# COMP 360 Group Project: RSA Explorations

Matt Adelman, Evan Carmi, Adam Forbes

October 7, 2012

For the group project, we would like to study the security algorithm RSA.

1) History 2) Make our own implementation 3) Visualization 4) Common implementation flaws 5) Fixes for these flaws

Main Goals: 1) Implementation 2) Visualization 3) "Good Key" checking

Additionally, we have all expressed interested in having this project serve as a example to show on our résumé or CV. To that end, having a project written in JavaScript, that runs in a web browser, would be both a portable and easily presentable choice of tools.

## 1 Implementation

To further explore the RSA algorithm and the difficulties in an actual implementation we will write the algorithm in JavaScript, embedded in a web page. There has been some research done on web based implementations and (http://www-cs-students.stanford.edu/ tjw/jsbn/) may serve as a resource. Additionally, we will explore possible speed improvements, such as Chinese remainder theorem, and error checking. If possible, providing a visualization of the process would also be a goal of ours. In terms of difficulty implementation the algorithm shouldn't be too difficult, although further improvements and a clean interface may provide interesting challenges. Ideally we wouldn't simply replicate previous JavaScript implementation's of RSA, rather creating a new, clean, fast and explicative version which would provide the base of further experimentation.

Our List of primary references is as follows: http://en.wikipedia.org/wiki/RSA_(algorithm)