Project 4, due September 11

You are independent mathematical and scientific technical contractors and have recently received a contract with the company OCRAI. The letter you received on the subject is attached.

You will work on this project with one or two other students from this class, and will turn in your project by the 11th of September at 4:30 PM. Additionally, you should send an email with the names and email addresses of your group members to jenkins@math.byu.edu by Tuesday September 8. Your project should be in the form of a typed technical report; you should carefully follow all instructions in the below requirements and in the attached letter.

OCRAI Technical Report Requirements

All reports submitted to OCRAI should be written so that all members of the board of directors can understand the issues raised therein and therefore be able to appropriately use the report. The board members can all boast of a good university education—however, you should not assume that they are experts in computer programming or mathematics beyond calculus.

Reports should:

- Be written in the first person plural (e.g. "We then manipulate the data by ...")
- Include mathematical formulas in the text of the body of the report as appropriate to describe the methods used and results obtained
- Clearly explain how any mathematical formulas that are included apply to the problem being solved
- Consist of
  - An *introduction*, describing the problem to be solved.
  - A *body*, describing the process used to solve the problem(s) posed in the introduction, and the solution.
  - A *conclusion*, summarizing the solution described in the body and clearly stating its relevance to the original problem.
- Be 2 to 4 pages in length.

This project will be graded using the following scale:

- 7 points: clear explanation of a nontrivial method of encryption
- 4 points: Clarity/organization, spelling/grammar/punctuation
- 3 points: encrypting a message using another group's cipher by September 16
- 3 points: successfully decrypting other group's message in your cipher by September 18
- 3 points: three $\geq$ 500-character ciphertexts

OCRAI
OCRA Creative Recursive Acronyms, Inc.
485 Primality Way
Provo, UT 84604

---

2 September 2015

Independent Mathematical Contractors, Inc.
136 TMCB
Provo, UT 84602

Dear IMC:

Our company has recently had several major security breaches when company employees unintentionally and erroneously used their mobile devices to send text messages to the wrong recipients. These text messages contained sensitive company information and trade secrets, and had the potential to cause acute embarrassment to the company and harm to our future revenue streams, should they have reached the media or our competitors in this cutthroat business. We are determined that such a fiasco must not happen again and, on the recommendation of one of your previous clients, have contracted with your company to create a method for keeping our information secure.

We would like your team to create a nontrivial method of encrypting plaintext English messages. This method will take a message of up to 140 characters—the maximum size of a standard text message—and output a ciphertext of up to 700 characters, so that the ciphertext can be sent in at most 5 text messages. The ciphertext should be in a form that can be typed on a standard computer or mobile device keyboard.

Our in-house engineers will use your cryptosystem to create a mobile application which will become mandatory for employee mobile devices; this application will encrypt all text messages using your cryptosystem before they are sent, and decrypt any messages received from other company employees. Thus, any messages sent to unauthorized recipients will be unreadable. Because of the fact that mobile devices have limited processing power, though, the encryption key for your cryptosystem must be of limited length—for example, not more than 10 letters long, if the key is a sequence of letters.

We expect a report in three parts from your team. The first part of your report should explain how to use a randomly chosen encryption key to encrypt and decrypt messages using your cryptosystem. This report should include enough information that other IMC teams can understand the cryptosystem you create and can use your report to encrypt messages (by hand) using the system. To confirm this, we would like you to bring a copy of the first part of your report to your Math 485 class on Friday, September 11. You will trade reports and email addresses with another IMC team. By Wednesday, September 16, the other team will use your report to choose an encryption key and encrypt a message of their choice using your system; they will send the encrypted message and the key they used to your group and to our consulting scientist, the idiosyncratic Dr. Paul Jenkins (whose fee was unfortunately beyond our ability to pay, resulting in our appeal to you). By Friday, September 18, your group will decrypt their message and submit the results as the second part of your report.

The third part of your report will consist of three messages encrypted with your cryptosystem. (These ciphertexts will not be given to another IMC team at this time; we have our own reasons for needing these messages.) Two of these three messages should be the same plaintext, encrypted using different encryption keys; each plaintext should be at least 500 characters long or take at least 4 text messages to send completely. Given Kerckhoff's principle, you should assume that an adversary will know your encryption system, perhaps by stealing a copy of the first part of your report. Thus, your report should not include the encryption keys you used to create these ciphertexts.

Our time constraints require that parts 1 and 3 of your report must be submitted by 4:30 PM on Friday September 11. This should be done by email to our consulting scientist at jenkinsbyumath485@gmail.com. The first part should be a .pdf file, and the third part should be a text file containing your three ciphertexts. Additionally, as noted above, a hard copy of the first part of your report should be brought to class on Friday September 11. Part 2 of the report is due at 4:30 PM on Friday September 18.

We look forward to seeing your finished report.

Yours sincerely,

Robert S. Andrews
Vice President, Security
OCRAI