(please type your answers)

Chapter 1 Questions (from textbook 1.6 Problems):

- 1 (6pts,  with1.a 3pts and 1.b, 1.c, 1.d 1pt each)

a. Confidentiality: assets (or data or information) are accessed only by authorized parties, (or prevent unauthorized data access). Integrity: Assets can be modified by authorized parties or only in authorized ways. Availability: Assets are accessible to authorized parties at appropriate times.

b. Confidentiality without integrity is of little use, since you would not be able to

trust the data.

c. Any transaction that is not secret, for example, the transfer of funds between

federal reserve banks in the U.S.

d. Availability is critical for any online business, such as amazon.com.

- 18  (7pts, 1 pt each subproblem)

-  (8pts in total) What is a security model? (2 pts) Describe the security model with the following application. Suppose you are developing a multi-play online gambling system.  The answer may not be unique, but you need to show a clear understanding of security model through the process. Refer to the slides for what you need to cover in your security model but not security solutions.  (6pts)

* Combination of trust model and threat model
* The answer may not be unique (as long as making sense).

Trust model: trust the server hosting the game to execute correctly.

Threat model: Game players may reverse engineer the software to change its logic, or further infer what other players, or deny their movements.

Chapter 2 Questions.

-1 (6 pts, with 2pts each subproblem)

a. See text.

b. Unfortunately, there are many such examples. For one, the crypto used in GSM

was designed in violation of Kerckho\_s' Principle. The crypto algorithms are

weak.

c. The design of any security features should be open and available for scrutiny.

- 6 (8pts) To unscramble, use the permutation 4,9,1,5,7,10,2,6,3,8. For example, the first line unscrambles to “If at first you don't succeed, try and try again."

-10 (hint: the first two words are:  never imagine) (12pts)

The key is ZGYHXIWJVKULTMSARBQCPDOENF and the plaintext is from Alice

in Wonderland: Never imagine yourself not to be otherwise than what it might appear

to others that what you were or might have been was not otherwise than what you had been would have appeared to them to be otherwise.

-14 (6 pts) The ciphertext is LEALETHRAWERGTOE.

-15 (11pts) Put the ciphertext in a 7 x 10 array. Then the letters of “there" will all appear (in scrambled order) in one row. This gives a start on the column permutation. Once the column perms are known, the row perms are easily determined. The answer is a quote from President Kennedy: “There are some who say that communism is the wave of the future. Let them come to Berlin."

-19 (8pts) 

-20 (8 pts, with 4 pts for each subproblem)

Let x be the 64-bit key. One approach would be to simply repeat x 16 times. However,

this would be equivalent to using a one-time pad 16 times so it would be very insecure.

A better idea would be to design a function f that produces a 64-bit output and

use x; f(x); f(f(x)); : : :. Of course, the security would depend on the choice of the

function f. In Chapter 3 we'll discuss stream ciphers, which are used to stretch a short key into a long stream of bits that can be used like a one-time pad. Theoretically speaking, it is not possible to achieve the same security strength as in one-time pad where each bit of key is randomly generated.

-24, hint: one letter of the keyword is “E” and one “R” has the plaintext “T”.  (12pts)

The plaintext is: Spoon feeding in the long run teaches us nothing but the shape of the spoon. The key is KEY.

- (8pts with 2pts for each concept including explanation) To design strong ciphers, what are the two security requirements and two design principles? Please explain their meanings.

two security requirements

* Large key space
  + *Exhaustive key search* takes too long
* No shortcut attacks
  + No better than *exhaustive key search*

two design principles

* Confusion *confusion* refers to making the relationship between the ciphertext and the symmetric key as complex and involved as possible;
* Diffusion *diffusion* refers to making the relationship between the plaintext and the ciphertext as complex and involved as possible (so that the plaintext statistics are spread over the ciphertext).