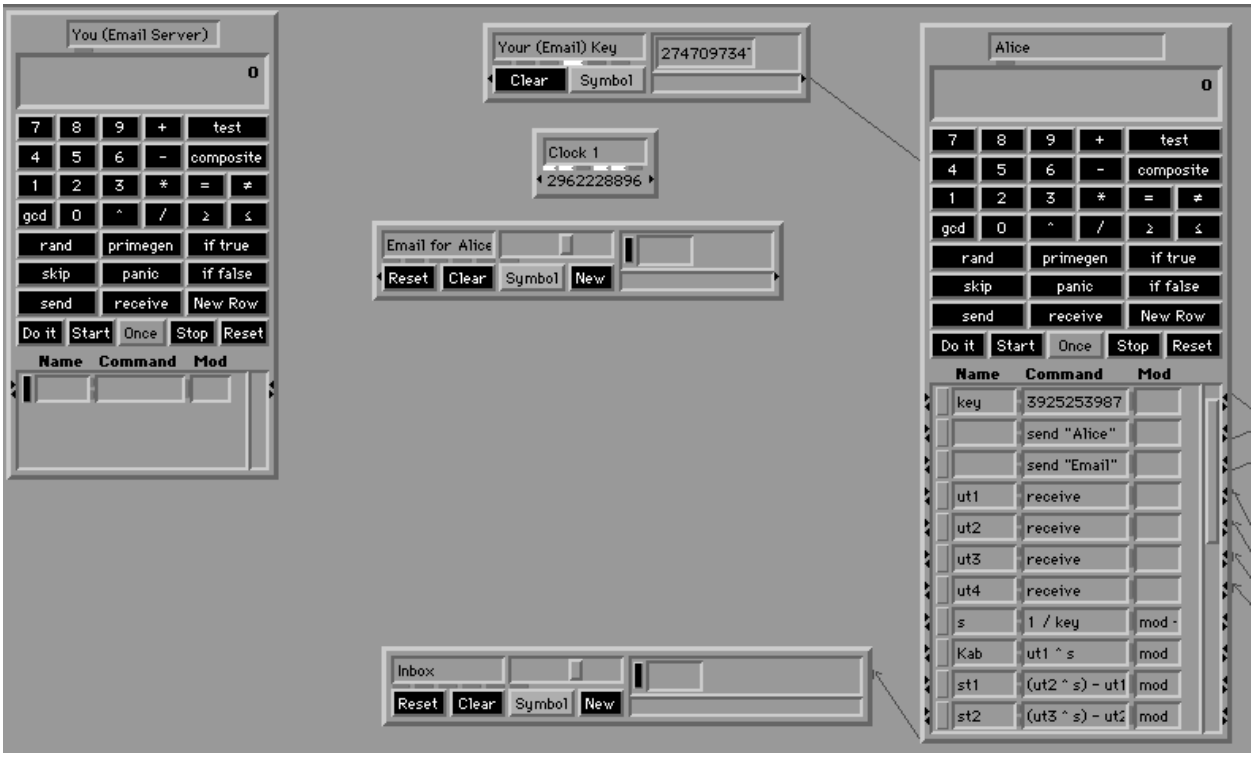

Figure 1: Experiment 1

Lab #7

Out : November 13, 1997; 2:30 pm
Due : November 20, 1997, 12:30 pm

Experiment 1:

In this experiment, you will act as an email server using Kerberos. You will be provided with a cell containing your key (known only to you and the Kerberos server), as well as a substitution box containing the "email" of various users. Your job is to receive a service ticket from another calculator and send them their email, encrypted using the session key. The service ticket is structured in the following manner, where K_b is the secret key of the service and K_{ab} is the session key:

$$\{K_{ab}, username, \text{time to expire}\}_{K_b}$$

In Brief...	
We give you:	A calculator for you, a substitution box containing users' "email", a cell containing your key, a hand-in cell
Your task:	Receive service ticket from user's calculator. Retrieve their email and send it to them, encrypted with the session key
Hand in:	Submit electronically when the user calculator has written your transmission to the hand-in (Inbox) cell

Experiment 2:

Recall from class how the Diffie-Helman key exchange protocol works. In this experiment, you will play the role of an active participant in this protocol. Your task will be to use Diffie-Helman to arrive at a shared key with a calculator Alice, and then use that key to decrypt a message she will send you encrypted using that key. The modulus for the modular exponentiation is 357565200525739. Then Alice will encrypt a message using the addition cypher with the same modulus. That is, the encryption function is

$$f(clear, key) = clear + key \pmod{357565200525739}$$

The key she will use is the key that the two of you have agreed upon. She will then send you the message.

