Lab #2

Out : September 11, 1997; 2:30 pm
Due : September 18, 1997; 12:30 pm

Experiment 1:

You work for the CIA. Until recently, you and your cohorts communicated using the Caesar cypher, but recently you were told by the NSA that, after conducting extensive research, they have found the Caesar cypher to be somewhat less secure than one might hope. They told you that the cutting edge in crypto research now points to a cypher that we saw in class known as the addition cypher. They claim that it is more secure because the block size is bigger than it was in the Caesar cypher, and therefore the keys are bigger so there are many more of them. You now need to use a calculator to decrypt a message being sent to you from the central office. The block size is 5 characters, which corresponds to 10 digits (remember, each character is represented by a two-digit number) so now instead of using a mod of 100, you want to use a mod of 10^{10} for your addition operations. You will find a calculator, a cell and two transcripts when you start up the experiment. A cell is simply a transcript with only one data box that repeatedly sends the same value when a calculator receives from it. This particular cell contains the key to be used in decrypting the message. One transcript is the message you want to decrypt and the other is a hand-in transcript. You can program the calculator. Decrypt the message and send it to the hand-in transcript, and if you think you have decrypted it correctly, submit the result.

In Brief...	
We give you:	A transcript with a message encrypted using the addition cypher and a cell containing the key to be used in decryption
Your task:	Decrypt the message (using a modulus of 10000000000)
Hand in:	Submit electronically once the hand-in transcript has received the plaintext.

Experiment 2:

The CIA is happy with its use of the addition cypher, *but* it has noticed that its employees are generally having a hard time remembering their key. They decide to implement a policy where each employee picks a four-letter English word to be her key. You see the flaw in this idea, and decide to decrypt a message sent to your immediate superior to demonstrate to the CIA that their new scheme is insecure.

In this experiment you will find a message encrypted using the addition cypher with a four-letter English word as the key. The message has been split into four blocks of four letters and each block of the message stored in a cell. Below the row of cells that contain the cyphertext message blocks, you will see annother row of cells labeled **Plaintext Blocks 1-4**. These cells are

