Name:____

Student ID:____________________________________

Midterm

CSE 5/7339

Computer System Security

Mark D. Hoffman

Instructions: Please keep all answers as concise as possible while still conveying all necessary concepts. Please show all necessary work. An extra page is provided in the event that you need more room.

Using the following word bank, select fill in the blank with the term most directly related to the concepts below:

Authorization
Cipher Text
Public Key System
Authentication
Kerckhoffs's Principle
Symmetric Key System
Plain Text

_______________________________ Can be used with a Message Authentication Code to provide Integrity to a message.

_______________________________ The scrambled version of the message in an encryption system.

_______________________________ The process of giving someone permission to do or have something. Limited by such technologies as firewalls, Intrusion Detection Systems, and Multilevel Security Systems

_______________________________ The idea that a cryptosystem should be secure even if everything about the system, except the key, is public knowledge.

_______________________________ Provides the ability to add a secure 'digital signature' to a message.

_______________________________ The original input into an encryption system before modification to obfuscate the message.

_______________________________ The process of determining whether someone or something is, in fact, who or what it is declared to be.

Name:____________________________________

Student ID:_________________________________

1) Briefly describe each of the three components of the C.I.A. Triad including what each is directed at protecting:

2) A Feistel Cipher is a general format for one possible method of performing a block cipher. Describe the basic flow of a Feistel cipher being sure to include what primary mathematical operator is required to meet this format. (Be able to describe the flow. This can be a flow chart, series of algorithms, or textual description.).

3) Compare and contrast Symmetric Key Systems vs. Public Key Systems:

4) a.What are the three primary components of Public Key Infrastructure?

b. Briefly describe one of the primary PKI Trust Models.

Name:______________________________________

Student ID:__________________________________

5) What is the name given to the primary method of exchanging a Symmetric Key (not used for encrypting or signing) based on a discrete log problem where each user must find the exponent k given g, p, and g^k mod p, with each user selecting their own private value for k. ____

Name:_______________________________________

Student ID:___________________________________

6) Solve the following modular arithmetic problems:

12 mod 9 = _________

-4 mod 9 = ________

11^{-1} mod 8 = ________

4^{-1} mod 9 = _________

49 mod 5 = _______

Name:____________________________________

Student ID:________________________________

7) Using the following word bank, select fill in the blank with the term most directly related to the Hashing concepts below:

Compression Efficiency One-Way
Weak Collision Resistance Strong Collision Resistance
Avalanche Effect Cyclic Redundancy Check

______________________ Given a value (y) it is infeasible to find a corresponding value (x) such that h(x) = y

______________________ Should be computationally easy to compute h(x) for any value of x

______________________ Requirement of all hash functions that the resulting output be significantly smaller than the given input

______________________ Form of non-cryptographic hash function that has been improperly used as a method to secure the Wired Equivalency Protocol (WEP)

______________________ given x and h(x), infeasible to find ***any*** x and y, with x ¹ y such that h(x) = h(y)

______________________ given x and h(x), infeasible to find y ¹ x such that h(y) = h(x)

______________________ a change to 1 bit of input should affect about half of output bits

8) Using a Shift Cipher with a key of 5, solve the following substitution cipher:

Ymj fsxbjw yt szrgjw knaj nx Inkknj-Mjqqrfs.

9) During the first round of a DES encryption cycle, the 32-bits of R_0 are found to be:

R_0 = 00000000000000000010101001100100

This is ran through the expansion permutation box [E] below to generate 48-bit $E(R_0)$
Find $E(R_0)$.

Name:______________________________________

Student ID:__________________________________

Expansion Permutation (E)

32	1	2	3	4	5
4	5	6	7	8	9
8	9	10	11	12	13
12	13	14	15	16	17
16	17	18	19	20	21
20	21	22	23	24	25
24	25	26	27	28	29
28	29	30	31	32	1

$E(R_0)$ = ____

10) For this same iteration of DES, K_1 is found to be:

K_1 = 010011110110110100110101001010101111110110101011

Using the solution, $E(R_0)$, from the previous question, and K_1 find the 48-bit input for the S-Boxes, (B).

