Lab #6

Out : November 6, 1997; 2:30 pm
Due : November 13, 1997, 12:30 pm

Calculator Help: The MarkCalc can calculate modular multiplicative inverses. To calculate the multiplicative inverse of d, put "$1/d$" in the Command field and put the appropriate modulus in the Mod field.

Experiment 1:

The Pie of the Month Club uses the exponentiation cypher to encrypt each month's recipe so that those who are not in the club will not be able to learn the super-tasty secrets they have to offer. Being a fan of pie, you sign on. Each month a different pie recipe is sent out encrypted with the exponentiation cypher. The modulus the Pie Club uses is 477500508660178935571, which is prime. In this experiment you will receive just the name of the pie for this month.

When you open this experiment, you will see one calculator and three cells. One cell contains the cyphertext (a single block). One cell contains your key. The third cell is a hand-in transcript. You are also provided with a calculator. Receive the key and the cyphertext, and then decrypt the message. Send the plaintext to the hand-in transcript, and submit. Remember that in order to decrypt, you raise the cyphertext to the power of the mod $\phi(m)$ multiplicative inverse of the key.

In Brief...	
We give you:	A cell containing the key, a cell containing the block of cyphertext to decrypt, a handin cell, and a calculator for you
Your task:	Decrypt the cypertext
Hand in:	Submit electronically when the handin cell contains the plaintext

Experiment 2:

The Dog of the Month Club sees the success that the Pie of the Month Club had using the exponentiation cypher and decide to adopt their encryption scheme. They send out tips on breeding and care of various expensive breeds of dog. In this experiment, you will be receiving a message encrypted using ECB mode. For this problem the modulus is 88245335319593, a prime.

When you open this experiment, you will see a cell containing the key, a transcript containing the cyphertext, and a handin transcript. You are also provided with a calculator. You will decrypt the message and send it to the handin transcript. Submit electronically when you have successfully done so.