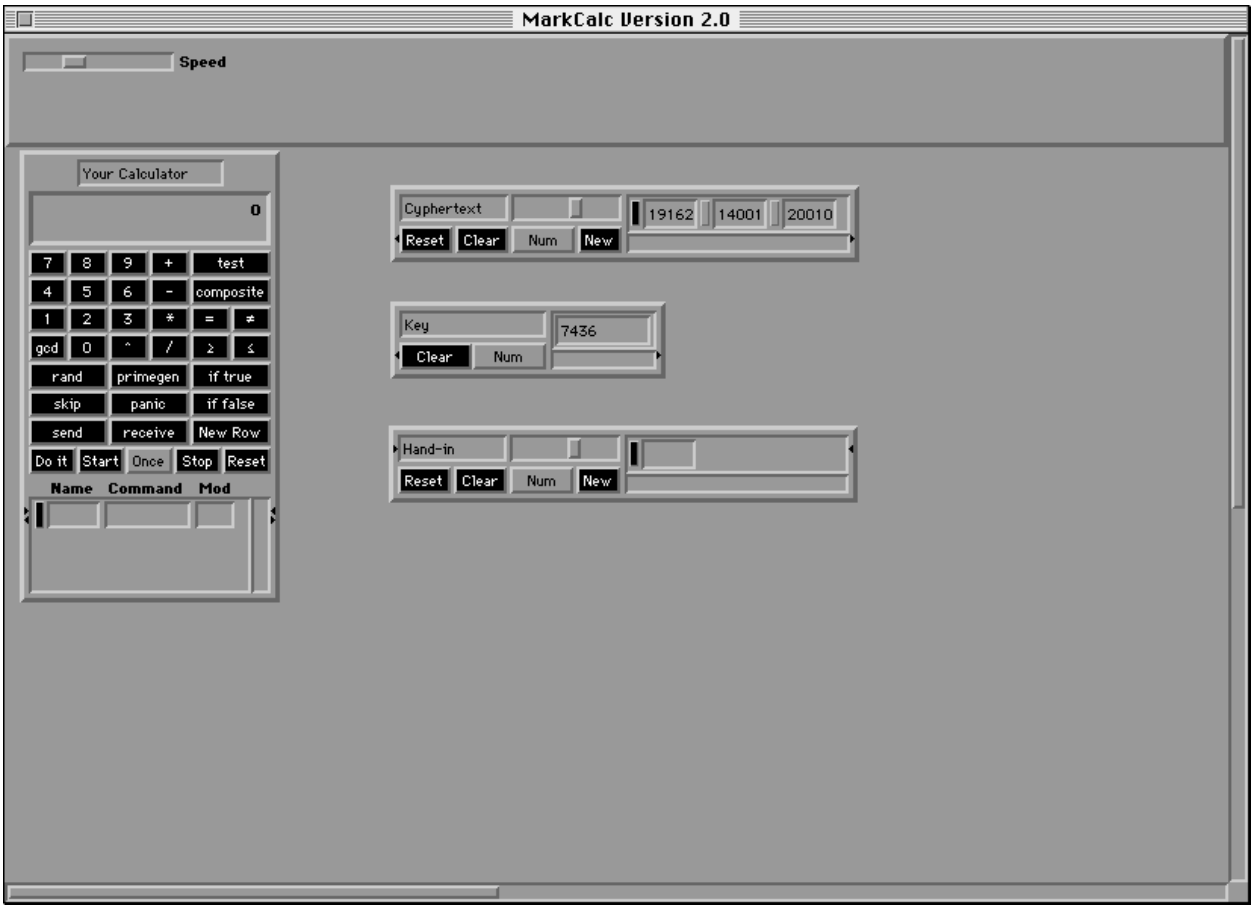

Figure 1: Experiment 1

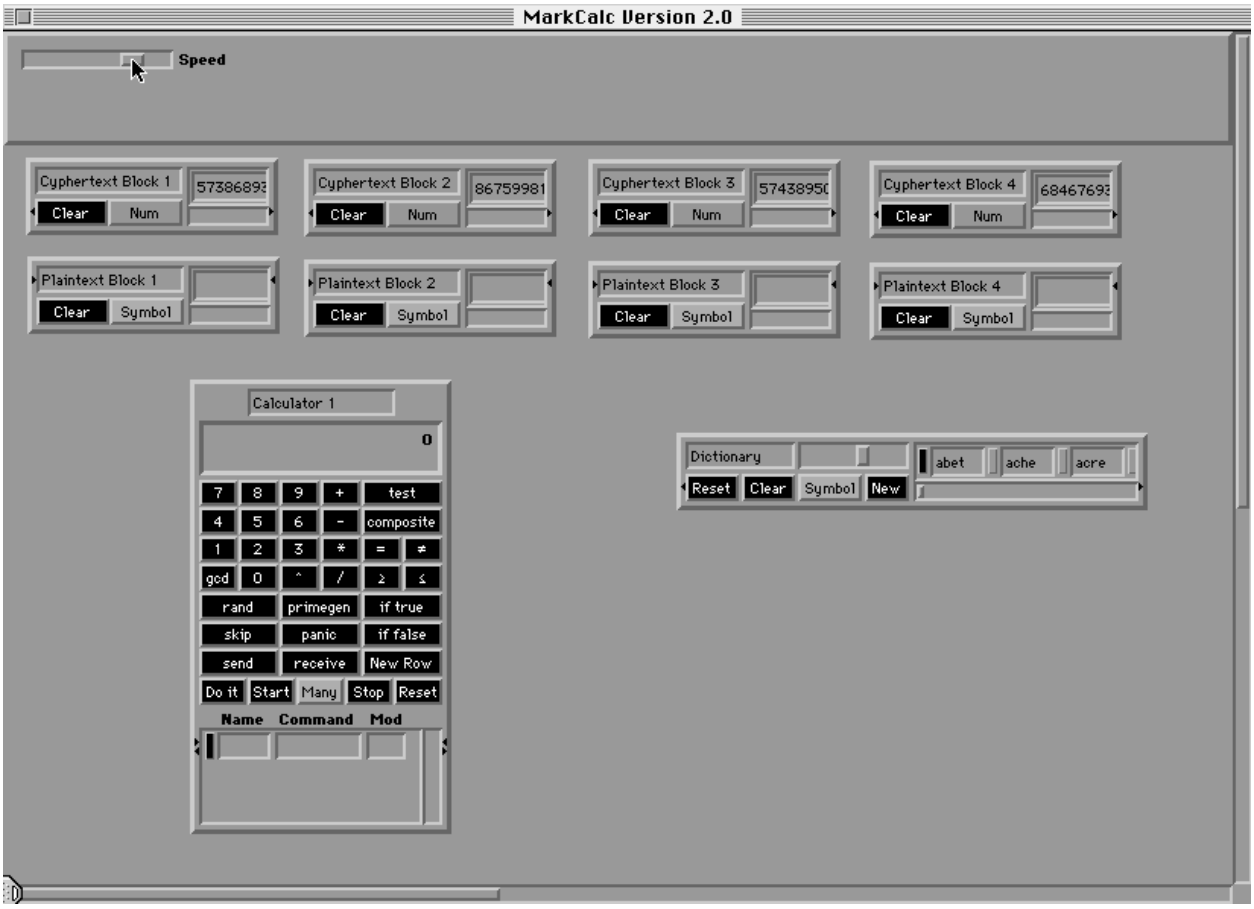

Figure 2: Experiment 2

where you will put the plaintext blocks as you decrypt the message. You are also provided with a dictionary of four-letter words. Armed with your dictionary, your job is to figure out the plaintext blocks and send them to the appropriate cells. Once you have decoded the message, an electronic submission will send the values in the cleartext cells to the TA's for grading. Remember that since the block size is four letters, or 8 digits, you need to use a modulus of 10^8. When you submit, your hand-in cells should each contain a block of the plaintext. Note: this experiment may take a little while to start up, due to the size of the dictionary that must be loaded. Similarly, once you are confident that you are doing the experiment correctly, you may wish to move the **speed** slider in the upper-left corner of the workspace further to the right in order to speed things up.

In Brief...	
We give you:	A series of cells containing the blocks of cyphertext and a transcript containing a dictionary
Your task:	Figure out the key and decrypt the message
Hand in:	Submit electronically once the plaintext is in the row of hand-in cells

Experiment 3:

(a) An IFF (Identification Friend or Foe) protocol is a method of determining if an unknown entity is a "friend" or a "foe" based on whether or not they can prove they know a shared key. In one use of IFF, an airplane sends annother airplane cyphertext and the other airplane proves it knows the key by sending back the corresponding plaintext. In the first part of this experiment, you will simply observe such an interaction, and try to figure out how the protocol can be broken (i.e., how to obtain the information necessary to prove that you are a legitimate plane when in fact you are not). You will need this information in the second part of this experiment.

