COMPX518-21A

Assignment 3

# Application Design

…

# Secure Random Number Generator

To guide my decision in choosing a random number generator for this application, I read the OWASP Cryptographic Storage Cheat Sheet. This document states that a Cryptographically secure pseudo-random number generator should be used when dealing with cryptography, and that in .NET / C#, I should use the **RNGCryptoServiceProvider** class instead of the standard **Random** class.

**RNGCryptoServiceProvider** is better suited for password generation because it provides a more secure random function that is not as repeatable as **Random** (at the expense of speed).

The graph below shows a distrubution of generated characters (50 million 80 character passwords). The least common character was **k** with *42538130* occurances, while the most common character was **w** with *42572116* occurances (a difference of 33,986).

Chart, bar chart

Description automatically generated

# Master Password Authentication

…

# Password Storage

…

# Resources

* <https://cheatsheetseries.owasp.org/cheatsheets/Cryptographic_Storage_Cheat_Sheet.html>
* <https://docs.microsoft.com/en-us/dotnet/api/system.security.cryptography.rngcryptoserviceprovider>
* <https://owasp.org/www-community/password-special-characters>