Karen West <karenwest15@gmail.com>

final course questions for hardware security

Karen West <karenwest15@gmail.com> Tue, Feb 24, 2015 at 11:10 AM
To: gangqu@umd.edu
Cc: Karen West <KarenWest15@gmail.com>

Hi Professor Gang Qu:

Thank you for offering on the discussion forum yesterday to answer my questions to complete my learning in hardware security by email, before the course deadline for the final exam gets here. I found your email address in the "about the instructor" page in the hardware security course.

Here are my questions:

From the final exam:

Montgomery Reduction Question - I got these answers correct by following the examples done in lecture, but my questions are as follows, since I got them incorrect in the first take of the final exam, and correct in the 2nd take of it.

I understand my mistake with a' and b' in the first take of the final exam, but in the 2nd take of the exam, I have one question about c'. In the class example, c' came out to be 178 (mod 109) and the answer was 69 (mod 109). On the final exam, I calculated 41 (mod 109) as the answer, but the first time I took the final exam, I entered as the answer 68 (mod 109) which was incorrect, and then 2nd time I figured it must have been 41 (mod 109) but I was not sure why. Is the reason in the class example that you entered 69 (mod 109) instead of say 40 (mod 109) because you came out with an answer that was greater than 109, (178) and in that case, you just subtract 109 from 178? This part was not clear for me.

I did also get the Montgomery Reduction question incorrect on quiz 3, but I think if you can clear up the above question, perhaps when I go back to it I will get it correct when I re-do it.

For the Modular Multiplicative Inverse question, using Euler's Theorem, that is the one question I got incorrect on the final exam, and I still do not understand it, if you could please help with this one. I did some web searching for examples to get a better understanding of how to figure it out but still came up with incorrect answers. I also looked at the hint of using Euler's square and multiply algorithms 1 and 2, and still got it incorrect, and I did get those correct on the quizzes, since in those cases, the exponent was large enough for the for loop to be entered in both algorithms 1 and 2. So here are more specific questions on this based on what I tried.

For the square and multiply algorithm 1, I got b = 1, since you do not even enter the for loop of that algorithm? The way I looked at it was as follows. You need to put it in the form a^e (mod n), so I thought that 5 (mod 38) may be 5^1 (mod 38). Taking e=1 and making that binary puts a 1 in the zero bit, so s=0, and the for loop is not entered, and b = 1 because of that and I tried that answer on the first take of the final exam and it was incorrect.

Looking at square and multiply algorithm 2, I came out with b = a^k0 = 5^1 = 5 since bit k0=1 for exponent = 1. I did not enter this answer because it differed from algorithm 1's answer and I thought that I must be doing something incorrect for these to come out differently. For algorithm 2, you do not enter the for loop either, since i starts at 1, but you do not enter unless i is less than or equal to s, and s=0, and you do not enter it, and be is as initialized at b=5.

So I then went to the web and did some reading about Euler's Theorem and multiplicative inverses. I found an example where it said for a = 5 and m = 38, co-prime numbers, you must find a value of x such that ax == 1 (mod m), and the gcd(5,38) = 1. To solve, it said to start multiplying a (5) by values from 0 to m-1 (37) and the answer x is the case where a*x mod m = 1. I found that value when I went through this exercise to be exactly 7.4, a decimal, so not the answer. (5*7)mod 38 = 35. 5*8 = 40 or 2 (mod 38) and there is never a value (between 7 and 8 it seems) where I saw the answer come out to be 1, giving me my value of x.

So for the 2nd take of the test, I entered the answer of just multiplying 5 * 38 = 190, and adding 1 to it, knowing it was most likely incorrect, but I was confused and out of time!

Perhaps I should have used the answer from the 2nd square and multiply algorithm (b=5) but that did not match what I calculated for square and multiply algorithm 1 where I calculated b=1. I did not think I should put the 7.4 decimal value I calculated since these numbers do not work in decimals.

So now perhaps you can better understand my confusion with the last question on the final exam.

From quiz 4, I also have 2 questions that remain unanswered (still confused):

phi(2015) - hint factor into it's primes - and I did this incorrectly by entering the prime factors of 5 * 13 * 31. I know in class you did some examples where you found the phi(5) and the answer was 4, since 1,2,3,4 are all the numbers less than 5 that are prime or relatively prime to the number 5. So I realize that I may have interpreted the hint incorrectly, and that you do not just enter the prime factoring of the number 2015. What would be the answer though? Would you take phi(5) * phi(13) * phi(31), which would be 4*12*30 = 1440? I'm still confused on this question.

The other question I got incorrect (and this one surprised me, since I come from an EE background way back when in ancient times) was the scan chain based attack on 5 flip flops, where it asked the correct order of attack. A was let TC=0 and let the system run for one cycle. B was TC=1 and read the output from scan-out for 5 cycles, C was TC=1 and send state info. to the system via scan-in for 5 cycles, and D was TC=0 apply the input at the system's primary input ports. On this day, my time was limited, and I could have gotten the answer by taking the quiz all 4 times, but I only had time this day to take it twice. So I entered the first time, the sequence of order of attack of: D,A,C,B which was incorrect, and the 2nd time I entered C,A,D,B which was also incorrect. So I see that I am missing something and wondering if you could explain why the answer is one of the other 2 choices, sequence of attack of C,D,A,B or A,B,C,D.

That's about it for the questions that I have that remain as I finish this course. If you can help answer them that would be great. Thank you for a great course in hardware security, that complemented the software security course I took last semester. I came out with a 111/120 for a grade.

Thank you.
Karen West