between N and the number you are modulating by. From the last operation we were left with 101, so now we do: 128-101 = 27 (mod 128), which is the modular negative inverse. In other words, where Dr. Qu's slide says -N^-1, you substitute 27.

Doing the first operation and then the second, get the you get the *modular negative inverse*. The two steps are order-dependent, *unlike* the negative of (109) raised to the (-1), where it's the same whether you calculate it as (-109)^(-1) or -(109^(-1)).

Asking for the Montgomery reduction, what he means is, he wants us to provide the value of t.

↑ 1 ↓ · flag

Karen West . in 4 minutes

Hi Michael Myers - thanks for the help with modular multiplicative inverse for the Montgomery Reduction. I'm going to have to go over this again later. Also - you are not the famous Mike Myers from Wayne's World movie? Just kidding - thank you for your help.

↑ ↓ · flag

+ Comment

Gang Qu INSTRUCTOR . 4 hours ago

I agree that I have underestimated the huge discrepancy in the background of coursera students, in particular on math and digital logic design. I have been trying to address some of these issues in week 4 and week 5 lectures. For modular multiplicative inverse, see the slide of "Euler's Theorem & An Application", the application here is how to use Euler's Theorem to compute the modular multiplicative inverse. I probably should have included one or two example on this. Will try in the next offering of the course.

↑ 0 ↓ · flag

Karen West . in 4 minutes

I'll look at the "Euler's Theorem and An Application" and write back to the discussion forum if I have any further trouble. Thanks. For me, some of these topics were things I did many, many years ago and have forgotten some things. In other cases such as the Montgomery Reduction and the modular multiplicative inverse - if I learned that it is nowhere in my memory! I do have a background from my BS (completed 1987!) and MS (completed 1997!) where I learned quite a bit about math and logic design but never from a security perspective which seems to be a big topic today. I took Mike Hick's software security course last semester as part of your cybersecurity series at Umaryland and Coursera, and when I found myself still without a job as 2015 began, I decided to follow on with hardware security too. Sometimes though I find even things I knew inside out from my BS and MS, if I have not done it recently, I need to refresh my memory! ;-) Thanks for your help.

· flag

+ Comment

New post

To ensure a positive and productive discussion, please read our forum posting policies before posting.

B | I | Link | <code> | Pic | Math | Edit: Rich | Preview

Resolve thread

This thread is marked as unresolved. If the problem is fixed, please check the above box and make a post to let staff know

that they no longer need to monitor this thread.

Make this post anonymous to other students

Subscribe to this thread at the same time

Add post