Project Report

**Part 3: Random Number Generator**

We are generating random numbers through the Middle Square Weyl Sequence, a pseudo-random number generator. This is an extension of the Middle Square Method by John von Neumann, which corrects the convergence to repeating loops. The test is noted to pass the BigCrush and PractRand statistical tests, but is not cryptographically secure. This implementation provides good performance.

[https://ieeexplore.ieee.org/abstract/document/9132873] [https://arxiv.org/abs/1704.00358]

**Middle Square Method**

The original method by von N

[John von Neumann, “Various techniques used in connection with random digits”, in A. S. Householder, G. E. Forsythe, and H. H. Germond, eds., *Monte Carlo Method, National Bureau of Standards Applied Mathematics Series*, vol. 12 (Washington, D.C.: U.S. Government Printing Office, 1951): pp. 36–38.]

Seed

Seed^2

Output, next seed

675248

455**959861**504

959861

**Middle Square Weyl Sequence**

**X, W, Seed**

**W += Seed**

**X \* X + W**

**Seed Correction**

**[Optional] Seed Entropy**

**Part 4**