Lab #1

Out : September 13, 1996; 5:00 pm
Due : September 20, 1996; 6:30 pm

Announcements

Learning how to use the calculator: Mini-lectures/demonstrations on the use of the calculator will take place in CIT 265 during our regular lab hours—see below. (You should only need to go to one of these times!) A handout on how to use the calculator is available for use with this lab and for future reference. The handout assumes you have some familiarity with using a mouse (clicking, double-clicking, and dragging). Students who are unfamiliar with this should see a TA during TA hours as soon as is convenient.
It is our hope that this first assignment will be relatively simple and provide a good illustration of the basics of the MarkCalc. If you find anything unclear, TAs will be available for office hours in CIT265..

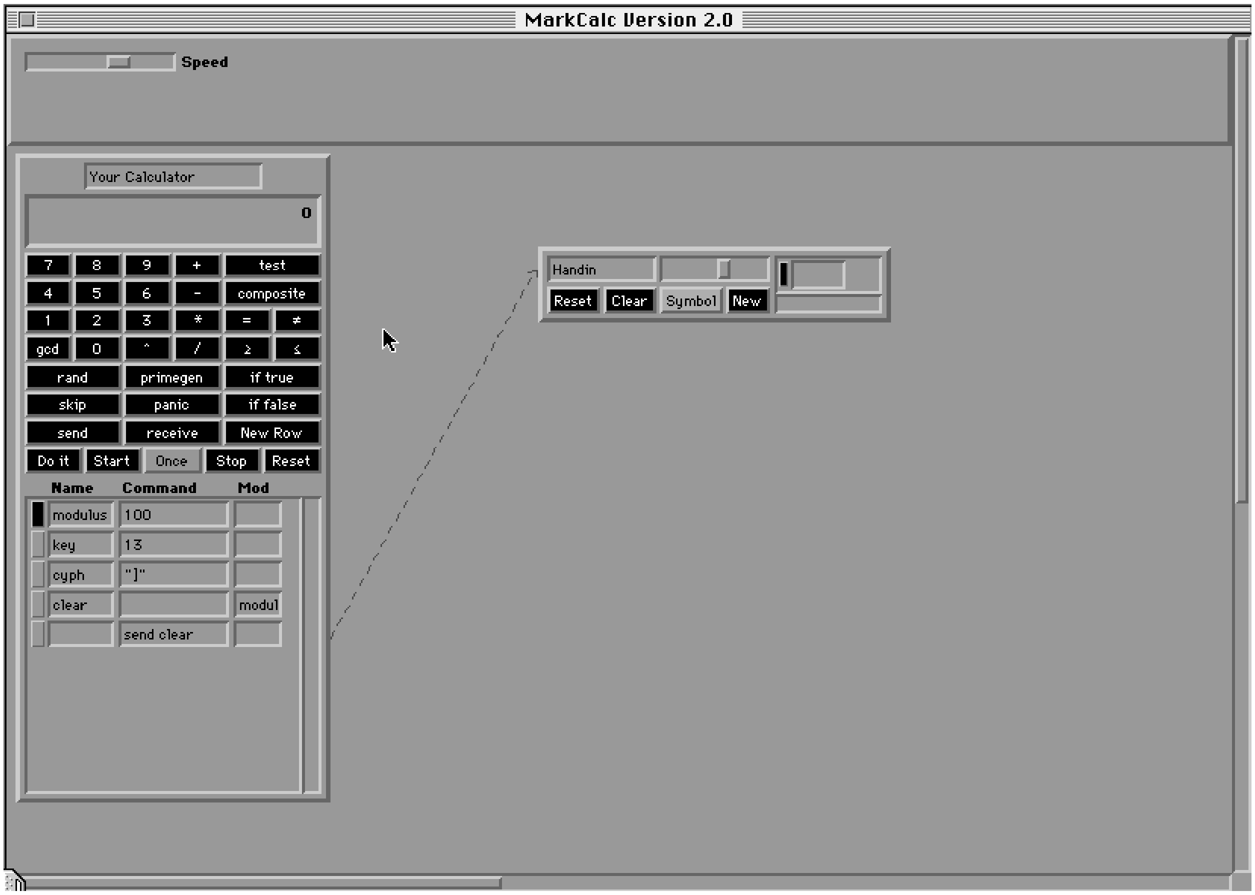
CIT265 Reservations: We have reserved CIT room 265 for several time slots each week for use by cs007 students. Keep in mind these are not sections, merely time slots when cs007 students who wish to work in the clusters will have priviledged use of the machines in room 265. We will occasionally hold optional help sessions during these times. The hours are:

