BCP / A.M.D.G.
Discrete Math

Name: _____
Fall Semester

# Cipher System Project

*Guidelines*

## Overview

This is a ***group project*** affording you the opportunity to synthesize and apply the concepts presented/discussed from graph theory, number theory, algorithms, spreadsheets and cryptography. The final product that your group submits must reflect/incorporate at least some of the ideas and concepts discussed/presented in class. You will be working in 3-4 person groups that have been assigned by the teacher based partly on your suggestions and performance on spreadsheet activities.

## Assessment

The baseline value of the project will be 75 points. Group projects will be assessed using a grading rubric consisting of 25 specific characteristics for which each group will be assessed a value between -1 and +1 points. Thus the maximum and minimum number of points that can be earned for submitting a project is 100 and 50 respectively. Zero points will be earned in the event that no project is submitted.

The total points earned will be multiplied by a factor of 2 so that the project will account for at least 28% the total possible points for the semester. Each members of a group will earn the same number of points. But at the discretion of the teacher, the Wiki site may be used to adjust the points for individual group members should it become apparent that an individual did not contribute his efforts towards the project.

During the course of project, the teacher reserves the right to establish *benchmarks* for your group to meet. These *benchmarks* might consist of deadlines for posting files to your group's Wikispace, request for documentation, a meeting with the entire group, etc.

## Sales Presentation

All members of the group are required to be in class on the day of their scheduled presentation. A student who is not in class on the scheduled presentation day will have those points deducted from his assessment score.

The presentation should last no more than 3 minutes and it should consist of the following elements:

- **an overview of your group's cipher system (PowerPoint)**
- **an example/explanation of how your group's cipher system works (Spec Sheet)**

Below are some *suggestions* for organizing your group work.

### Planning

- Become familiar and regularly consult the grading rubric.
- Develop an Action Plan for this project – discuss and decide as a group who is going to be responsible for the various parts of the project, establish deadlines, identify strategies to follow, etc.

### Production

- Maximize the productive use of class time – this is uninterrupted time when you will be provided access to computers and the internet, but more important you will have all your group members together!
- Maximize the use of your group Wikispace – this is the most effective vehicle to prove/document your level of participation and contribution
- Develop an Action Plan for this project – discuss and decide as a group who is going to be responsible for the various parts of the project, establish deadlines, identify strategies to follow, etc.

### Review & Rehearse

- Schedule a time prior to your designated presentation day to review your files and rehearse your presentation – this will help minimize or eliminate confusion as to who is supposed to do what, where the files are located, etc. when your group gives its presentation

# 2012 Discrete Math Cipher System Project Evaluation Rubric

| | – 1 | 0 | + 1 |
|---|---|---|---|
| **Spec Sheet** | ❑ not submitted or length of 2 or + pages<br>❑ minimal or vague explanation of the enciphering/deciphering process<br>❑ format lacks intentional planning or time spent on the visual design | ❑ length more than a single side of paper<br>❑ substantial explanation of the enciphering/deciphering process<br>❑ format exhibits intentional design elements with more than just text | ❑ completely fits on a single side of paper<br>❑ clear, detailed explanation of the enciphering and deciphering process<br>❑ format exhibits exceptional, easy to follow design mixed with text & graphics |
| **Project Development Wikispace** | ❑ more than 2 days between updates and/or lacking substantive info<br>❑ roles and/or timeline not clearly defined<br>❑ disorganized or difficult to follow<br>❑ many files not accessible/missing | ❑ less than 2 days between updates with broad/general summaries<br>❑ roles and timeline clearly defined<br>❑ organized with minor inconsistencies<br>❑ most files accessible | ❑ daily updates with concrete & detailed reports from all members<br>❑ roles and timeline are clear & described<br>❑ clearly organized and easy to follow<br>❑ all files accessible & annotated |
| **PowerPoint** | ❑ 7+ slides and/or incomplete slides<br>❑ too much text / no visuals<br>❑ excessive/irrelevant use of effects | ❑ 5 or 6 slides<br>❑ too much visual inclusion<br>❑ effects used and appropriate | ❑ less than 5 slides<br>❑ balanced of text & visual elements<br>❑ effects used to highlight/accentuate |
| **Spreadsheet** | ❑ non-functional and/or incomplete<br>❑ fails to automate ciphering process<br>❑ poorly organized or difficult to navigate<br>❑ little care given to visual layout | ❑ functional & complete w/ few errors<br>❑ mostly automates ciphering process<br>❑ organized and relatively easy to navigate<br>❑ adequate care given to visual layout | ❑ functional & complete w/ no errors<br>❑ fully automates ciphering process<br>❑ extremely organized & easy to navigate<br>❑ significant care given to visual layout |
| **Productivity** | ❑ ineffective/unproductive use of class time | ❑ effective/productive use of class time | ❑ maximized productive use of class time |
| **Sales Presentation** | ❑ poor execution/lack of coordination<br>❑ overall difficult to follow and unclear<br>❑ no attempt to engage audience | ❑ good execution/mostly smooth flow<br>❑ minor parts unclear/difficult to follow<br>❑ some attempt to engage audience | ❑ excellent execution/consistent flow<br>❑ clear and easy to follow<br>❑ successfully engaged audience |
| **Cipher System** | ❑ lacks both substitution & transposition<br>❑ does not utilize an algorithmic process<br>❑ no elements of mathematical concepts discussed/presented in class<br>❑ major problems with both the enciphering and deciphering process<br>❑ lacking in creative ideas/elements<br>❑ manual ciphering impossible<br>❑ static / no options for variations | ❑ lacks substitution or transposition<br>❑ portions utilize an algorithmic process<br>❑ some elements mathematical concepts discussed/presented in class<br>❑ minor problems with either the enciphering or deciphering process<br>❑ contains some creative ideas/elements<br>❑ manual ciphering reasonable<br>❑ dynamic / some options for variations | ❑ contains substitution and transposition<br>❑ completely defined algorithmic process<br>❑ significant use of mathematical concepts discussed/presented in class<br>❑ no problems with either the enciphering or deciphering process<br>❑ clever, non-standard ideas/elements<br>❑ manual ciphering cumbersome<br>❑ robust / several options for variation |