ACCESS 2009

Group Project - Week 1

Due Thursday, June 25, before midnight

Part I Genetic Code: Write a careful explanation of your solution to the genetic code problem you've been working on. The precise questions you are to answer are in the email Alla sent you, which is also posted on our ACCESS Math homepage.

Part II RSA Public Key Lab: Set up, use, and explain an RSA public-key cryptography system for the 10 ACCESS groups. Follow the steps below carefully!!!

(1) Each team should choose two primes p,q between 10^30 and 10^31, so that the modulus N=pq is greater than 10^60 - and thus will have at least 61 digits. This means that when you send people messages you can use up to 60 digits in each number packet , **before** encoding with their public key. This forces each packet number to be safely in the residue range for the recipient's modulus before you encrypt it, so that when the recipient decrypts it, they will recover your original message. (After you encode a packet it will quite likely have 61 or 62 digits, but it will still be in the recipient's residue range because of how the encryption algorithm works.) Real RSA systems use much larger primes, but I have chosen these lengths so that each digit packet fits onto a single text line.

(2) After picking your primes find a suitable encryption power e. Use e and the auxillary modulus to compute your secret decryption power d. Make sure e and d are multiplicative inverses mod N2, check that you can successfully encrypt and decrypt messages using your own public and private information, and verify that N really is bigger than 10^60, before proceding to step (3) - This double-checking should prevent errors which have occurred in some unfortunate ACCESS groups, and which have led to strings of emails with different attempts at a public key, all from the same group....and then other ACCESS groups became innocent victims.

(3) As a further check that your data is correct, send an email to Nick (korevaar@math.utah.edu) containing your p,q,N,N2,e,d. Include your group number in the email header, and in the email body include your names and email contacts for this project. Wait until Nick verifies your data before proceeding to step 3.

(4) Send a plain text email to *access-2009@lists.utah.edu,* identifying your group by number, with your three names, with contact email address(es) for the group, and with your public key information. Make sure your encryption power e and modulus N are text numbers and NOT a picture image, so that the recipients can use them.

(5a) Create a favorite secret message and convert your letters to numbers using the table on page 9 of Davis' notes. Let us agree that your plain text message is no longer than 90 characters long, including punctuation marks and spaces. This means that after conversion to numbers, there will be at most 180 digits. Break this string of digits into packets at most 60 digits long, so that each packet will be in everyone's residue number range. (Make sure that no packet starts with the digit "0", since this "0" at the start of a number wouldn't be visible to any unfortunate ACCESS group who correctly decrypted the encrypted message you sent them!) At the end of this step you will have at most 3 packets of numbers, each of which has at most 60 digits. You can check that each packet has at most 60 digits by dividing it by (10.0)^60 - you should get a decimal less than 1.

(5b) Create any plaintext signature which identifies your group, using at most 30 characters. Convert your signature into a number with at most 60 digits, using Davis' table. We are using the secure signature feature, so decrypt your signature using your own (secret) decryption power. This will create a long sequence of digits (a number less than your groups' modulus but probably with 61 or 62 digits). Unfortunately you have no guarantee that your decrypted signature lies in your receivers' residue range (it could be too big!). This means you'll need to break your decrypted signature into two packets of at most 60 digits each (and so that the second one doesn't have a lead "0")

(5c) You now have up to 5 packets of at most 60 digits: 3 from your plaintext secret message and 2 from your decrypted signature. If you are group x then you will be sending messages to groups (x+1) and (x-1), mod 10. For example, group 3 sends messages to groups 2 and 4; group 10, also known as group 0, sends messages to groups 9 and 1. Encrypt the (up to) 5 packets you've created in parts (5a),(5b), using the public encryption keys for the two groups you're sending to, and then email out your encrypted packets.

(6) Use your private key and reverse the encryption process to decode the messages you receive from your two neighbor groups. After you use your decryption key to decrypt the signature part of their messages, you'll need to glue the last two packets back together, and then encrypt with the sender's public key, in order to verify their plain text signature.

(7) Create a lab report for this experiment: Describe the process you went through to set up the ACCESS RSA system. Exhibit your public and private key information, your original plain text message and signature, and the various transformations of your message and signature as you prepared them for transmission to your two target groups. Exhibit the encoded messages you received, explain how you decoded them, and exhibit the final results. Make sure all numerical representations of your messages are numbers and not pictures, so that we will have an easy time checking your work (which we will do!). Present this data in a careful, organized way. Explain well.

Part III Public Key Cryptography and Internet Security Report: Research and write an approximately 5 page paper on public key cryptography.

Explain what public key cryptography is and why its advent was such a revolutionary development. Explain the RSA algorithm and why it works for public transactions. We have given you various references for this part of your report, but we encourage you to also do more independent research. Questions we would enjoy you finding answers to are: When you engage in secure internet transactions (i.e. at any URL starting with https://....) how much of this interaction is typically made using public key cryptography? Is the RSA algorithm universally used for public key cryptography or are other algorithms also being applied? When RSA is being used, what is the typical modulus size? How is "security certificate" authentication related to the RSA secure signature feature, if at all? Is it now possible to not only send documents, but also to make secure phone calls over the internet, using "pretty good privacy"? What strategies do groups like the National Security Agency adopt in their quest to track potential enemies, in order to get around the fact that public key cryptography apparently allows for secure information transmission?

Style and Formatting: Please create MSWord .doc documents (and not .docx. Non-PC's still have trouble reading the newer MSWord formats.)

Although different subjects and professors may have different standards for how papers should be formatted, there are certain common elements. Reports should begin with a cover page or title area, containing the title, the authors, and the date. This should be followed with an introduction or abstract

which summarizes the report's contents. The body of the project report may be split into sections, and a conclusion section may be appropriate. Make sure to cite all references. With MSWord the easiest way to do this is by inserting footnotes, and we prefer that they be endnotes. For internet references include a link to the web page, the site title, author and download date. The RSA paper by Rivest-Shamir-Adelman is an excellent example of how to write a paper in mathematics.

Paper submission: Please submit your group work to me (Nick, korevaar@math.utah.edu) and Darci (darci@math.utah.edu), as 3 attachments in an email. This project is due by Thursday June 25, before midnight. Help each other - you're all on the same ACCESS team! If you think a group sent you a defective message, contact them and explain what isn't working, as a prelude to both sides trying to troubleshoot the problem. If you can't unstick each other, see if Darci, Alla, Ashley or I can help. I will also plan to be available from 2-4 on Wednesday afternoon next week, in the large 2nd floor Marriott computer room, in case any groups are stumped. Please send me an email if you wish to take advantage of this meeting time, since if no one asks I won't show up. Have fun!!