Sunday	7:30-9:30pm
Monday	7:30-9:30pm
Wednesday	8-9:30pm

Experiment 1:

(a) You and your government contact have agreed to meet in the fiction section of the local public library to exchange information, but at the time this agreement was made you did not want to decide on a particular place for the meeting. Now, you have received a message telling you the letter of the alphabet that determines where in the fiction section you will meet. The message is encrypted using the Caesar cypher. You know that the key is 13 and the message you have received is the symbol "]" (the numeric equivalent is 28). **The modulus used is 100, not 26.** Use the calculator to decrypt the letter that represents the meeting place. (Obviously this can easily be done by hand, but we want you to get some practice with the calculator.)

When you open up the experiment, you will find a calculator that is mostly set up to perform this operation. There will be a transcript labeled "Hand-in" next to the calculator. Your task for this experiment is simply to put the appropriate equation in the row that computes the plaintex. Having done this, pressing the calculator's *Start* button will cause the decryption to begin. The last line in the calculator uses the *send* command to send the value for the plaintex you computed over a wire to the hand-in transcript. Once you have decrypted the secret message, selecting *Submit Results* from the File menu will send the value in the hand-in transcript to the TAs for grading.



Name	Command	Mod
modulus	100	
key	13	
cyph	"]"	
clear		modul
	send clear	

Figure 1: Experiment 1a

A note about submitting: Make sure that the Hand-in transcript contains only one value. This will not be a problem if you clear the Hand-in transcript after making any mistakes.

In Brief...	
We give you:	A calculator ready to perform a Caesar cypher decryption.
Your task:	Fill the command line labeled "cyph".
Hand in:	Submit electronically once the hand-in transcript has received the plaintex.

(b) The library meeting was such a success that you have arranged for your next meeting to take place in the fiction section of annother library branch. Being a rabid fan of Ernest Hemingway, you intend to meet in the "H" section. The task at hand, then, is to use the Caesar cypher to encode the letter "H" using your agreed-upon key of 13 (and the modulus of 100).

In this experiment, you will be given a blank calculator and a *Hand-in* transcript. You must set up the calculator to encrypt your message and then use the *send* command to transmit the

