

Assignment 1
Computer Science 349
Spring 2004

Due: Start of class on Thursday February 5

Reading: Singh, Introduction and Chapter 1; Stinson, Sections 1.1.1 – 1.1.2.

Exercise 1.0. Choose three passwords (that you must remember without any written cues for the next five weeks). Write your name and your three passwords on the 3 x 5 index card attached to this assignment and give the card to your instructor before leaving class today. Warning: Do not choose a password that you have used in the past, are currently using, or plan to use in the future. But, do try to remember them.

Exercise 1.1. The mysterious sect of the Knights Templar guards an ancient secret. For centuries their members have protected this vital information from prying eyes. Just one record of their secret exists in written form and you have just discovered what you believe is a reference to it in an old book. However, the exact location has been cunningly encoded. Can you work it out?¹

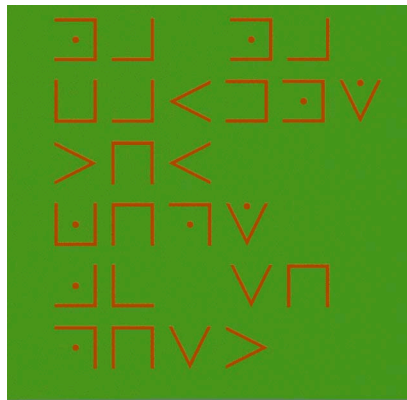


Figure 1.1 Message of the Knights Templar.

Exercise 1.2. A disadvantage of the general monoalphabetic cipher is that both sender and receiver must commit the permuted cipher sequence to memory (or worse still, write it down). A common technique for avoiding this is to use a keyword from which the cipher sequence can be generated. For example, using the keyword CIPHER, write out the keyword followed by unused letters in normal order and match this against the plaintext letters:

¹ From *Mensa for Kids: 75 Secret Codes*, Chronicle Books. *Hint:* There's not much text here, but you do have several things going for you. First, the Mensa folks left spaces unencrypted. Also, you know it's a pigpen cipher and you might suspect, given the audience, that arrangement of the alphabet within the pigpens is particularly simple. (Similar, but not quite the same as given in Singh.)

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

If this does not produce sufficient mixing, write the remaining letters on successive lines and then generate the sequence by reading down the columns:

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

This yields the sequence:

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

Such a system was used in the following example:

UZQSOVUOHXMOPVGPOZPEVSGZWSZOPFPESXUDBMETSXAIZ
itwasdisclosedyesterdaythatseveralinformalbut

VUEPHZHMDZSHZOWSFPAPPDTSVPQUZWYMXUZUHSX
directcontactshavebeenmadewithpolitical

EPYEPDPDZSZUFPOMBZWPFUPZHMDJUDTMOHMQ
representativesofthevietcong inmoscow

Determine the keyword. (*Hint: After the first row, the letters in each row appear in order.*)

Exercise 1.3. In the first lecture we discussed a way to split a key, or a secret, into two equal parts so that the secret can only be recovered if both the parts are available. The secret in this case was an ordered pair of integers representing the combination of a toy safe. The secret was divided by giving each partner the two equations in two variables, representing the equations of two lines in the real plane. To recover the first number of the combinations, the partners find the point of intersection of the first two lines and take its x coordinate. To recover the second number of the combination, the partners find the point of intersection of the second pair of lines and take its y coordinate.

- Why not give both partners the equation of a single line in the real plane and let the combination be point of intersection?
- How would you share a secret among three partners? Generalize your approach to n partners.
- There are many reasons why you might want to recover a secret even if you don't have all the parts. For example, if a corporation has five directors, you might require that three be present to unlock the corporation's secret key used to

sign documents. Describe a scheme in which a secret can be split into n parts and any k must be available to recover the secret.

- d. In each of the schemes described above, the secrets are split into n parts, each of the n parts begin equal. Humans, being human, are never satisfied with anything as fair as that – some people will want some parts to be more powerful than others. The most straightforward way to accomplish this is to give some people more parts. For instance, imagine a scheme where you need six parts to reconstruct the secret. For the sake of example, let's say it takes two commanders, three sergeants, or six privates to launch a missile. This can be accomplished by giving three parts to the commanders, two parts to the sergeants, and one part to each of the privates.

One problem with this solution is that arbitrary combinations of different ranks can join together. So, one commander, one sergeant, and one private can work together to uncover the secret. This might not be permitted in some cases. For example, the U.S. Congress requires a majority of both the House and Senate to pass a bill. But the votes from one chamber cannot be counted against the other. So even though there 100 senators and 435 members of the House, a senator is not really worth 4.35 House members. A bill won't pass just because 99 senators vote for it and only 10 house representatives. But this could be the situation if someone naively created a secret-sharing scheme by parceling out parts to both sides of congress from the same shared secret. Devise a better solution to the problem of unequal sharing and apply it to the example of the US Congress. (For the purpose of this discussion, you may treat all the secret splitting techniques given in parts *a*, *b*, and *c* as black boxes which may be used here to help with the uneven division problem.)

Exercise 1.4. Mary Queen of Scots and her coconspirators used a combination of (a rather crude) steganography and cryptography to hide their assassination plot. Why use both?

Exercise 1.5. During the great depression homeless men traveling about the country were known as hoboes. Their lives were often romanticized in novels, songs, and movies. It was said that hoboes formed a kind of brotherhood to help each other, with their own secret marks. These were left outside houses, usually chalked on a gatepost, to signal to others what sort of reception they might get. Figure 1.2 illustrates common warning signs from the Midwest during the great depression. Was this system a cipher or a code? Briefly justify your answer.



Figure 1.2. Hobo warning signs

The following exercises are from the Stinson text. Please read the discussion of modular arithmetic in Section 1.1.3 before completing these problems. Modular arithmetic will play an important role in many of the cryptographic systems we will study this semester.

Exercise 1.6. (Stinson 1.1) Evaluate the following

- a. $7503 \bmod 81$
- b. $(-7503) \bmod 81$
- c. $81 \bmod 7503$
- d. $(-81) \bmod 7503$

Exercise 1.7. (Stinson 1.2) Suppose that $a, m > 0$, and $a \not\equiv 0 \pmod{m}$. Prove that $(-a) \bmod m = m - (a \bmod m)$.

Exercise 1.8. (Stinson 1.3) Prove that $a \bmod m = b \bmod m$ if and only if $a \equiv b \pmod{m}$.

Exercise 1.9. (Stinson 1.5) Use exhaustive key search to decrypt the following ciphertext, which was encrypted using a *Shift Cipher*:

BEEAKFYDJXUQYHYJIQRYHTYJIQFBQDUJIIKFUHCQD.