CS 5173/4173 Computer and Network Security

Fall 2020, In-Class Midterm

Test Exam 1

Name:______________________________ score:______________________________

Instructions:

1) This test is closed books, notes, papers, friends, phones, neighbors, smartwatches, etc.
2) This test is 5 pages in length.
3) You have 75 minutes to complete and turn in this test.
4) Use the backs of pages in this test packet for scratch work. If you write more than a final answer in the area next to a question, circle your final answer.

5) Write and sign the following: "I pledge my Honor that I have not cheated, and will not cheat, on this test."

   ____

   ____

Signed: ____

Section I (Single Choice) Write the answer above _______

1. Suppose that in a Feistel Cipher, the sub-key generation function is to flip all the bits of the key K (e.g., K=0001 ➔ K'=1110), and the scrambling function is f = M XOR K', where M is the second half of input bits and K' is the sub-key. Given the original key K = 1100, and input bits M = 1100 1100, compute the output of the Feistel Cipher.

(A) 1111 1100 (B) 1100 1100 (C) 1100 0011 (D) 1100 0000

Answer: ________________

2. Consider the following S-Box for the DES algorithm:

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

Given input $(000000)_2$, the output of the S-Box is:

(A) 5 (B) 15 (C) 11 (D) 6

Answer: ________________

3. Meet-in-the-middle attack against double DES is

(A) Ciphertext only cryptanalysis (B) Known plaintext cryptanalysis
(C) Chosen cipher text cryptanalysis (D) Chosen plaintext cryptanalysis

Answer: ________________

4. If a good-quality hash of a message produces a 256-bit output, how many messages would you need to try at random to have at least a 50% chance of generating the same hash output?

(A) 128 (B) 2^{256} (C) 2^{128} (D) 256

Answer: ________________

5. If a bit error occurs in the transmission of a ciphertext character in the 32-bit CFB mode, how many future blocks does the error affect (including itself) assuming DES is used?

(A) 1 (B) 2 (C) All (D) Not of them is true

Answer: ________________

6. Message authentication codes (MAC) and digital signatures both serve to authenticate the content of a message. Which of the following best describes how they differ?

(A) A MAC can be verified based only on the message, but a digital signature can only be verified with the secret key used to sign the message

(B) A MAC can be verified based only on the message, but a digital signature can only be verified with the public key of the party that signed the message.

(C) A MAC can only be verified with the secret key used to generate it, but a digital signature can be verified based only on the message.

(D) A MAC can only be verified with the secret key used to generate it, but a digital signature can be verified with the public key of the party that signed the message.

Answer: ________________

Section II (Short Answer)

7. What is non-repudiation?

8. Please compare asymmetric and symmetric key crypto and discuss their best application scenarios.

Section III. Answer the following questions. Show your steps or reasons. [39 pts]

9. Alice needs to send n packets to Bob. Alice and Bob wish to use n different random one-time pads to encrypt the n packets. The encryption is simply bit-wise XORing a packet and an one-time pad. Assume each packet is of 128 bits. Describe how Alice and Bob can generate n different one-time pads and apply them by using a shared secret key S and a cryptographic hash function h.

10. Suppose the Oklahoma State tries to find a cost-effective way to design a centralized secure information system to store all students' records. It must be very easy for a system administrator to retrieve/revise/restore a student's record as well as search a student's record. The system must be secure against some intruders that can physically steal the disk storage and attempt to recover the student information as much as possible from the storage. Reason your design to balance the cost and security (in terms of confidentiality or/and integrity).

Undergraduates stop here

11. (**Graduates Only)** A protocol named TESLA has been developed for authentication. In its simplified form, TESLA randomly generates a key K_n and computes $K_i = H(K_{i+1})$ for $i = n – 1$, $n – 2$, …, 0, where H is a hash function. In addition, TESLA partitions a period of operation time into n time intervals, denoted as I_1, I_2, …, I_n. Each key K_i is associated with the time interval I_i, and used to generate MACs for all the messages the sender broadcasts during I_i. However, the sender doesn't disclose K_i until T time units after I_i. Let's denote the beginning time of I_i is T_i. Then the sender doesn't disclose K_i until $T_{i+1} + T$. Each receiver buffers the messages received during I_i. It can authenticate the messages sent during I_i after it receives K_i disclosed by the sender.

(a) Develop a way so that each receiver can authenticate each K_i disclosed by the sender.

(b) When a receiver receives a message authenticated with K_i at time t, how can it determine if the message wasn't forged by an attacker that just learned the K_i disclosed by the sender? In other words, develop a security condition, by checking which a receiver can determine if the message was sent before K_i is disclosed. Assume the maximum clock discrepancy between the sender and the receiver is Δ, and the time required for message transmission is negligible.