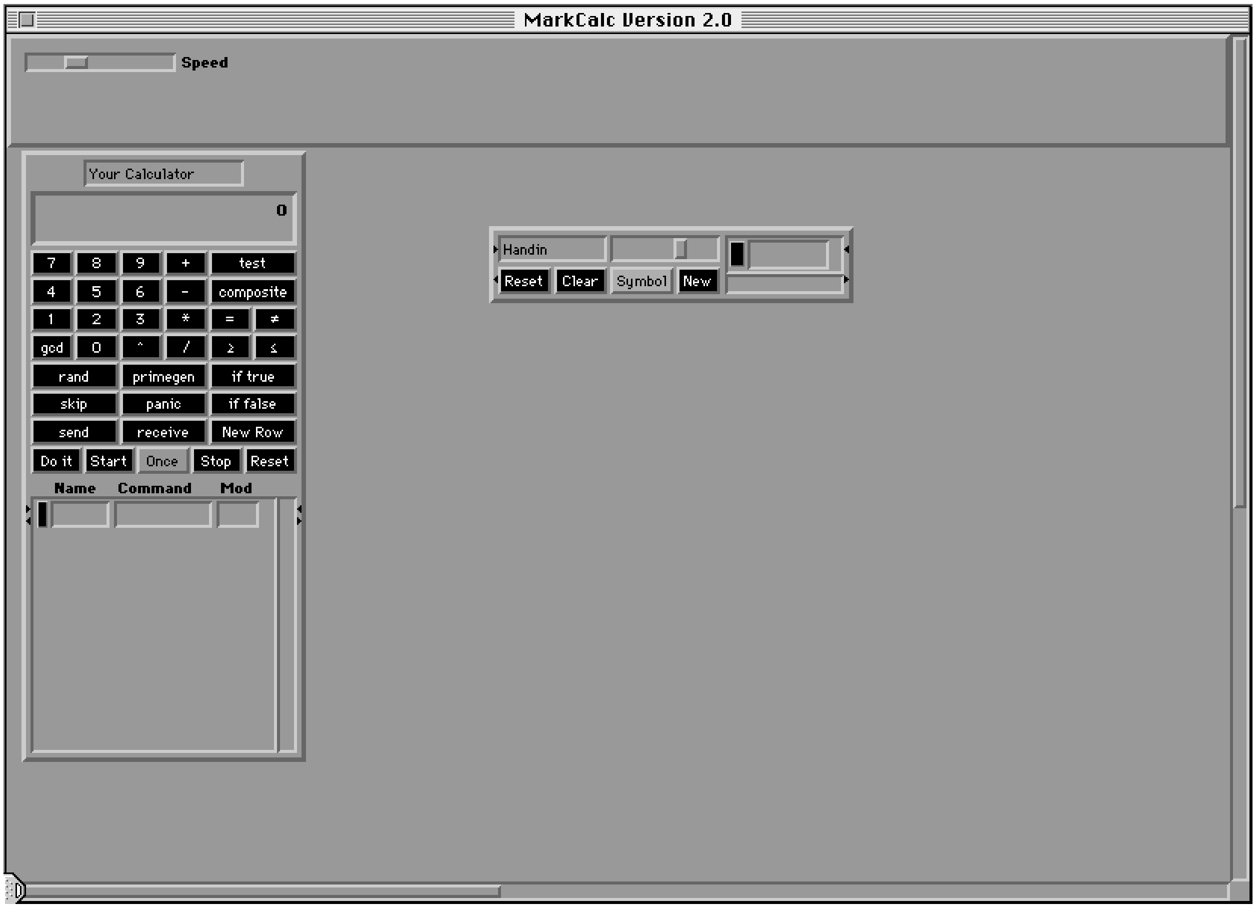


Figure 2: Experiment 1a

encoded message to the hand-in transcript. Before you can send a value to the hand-in transcript, however, you must draw a wire from the appropriate row of your calculator to the transcript.

Note about the Send command: When you want to send something, it is important that you enter the *send* command in the Command column by moving the cursor to that column and actually pressing the *Send* button on the calculator keypad. **If you type in the word** *send by hand, it will not work.* When you press the send button, the word *send will appear in the command column. Then use the keyboard to enter the name of the value you wish to send.*

In Brief...	
We give you:	A blank calculator and hand-in transcript.
Your task:	Fill in the calculator to perform the encryption and send to the transcript.
Hand in:	Submit, electronically, the encrypted letter “H”.

