Group Members: Khizar Amin (l14-4037) Jamshaid Suhail (l14-4340)

**Main concept:**

1. User inputs a 16-bit seed.
2. Seed is passed through shift registers and XOR gates to generate a 16-bit pseudo-random number.
3. Number is generated when user enters a clock pulse input.

**Implementation:**

1. Seed is XORed with the output of the circuit and is passed to D flip-flops.
2. The output of the D flip-flops is attached to the serial input of corresponding 4-bit shift registers.
3. The outputs of shift registers are XORed randomly.
4. The output of XOR gates is attached to HEX display to display the output conveniently.
5. All the D flip-flops are synchronized by a single clock while the clock of all the shift registers is connected to a binary switch. User turns the switch off and then back on again to generate a pulse which creates a new random number.
6. The reset button of the D flip-flops is also available to the user in order to clear the data stored in the D flip-flops

**Working:**

1. User inputs a 16-bit seed which is XORed with the output of circuit.
2. Depending on the initial state of the circuit, the data stored in the D flip-flops varies every time, which results in the generation of a new random number for every seed.
3. Each output of D flip-flop is the serial input of a 4 bit shift register. This generates a 64-bit number.
4. The outputs of the shift registers are randomly passed to 16, 4-bit XOR gates to generate the output 16 bit random number.
5. The output of the XOR gates is connected back to the XOR gates at input, for the generation of a different random number every time.
6. The random numbers change at every tick of the clock of the shift registers, therefore, the clock input of the shift registers is available to the user to give the user full control of the clock pulse. The D flip-flops however, user the built in clock.

**Caution:**

1. If the reset button is set to off, generator will not work. However, the number already on display will be consistent.
2. If the clock pulse is not generated, new random number will not be generated even if the seed is changed.