Project 40, due 12/10

In a group of one to three students, analyze three of the cryptosystems created by other students in the class. In a report written to your fellow students in the class, describe strengths (if any), weaknesses (if any), and possible attacks on these three cryptosystems. Address each cryptosystem in a separate section of your report.

Each cryptosystem has three associated ciphertexts, two of which come from identical plaintexts. You should attempt to determine which of the three messages came from a different plaintext. Deciphering all three messages is certainly one way to do this; you should give the complete plaintexts for at least one of the three cryptosystems you analyze, if possible.

You should choose at least one nontrivial cryptosystem to attack for the report to be given full credit. Nontrivial cryptosystems have at least one of the following properties:

- They are not minor modifications of systems we studied in class.
- Decrypting messages may be quite time-consuming without writing a computer program to help.

Nontrivial cryptosystems include those created by groups C, L, and M. A nontrivial cryptosystem does not have to be completely broken in your report to receive full credit, if a solid analysis is made.

You should not discuss these cryptosystems with their creators during this project, and you should not analyze a system created by any of the members of your group for this project.

This report is due by 4:30 PM on Thursday December 10, the last day of class. Reports will be graded on the following:

- Clear explanation of strengths and weaknesses of cryptosystems
- Clear descriptions of feasible attacks
- Successful determination, for each cipher, of which ciphertext is from a different plaintext
- Choice of at least one nontrivial system to attack
- Clarity/organization, spelling/grammar/punctuation