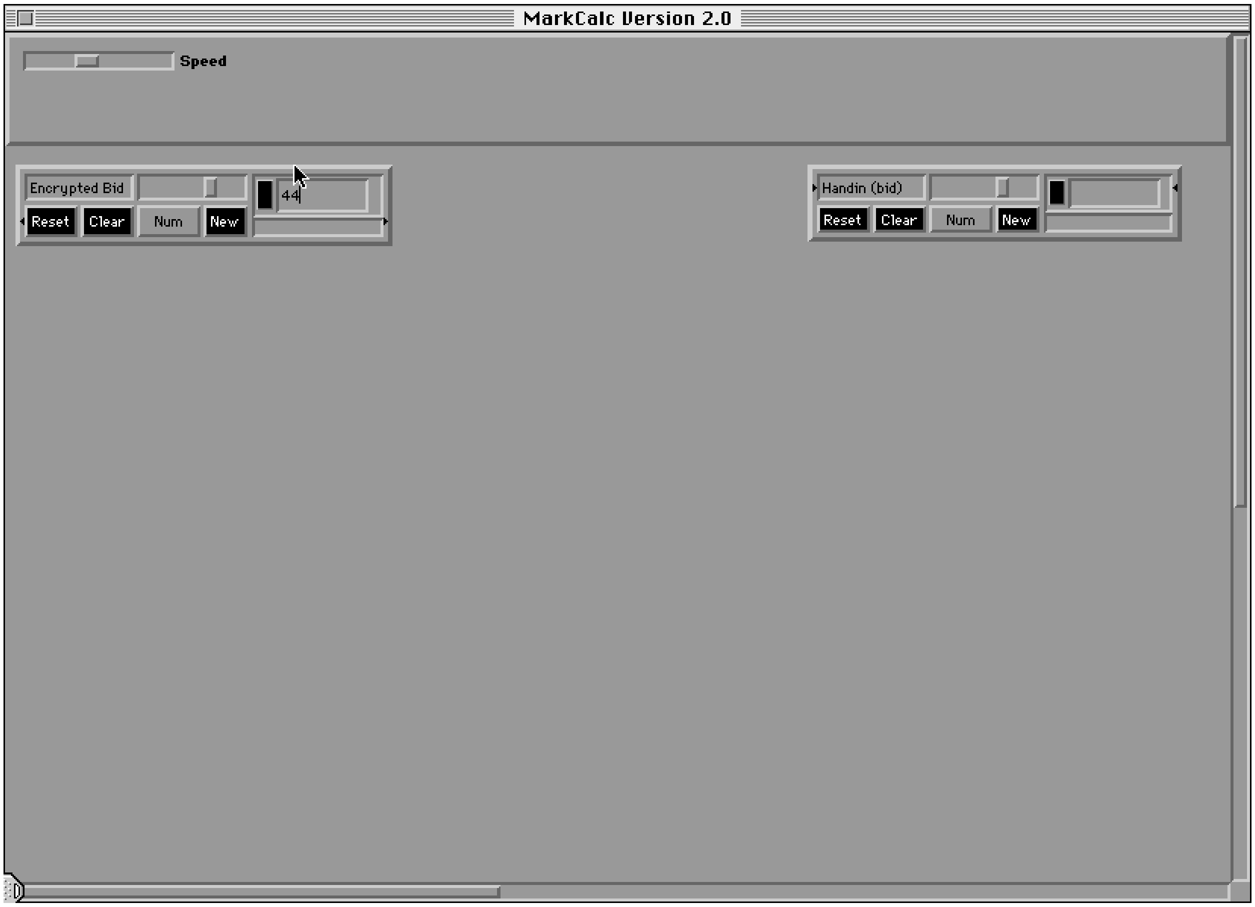


Figure 3: Experiment 1a

Experiment 2:

(a) You are acting as a proxy for a Australian sheep shearing company that is bidding in an auction for a new shearing robot of which there is only one in existence. You need to know how high the company is willing to bid in order to obtain this amazing new piece of technology, but you don't want your competitors to know what your maximum bid will be. The maximum bid is somewhere between 0 (if they have suddenly decided they don't want it at all) and 99 dollars. Your company has decided to use the Caesar cypher to encrypt the bid, using an agreed-upon key of 19 and a modulus of 100, and send it to you.

When you open up this experiment, you will see a transcript labeled *Encrypted Bid*. This contains the coded message from your company. There will also be a transcript labeled *Hand-In*. You will need to add a new calculator to the workspace and set it up to receive the contents of the *Encrypted Bid* transcript, decrypt the message, and send the result to the hand-in transcript.

In Brief...	
We give you:	A transcript containing a message encrypted with Caesar's cypher.
Your task:	Decrypt the message.
Hand in:	Submit, electronically, the plaintext message.

(b) By a stroke of good luck, you have stumbled upon a memo from a competing shearing company to *their* bidding proxy. The memo reads:

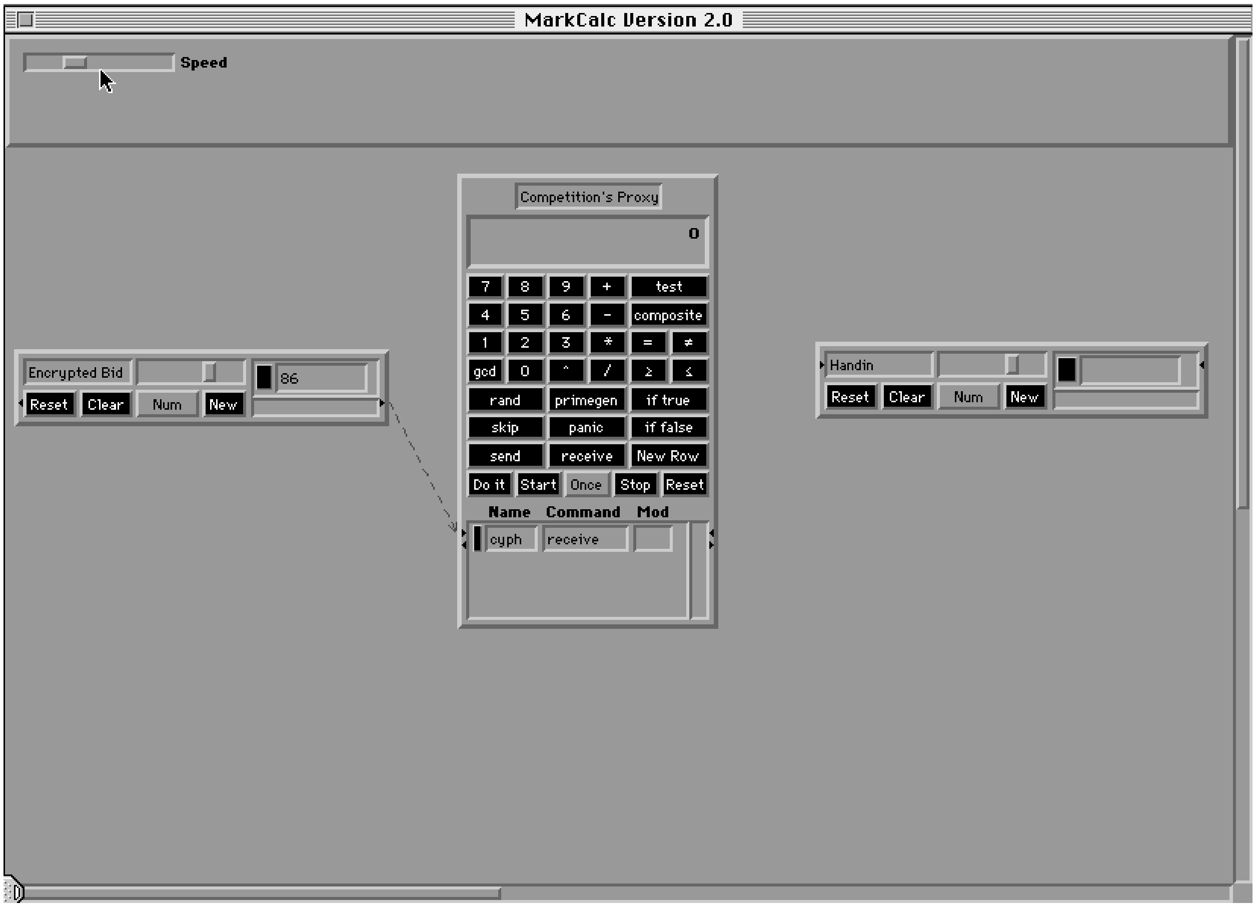
> "In an effort to prevent our competition from discovering our maximum bidding price, we will encode our messages to you using Caesar's cypher with a key of 76 and a modulus of 100.
> It is *imperative* that you destroy this memo after committing this secret key to memory!
> - The Management"

In this experiment, you will eavesdrop on the communication between the competition and their proxy. Using the information in the memo, you must decrypt the message and submit it. The transcript on the left contains the encrypted message from the competition, and the calculator on the right represents their bidding proxy. Notice that the wire which connects the transcript to this calculator is a dotted arrow. That means that this wire is "insecure"; you should be able to "tap" it by clicking on it and drawing annother wire to your own calculator. You must add a calculator to listen in on the message when it is sent, decrypt it, and then send the result to the hand-in transcript. Remember to press *Start* on the enemy calculator as well...

In Brief...	
We give you:	An enemy calculator reading a message from a transcript along an insecure wire
Your task:	Tap the wire and, using the information in the experiment description, decrypt the message.
Hand in:	Submit, electronically, the plaintext of the message you intercepted

Experiment 3:

You work for a cosmetics company that specializes in hair tonic for balding men. You have received word from your corporate spy that a secret ingredient has been discovered by a competing hair tonic firm. You need to know the secret ingredient, but you don't want the company from which you are stealing the idea to know you are stealing it, and you don't want any of the other hair tonic companies to know the special ingredient. Your spy plans to send you the ingredient encrypted with the Caesar cypher used as a block cypher in ECB mode with a block size of one symbol and a modulus of 100 (Remember that each symbol is represented by two digits). The transcript on the left contains a series of blocks that make up the coded message from your spy. You can read from this transcript one block at a time. By putting the calculator in *Many* mode, receive and decrypt each symbol of the ingredient using a key of 23. Submit your answer using the hand-in transcript.