Your job is to program your calculator to carry out Diffie-Helman's exponential key agreement protocol with Alice, calculate the shared key, receive Alice's cyphertext, decrypt it, and send the plaintext to your hand-in transcript. The plaintext will be an English word. Once your hand-in cell contains the plaintext, you should electronically submit.

In Brief...	
We give you:	Calculator Alice, a calculator for you, a cell from which Alice reads her message, and a hand-in cell
Your task:	Perform your part of the Diffie-Helman key exchange protocol, and receive and decrypt a message sent to you by Alice
Hand in:	Submit electronically when you have placed the plaintext message in the hand-in cell

Experiment 3:

In this experiment, Alice and Bob need to arrange to meet to discuss their secret plans for the overthrow of the government. They plan to meet on one of the floors of the CIT. Alice must send the number of the floor (0 for the basement, 1 for the first floor, ..., 6 for the mysterious sixth floor) where the meeting is to take place.

To keep the message secure, Alice and Bob will first carry out the exponential key agreement protocol with a modulus of 7. Alice will then use the key obtained to encrypt the number of the floor where they will meet. The encryption method is mod 7 addition. Finally, Alice will send the cyphertext to Bob.

You are Eve, and you work for the FBI, so naturally, you wish to foil their plans by showing up at their little meeting with some handcuffs. Your job is to eavesdrop on the key exchange, determine

