

Computer and Network Security

Homework 2

Dr. Edwin Sha

Due Date: 10am, April 10, 2012

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.

- (20 points) This is to test your knowledge on TCP/IP. (A) Explain the 3 steps that make a connection be set up by TCP protocol. (B) Explain what is the so-called TCP SYN Flooding Attack. (C) Assume that Computer X trusts Computer Y. What are the common steps by using IP Spoofing method such that Z can pretend to be Y to connect with X and may run a remote shell in X? (D) Show the basic idea of using SynCookie that is trying to reduce possibility of SYN Flooding attacks.
- (15 points) Though Email Spam is not a virus, worm or Trojan horse, it is very annoying. Go to the web to find how email spam work, for example, http://en.wikipedia.org/wiki/Email_spam. Email spam is actually becoming a crime in US. But for protecting from Email spam, lets assume that if you were an email spammer, tell me how you can do an effective email spam.
 - How email addresses are gathered?
 - What are your ideas to design an efficient anti-spam tool? Please give me TWO ideas and show the pros and cons for each. You can design a good product and even start your own company based on your ideas.
- (20 points) (a) Encrypt the message "dead" using the Hill Cipher with the key matrix $K = \begin{pmatrix} 3 & 4 \\ 4 & 7 \end{pmatrix}$. Show your calculation and result. Note that all computations are based on mod 26.
 - What is the determinant of matrix K ? What is the value of $1/\text{determinant}$? **Make sure that the answer is between 0 and 25.**
 - 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 element in the inverse matrix is between 0 and 25.**
- (15 points) This question is for Hill cipher. Lets make the question simple. Assume an input character only can be $\{0, \dots, 11\}$; i.e., from 'a' to 'l' where 'a' is 0 and 'l' is 11. So it is modulo 12 rather 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: $((1, 2), (4,6)), ((3, 4), (10,0))$ and $((2, 5), (9, 3))$. What is the key matrix K ? In your answer each element in K must be within 0 to 11.
5. (10 points) Encrypt the message “texasfirst” using Playfair Cipher with key= “university”. If necessary, use filler ”x” and use ”I” for the pair ”I/J” in the table.
6. (20 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.
7. (10 points) Consider the following algorithm to find the factorization of a given number N .

```

Input n;
Output x, y such that x * y = n;

for (x= 2; x <= sqrt(n); x++)
    if (x divides n) return (x, n/x);

return (n, 1);

```

- (a) Is the complexity of this algorithm $O(\sqrt{n})$?
- (b) Is this a so-called polynomial-time algorithm? Is it efficient? Why or why not? Explain it clearly. You should explain what “polynomial-time” means.
8. (10 points) In the lecture, I gave a simple example which can provide data integrity using a shared secret key. Now lets change it a little bit by using pure public/private keys instead. Let $H=Hash(M)$ and $C= E(M\&H, \text{public key of Alice})$, and then Bob sends C to Alice. Alice will use its own Private key to decrypt it. Will this method provide data integrity (or called message authentication)? Why or why not?
9. (20 points) Lets make the question simple. Assume an input character only can be $\{0, \dots, 11 \}$; i.e., from 'a' to 'l' where 'a' is 0 and 'l' is 11. So it is modulo 12 rather than 26.

The encryption of the **shift cipher** or called **Caesar Cipher** is given by a function of $e(x) = (x + b) \bmod 16$. Lets define a similar cipher whose encryption function is defined as $e(x) = (ax + b) \bmod 12$ where $0 \leq a, b \leq 11$. 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 $(a, b) = (5, 3)$, list all the $e(x)$ values for x from 0 to 11. Show it is feasible or not; one-to-one mapping or not?

(b) When $(a, b) = (5, 3)$, 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 $0 \leq c, d \leq 11$. For example, when $y=9$, what is x ?

(c) Is $(a, b) = (3, 4)$ 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 $e(x) = (ax + b) \bmod Y$ where Y can be different from 12.

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.