ECE 3170

Cryptographic Hardware for Embedded Systems

Midterm I

September 29, 2022

This test is open book for the Schneier textbook and 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 classroom 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.

Question	Score	Max
1		**25**
2		**20**
3		**20**
4		**10**
5		**10**
6		**15**
Total		**100**

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__________________________________

1. **(25 pts.) The Interlock Protocol.**

Consider the interlock protocol where Alice and Bob keep track of all public keys claimed by anyone with whom they try to communicate. Recall that the Man-in-the-Middle (MitM) attack depends on Mallory providing fake public keys to Alice and Bob. Assume that Mallory (i) does **not** know the message format and that (ii) Alice and Bob do **not** communicate with anyone who sends two different claimed public keys. With regard to condition (ii), for example, if Alice receives two messages both claiming to be from Bob but with two different public keys, Alice will refuse to communicate with Bob under any circumstances.

(a) (10 pts.) Please describe an assumption which results in Mallory never succeeding in carrying out an MitM attack. You may also provide two or three assumptions (or more!) which are interrelated in some important way(s) if you feel this is necessary, but please keep your answer to less than 10 sentences. Please make sure that the assumption(s) is(are) clearly and unambiguously described.

(b) (10 pts.) Please describe an assumption which results in Mallory potentially succeeding in carrying out an MitM attack. It is enough if Mallory succeeds sometimes but not all of the time (in general, attackers only need to succeed once out of 100 tries to win whereas defenders need to defend successfully 100 out of 100 attack attempts in order to win). You may also provide two or three assumptions (or more!) which are interrelated in some important way(s) if you feel this is necessary, but please keep your answer to less than 10 sentences. Please make sure that the assumption(s) is(are) clearly and unambiguously described.

(c) (5 pts.) Does the protocol as described at the beginning of this question (i.e., involving keeping track of all public keys) possibly result in efficient denial-of-service (DoS) attacks? If yes, explain specifically how service is denied (i.e., communication is prevented between Alice and Bob) by Mallory. Otherwise, if DoS attacks are not possible, explain at least one valid reason why not. Please note that a correct "yes" or "no" answer without a valid reason will earn zero points. Please limit your answer to 10 sentences or less (feel free to circle what you want graded).

2. **(20 pts.) Kerberos.**

In Chapter 3.3 on page 60 in the course textbook, Schneier says the following about Kerberos: “The protocol works, but it assumes that everyone’s clocks are synchronized with Trent’s clock. In practice, the effect is obtained by synchronizing clocks to within a few minutes of a secure time server and detecting replays within the time interval.” Here is the Kerberos protocol as described in the lecture notes:

- Alice sends Trent her identity and Bob’s: A,B
- Trent generates key K and adds a timestamp T plus a lifetime L; he then encrypts two messages as follows and sends them to Alice
  - $E_A(T,L,K,B)$; $E_B(T,L,K,A)$
- Alice then uses K to send Bob her identity and timestamp, plus Trent’s message
  - $E_K(A,T)$; $E_B(T,L,K,A)$
- Bob creates a message consisting of the timestamp plus one, encrypts it in K, and sends it to Alice
  - $E_K(T+1)$

Propose how replay attacks within a few minutes may be detected. There are many correct answers to this question. Please limit your answer to 10 sentences or less (feel free to circle what you want graded); equations and protocol steps do not count towards the 10-sentence limit, e.g., “$E_K(T+1)$” is not a sentence and is free in terms of you may repeat “$E_K(T+1)$” as many times as you feel necessary in your answer.

3. **(20 pts.) The Padding Oracle Attack.**

The lecture “Crypto VIII: Two Attacks on Encryption” covered the padding-oracle attack on Construction 3.30. For ease of access, here is Construction 3.30:

- F_k is a pseudorandom function which varies with a key *k*
- A uniformly random *n*-bit key is selected and provided to the sender and receiver (but not to the adversary, of course)
- Enc_k : given an *n*-bit message *m*, choose a uniformly random *n*-bit number *r*
  - $c := <r, F_k(r) \oplus m>$
- Dec_k : given length 2*n* ciphertext $c = <r,s>$
  - $m := F_k(r) \oplus s = F_k^{-1}(c)$

Suppose that instead of using a pseudorandom function F_k, DES is used as follows:

- E_k is DES encryption with key *k*
- D_k is DES decryption with key *k*
- A uniformly random *n*-bit key is selected and provided to the sender and receiver (but not to the adversary, of course)
- Enc_k : given an *n*-bit message *m*,
  - $c := E_k(m)$
- Dec_k : given length *n* ciphertext *c*,
  - $m := D_k(c)$

Can you extend the padding oracle attack to work if DES is used? If so, intuitively explain how and describe at least one of the key (i.e., most important) reasons it is possible. If not, intuitively explain why not and describe at least one of the key steps where Mallory fails to succeed. (Please note that a correct “yes” or “no” answer without a valid explanation and one clearly articulated intuitive reason will earn zero points.) Please limit your answer to 10 sentences or less (feel free to circle what you want graded); equations and protocol steps do not count towards the 10-sentence limit.

