Lab #8

Out : November 25, 1997; 2:30 pm
Due : Dec 4, 1997, 12:30 pm

Experiment 1:

You have recently come to appreciate the aesthetic beauty of lava lamps, and want to purchase one. You've found a great store in California that allows you to purchase lava lamps over the Internet. Being the educated consumer that you are, you don't want to send your credit card number over the internet in the clear. Luckily the store provides a public key; you can encrypt your credit card number using El Gamal's public-key cryptosystem and send the encrypted credit card number to the store. After they receive your order, they will send an encrypted confirmation message to you, using your public key. The store uses El Gamal's system with a base of two. The system-wide modulus is 357565200525739.

In the first part of this experiment, you will be sending your credit card number to the store, encrypted using the store's public key. In the second part, the store will send you an acknowledgement encrypted with your public key.

(a) Addition cypher Your first job is to send your encrypted credit card number to the store. When you open this experiment, you will see a cell containing your "credit card number" and a cell containing the public key of the store. You are to use El Gamal encryption, so you must calculate and send a part so that the store can determine the session key. You should also determine the session key and use it to encrypt your credit card number using the addition cypher. Send your part and the cyphertext to the store. If your order was received properly, "Order Received" will appear in the handin transcript.

In Brief...	
We give you:	A cell containing the plaintext (credit card number), a cell containing the store's public key, a calculator for you, a calculator for the store (and the attached handin transcript)
Your task:	Use El Gamal's scheme to arrive at the session key. Encrypt your credit card number, and send it to the store.
Hand in:	Submit electronically when the store writes "Order Accepted" to the handin transcript

(b) You are now going to receive confirmation of your order. Using your public key, the store will calculate a session key, and send you their part. Using the session key, they will encrypt a message to you using the addition cypher with a block size of 5 symbols (10 digits) and a modulus of 10^10.

When you open this experiment, you will be given your private key in a cell. The session part will be made available to you in annother cell. There will also be a transcript labeled "Cyphertext", which contains the encrypted confirmation message. You must first receive the session part and use it to calculate the session key. Next, receive the blocks of cyphertext and decrypt the message. Send the plaintext to the handin transcript and submit your results.

In Brief...	
We give you:	A calculator for you, a cell containing your private key, a cell containing the store's session part, a transcript containing the message, and a handin transcript
Your task:	Receive the session part and calculate the session key. Use that key to decrypt the confirmation message for your order
Hand in:	Submit electronically once you have sent the plaintext to the handin transcript

Experiment 2:

(a) You and your buddy Lefty have always lived on the shady side of the law. Recently Lefty slipped up and got 6 years in the slammer for your latest escapade. Lefty needs to send you a message, but jail policy allows the guards to censor all mail sent out by inmates. You weren't clever enough to set up a key in anticipation of such an event, but your RSA public key is available to Lefty. He has encrypted a message by raising it to the power of three modulo your public modulus.

In this experiment, you must receive the cyphertext from a transcript. The modulus m and its two factors p and q are given to you in cells. Decrypt the cyphertext and send the plaintext to the hand-in transcript. Submit your results.

In Brief...	
We give you:	A calculator for you, a cell containing the modulus, a pair of cells containing the factors of the modulus, a transcript containing the cyphertext, and a handin transcript
Your task:	Decrypt the message in the transcript
Hand in:	Place the plaintext in the handin transcript and submit

(b) After his first month, Lefty has grown tired of his incarceration. So tired, in fact, that he has hatched an escape plan. In his next message to you, he has outlined this plan. To avoid arousing the guards' suspicion, he has used your RSA public key to encrypt a session key. This block containing the session key is then followed by his real message. This message is encrypted using the addition cypher with the above session key.

As in the previous experiment, you are given the modulus m, as well as its two prime factors p and q. Encryption is done by raising the plaintext to the power of 3 (mod the recipient's public modulus). In this instance, the RSA-encrypted message is a single block message which decrypts to an addition cypher key. After decrypting the first block of the message to obtain the session key, you will then decrypt the remaining blocks and send the plaintext to the hand-in transcript. The block size for the addition cypher will be 5 characters (10 digits), and the corresponding modulus will be 10^{10}.

In Brief...	
We give you:	A cell containing your public key m, a cell containing p, a cell containing q, a transcript containing a message from Lefty (the first block is encrypted with RSA and is the key for the later blocks, which were encrypted using the addition cypher), a hand-in transcript, and a calculator for you
Your task:	Decrypt the first block to obtain the session key. Then decrypt the following blocks to obtain the plaintext message
Hand in:	Submit when you have sent the plaintext to the hand-in transcript

Experiment 3:

You've been eavesdropping on the local area network in your dorm and you notice that one of your dormmates is ordering something from a highly sketchy online store calling itself the Plain Brown Wrapper Mail-Order Company. He has encrypted the name of the item using the RSA public key of the mail-order company and sent the cyphertext across the network. (*Note:* The message uses plain RSA for the encryption, as in experiment 2a). The cyphertext was obtained by raising the cleartext to the power of three (modulo the company's modulus). You are just a bit curious. Your curiosity is further piqued when you realize a flaw in the Plain Brown Wrapper Mail-Order Company's implementation of RSA...

