PRBS CIPHERING / DECIPHERING

Background

As you are aware, the linear feedback shift register (LFSR) can readily be used to create the basis for cryptographic transmission and decoding. This lab validates the secure communication process using a Pseudo Random Binary Sequence (PRBS) and could show - but not now - the evidence of not knowing the start point of the sequence.

Theory

The maximum sequence that can be obtained from a PRBS generator is 2^n-1. The 'minus 1' is because the all zeroes state causes the PRBS to stop. Extra background is in Module 10.4.

Procedure

Design a circuit that uses a 4-bit register (A) as the source of the data to be transmitted. The data is to be transmitted by XOR gating with a PRBS sequence to produce an unintelligible message to all but the intended recipient. The encrypted message will be XORed with an identical PRBS sequence, and this output is to be sent to a destination 4-bit register (B).

The PRBS generator (flip-flops are WXYZ where Z is the LSB) has XOR feedback from bits X and Z. In other words, after each clock, W becomes X XOR Z, and everything else is shifted right.

Testing

1. Set up a BCD value from 1 to 9 in your 4-bit data register (A). (Remember to use flip flops with S/R inputs to set initial states.) Use your clock input signals to transmit it through the PRBS generator, starting with a `0001` state.
2. Show that the system you have built will also work if the PRBS is initialized to the state `0011`.

Deliverables

Refer to the rubric for report specifics.