When you open the experiment, you will two calculators that are set up to go through the protocol. There is also a cell from which the calculators receive the key that they use in the protocol. Since the pilots have agreed on the key in advance, we have used secure wires to connect the calculators to their key. Note that the wires connecting the two calculators are insecure. You know that the two airplanes use the addition cypher with a block size of 10 digits as their encryption scheme, but you do not know the key. If you wish to run through the experiment again, you can use the buttons at the top of the workspace labeled **Reset** and **Start**.

In Brief...	
We give you:	Two calculators set up to do IFF using the addition cypher
Your task:	Observe the interaction and try to learn enough to break the scheme
Hand in:	Nothing

(b) When you open this experiment, you will find two calculators. The one on the left is the calculator representing the airplane who will send you a challenge; the other is for you. Again this calculator receives its key from a cell, but the wire connecting the calculator to its key is secure. They want you to prove your identity by decrypting the message they send to you. You must receive the challenge from the other plane and, using the information you got from watching the interaction in part (a), validate yourself to the challenging plane by sending back your response. Remember that the block size is 10 digits, so you need to use a modulus of 10^{10}. If you do everything right, the other calculator will write "Authenticated" in the hand-in transcript. If not, the calculators will go into "Panic" state, to let you know that you didn't do it correctly. If this happens, you will have to restart the experiment. We have provided buttons at the top of the workspace to **Reset** and **Start** the experiment, just as in part 1. Once the calculator has written to the hand-in transcript,