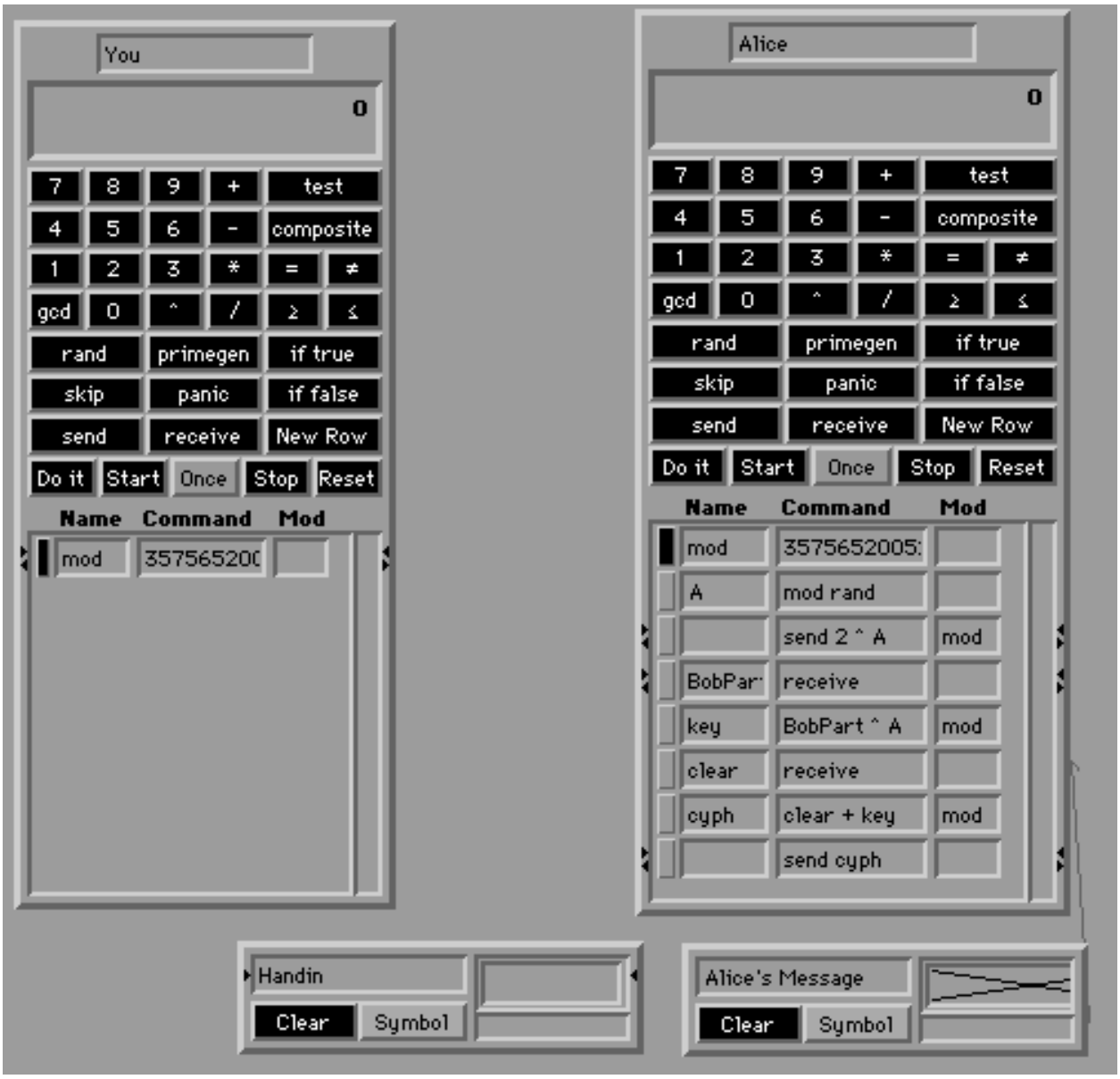

Figure 2: Experiment 2

what key they are using, and use the key to decrypt the cyphertext, obtaining the floor number. Don't interfere with the messages they send each other. However, you are allowed to add wiretaps in order to eavesdrop.

Hint: the numbers are small enough that you should be able to compute the mod7log by hand.

> **Note:** *When receiving from a wiretap, you will successfully manage to eavesdrop on transmissions only if your calculator is attempting to receive from the tap at the time the message is sent along the tapped wire. Since Alice and Bob send messages to each other at roughly the same time, you will not be able to use a MarkCalc brand wiretap alone to do this. To insure that you capture each message, use the following procedure for wiretapping: Tap the wire you wish to listen on, and route it into a cell. Then connect a wire from that cell to the line where you* receive *the message. Using this procedure, a cell will hold onto the message until you are ready to receive it.*

In Brief...	
We give you:	Calculators Alice and Bob, a calculator for you, a cell from which Alice reads the message to send, and a hand-in transcript
Your task:	Eavesdrop on the transmissions and decode the message Alice sends to Bob
Hand in:	Submit when the hand-in cell contains the plaintext message

Experiment 4:

In this experiment, strategic allies Alice and Bob wish to plan their next summit meeting. You (Eve) are a CIA agent charged with determining the location in advance. Alice and Bob plan to use Diffie-Helman's exponential key exchange protocol to establish a key; then Alice will encrypt and send to Bob the name of the city in which they will meet. The modulus used in all modular arithmetic for this problem is 357565200525739. As in Experiment 2, the encryption method is the addition cypher with this number as modulus.

Your job is to find out the plaintext of Alice's message. However, you must also make sure that Bob decrypts his message to correctly obtain the location. (Alice and Bob would immediately suspect the CIA in the event of an error). Once you know the plaintext of Alice's message, send it to the Hand-in cell. Bob, once he decrypts the cyphertext that he receives, will send the plaintext to his cell.

Hint 1: in this experiment you will have to actively interfere with the messages going across by disconnecting and reconnecting new wires (arrows). Hint 2: in this experiment Alice and Bob have no way of knowing precisely who they are communicating with.

