Information Security
Homework 2

Dr. Edwin Sha

Due Date: **4PM, Oct. 12, 2003**

The homework is important to help your learning. In this course, some homework questions do not have standard solutions. And many questions are intended to be vague. So try your best and make your reasonable assumptions.

If you have questions, ask TA first. TA will grade your homework. It is YOUR responsibility to make your answers understandable.

PUT DOWN YOUR EMAIL ADDRESS IN YOUR REPORT. By the way, I don't like handwritten report. Please use some computer formatting tool such as LaTex or Word.

1. (10 points) Go to http://www.cert.org/advisories/ to check all the advisories appeared in 2003.

   (a) Which advisories are related to buffer-overflow vulnerability in a general sense.

   (b) Describe CA-2003-21 advisory. Explain what is this *kmod/ptrace* vulnerability. You can find the information using google search.

2. (15 points) Read the documents posted in the course web page or any documents you find in the web. Answer the following questions:
   (a) If you are asked to write password cracking programs, what are the rules or algorithms you will try. For example, check the dictionary words can be one of the patterns. You also can look into password cracker programs on the web for your reference.

   (b) What your ideas to strengthen the operating systems, so it is hard for anyone trying to crack a weak password?

3. (15 points) (a) In my lecture, I presented the first method of implementing digital signature using the public-key cryptosystem in which S=E(M, Private key of Bob), and then Bob encrypts the concatenation of M and S and sends it to Alice. How about we just encrypt S, C= E(S, Public key of Alice) and Bob sends this C to Alice? This looks like a more efficient method. Does this gives the property of digital signature. Based on what assumption, this indeed provides digital signature property?

   (b) Assume the hash function is not well designed so the hashed values are not randomly uniformly distributed. What is the problem?

4. (10 points) (a) Encrypt the message "beat" using the Hill Cipher with the key matrix K $\begin{pmatrix} 5 & 4 \\ 5 & 7 \end{pmatrix}$ Show your calculation and result. Note that all computations are based on mod 26.

   (b) Show the calculation for the corresponding decryption of the ciphertext to recover the original plaintext. You must show what the inverse of K is. Make sure that each final element in the matrix is between 0 and 25.

5. (15 points) This question is for Hill cipher. Lets make the question simple. Assume an input character only can be {0, ..., 11 }; i.e., from 'a' to 'l' where 'a' is 0 and 'l' is 11. So it is

modulo 12 rater than 26.

(a) Is there any problem to encrypt and decrypt a message using the Hill Cipher with the key $\begin{pmatrix} 7 & 10 \\ 2 & 4 \end{pmatrix}$ What is the problem? Explain clearly.

(b) Based on the same assumption, this is to ask you to find out what the key matrix, K, is. Assume that you know three plaintext-ciphertext pairs (p, c) as follows: ((1, 2), (3, 0)), ((3, 4), (5,2)) and ((1, 7), (1, 1)). What is the key matrix K? Each element in K is within 0 to 11.

6. (10 points) Encrypt the message "attackhmsfleet" using Playfair Cipher with key= "security". Use filler "x" and use "I" for the pair "I/J" in the table.

7. (15 points) This question is about the cryptanalysis for Vigenere cipher I talked about in class. Please read the handout. (a) Please describe the method using so called the Index of Coincidence to find the key length. What is the idea behind? Why is the index of Coincidence defined in such a way?

   (b) Briefly describe the method of using that function M_g to determine the value of each key. What is the idea behind.

   (c) If $M_g = \sum_{i=0}^{25} f_{i+g}/n' \times f_{i+g}/n'$, will it work well to determine the value of each key? Explain your reasons clearly.

8. (20 points) Lets make the question simple. Assume an input character only can be {0, ..., 13 }; i.e., from 'a' to 'n' where 'a' is 0 and 'n' is 13. So it is modulo 14 rater than 26.

   The encryption of the **shift cipher** or called **Caesar Cipher** is given by a function of $e(x) = (x + b)$ mod 14. Lets define a similar cipher whose encryption function is defined as $e(x) = (ax + b)$ mod 14 where $0 \leq a, b \leq 13$. It is clear that shift cipher is a special case of this cipher. Not all possible values of (a, b) can be used to construct this cipher. Think about it.

   You should try to figure out what values of (a, b) are feasible for such an affine cipher; in other words, you must be able to decrypt any $e(x)$ using such (a, b); i.e. $e(x)$ must be invertible so you can decrypt $e(x)$ and get x back.

   (a) When (a, b) = (3, 7), list the e(x) values for x from 0 to 13. Show it is feasible or not.

   (b) When (a, b) = (3, 7), show the mathematical way to decrypt such an $e(x)$? Given an $y = e(x)$, express the decryption function in the form of $d(y) = cy + d$, where $0 \leq c, d \leq 13$.

   (c) Is (a, b) = (6, 4) feasible or not? Show your reason.

   (d) Can you come out a simple way to test if a given (a, b) is feasible to build an affine cipher or not? Lets generalize it to be $e(x) = (ax + b) mod Y$ where Y can be different from 14.

   Hint: It is known that $ax = b \pmod{m}$ has a unique solution x, $0 \leq x \leq m - 1$, if and only if gcd(a, m) = 1.

No cheating is allowed. I will be very upset if we find any cheating. You must do the homework by yourself.