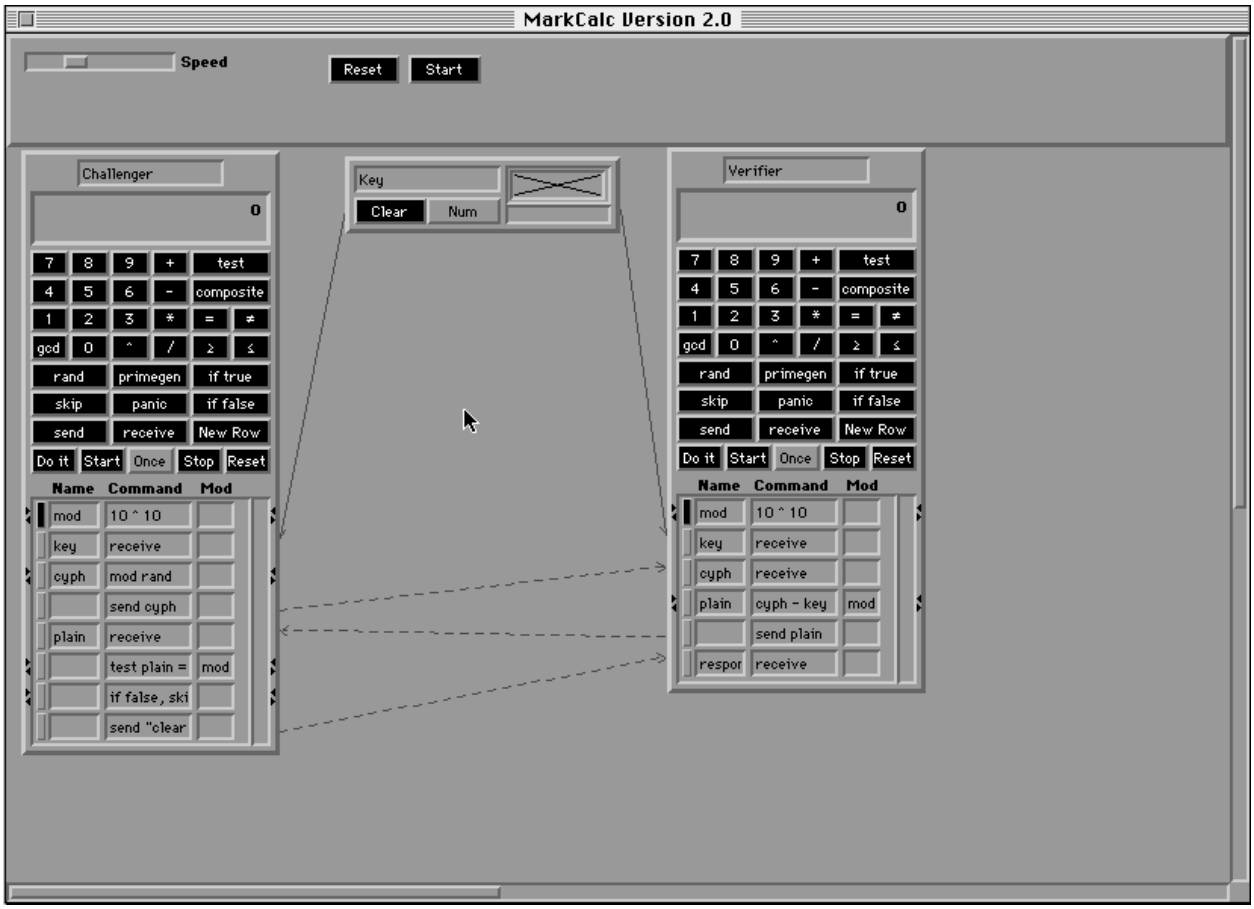

Figure 3: Experiment 3a

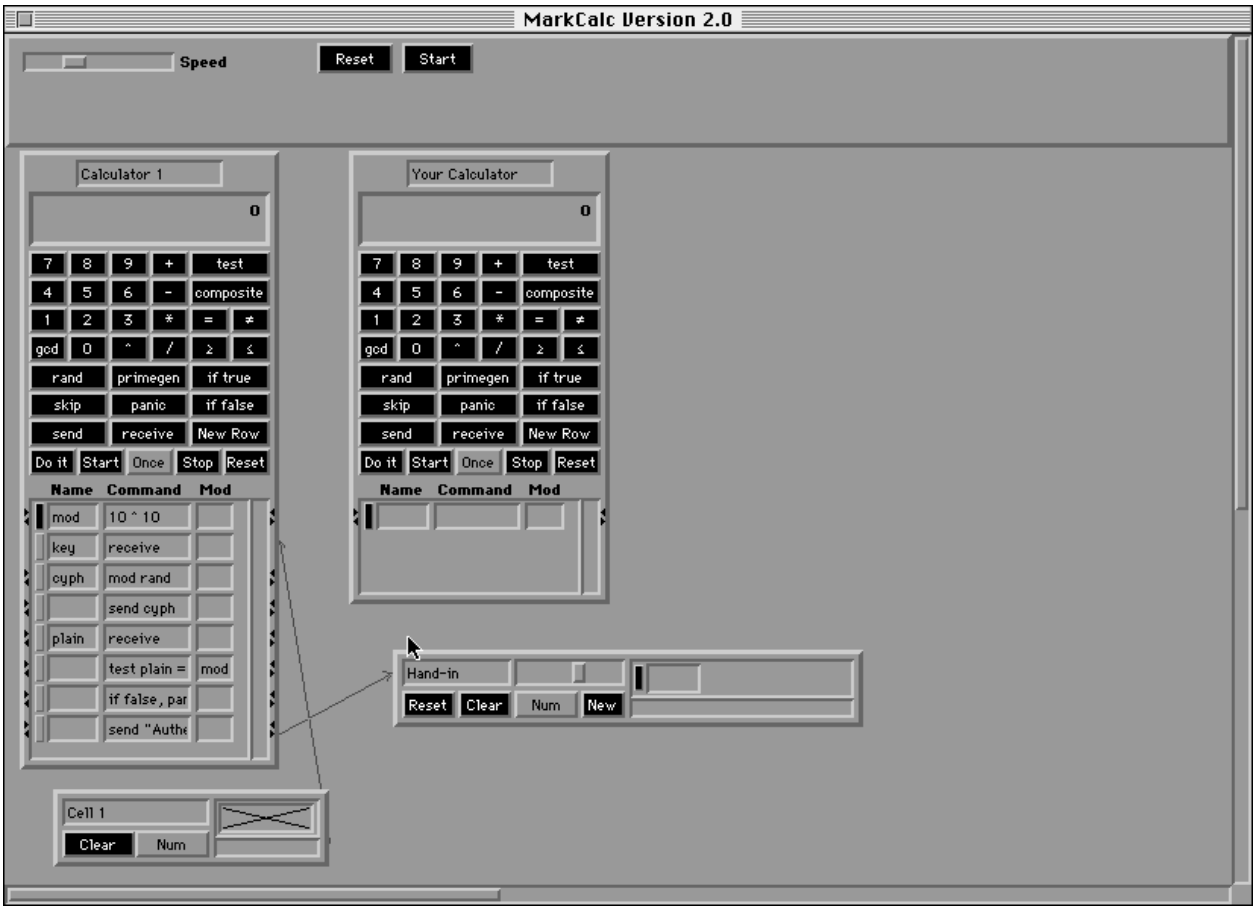

Figure 4: Experiment 3b

submit your results.

In Brief...	
We give you:	Two calculators: one set up to send a challenge to you, and annother calculator to represent you
Your task:	Authenticate yourself to the challenger using the information you got in part (a)
Hand in:	When the hand-in transcript has been filled by the challenging calculator, submit electronically

Experiment 4:

You and your cousin Bill are the sole remaining heirs of your great-aunt Mildred. Your cousin Bill has always been the favorite great-nephew, and you suspect that your great-aunt may let him in on

the location of her vast treasure. You have recently intercepted an encrypted message from Mildred to Bill, and you want to know the contents of the message just in case it includes the information you need to become independently wealthy. You know that the message was encrypted using the addition cypher with a block size of 10 digits (i.e., 5 character symbols), but you do not know the key.

(a) What information do you already know about the contents of the message? (You do not necessarily need to open up the experiment in the MarkCalc to answer this question).

In Brief...	
We give you:	A message encrypted using the addition cypher
Your task:	Make educated guesses about the possible content of the message
Hand in:	Write down your guesses on paper and hand them in

(b) Making some educated guesses about the content of the message, try out the keys that would give you the parts of the message that you think you might know, and see if this gives you something that makes sense in the other parts of the message. Using this method, piece together the plaintext that Aunt Mildred is sending to Bill. Since you don't have to have the entire key to get enough of the message to guess the rest, you can just write down what you think the plaintext is and hand it in on paper.

