

Name:

Information Assurance: Homework 2

Due September 12, 2007 on compass.

1. Consider online credit card transactions. Describe an example of each of the following:
 - a. A security requirement
 - b. A security constraint.
 - c. A security control.
2. A team of experts using the quantitative risk analysis approach has reviewed a software development organization. They identified the two most important assets of the organization, the value of each asset, and the probability that a threat would be successfully launched against each asset of a 12 month period.

Asset	Value	Risk over a year
Product Source	\$1,000,000	1%
Customer Records	\$250,000	10%

- a. What is the risk exposure/annual loss expectancy for each asset?
- b. The experts have identified two control options

Control	Cost	New Risk for Source	New Risk for Records
Wonder Security Product	\$100,000	0.5%	1%
Hire Security Officer to Improve Implementation of Existing Controls	\$200,000	0.1%	5%

Calculate the Risk Leverage in both cases. Based on the Risk Leverage numbers, which control would you recommend trying first.

- c. Identify two additional assets of the organization
 - d. Identify three potential threat sources. Use the MOM (method, opportunity, motive) technique to characterize the threat sources.
 - e. For each threat source identify the asset of greatest interest.
3. Cipher texts resulting from substitution and transposition ciphers have different characteristics. Identify the most likely class of cipher in each case below:
 - a. Characters in the message have a statistical distribution close to that of standard English messages

Name:

- b. Digrams in the message follow the same statistical frequencies as those found in standard English.
4. The message below is encoded using a book code with the course syllabus page as the key <http://www.cs.uiuc.edu/class/fa07/cs461/syllabus.html>. Decode the message.

VVVYTONLDEIZSFWGHVALWNCFPZHVL

5. Determine the key and decode the vigenere encrypted text assigned to you in compass. You may use automated tools such as the applet discussed in class <http://math.ucsd.edu/~crypto/java/EARLYCIPHERS/Vigenere.html>.
6. Encode the following message using columnar transpositions. Use Z as a pad character as necessary
Twas brillig, and the slithy toves
Did gyre and gimble in the wabe:
All mimsy were the borogoves,
And the mome raths outgrabe.
 - a. Encode using a 2-columnar transposition (also known as a rail transposition).
 - b. Encode using a 7-columnar transposition.
7. One time pads are “perfect” ciphers if the keys never predictably cycle. If the key stream is random so is the ciphertext. However, if the key stream repeats, the interceptor can get two streams of ciphertext that use the same key sequence. He can use these two ciphertext streams to get a text sequence that is only a function of the plaintext (the keys are canceled out).

In substitution cases discussed in the book, the encryption algorithm is $E(p_i, k_i) = (p_i + k_i) \bmod 26$. Assume you are given two ciphertext sequences X and Y that are results of encrypting different plaintext with the same keys. Show how X and Y can be combined to create a function that is only a function of the plaintext of X and Y.