Proof of Concept Demonstration Plan

Jean Lucas Ferreira, Ocean Cheung, Harit Patel

October 2, 2015

Will a part of the implementation be difficult?

The algorithms for encrypting and decrypting passwords used in bCrypt are complicated. Re-Implementing these algorithms may be difficult considering we have little prior knowledge of encryption algorithms. However, there are plenty of resources on the web regarding these algorithms that provide insight on their purpose and implementation.

Will testing be difficult?

Many of the functions of the API we are creating will be relatively easy to test. We can simply send in automated inputs and check if the appropriate output is returned. Testing the functions that do the encrypting and decrypting would be more complicated. These functions are very large and have a long process leading to encryption or decryption. We can however test these functions by encrypting a string then decrypting it to check if the original string is returned.

Is a required library difficult to install?

The only required library for this project is NodeJS, it is simple to install on any operating system. All team members have successfully installed it.

Will portability be a concern?

If a developer wishes to use our library with their application, it will be necessary that they have NodeJS installed on their system. Once NodeJS is installed, the library will be able to run on on any web browser (Chrome, Firefox, Safari, Opera, IE) given that the user of the browser has enabled javascript, under any operating system such as Windows, MacIntosh,Linux, and mobile devices. NodeJS also allows javascript functions to be called on a command line (Windows and Linux/Unix).

Will the project size/scope be feasible?

The project is feasible, all team members understand language being used. But the actual implementation of the project can become complex, and will take time to get a grasp of the algorithms needed, but is still feasible.

Describe what you will demonstrate to show the risks can be overcome.

The main risk in this project is understanding the Eksblowfish algorithm.We are currently researching this algorithm through various research papers and implementations of the algorithm in different languages.