ECE 4156/6156

Hardware-Oriented Security and Trust

Midterm I

February 24, 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). 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!

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_____

Question	Score	Max
1		**10**
2		**10**
3		**15**
4		**10**
5		**10**
6		**15**
Total		**55 or 70**

1. **(10 pts.) Pseudorandom Functions versus Permutations.**

One common way to implement an encryption scheme π_E = (Gen, Enc, Dec) is with either (i) a pseudorandom function or (ii) a pseudorandom permutation. Consider the use of CBC mode versus the use of CTR mode. Keep in mind that unlike a (ii) pseudorandom permutation, in the case of a (i) pseudorandom function, two n-bit inputs x and y where for $x \neq y$ may result in $f(x) = f(y)$ with probability $\frac{1}{2^n}$.

(a) (5 pts.) Can a (i) pseudorandom function be used to implement an encryption scheme π_E using CTR mode? For full credit, you must explain your answer.

(b) (5 pts.) Can a (i) pseudorandom function be used to implement an encryption scheme π_E using CBC mode? For full credit, you must explain your answer.

2. **(10 pts.) Basic CBC-MAC.**

Consider the basic CBC-MAC construction using a keyed pseudorandom permutation and messages of length 2*n*. Say that the sender and receiver agree that all messages must be of length 2*n*; as a result, $\mathrm{Vrfy}_k(m, t) \stackrel{?}{=} 1$ if and only if **both** $t = \mathrm{Mac}_k(m)$ **and** the length of *m* is 2*n*. Can an adversary forge a valid tag? If so, give at least one example how. If not, provide one valid reason why not. Please note that a correct "yes" or "no" answer without proper justification will receive zero points. (Please do not write more than 10 sentences; if you do write a long answer please indicate which part of the answer you want graded, otherwise answers longer than 10 sentences will receive zero points.)

3. **(15 pts.) Secret Sharing.**

Consider a secret sharing scenario where $N = 5$ and $t = 2$. There are five company executives where two out of the five must be present to enter their passwords in order to open a safe. Now consider the case of a 10-bit key required to carry out an action (e.g., open a safe). This key will be predicted from the inputs provided by any two of the executives.

A group of six personnel claim to have valid secret shares (of which there are only five valid secret shares). They have the following values:

Person 1: (80, 490)

Person 2: (50, 400)

Person 3: (200, 850)

Person 4: (90, 520)

Person 5: (125, 350)

Person 6: (250, 1000)

(a) (5 pts.) What is the value of the key in the scheme? You must provide a clear explanation of how you obtained the key to receive any credit.

(b) (5 pts.) Which of the six personnel has an invalid secret share? You must provide a clear explanation of why the secret is invalid to receive any credit.

(c) (5 pts.) Provide one forged secret share that would allow entry into the safe (given the presentation of a second valid secret share simultaneously) for the invalid personnel you determined in (b). You must provide a clear explanation of how you obtained the forged secret to receive any credit.

4. **(10 pts.) (i) Encrypt-and-Authenticate versus (ii) Authenticate-then-Encrypt versus (iii) Encrypt-then-Authenticate.**

Consider (i) encrypt-and-authenticate, (ii) authenticate-then-encrypt and (iii) encrypt-then-authenticate. Explain for each mode a scenario which would cause you to employ that mode. If there is no scenario, then clearly explain why you would never use that mode of combining encryption with tag generation. For full credit, clearly explain at least one advantage for using a given mode in the scenario you have provided for that mode.

5. **(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	2592	10	5	9
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	2592	8	9	5
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	9
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
9,12	10077696	2176782336	5	1	1

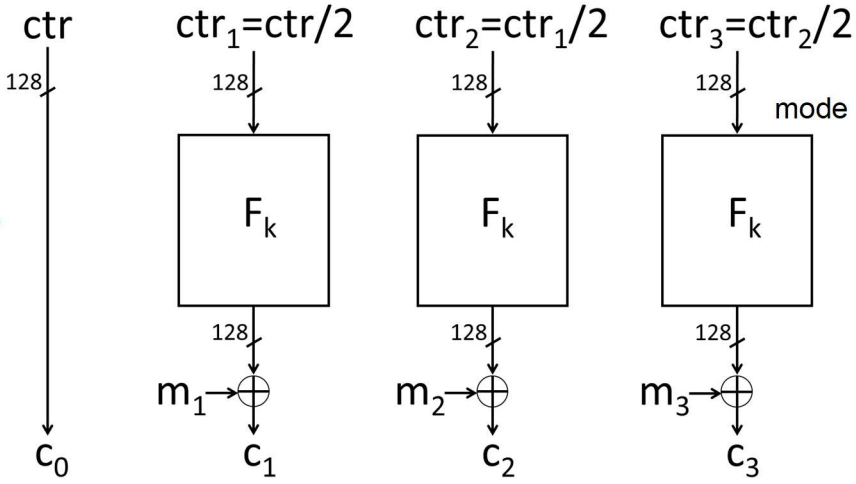
6. **[ECE 6156 only!] (15 pts.) New encryption mode.**

Let F be a pseudorandom permutation. Assume that CTR mode is chosen where the n-bit counter is generated from uniform $k \in \{0,1\}^{n-2}$ where $n = 128$. And both the most significant as well as the least significant bit are set to one.

Pictured to the right is how the ctr value is chosen each time: a 126-bit random number is used to create a resulting 128-bit number with a "1" at both ends.

Now the counter value is divided by two each time and rounded down; in other words, any least significant bits that drop off are ignored (there is no rounding). Shown in the picture below is this new mode. Each time the previous ctr value is divided by two without any rounding at all. Only the first three message blocks are shown.

Consider using 128-bit blocks for messages of maximum size 16MB. Is this newly defined CTR secure? Please note that the correct answer (secure or insecure) without a valid reason will earn zero points; for full credit you must explain at least one clear and valid reason for your answer – vague and/or unclear reasons will not be accepted for credit.



THIS IS THE LAST PAGE OF THE EXAM!