4. **(10 pts.) Inverse Modular Exponentiation.**

Consider inverse modular exponentiation: find *x* where $a^x \equiv b \pmod{n}$.

If $3^x \equiv 5 \pmod{11}$, then x = ? Give an answer for *x* or state that no solution exists.

5. **(10 pts.) Combining Encryption with Message Integrity.**

Consider S-box 1 of DES. Below is Table 12.6 from the course text and, for ease of reference, S Box 1 in a format showing binary values for rows and columns. Give the result for the following substitution: 0x38. Give your answers in both decimal as well as hexadecimal.

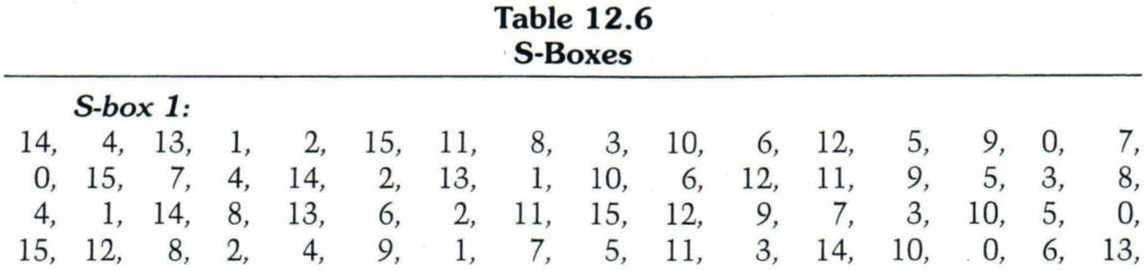
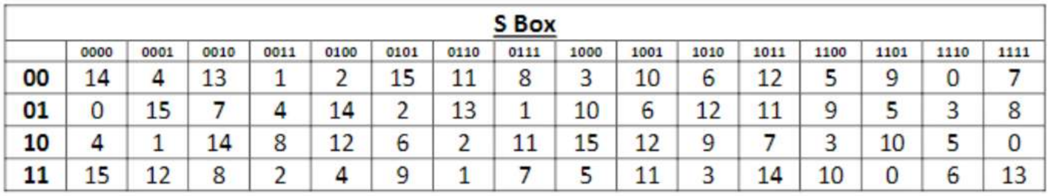


Table 12.6
S-Boxes

S-box 1:

14,	4,	13,	1,	2,	15,	11,	8,	3,	10,	6,	12,	5,	9,	0,	7,
0,	15,	7,	4,	14,	2,	13,	1,	10,	6,	12,	11,	9,	5,	3,	8,
4,	1,	14,	8,	13,	6,	2,	11,	15,	12,	9,	7,	3,	10,	5,	0,
15,	12,	8,	2,	4,	9,	1,	7,	5,	11,	3,	14,	10,	0,	6,	13,



S Box

	0000	0001	0010	0011	0100	0101	0110	0111	1000	1001	1010	1011	1100	1101	1110	1111
00	14	4	13	1	2	15	11	8	3	10	6	12	5	9	0	7
01	0	15	7	4	14	2	13	1	10	6	12	11	9	5	3	8
10	4	1	14	8	12	6	2	11	15	12	9	7	3	10	5	0
11	15	12	8	2	4	9	1	7	5	11	3	14	10	0	6	13

6. **(15 pts.) Symmetric versus Asymmetric Keys.**

   (a) (5 pts.) Give at least one **advantage** or benefit of asymmetric encryption (i.e., with a public and a private key) over symmetric.

   (b) (5 pts.) Now give at least one **advantage** or benefit of symmetric encryption (i.e., with a single key) over asymmetric.

(c) (5 pts.) Now compare and contrast your answer to part (a) with your answer to part (b) on the previous page. Overall, considering (i) authentication and (ii) encryption, when does (do) the advantage(s) **asymmetric** techniques outweigh the disadvantage(s) as compared to **symmetric** techniques? Similarly, considering (i) authentication and (ii) encryption, when does (do) the advantage(s) **symmetric** techniques outweigh the disadvantage(s) as compared to **asymmetric** techniques? (NOTE: if you feel it may help you, it is OK to repeat, in part or in whole, from your answers on the previous page; nevertheless, please write out your answer completely here on this page – any statement such as "please see the previous answers" will earn zero points.)

THIS IS THE LAST PAGE OF THE EXAM!