B = ____

Name:____

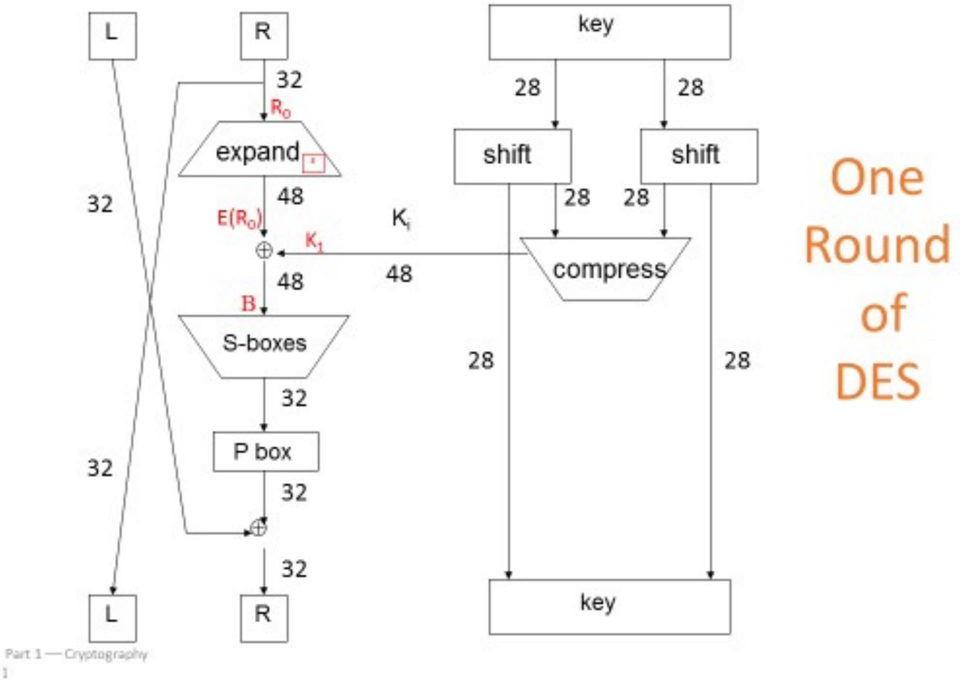
Student ID:__________________________________

11) Using the solution, B, from the previous question, determine the proper input and solution to S-Box, S_1 below:

B_1 = ______________

	0000	0001	0010	0011	0100	0101	0110	0111	1000	1001	1010	1011	1100	1101	1110	1111
00	1110	0100	1101	0001	0010	1111	1011	1000	0011	1010	0110	1100	0101	1001	0000	0111
01	0000	1111	0111	0100	1110	0010	1101	0001	1010	0110	1100	1011	1001	0101	0011	1000
10	0100	0001	1110	1000	1101	0110	0010	1011	1111	1100	1001	0111	0011	1010	0101	0000
11	1111	1100	1000	0010	0100	1001	0001	0111	0101	1011	0011	1110	1010	0000	0110	1101

S_1 Output = ________

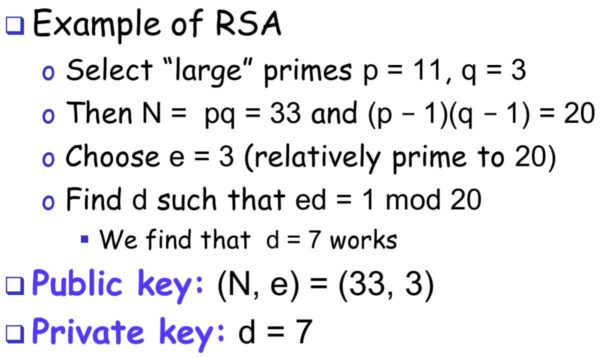


One Round of DES

Name:____

Student ID:____________________________________

13) Given the example below, generate a unique key pair by selecting p, q, N, e, and d (DO NOT USE ANY OF THE VALUES LISTED BELOW FOR p or q)



❑ Example of RSA

- Select "large" primes p = 11, q = 3
- Then N = pq = 33 and (p – 1)(q – 1) = 20
- Choose e = 3 (relatively prime to 20)
- Find d such that ed = 1 mod 20
  - We find that d = 7 works

❑ **Public key:** (N, e) = (33, 3)

❑ **Private key:** d = 7

p =________, q =________, N =________, e =________, d = _______

Name:______________________________________

Student ID:__________________________________

Extra Work (to be turned in with Exam).