In Brief...	
We give you:	The same message you used in part (a)
Your task:	Use your guesses about the content to figure out the key and the whole message
Hand in:	Either electronically submit a transcript with the decrypted message *or* write the decrypted message on paper and hand it in

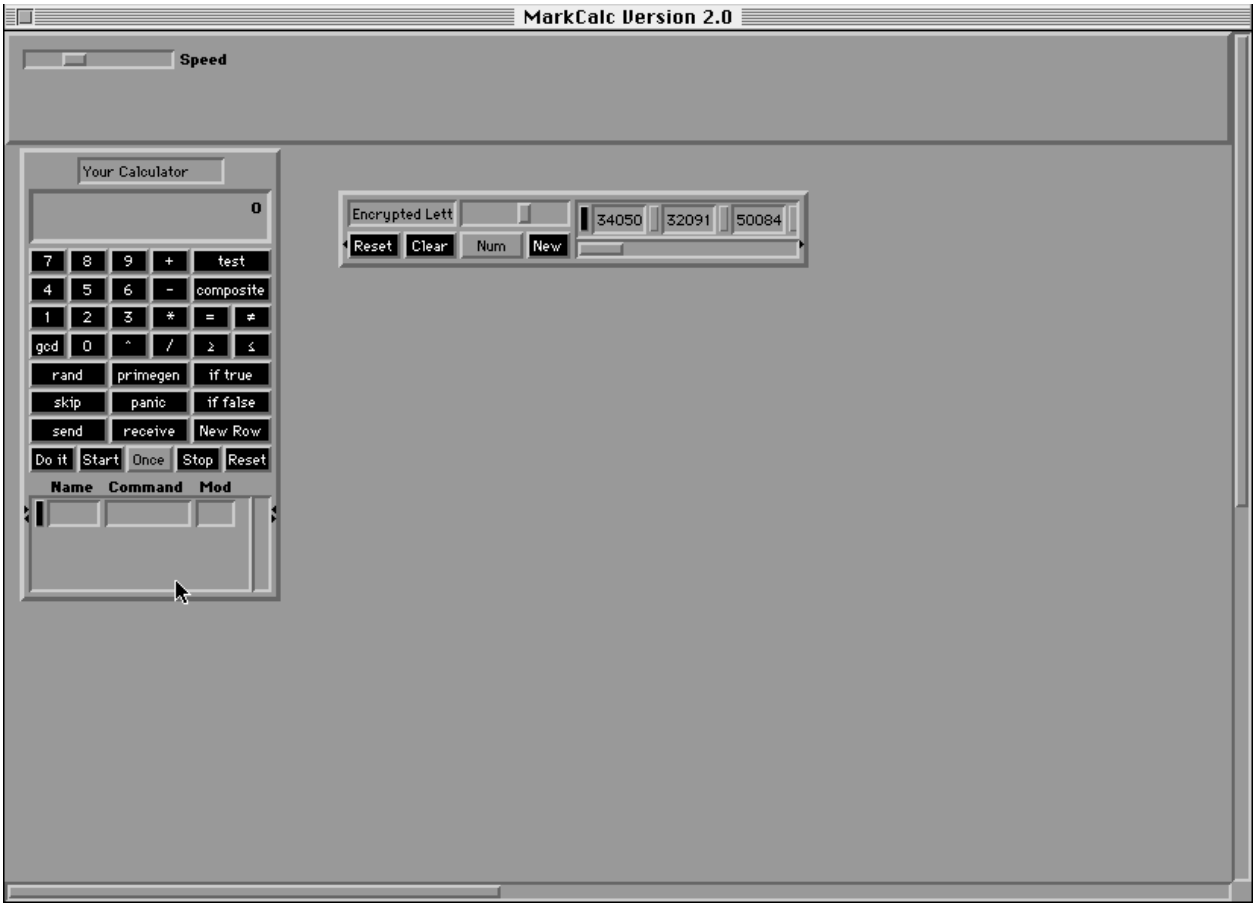

Figure 5: Experiment 4