ECE 4156/6156

Hardware-Oriented Security and Trust

Midterm II

April 14, 2022

*This test is open book for the required as well as the optional textbooks. This test is also open note. Calculators are permitted but no programs may be used. Open notes include electronic notes with any handwritten or typed information you may have added. For electronic notes, all wireless connectivity must be turned off, and cell phones are not allowed; in other words, no connection to any information source outside of the open books, open notes and the course website is allowed during the exam. Open notes also include all course assignments (homeworks or labs) as well as solutions (including both your solution as well as official solutions posted on the course website or passed out for previous exams). All aspects of the Georgia Tech Honor Code apply. Please follow the instructions precisely. If you need to continue a problem, please use the back of the **previous** page. The meaning of each question should be clear, but please state any assumptions and ask for clarification if necessary.*

You can do it!

Question	Score	Max
1		**20**
2		**15**
3		**20**
4		**10**
5		**5**
6		**20**
Total		**70 or 90**

Name (Please print)_____

This test will be conducted according to the Georgia Tech Honor Code. I pledge to neither give nor receive unauthorized assistance on this exam and to abide by all provisions of the Honor Code.

Signed_____

1. **(20 pts.) Needham-Schroeder Protocol.**

Consider the public-key Needham-Schroeder protocol as modified by Lowe:

1) Alice to Trent: A, B
2) Trent to Alice: $E_{Tpriv}(B_{pub}, B)$
3) Alice to Bob: $E_{Bpub}(N_A, A)$
4) Bob to Trent: B, A
5) Trent to Bob: $E_{Tpriv}(A_{pub}, A)$
6) Bob to Alice: $E_{Apub}(B, N_A, N_B)$
7) Alice to Bob: $E_{Bpub}(N_B)$

(a) (5 pts.) What was the modification to step 6 above made by Lowe? In other words, what was step 6 as published by coauthors Needham and Schroeder, and then what specific modification was proposed by Lowe?

(b) (15 pts.) How does Lowe's modification prevent a possible successful attack on the original Needham-Schroeder protocol? Please limit your answer to 10 sentences or less. You may write out an example if helpful (however, an example is **not** required). Please note that any rewrite of any of the steps one through seven above does not count towards your 10-sentence limit. If you write more than 10 sentences, please circle or otherwise clearly indicate the portion of your answer that you want to be graded.

2. **(15 pts.) Advanced Encryption Standard.**

Consider the following figure from the AES lecture notes:

		y														
		0	1	2	3	4	5	6	7	8	9	a	b	c	d	e	f
x	0	63	7c	77	7b	f2	6b	6f	c5	30	01	67	2b	fe	d7	ab	76
	1	ca	82	c9	7d	fa	59	47	f0	ad	d4	a2	af	9c	a4	72	c0
	2	b7	fd	93	26	36	3f	f7	cc	34	a5	e5	f1	71	d8	31	15
	3	04	c7	23	c3	18	96	05	9a	07	12	80	e2	eb	27	b2	75
	4	09	83	2c	1a	1b	6e	5a	a0	52	3b	d6	b3	29	e3	2f	84
	5	53	d1	00	ed	20	fc	b1	5b	6a	cb	be	39	4a	4c	58	cf
	6	d0	ef	aa	fb	43	4d	33	85	45	f9	02	7f	50	3c	9f	a8
	7	51	a3	40	8f	92	9d	38	f5	bc	b6	da	21	10	ff	f3	d2
	8	cd	0c	13	ec	5f	97	44	17	c4	a7	7e	3d	64	5d	19	73
	9	60	81	4f	dc	22	2a	90	88	46	ee	b8	14	de	5e	0b	db
	a	e0	32	3a	0a	49	06	24	5c	c2	d3	ac	62	91	95	e4	79
	b	e7	c8	37	6d	8d	d5	4e	a9	6c	56	f4	ea	65	7a	ae	08
	c	ba	78	25	2e	1c	a6	b4	c6	e8	dd	74	1f	4b	bd	8b	8a
	d	70	3e	b5	66	48	03	f6	0e	61	35	57	b9	86	c1	1d	9e
	e	e1	f8	98	11	69	d9	8e	94	9b	1e	87	e9	ce	55	28	df
	f	8c	a1	89	0d	bf	e6	42	68	41	99	2d	0f	b0	54	bb	16

Figure 7. S-box: substitution values for the byte xy (in hexadecimal format).

(a) (5 pts.) What does it mean to say that the S-box provides the property of confusion in AES? Please do not copy an answer from any source; instead, please use your own words right now upon reading this question to provide an answer from your understanding. Furthermore, please limit your answer to 10 sentences or less (you may circle your answer if you end up writing more than 10 sentences; e.g., if you rewrite your answer and do not want your initial attempt to be graded, please clearly circle the rewritten or reworded final answer you want to be graded).

(b) (5 pts.) Consider a PUF – e.g., a PUF based on or nearly identical to HELP – which uses a circuit implementation of multiple AES S-boxes as an entropy source. Furthermore, consider a 128-bit challenge which is processed at the same time (in parallel; i.e., no S-box is used more than once given a specific challenge input to the PUF). How many AES S-boxes are required to be implemented in circuitry (i.e., gates implementing Boolean logic) for this PUF?