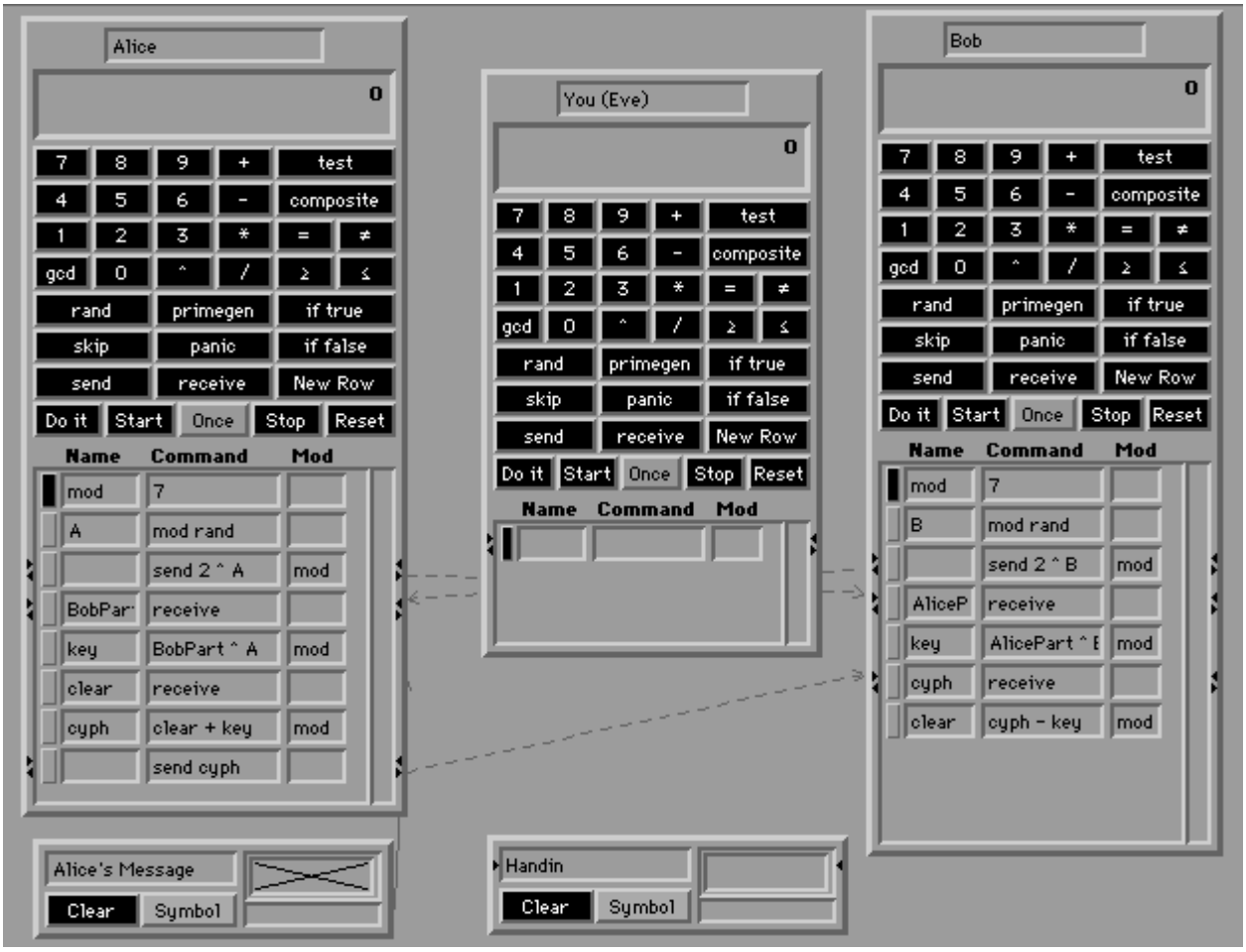

Figure 3: Experiment 3

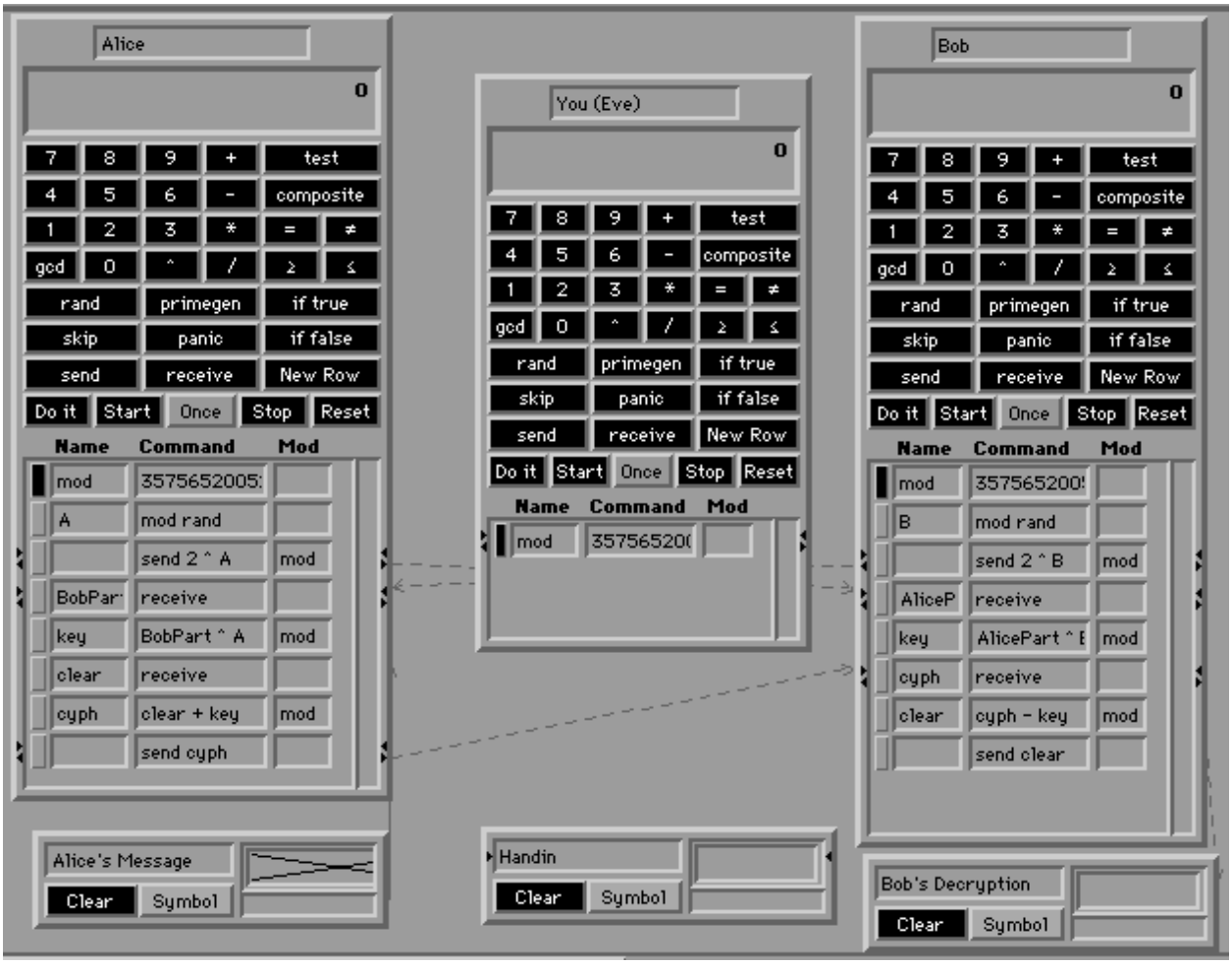

Figure 4: Experiment 4

In Brief...	
We give you:	Calculators Alice and Bob, a cell from which Alice reads her message, a cell to which Bob writes what he receives, a calculator for you, and a hand-in cell
Your task:	Intercept communication between Alice and Bob such that you can decode the message Alice sends to Bob while making sure that Bob decrypts the message he receives to obtain the proper location
Hand in:	Submit electronically when your hand-in cell contains the true location and Bob has decrypted the message sent to him

Experiment 5:

In this experiment, international terrorists Alice and Bob wish to plan their next meeting. You (Eve) are the chief Interpol agent in the Munich branch. Alice and Bob plan to use exponential key exchange to establish a key; then Alice will encrypt and send to Bob the name of the city in which they will next meet. The modulus used in all modular arithmetic for this problem is 357565200525739. As in Experiment 2, the encryption method is the addition cypher with this number as modulus.

You figure that this is your big chance to interfere. Your job is to find out the plaintext of Alice's message, and send Bob a cyphertext that he will decrypt as "Munich". This way, you can have the proper authorities deal with Alice, and lure Bob into your clutches as well. Once you know Alice's plaintext, send it to the Hand-in cell. Bob, once he decrypts the cyphertext that he receives, will send the plaintext to his cell. Be sure that it reads "Munich".

Hint 1: in this experiment you will have to actively interfere with the messages going across by disconnecting and reconnecting new wires (arrows). Hint 2: in this experiment Alice and Bob have no way of knowing precisely who they are communicating with.

