**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 | Authentication | Symmetric Key System |
| Cipher Text | Kerckhoffs’s Principle | Plain Text |
| Public Key System |  |  |

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.

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.

1. 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 gk mod p, with each user selecting their own private value for k.
2. Solve the following modular arithmetic problems:

12 mod 9 =

11-1 mod 8 =

-4 mod 9 =

4-1 mod 9 =

49 mod 5 =

1. 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

1. Using a Shift Cipher with a key of 5, solve the following substitution cipher:

Ymj fsxbjw yt szrgjw knaj nx Inkknj-Mjqqrfs.

1. During the first round of a DES encryption cycle, the 32-bits of R0 are found to be: R0 = 00000000000000000010101001100100

This is ran through the expansion permutation box [E] below to generate 48-bit E(R0) Find E(R0) .

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(R0) =

1. For this same iteration of DES, K1 is found to be:

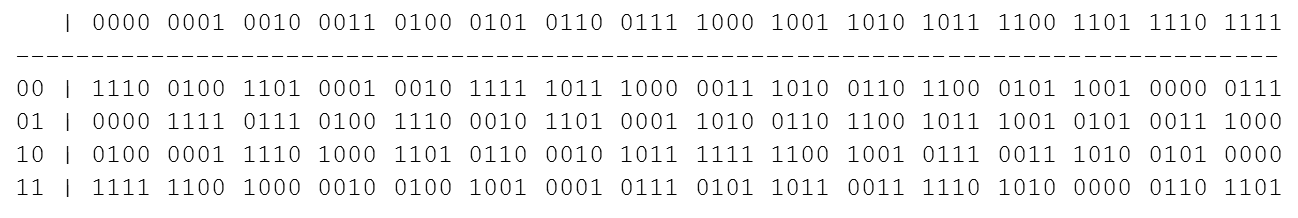
K1 = 010011110110110100110101001010101111110110101011

Using the solution, E(R0), from the previous question, and K1 find the 48-bit input for the S-Boxes, (B).

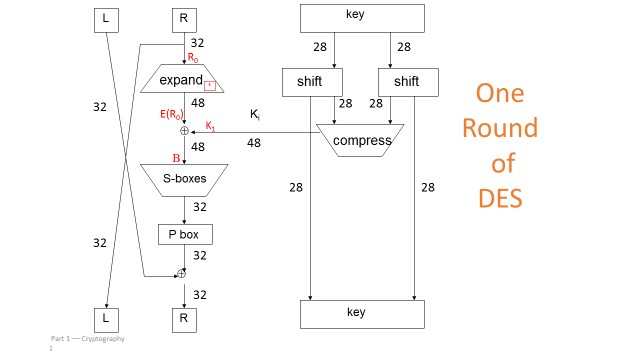
B =

1. Using the solution, B, from the previous question, determine the proper input and solution to S-Box, S1 below:

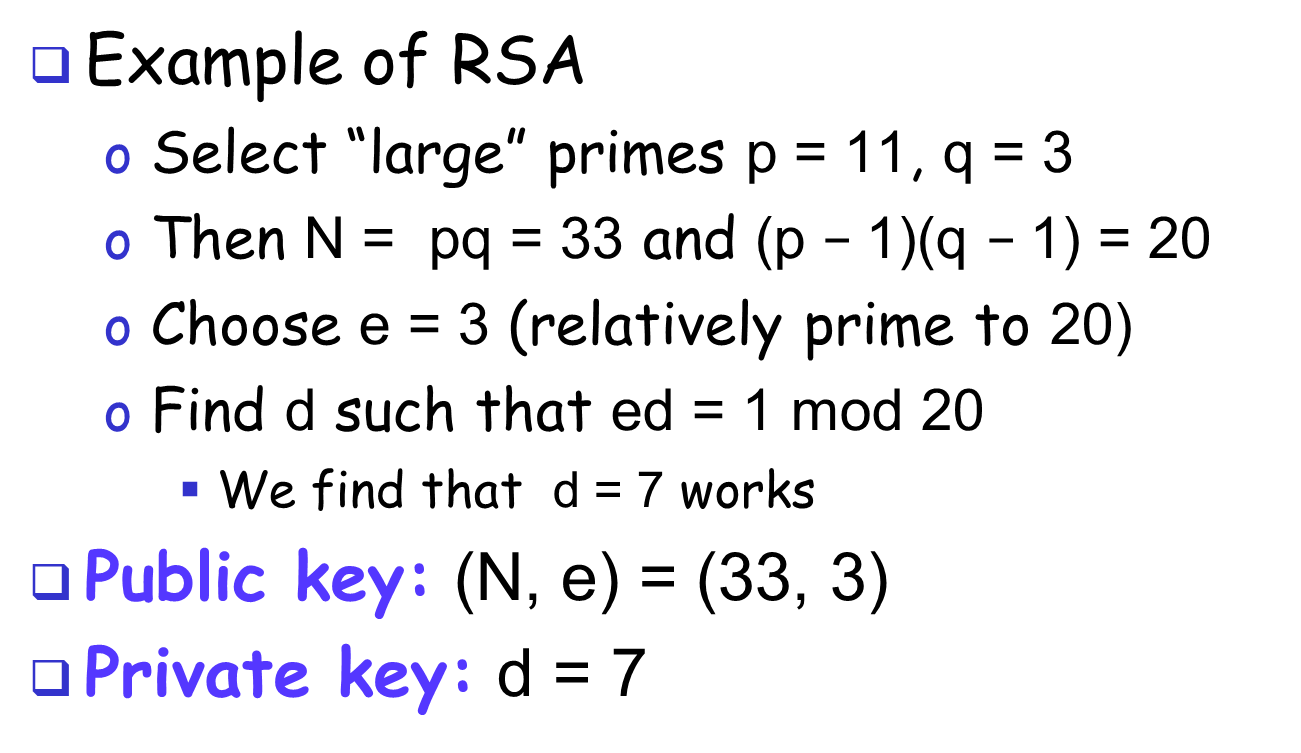
B1 =



S1 Output =



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)



p = , q = , N = , e = , d =

Extra Work (to be turned in with Exam).