CS 4920/5920 Applied Cryptography Spring 2018

Assignment 1

This assignment covers Ch. 1 and Ch. 3 and is due at the beginning of class on January 31st. Please explain how you reached your answers.

Problem 1:

Consider a desktop publishing system used to produce documents for various organizations.

a. Give an example of a type of publication for which confidentiality of the stored data is the most important requirement and explain why.
b. Give an example of a type of publication for which data integrity is the most important requirement and explain why.
c. Give an example in which system availability is the most important requirement and explain why.

Problem 2:

A generalization of the Caesar cipher, known as the affine Caesar cipher, has the following form: for each plaintext letter p (where p can be an integer between 0 and 25 inclusive), substitute the ciphertext letter C:

$$C = \mathrm{E}([a, b], p) = (ap + b) \bmod 26$$

A basic requirement of any encryption algorithm is that it needs to be one-to-one. That is, if $p \neq q$, then $\mathrm{E}(k,p) \neq \mathrm{E}(k,q)$. Otherwise, decryption is impossible, because more than one plaintext character maps into the same ciphertext character. The affine Caesar cipher is not one-to-one for all values of a. For example, for a=2 and b=3, then $\mathrm{E}([a,b],0) = \mathrm{E}([a,b],13) = 3$.

a. Are there any limitations on the value of b? Explain why or why not.
b. Determine which values of a are not allowed.
c. Provide a general statement of which values of a are and are not allowed. Justify your statement.
d. How many one-to-one affine Caesar ciphers are there?

Problem 3:

a. Using this Playfair matrix:

M	F	H	I/J	K
U	N	O	P	Q
Z	V	W	X	Y
E	L	A	R	G
D	S	T	B	C

Encrypt this message:

Must see you over Cadogan West. Coming at once.

Note: The message is from the Sherlock Holmes story, *The Adventure of the Bruce-Partington Plans*.

b. Repeat part (a) using the Playfair matrix with the key *largest*.
c. How do you account for the results of this problem? Can you generalize your conclusion?

Problem 4:

a. How many possible keys does the Playfair cipher have? Ignore the fact that some keys might produce identical encryption results. Express your answer as an approximate power of 2.
b. Now take into account the fact that some Playfair keys produce the same encryption results. How many effectively unique keys does the Playfair cipher have?

Problem 5:

This problem explores the use of a one-time pad version of the Vigenere cipher. In this scheme, the key is a stream of random numbers between 0 and 25. For example, if the key is 3 19 5 …, then the first letter of plaintext is encrypted with a shift of 3 letters, the second with a shift of 19 letters, the third with a shift of 5 letters, and so on.

a. Encrypt the plaintext sendmoremoney with the key stream 9 0 1 7 23 15 21 14 11 11 2 8 9.
b. Using the ciphertext produced in part (a) , find a key so that the cipher text decrypts to the plaintext cashnotneeded.
c. Without knowing the key, can a brute-force attacker decrypt the ciphertext from part (a)?