You will find cells with both the modulus and the cyphertext in them. Figure out the flaw in this implementation of RSA, decrypt the cyphertext, and send it to the hand-in transcript. Submit your results. Write a description of what you did to break the scheme and what flaw in this implementation of RSA allowed you to do this.

In Brief...	
We give you:	A calculator for you, a cell containing the modulus, a transcript containing the cyphertext, and a hand-in transcript
Your task:	Exploit a flaw in this implementation of RSA and decrypt the message
Hand in:	Submit electronically once the plaintext is in the hand-in transcript. Submit, on paper, a description of the flaw you exploited in order to decrypt the message

Experiment 4:

In order to stem the tide of prank phone calls he has lately been receiving, Professor Klein has had second thoughts about giving out his home phone number to the CS007 TA staff. However, he would like them to be able to contact him in an emergency. In order to meet this goal, he has decided to employ a threshold secret-sharing scheme.

Professor Klein choses a mod-44019301 line. The slope of this line is the secret (his telephone number), and the y-intercept was chosen randomly. He then provides each TA with an (x, y) point on

that line.

Anxious to re-enact a phone prank you heard on a popular radio morning show, you coerce two of the TA's into giving you their parts of the secret. When you open this experiment, you will find cells containing values x_1, x_2, y_1, y_2. There will also be a handin cell. You must piece together Professor Klein's phone number and send it to the handin cell.

In Brief...	
We give you:	The x and y-coordinates of two points on a modular line
Your task:	Find the secret, which is the slope of that line
Hand in:	Write that value to the handin cell, and submit electronically

Experiment 5:

The president of BunjiCorp has arranged to receive messages encrypted using the exponentiation cypher in ECB mode with a modulus of $m = 3854210329$. She has calculated the mod $\phi(m)$ inverse s of the key, so to decrypt a cyphertext, she need only raise each block of the cyphertext to the power of s mod m.

She is going on vacation, and wants to make sure that cyphertexts sent to her can be decrypted by the vice-presidents while she is away. She uses threshold secret-sharing to share the decryption exponent s with her vice-presidents: she chooses a random b and writes down an equation for a mod $\phi(m)$ line with slope s,

$$y = s \cdot x + b \pmod{\phi(m)}$$

She then provides each vice-president with one point on that modular line. That way, any two vice-presidents can combine their parts using mod $\phi(m)$ arithmetic to obtain s.

The president gave Vice-President Alice the point (x_1, y_1), Vice-President Bob the point (x_2, y_2), and Vice-President Carol the point (x_3, y_3). Here $x_1 = 1$ and $x_2 = 2$. (Since we only need two points to define a line, we won't worry about Carol's x_3.)

You are Alice, and you and Bob are trying to decrypt a cyphertext w. The trick is that Bob will not tell you the value of y_2 because he realizes that once you know it you can decrypt on your own. However, Bob he is willing to do his part towards decrypting the cyphertext. He will send you the value of $w^{y_2} \pmod{m}$. You must use this value and the value of y_1 (provided in a cell called "Your part (y1)") to obtain all the blocks of the plaintext and send them to the Hand-in transcript.

In Brief...	
We give you:	A calculator for you, calculator Bob, a cell containing your part, a transcript containing the cyphertext, and a handin transcript
Your task:	Combine forces with Bob to decrypt the plaintext blocks
Hand in:	Submit when the plaintext has been entered into the hand-in transcript

Experiment 6:

In previous labs, we explored some of the basics of Kerberos, and you had the opportunity to actively participate as one of several parties in this protocol. In this exeriment, you will play the role of the notorious Eve, eavesdropping in an effort to learn information that does not belong to you.

In this case, you happen to know that Alice has chosen a very easy-to-remember secret key: a single vowel (you are not sure whether it is upper or lower-case, however). Armed with this knowledge, you are to observe as Alice obtains a service ticket for the email server, and then checks her email. Using the fact that her password is one of a few possibilities, try to read her email. When you have obtained a likely (English) decryption, submit the message to the hand-in transcript. The system-wide modulus is 88245335319593.

In Brief...	
We give you:	Alice, Kerberos server, Email server, a calculator for you and a handin transcript
Your task:	Eavesdrop on Alice's communication with the Kerberos server and use the information you know about her password to figure out the session key and decrypt the email sent to her by the email server.
Hand in:	Send Alice's email to the hand-in transcript and submit electronically.