Name	Command	Mod
cyph	receive	

Figure 4: Experiment 1a

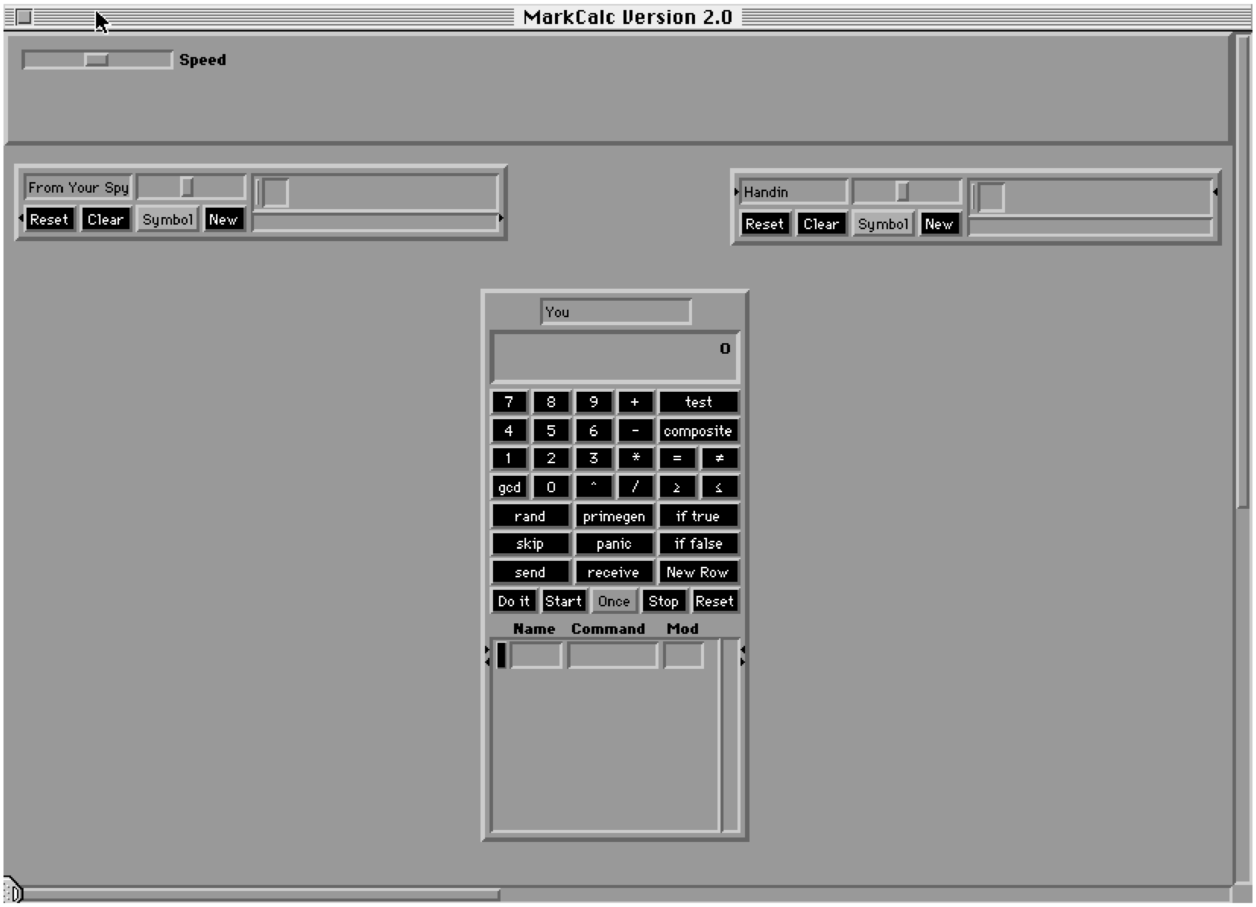


Figure 5: Experiment 1a

In Brief...	
We give you:	A transcript containing a message encrypted with Caesar's cypher as a block cypher
Your task:	Decrypt the message
Hand in:	Submit, electronically, the plaintext message

Experiment 4:

In this pair of experiments, you will make use of a new MarkCalc structure known as a *Substitution Box*. The substitution box acts as a sort of filter, translating symbols on input wires into different symbols sent on output wires based on the substitution table it contains. Wires can be connected going into and coming out of the substitution box. The table is set up as a two side-by-side columns, the left column containing input values to translate, and the right column containing the corresponding output values to translate to.

(a) You have discovered that one of your fellow CIA employees is a mole. You must get word out to the counterintelligence branch immediately, but without letting the enemy agent know that they have been discovered. Luckily, each agent has been provided with a special substitution key for such emergencies:

a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z
c	g	b	y	z	o	s	j	i	a	d	e	p	u	q	k	v	f	t	x	n	w	m	h	l	r

In this experiment, you will be given a transcript containing a message identifying the spy. You will need to set up the provided substitution box by filling in the substitution key and then use it to encrypt the message you are given and send it to the transcript labeled *Hand-in.*

In Brief...	
We give you:	A transcript containing a plaintext message, a substitution box, and a hand-in transcript.
Your task:	Encrypt the message by filling in the substitution box and connecting the transcripts to it.
Hand in:	Submit, electronically, the encrypted message

(b) Your crazy uncle Nelson is under the mistaken impression that Russian spies are reading his mail. In an effort to prevent them from learning his secrets, he has taken to encrypting his letters with a substitution cypher. Unfortunately, as his paranoia is in a rather advanced stage, he has refused to divulge the substitution table to anyone, even his family members. Naturally, this makes matters quite difficult for the intended recipients of his correspondence. Fortunately, you are in posession of some of his writings from saner times and, being the cryptography expert that you are, you know that this information can help you to make educated guesses about the code Uncle Nelson has used in his latest letter to you...

