Name:

Information Assurance: Homework 2

Due September 8, 2010 on compass.

1. Policy or mechanism. For each item below, is it a policy or an enforcing mechanism? If it is a policy, identify a mechanism that could enforce it. If it is a mechanism, identify a policy it could be enforcing.
   a) Data classified as critical must be strongly encrypted when moving over public networks.
   b) All desktop computers must have password-based screen savers configured to go on after 30 seconds.
   c) Students and staff may not loan their their university key cards to other individuals.
   d) Only residents of Urbana may enroll their children in Urbana schools.
   e) Meijer's cashiers must check the ID of anyone who appears to be under 40 when they purchase alcohol.

2. You own a jewelry store. In your neighborhood, there is a 15% chance of a store like yours being the victim of a robbery during the course of the year. On average, your store has $100,000 in cash and products on hand. You are considering two controls. The first option is to hire a full time guard at the cost of $5,000 per month. Based on experience in your industry, this should reduce your risk of robbery to 3% over a year. The second option is to hire an alarm/monitoring company. They will install cameras and have a staff at their offices reviewing the camera feeds. This will reduce the risk of a non-recoverable robbery to %8 and will cost $2,000 a month.

a) What is your current annual loss expectancy (ALE) (you've implemented neither control)?

b) Compute the risk leverage for the first option (hiring a guard).

c) Compute the risk leverage for the second option (install cameras and employ the monitoring company).

d) Based on the risk leverage computation, which option should you go with?

Name:

3. Consider the rail cipher or the n-columnar transposition cipher:

a) Encrypt the following phrase using the rail cipher or 2-columnar transposition cipher: **Now is the time for all good men to come to the aid of their country.**

b) Decrypt the following phrase using a 3-columnar transposition TQCRNXMDEHADHUKOFJPOREZOEIBWOUEVTLYG

c) Given a piece of cipher text, how would you first test to see if it was a transposition cipher?

d) Assuming it appears to be a transposition cipher, and you think it is probably a n-columar cipher, how would you start determining the **n** for the n-columnar transposition?

4. Consider Vigenere cipher:

a) Use the Vigenere tableau at the end to encrypt the phrase “Labor Day” with the key “work”.

b) Use the Vigenere tableau to decrypt “YHPRWELEUUXAPIY” with the key “fall”.

c) Determine the key and decode the Vigenere encrypted text posted at http://www.cs.illinois.edu/class/fa10/cs461/assignments/cipher.txt. You may use automated tools such as the applet discussed in class http://math.ucsd.edu/~crypto/java/EARLYCIPHERS/Vigenere.html.

d) Describe how you determined the period. Make sure you do more than just mess about with the applet.

Name:

```
  | a b c d e f g h i j k l m n o p q r s t u v w x y z
-------------------------------------------------------
A | a b c d e f g h i j k l m n o p q r s t u v w x y z
B | b c d e f g h i j k l m n o p q r s t u v w x y z a
C | c d e f g h i j k l m n o p q r s t u v w x y z a b
D | d e f g h i j k l m n o p q r s t u v w x y z a b c
E | e f g h i j k l m n o p q r s t u v w x y z a b c d
F | f g h i j k l m n o p q r s t u v w x y z a b c d e
G | g h i j k l m n o p q r s t u v w x y z a b c d e f
H | h i j k l m n o p q r s t u v w x y z a b c d e f g
I | i j k l m n o p q r s t u v w x y z a b c d e f g h
J | j k l m n o p q r s t u v w x y z a b c d e f g h i
K | k l m n o p q r s t u v w x y z a b c d e f g h i j
L | l m n o p q r s t u v w x y z a b c d e f g h i j k
M | m n o p q r s t u v w x y z a b c d e f g h i j k l
N | n o p q r s t u v w x y z a b c d e f g h i j k l m
O | o p q r s t u v w x y z a b c d e f g h i j k l m n
P | p q r s t u v w x y z a b c d e f g h i j k l m n o
Q | q r s t u v w x y z a b c d e f g h i j k l m n o p
R | r s t u v w x y z a b c d e f g h i j k l m n o p q
S | s t u v w x y z a b c d e f g h i j k l m n o p q r
T | t u v w x y z a b c d e f g h i j k l m n o p q r s
U | u v w x y z a b c d e f g h i j k l m n o p q r s t
V | v w x y z a b c d e f g h i j k l m n o p q r s t u
W | w x y z a b c d e f g h i j k l m n o p q r s t u v
X | x y z a b c d e f g h i j k l m n o p q r s t u v w
Y | y z a b c d e f g h i j k l m n o p q r s t u v w x
Z | z a b c d e f g h i j k l m n o p q r s t u v w x y
```