(c) (5 pts.) Now consider a single S-box. Suppose that for each output there are eight choose two unique paths of logic gates, i.e., $\binom{8}{2} = \frac{8!}{2!6!} = \frac{7*8}{2} = 28$. How many unique paths are there in the circuit implementation of each S-box (under this assumption of eight choose two unique paths per output bit)? Please provide an answer for only one S-box.

3. **(20 pts.) Weak versus Strong PUFs.**

Consider a weak PUF and a strong PUF. Furthermore, consider two applications: (i) Authentication and (ii) Encryption. Please add any assumptions believed to be necessary for each answer below.

(a) (10 pts.) Which PUF – weak or strong – is preferred for **entity authentication** and why? A third possibility is that both are equally capable and thus neither provides any substantial advantage or significant disadvantage over the other. For full credit, at least one valid reason and no invalid or false reasons must be provided for your answer. Furthermore, please limit your answer to 10 sentences or less (you may circle your answer if you end up writing more than 10 sentences).

(b) (10 pts.) Which PUF – weak or strong – is preferred for **symmetric encryption** and why? A third possibility is that both are equally capable and thus neither provides any substantial advantage or significant disadvantage over the other. For full credit, at least one valid reason and no invalid or false reasons must be provided for your answer. Furthermore, please limit your answer to 10 sentences or less (you may circle your answer if you end up writing more than 10 sentences).

4. **(10 pts.) Diffie-Hellman Key Exchange.**

Consider the case of Diffie-Hellman Key Exchange using $\alpha = 6$ as a generator for Z_{13}^*. Below are a list of possible secrets x, y and associated modulus answers including the final shared key K. Are any of the answers below incorrect? If your answer is "yes," you must correctly indicate at least one answer which is incorrect. If your answer is "no," then obviously there is no need to say anything additional. Please note that to receive full credit for this problem you must not have any incorrect answers to this question; for example, if you say "yes" and indicate two answers are incorrect where in fact only one of the answers is incorrect, you will receive half credit.

x, y	α^x	α^y	$(\alpha^x) \bmod p$	$(\alpha^y) \bmod p$	K
2,3	36	216	10	8	12
2,4	36	1296	10	9	3
2,5	36	7776	10	2	4
2,7	36	279936	10	7	10
2,8	36	1679616	10	3	9
2,10	36	60466176	10	2	3
3,4	216	1296	8	9	1
3,5	216	7776	8	2	8
3,6	216	46656	8	12	12
3,7	216	279936	8	7	5
3,11	216	362797056	8	11	5
4,6	1296	46656	9	12	1
4,7	1296	279936	9	7	9
4,8	1296	1679616	9	3	3
4,9	1296	10077696	9	5	1
4,11	1296	362797056	9	11	3
5,6	7776	46656	2	12	12
5,7	7776	279936	2	7	11
5,8	7776	1679616	2	3	9
7,8	279936	1679616	7	3	3
7,9	279936	10077696	7	5	8
7,11	279936	362797056	7	11	2
8,10	1679616	60466176	3	4	3
9,11	10077696	362797056	5	11	8

5. **(5 pts.) NIST Tests for Randomness.**

Which applications or industries prefer Type I errors over Type II in the NIST Test Suite for Random Number Generation? For full credit you must clearly explain why such Type I errors are preferred over Type II; only stating a particular application or industry with no specific reasons will earn zero points.

6. **[ECE 6156 only!] (20 pts.) Modulus and Entropy.**

Consider the following PUF Number Difference (PND) outputs:

{200, 222, 235, 257, 289, 302, 323, 355, 377, 399}

We are going to discuss mapping each PND value to a single output bit.

(a) (5 pts.) Suppose that the PUF Number Difference is categorized as indicating a one versus a zero as follows: the range 200 to 299 results in a zero bit while the range from 300 to 399 results in a bit with value one (i.e., the PUF response bit has value '1'). Please provide the response bit for each PND value above.

(b) (5 pts.) Now consider applying the modulus operation as follows. First, calculate each PND modulus 20. Then categorize the one-bit PUF response as follows: the range 0 to 9 results in a zero bit while the range 10 to 19 results in a bit value of one. Please provide the response bit calculated for each PND value above.

(c) (10 pts.) Now consider that this is a test question and so if your answers to parts (a) and (b) above result in the same number of '0' and '1' values (for the PUF response bits), this is likely due to the fact that Professor Mooney picked the numbers given in this problem resulting in the answers to parts (a) and (b) above. Would a uniformly random number sequence with values exclusively in the range 200 to 399 with a large enough sample size also result in equal (or nearly equal) answers to parts (a) and (b) above, or is there a **statistically significant chance** that a truly random sequence of numbers in the range 200 to 399 would result in unequal (i.e., differing by a nontrivial percentage) answers to parts (a) and (b) above? For full credit you must give at least one valid reason for your answer. A correct answer with no valid reason given will earn zero points; furthermore, a collection of reasons including some which are invalid will also lose significant points. Please limit your answer to 10 sentences or less (math equations do not count towards this limit).

THIS IS THE LAST PAGE OF THE EXAM!