You will be provided with several transcripts in this experiment. The transcript labeled *Old Letter* contains an old letter from Nelson. The transcript labeled *New Letter* contains the most

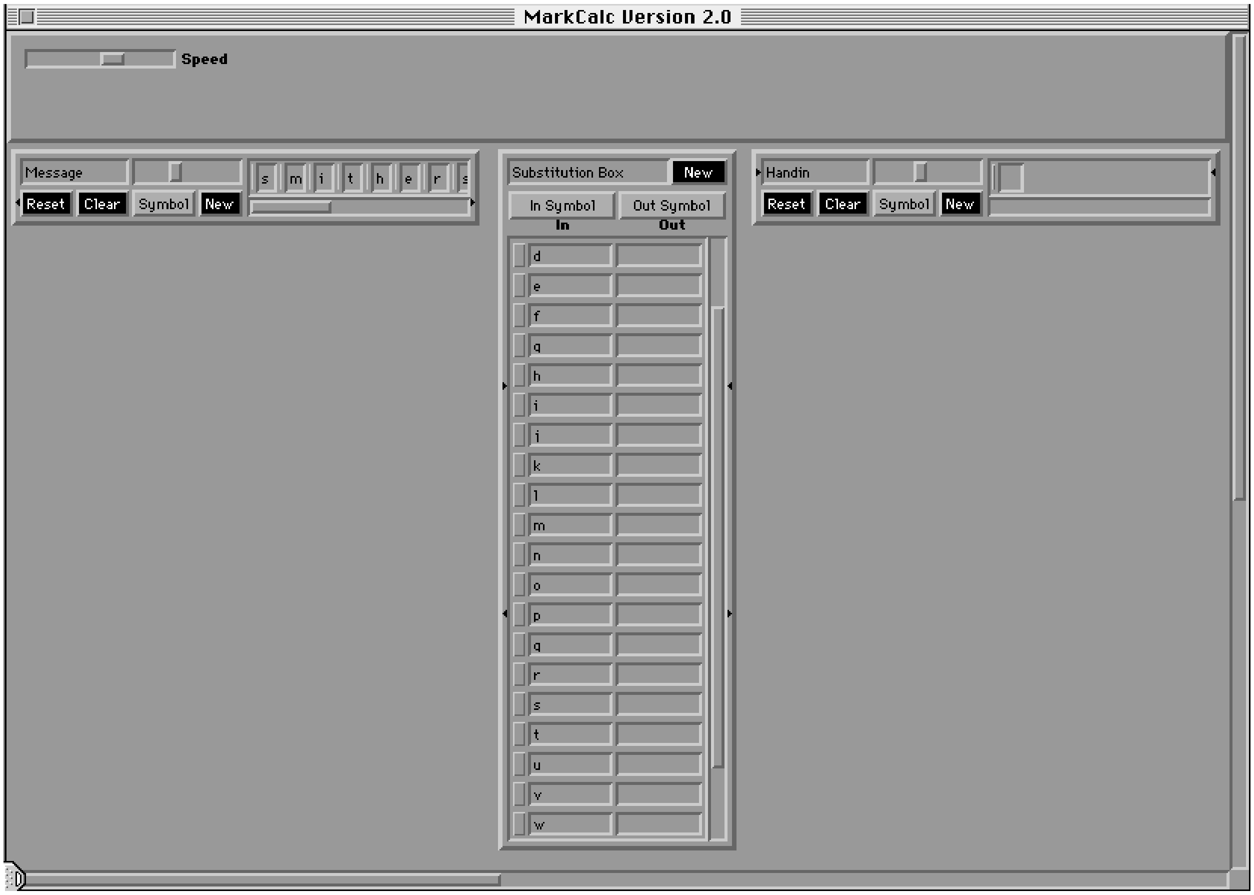


Figure 6: Experiment 1a

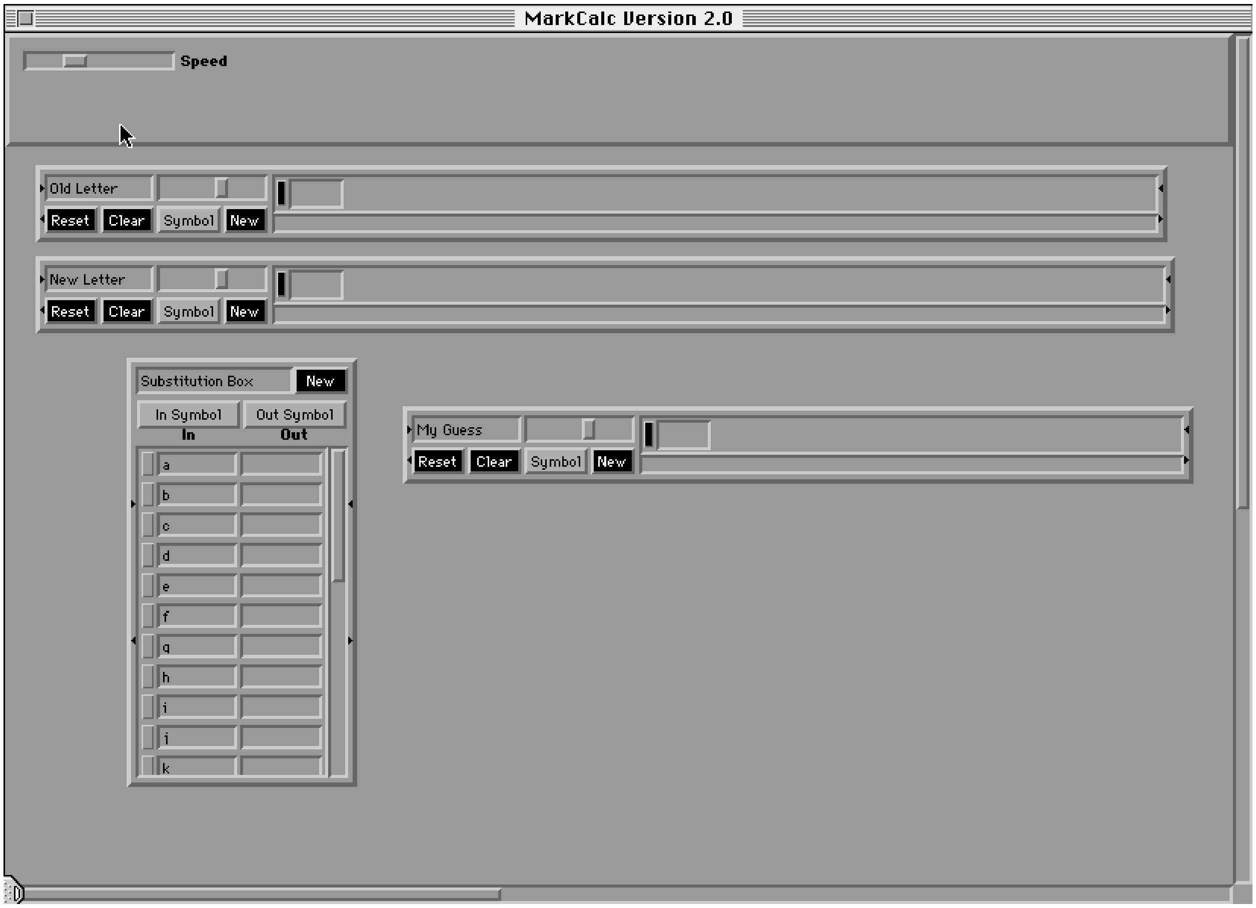


Figure 7: Experiment 1a

recent encrypted message. You will want to add a substitution box and draw wires so that each character is sent through it to a transcript. Using this setup, you can guess the substitution one symbol at a time. It may not be possible to guess the entire substitution, but you should be able to figure out enough to guess what the letter says. Using the Histogram feature of the MarkCalc (found under the Workspace menu), you can compare the distribution of letters in the *Old Letter* and the encrypted *New Letter*. You will notice that some letters predictably appear with a certain frequency. For instance, it is widely agreed that "e" is the most common letter in the English language. Based on this information, you can probably deduce that whatever letter appears most frequently in the cypertext has been substituted for "e".
Write your best answer on paper, and hand it in to the hand-in box in CIT242 .

CS007 **Fall 1997**

In Brief...	
We give you:	A transcript containing a writing sample in English, and a transcript containing a message encrypted with a substitution cypher for which you do not know the key.
Your task:	Use the Histogram feature and some trial-and-error to guess. as much of the message as possible.
Hand in:	Submit this guess on paper to the hand-in box in CIT242.