**CSE 8349**

**Advanced Network Security**

Project 3

Crack MD5 Hashes

This project contains an input file which is formatted as

number:salt:MD5\_HASH:password:

The expectation is that the MD5 hash of "salt""password" (concatenated together) is MD5\_HASH. The first two lines have a password of "example" You can use these two lines to ensure you are correctly evaluating the hashes as expected.

Use any legal method you can (other than classmates in other groups) to crack as many hashes as possible.

You should submit your copy of the input file with the password column filled out for the hashes you cracked. Do not reorder or remove any lines in the file. This is very important. I want to combine the files and have all of the same hashes line up for analysis.

You should also submit a report with your project.

Please include the following in your report:

* Any source code or scripts you wrote to help you.
* A discussion of difficulties you encountered.
* A discussion of the surprises you encountered.
* Anything else you find interesting.

What to submit: The report and the output file. I will have a place for each of these on blackboard.

Presentation: Consider a class presentation to discuss the solution