Lab #9

Out : December 4, 1997; 2:30 pm
Due : December 11, 1997, 12:30 pm

Experiment 1:

The computer science department is losing money because students refuse to pay their copy fees. A new policy is implemented, requiring the students to submit a signed IOU when they register for the class. You are hired by the CS department to check these signatures, and issue a signed receipt to the student acknowledging their IOU.

(a) In this part, you will verify a signed IOU and signature from a student. The IOU is a single block, as is the signature. You will be provided with two cells containing the document and the signature. Additionally, there will be a cell containing the student's public key. You must determine whether or not the document matches the signature. If it was forged, send "forged" to the hand-in cell, otherwise send "OK". When you have sent your response to the hand-in cell, submit your results electronically.

In Brief...	
We give you:	A cell containing a document, a cell containing the signature, and a cell containing the public key of the signer. Additionally, there is a calculator for you and a hand-in cell
Your task:	Verify the signature on the document
Hand in:	Write whether or not the signature was forged to the hand-in cell and submit electronically

(b) Next your job is to send a signed receipt to a student. You will be given a cell containing the plaintext to send, as well as cells containing the department's public key(modulus) m and its two factors, p and q. Receive the plaintext for the receipt from the cell and sign it using the department's private key. Send the document-signature pair to the calculator labeled *student*. The student calculator will write "OK" to the hand-in cell when the receipt has been verified. When "OK" has been written to the handin cell, submit electronically.

In Brief...	
We give you:	A calculator representing a student, cells containing the department's public key(modulus) and it's factors, a cell containing the message to sign, and a hand-in cell
Your task:	Send the message and signature to the calculator labeled *student*
Hand in:	Submit electronically when the hand-in cell displays "OK"

Experiment 2:

The Plain-Brown-Wrapper Mail-Order Company sells everything from toothpicks to used fingernail brushes. They use RSA signatures to verify that each order is coming from a specific client. You know

that your roommate Pat continually purchases items from this company. You have intercepted a number of messages in which your roommate requested various items from another mail-order company. You want to use two of those messages to create another message requesting an item that your roommate Pat didn't actually order. The legitimate messages are signed by Pat using RSA; however, they are signed on a block-by-block basis rather than all together. That is, each message consists of a sequence of blocks, and the signature for the message consists of a signature for each block.

When you open this experiment, you will find two pairs of transcripts: one transcript in each pair contains the blocks of the message and the other contains the blocks of the signature. There is another transcript that contains the plaintext for the mischievous message you are supposed to send. You should send each block of this message, followed by a valid signature for that block to the "Store" calculator. It will check the validity of the signature, and if it believes that the message was sent by your roommate, it will send the order to a transcript. Once your message has been sent to the hand-in transcript, submit your results.

In Brief...	
We give you:	Four transcripts containing two document-signature pairs, two hand-in transcripts, and a calculator for you
Your task:	Create a forged document. For each block of your forged message, send the plaintext to the transcript labeled "Handin Message", and the corresponding signature block to the transcript labeled "Handin Signature"
Hand in:	Submit electronically when you have forged a document and signature

Experiment 3:

Ever since they got ahold of their first copy of the MarkCalc, the KGB has been using it to compute RSA signatures for diplomatic documents of the utmost gravity. Unfortunately, the new and improved (and hopefully faster) version of the MarkCalc has not made its way back to Moscow yet and the Russian cryptographers have quickly grown tired of waiting while the MarkCalc signs long documents. Instead, they run a hash function on the documents and sign the output. The hash function used takes three blocks as inputs, and outputs a single block. The function is: $f(x, y, z) = 2^x 3^y 5^z \pmod{1)0^{10}}$.

In this experiment, you must send a signed, 3-block message to the Russian Prime Minister. The message to be sent is provided to you in a transcript. There will also be cells containing your public key(modulus) and its two factors p and q. You must first compute the hash of the message, and then sign that block. You will then send the signature to the calculator labeled *Russian PM*. When the signature has been verified, the words "Valid Signature" will appear in the hand-in cell. If the signature is invalid, the words "Invalid Signature" will appear instead. Submit electronically once the message has been received and your signature verified.

In Brief...	
We give you:	A calculator representing the Russian Prime Minister, a transcript containing a message to send, cells containing your public key(modulus) and its factors, a calculator for you, and a hand-in transcript
Your task:	Compute the hash of the message, and compute the signature of that value. Send the message and the signature to the Prime Minister.
Hand in:	Submit when the Prime Minister's calculator has written "Valid Signature" to the hand-in transcript

Experiment 4:

In this experiment you will demonstrate your understanding of blinded signatures. Due to the rampant forgery of student ID numbers, the University has instituted a signature scheme. Under the new policy, student ID numbers will not be considered valid unless they are accompanied by a signature from a signing authority, in this case the Office of Student Life. Unfortunately, your scathing public criticisms of O.S.L. affairs have made you somewhat reluctant to reveal your ID number to them. Instead, you will have the signing authority *blindly* sign your ID number. After you have obtained a signature for you ID number, you will send it to a verifying agent.

When you open up the experiment, you will find a cell containing your ID number. You must have the calculator labeled *Signing Authority* blindly sign this number, and then send your signed ID number to the calculator labeled *Verifier*. When this second calculator writes "Valid Signature" to the hand-in cell, submit electronically. Remember that you are not supposed to send your ID number because you want to keep that number secret. (For this reason, the Authority is programmed not to sign your ID number.) You must find another way to obtain the Authority's signature for your ID number.

In Brief...	
We give you:	A cell containing a secret number, a calculator representing the signing authority, a verifying calculator, a calculator for you, and a hand-in cell
Your task:	Have the signing authority sign your secret blindly (it will check to make sure that you do not ask it to sign the secret as plaintext) and then send your signed ID number to the verifying calculator
Hand in:	When the verifying calculator has pronounced the signature on your ID valid by sending "Valid Signature" to the hand-in cell, submit electronically