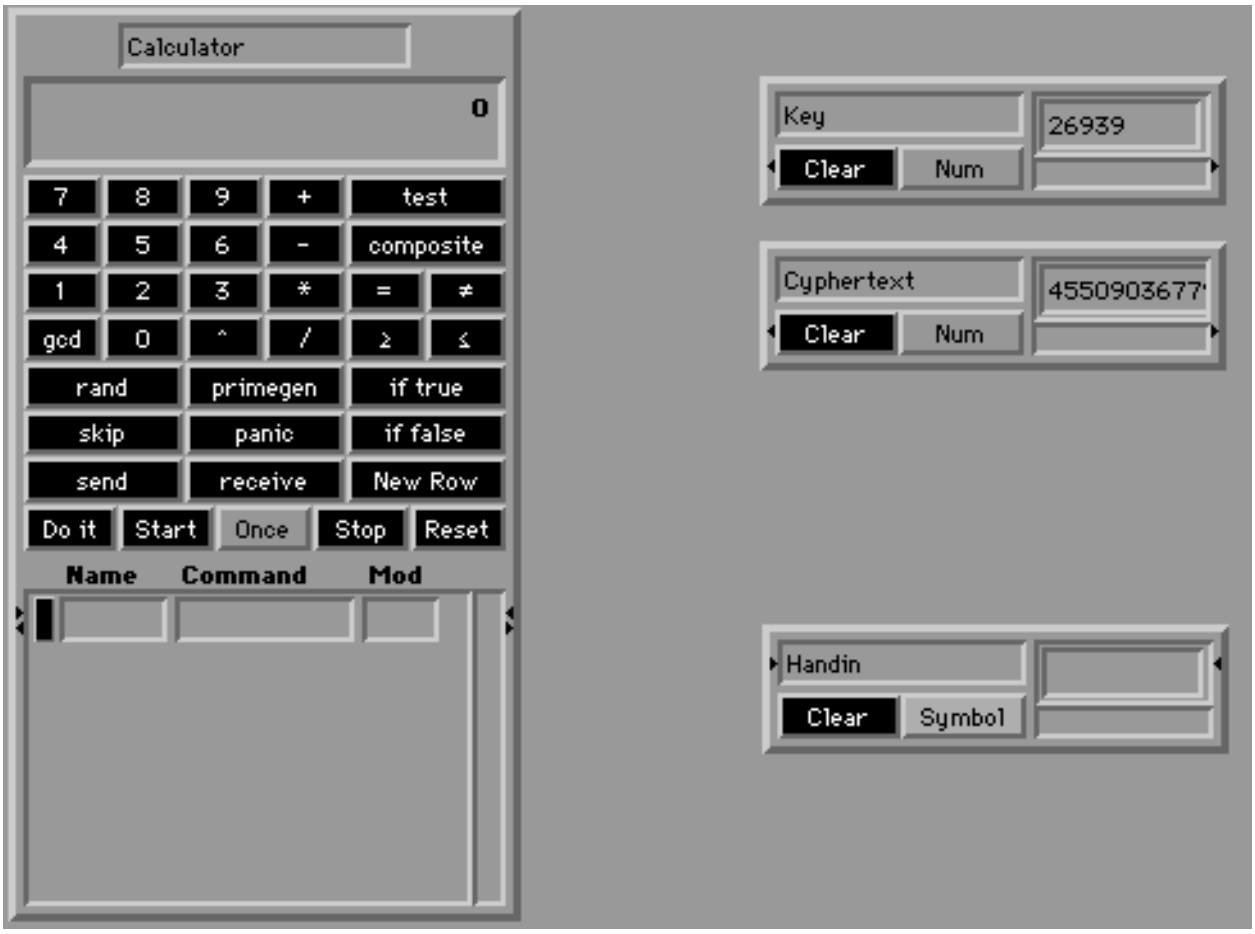

Figure 1: Experiment 1

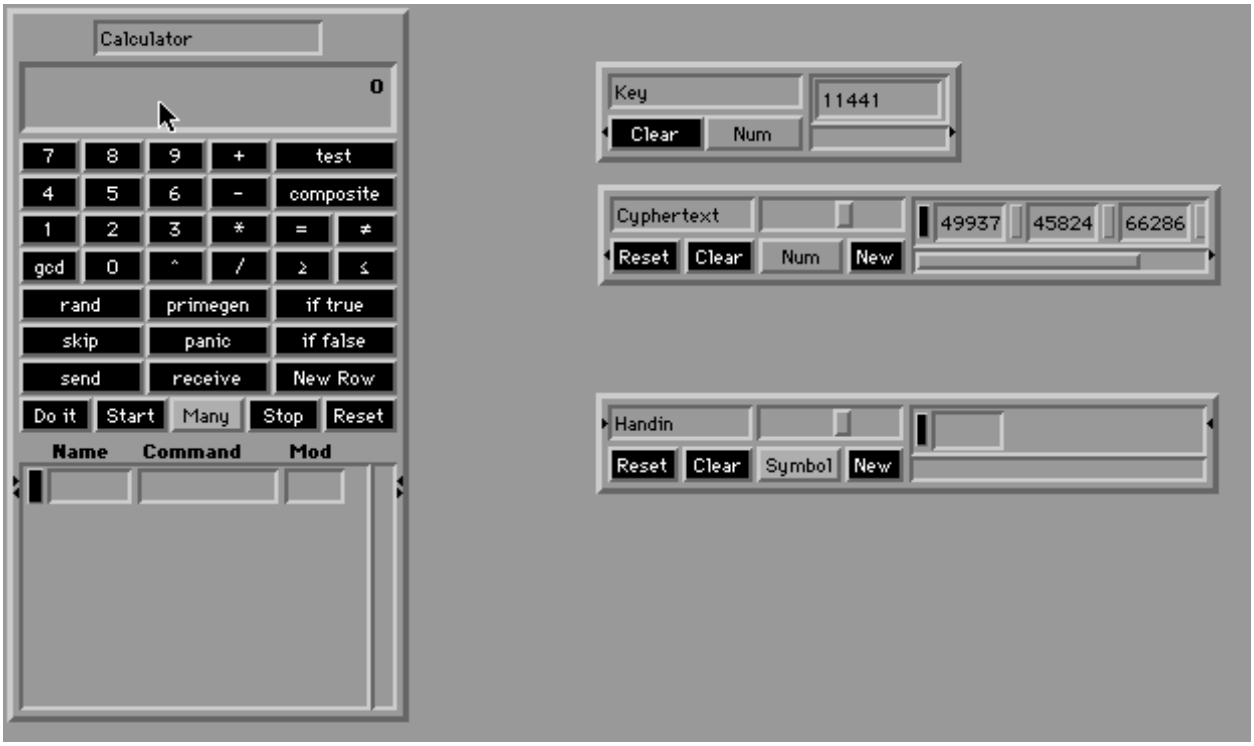

Figure 2: Experiment 2

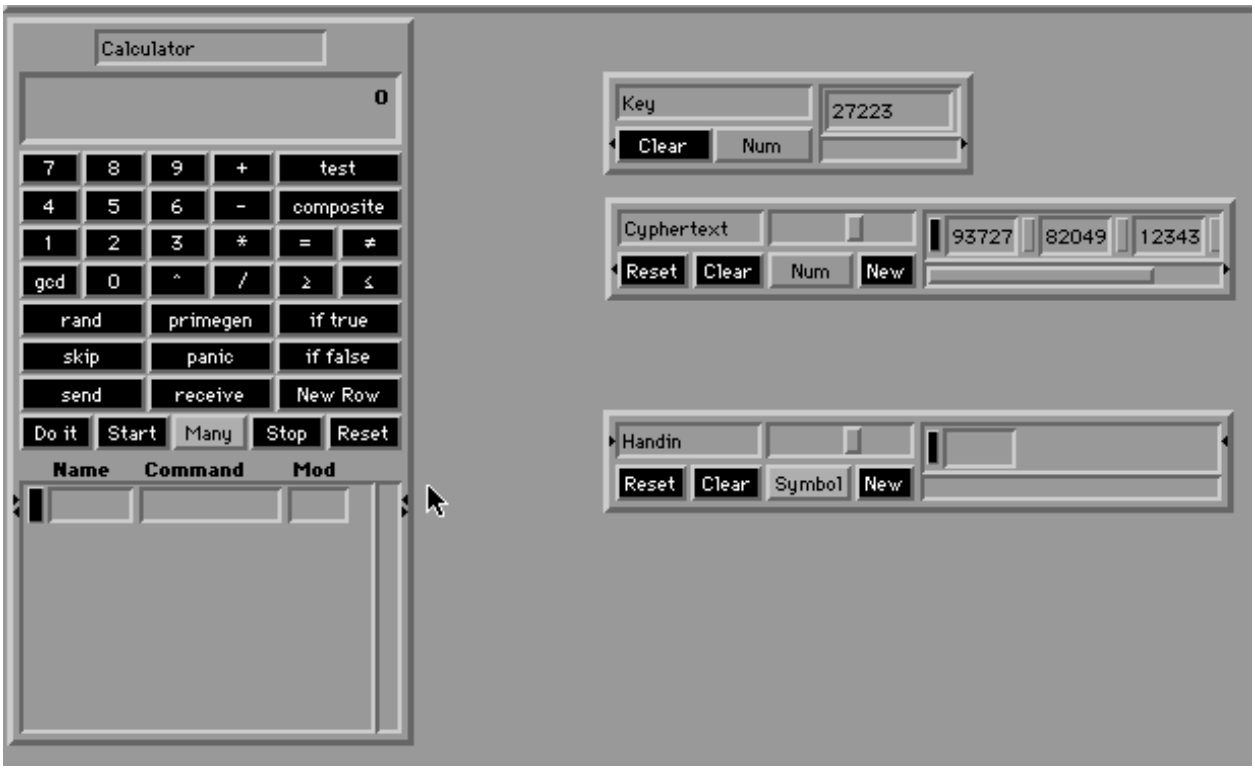

Figure 3: Experiment 3

In Brief...	
We give you:	A cell containing the key, a transcript containing the blocks of cyphertext, a handin transcript, and a calculator for you
Your task:	Decrypt the message (ECB mode)
Hand in:	Submit the plaintext electronically

Experiment 3:

The Gadget of the Month Club has also decided to begin using the exponentiation cypher to mail product announcements to their members. However, they have chosen to use cypher block chaining (CBC mode) with no I.V. and a modulus of 88245335319593, a prime.

When you open this experiment, you will see a cell containing the key, a transcript containing the cyphertext, and a handin transcript. You are also provided with a calculator. You will decrypt the message and send it to the handin transcript. Submit electronically when you have sucessfully done so. Remember that this message was encrypted using CBC mode.

In Brief...	
We give you:	A cell containing the key, a transcript containing the blocks of cyphertext, a handin transcript, and a calculator for you
Your task:	Decrypt the message (CBC mode with no I.V.)
Hand in:	Submit the plaintext electronically

Experiment 4:

In this experiment, you will assume the role of Alice and perform a series of tasks using Kerberos. Specifically, you will retrieve "email" from a calculator acting as the mail server and then send that email text to a calculator acting as the print server. In each of these exchanges, you will use Kerberos tickets to authenticate yourself to the servers and arrange for a session key with which the actual data (in this case, Alice's email) will be encrypted. Figure 4 illustrates this protocol.

