Cryptanalysis Project Requirements

- You must attempt to solve one of the challenge problems posted here http://www.mysterytwisterc3.org/
  (level II or higher) or obtain instructor approval for a cryptanalysis project not on this site. The precise details of your project will vary somewhat depending on the challenge you select, but, in general, you will be expected to do all of the following:
  - Study your selected cryptosystem
  - Write software to implement the system
  - Write software to implement the attack on the system
  - Estimate the work factor for your attack
  - Conduct computational experiments to verify your analysis
  - Ideally, you will provide a complete solution for your selected challenge problem
  - write a report that includes a detailed description and analysis of your work and results

  In summary, you must become an expert on the system that you choose to attack, and your work must demonstrate your newfound expertise.

- You are expected to work with a partner. All projects will be ranked against all other projects.
- You must select your project topic by the date given in the course syllabus. Instructor approval of your topic is required. This must be done via email. The topics are first come, first served. For your email, use subject line "CS265-01 Cryptanalysis Topic" or "CS265-02 Cryptanalysis Topic" as appropriate. Send your email to auston.davis@sjsu.edu . If I have any concerns regarding your selected topic, I will let you know promptly. It is to your advantage to spend some effort to initially select a good topic.
- All software must be written in C (if you do not know C, the language must be approved by me). In most cases, the number of lines of code will be relatively small, but the coding may be technical and challenging.
- You must write a report that includes a detailed description and analysis of your work and results. There is no minimum or maximum length for this paper, but quality is far more important than quantity. Your paper should be concise and to the point. Your grade for the project will be largely determined by the content and substance of your paper. While this is not a writing class, poor grammar, usage, organization, etc., will definitely not help your cause and may detract significantly from your grade. Every page of your report must include the authors' names and email addresses.

- Papers may be submitted to www.turnitin.com, an online plagiarism detection tool. If the instructor determines that you have committed plagiarism, you will fail the course and an academic dishonesty report will be submitted. The official SJSU policy on academic dishonesty (including plagiarism) can be found at http://www2.sjsu.edu/senate/s98-1.htm.
- On or before the due date, submit all material (including source code), put all info in a single zip file named Lastname1_Lastname2.zip, where Lastname1 and Lastname2 are the last names of you and your partner. The subject line of the email must read "CS265-01 Cryptanalysis Project" or "CS265-02 Cryptanalysis Project", as appropriate. You will upload your final project to Canvas under the assignment section titled “Cryptography Poject”
- Finally, it is imperative that you begin working on this project immediately and that you work on it consistently. This is not the type of project that can be completed in a few days, no matter how many hours you work each day. It is also not the kind of project that you can drop and easily pick up where you left off. These are highly technical and challenging problems that require constant and ongoing effort to make any real progress.