ECE404: Introduction to Computer Security

Purdue University

Spring 2020: Midterm-II Version 2

Instructions

1. Write or type your answers and email them in PDF form to the provided email address. You do not have to write your answers in this booklet (i.e. you can write them on a separate sheet).
2. Your answers for each questions must be clearly legible and labelled for the respective question. You may lose points if your work is illegible.
3. This is an open book, open notes exam. You may use a calculator but you must show the equations you calculate in your work.
4. Unless otherwise instructed, justify your answers fully.
5. **Answers that are directly copied from the lecture notes will not be accepted**.
6. **You must not consult other students or anyone else for help with answers to the exam questions.**
7. **Purdue Honor Pledge: As a Boilermaker pursuing academic excellence, I pledge to be honest and true in all that I do.**

You must include the following information in your submitted PDF:

Name :

Student ID :

Email :

Signature (For PDFs, use Adobe Reader's Signature tool. For DOCX files,in Word go to Insert →Shapes→Lines →Scribble) :

Problem #	Total Points Possible
1	22
2	23
3	15
4	20
5	20
Total	100

Problem 1 [22 points]

1. Let x be the number of muffins on the table at a workshop, and they deplete at an average rate of 4 a minute (and once depleted, they are not replaced). The workshop starts at 9 AM, and ends at 5 PM. You skip the first session and go in at 10:10 AM (i.e. 70 minutes after the start time). Assuming x is an integer multiple of of 7, will there be a muffin left for you? You can assume the congruences below are true for x. Solve them to explain your answer. (Show your work: a simple yes or no will NOT suffice.) [**12 points**]

$$x \equiv 1 \ (mod\ 2)$$
$$x \equiv 1 \ (mod\ 3)$$
$$x \equiv 1 \ (mod\ 4)$$
$$x \equiv 1 \ (mod\ 5)$$

2. Calculate the following. You must show your work to receive credit. [**10 points**]

   (a) $(473)^{54433}$ mod 91

   (b) $(196)^{1123456}$ mod 13

   You may or may not need to invoke the totient rule on the exponent.

Problem 2 [23 points]

1. Compute the Euler-Totient function, $\phi(.)$ for the following values:
   (a) 58, (b) 383, (c) 22214, (d) 8507962

   Use properties of the totient function $\phi(\cdot)$ to solve for larger values. Show your work - no points will be granted if you only give the totient value. **[8 points]**

2. Use the Miller-Rabin primality test to show that the integer 25 is not a prime number. Clearly indicate the steps taken. **[9 points]**

3. Mr. X claims that he has discovered a prime number **'p'** greater than the largest known prime number. Two of his colleagues A and B decide to test his claim. **[6 points]**

   - Colleague A chooses a random number **'a'**. He applies the Miller Rabin test on **'p'** using **'a'** as the probe and finds that both the conditions are not satisfied. He claims that the number is composite.
   - Colleague B also decides to use the Miller Rabin test but chooses a different random number **'b'**. When he applies the Miller Rabin test on **'p'** using **'b'** as the probe, one of the two conditions is satisfied and he claims that the number is indeed prime.

   Who do you think is right and why?

Problem 3 [15 points]

1. A message is encrypted with RSA to produce the ciphertext, $c = 27$. The parameters used for RSA encryption are $p = 3, q = 11, n = 33$ and the public key used is $e = 7$. Find the original plaintext message. (Note: the original message may not be an ASCII-printable character. In which case you can give your answer as a decimal or hexadecimal number) **[6 points]**

2. An 8-bit message M is transmitted using RSA encryption to three different destinations. The public key used for the RSA encryption is $e = 3$ while the moduli n_1, n_2, n_3 used for the three destinations are 82, 85 and 115 respectively. The encrypted values generated for the transmission are:

$$\begin{aligned} C_1 &= 28 \\ C_2 &= 66 \\ C_3 &= 96 \end{aligned}$$

   (a) Recover the original message, M. (Note: the original message may not be an ASCII-printable character. In which case you can give your answer as a decimal or hexadecimal number) **[5 points]**

   (b) What would be the smallest value of e that can ensure a safe transmission of this message? **[4 points]**

Problem 4 [20 points]

1. Consider the elliptic curve, $y^2 = x^3 - 4x + 1$. Let $P = (10, 31)$, $Q = (12, 41)$. With this information, determine: **[6 points]**

   (a) P + Q

   (b) 2Q

2. Two users A and B wish to establish a secure communication session using the Diffie-Hellman key exchange algorithm. The parameters for the DH method include the modulus prime, $p = 17$ and the generator, $g = 2$. The private keys used by the two users are $X_A = 3, X_B = 5$ respectively. **[6 points]**

   (a) Determine the public keys Y_A, Y_B.

   (b) Determine the shared session key, K.

3. Now consider that the above session was established using the Elliptic Curve Diffie-Hellman (ECDH) key exchange algorithm. The ECC parameters include the elliptic curve, $E_8(2, 1)$ over a Galois Field $GF(2^3)$ and the base point $G = (1, 1)$. The private keys used by the two users are the same as in 4.2 . **[8 points]**

   (a) Determine the public keys Y_A, Y_B generated by the ECDH algorithm.

   (b) Explain how the secret key will be generated using ECDH (You do not need to calculate the key value).

Problem 5 [20 points]

1. The following problems are related to the *Birthday Paradox:*

   (a) What is the Birthday Paradox? Explain your answer by deriving the probability of there being at least two students in a class of 200 with the same birthday. Assume that all birthdays are equally likely. **[3 points]**

   (b) Using the same logic, determine the probability of there being at least three students in a class of 200 with the same birthday. **[6 points]**

2. The initialization vector for SHA-1 consists of the following five 32-bit words (shown in hex):

$$\begin{aligned} H_0 &= 67452301 \\ H_1 &= efcdab89 \\ H_2 &= 98badcfe \\ H_3 &= 10325476 \\ H_4 &= c3d2e1f0 \end{aligned}$$

   How are these numbers selected? Why?
   (**Hint**: Do you see any pattern in the values of $H_0 - H_5$?) **[5 points]**

3. Given N numbers at the output of a random number generator, let p be the probability that at least two of the numbers will be the same. Assume that the random number generator outputs *24-bit* numbers and every number is equally likely to be produced as output by the number generator. What is the smallest possible value for N so that the set is guaranteed to contain at least two numbers that are the same? **[6 points]**

[*You can use this page if you run out of room on the other ones*]