In Brief...	
We give you:	Calculators Alice and Bob, a cell from which Alice reads her message, a cell to which Bob writes what he receives, a calculator for you, and a hand-in cell
Your task:	Intercept communication between Alice and Bob such that you can decode the message Alice sends to Bob as well as substitute your own message for Bob to decode
Hand in:	Submit electronically when your hand-in cell contains the true location and Bob's cell says "Munich"

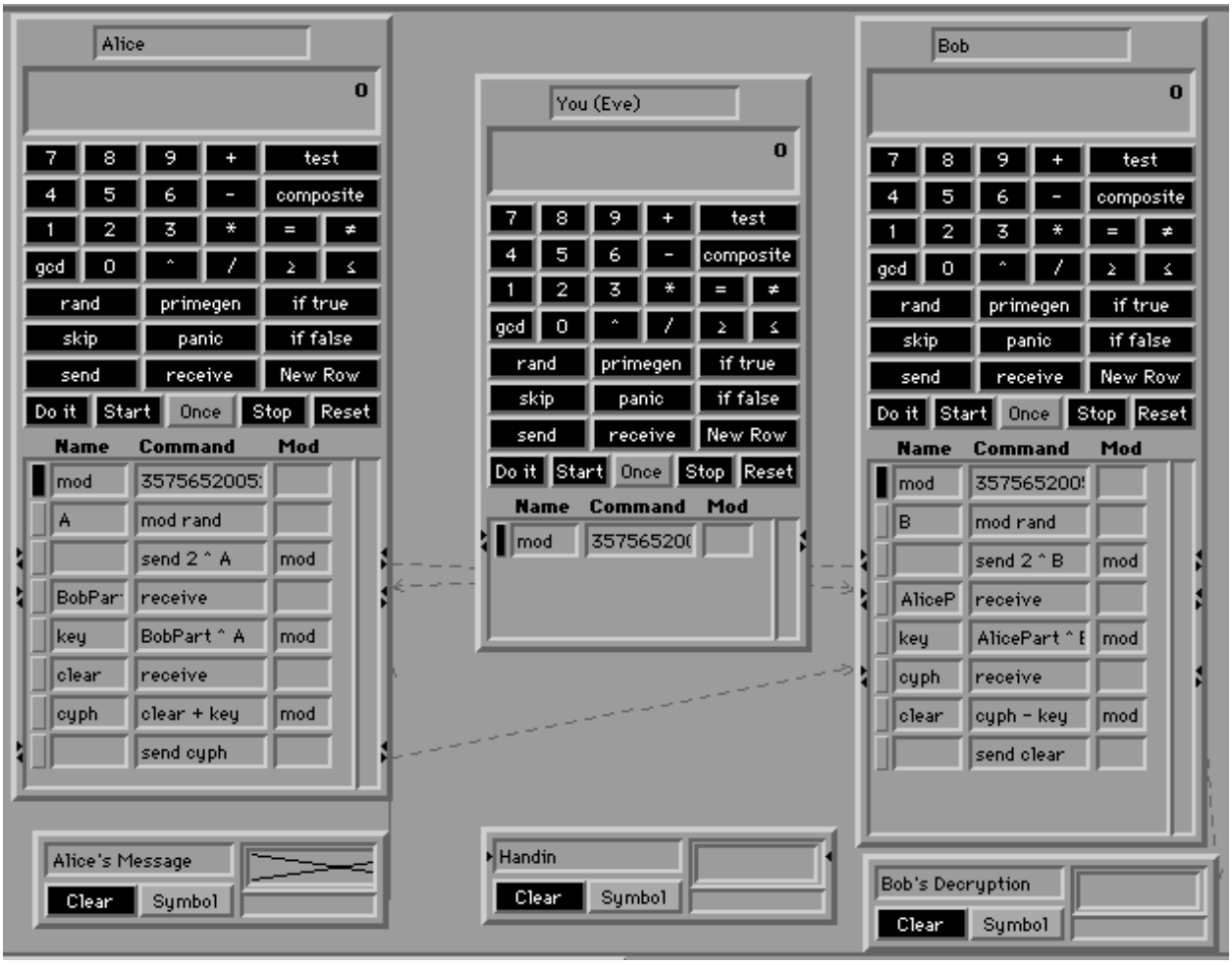

Figure 5: Experiment 4