BLG351E Experiment 8 “Random Number Generator” REPORT	CRN	12635
	Group	Group 11
	Name #1	Fatih Baskın
	Name #2	Mehmet Eymen Ünay
	Name #3	Nada Malek
	Name #4	Rojen Arda Şeşen

Q1) (30 pts.) Explain how you set the limit for the generated random numbers as 128.

As the resulting random number is the square of S modulus M (S’ = (S^2)%M) and M is equal to p x q (M = p*q), p and q can be selected to result 128 in multiplication.

Q2) (40 pts.) What is the expected distribution of numbers for the part 3? Explain briefly.

The expected distribution of numbers in part 3 is uniform. The reason for this expectation is that a random number generator should not favour some outputs more than others and generate every number in similar quantities over a large sample space.

This occurs because each time function generates a number X, it generates a random value by swapping least significant and most significant 4 bits as a block using shift operations.

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.

They both make use of a seed which determines the complete path of every value. Even though their number distribution is uniform, they will generate numbers as a pattern in accordance to their seeds. Thus they are pseudo random number generators.