The Kerberos server will be represented by a calculator. Tickets will consist of a series of 10-digit blocks, and encryption will be done using the exponentiation cypher in CBC mode with no I.V. To illustrate, a calculator Alice obtains a service ticket using the following procedure:

- Send your name ("Alice") to the Kerberos server.
- Send the name of the service you wish to use ("Email" or "Print").
- Receive four blocks encrypted with the expo cyper using your key in CBC mode. The first block will decrypt to yield the session key you will use for communicating with the service you wish to use. The remaining three blocks, once decrypted, are the service ticket.
- Send the three blocks that comprise the service ticket to the service you wish to use. If this procedure has been performed correctly, you will now be authenticated to that service and share a session key with it.

For this experiment, you will be given a set of calculators representing the Kerberos server, the Email server, and the Print server. The sequence of actions you will will need to perform is thus:

- Obtain a ticket for the mail server from the Kerberos server.
- Give that ticket to the mail server.
- Receive mail from the mail server encrypted with the session key.
- Decrypt the mail, which is a single block of text.
- Obtain a ticket for the print server from the Kerberos server.
- Give that ticket to the print server.
- Encrypt the mail you received earlier using the session key for use with the print server.
- Send the resulting cyphertext to the print server.

Figure 4: Alice interacting with a single server via Kerberos

When you have successfully accomplished this, the cell labeled *Printer Output* will contain, as plaintext, your email message.

In Brief...	
We give you:	A collection of calculators designed to emulate the Kerberos server, an email server, and a print server
Your task:	Perform the transactions necessary to retrieve Alice's email and send it to the printer
Hand in:	Submit once the *Printer output* cell contains the email plaintext