|  |  |  |
| --- | --- | --- |
| BLG351E  Experiment 8 “Random Number Generator”  REPORT | CRN |  |
| Group |  |
| Name #1 |  |
| Name #2 |  |
| Name #3 |  |
| Name #4 |  |
| Q1) (30 pts.) Explain how you set the limit for the generated random numbers as 128. | | |
| In Middle Square Weyl Sequence algorithm, by applying OR with the 4 right-shifted value and the 4 left-shifted value, we get an 8 bit number. By converting it into 7 bits by right-shifting it by 1, a 7 bit number (a maximum value of 127) is obtained. | | |
| Q2) (40 pts.) What is the expected distribution of numbers for the part 3? Explain briefly. | | |
|  | | |
| Q3) (30 pts.) If the given algorithms (Blum-Blum-Shub, Middle Square Weyl) are used for number generation, the generator would be a pseudo random number generator or a random number generator? Explain. | | |
| It would be a pseudo random number generator since by starting the same initial value which is called seed, we get the same sequence. Because of that, the values from the function are not truly random. Both Blum-Blum-Shub and Middle Square Weyl are pseudo random number generators, since they just apply some mathematical operations on the seed, and deterministically maps the seeds to output values. | | |