CSC/MAT 483 – 001

Spring 2010

Do five problems. Due no later than F, April 23.

1. Using a LFSR with seed C6 and feedback 5D determine the first 32 bits of a keystream.

2. Construct addition and multiplication tables for a finite field of 8 elements (ordered 000, 001, …, 111) with modulus .

3. In the finite field of 16 elements with modulus , find the additive and multiplicative inverses of 1011.

4. Do one round of simplified IDEA.

Plaintext: 0110 1011 0100 0000

Key: 0101 1011 1010 0100 1011 0001 1100 1000

5. Do 5 rounds of KeeLoq.

Plaintext: 1011 0110 0101 1111 1000 1100 0010 1011

Key: 0010 0100 0101 0111 1011 0100 1100 0001 1100 1000 1010 1111 0110 1001 1000 0011

6. Take the plaintext

0010 1011 0011 1011 1100 0001 0101 1001 1101 1110 0000 1010 1100 1110 1111 0000

through the sBoxLayer of PRESENT followed by the pLayer.

7. Use simplified AES to encrypt the plaintext 0010 0101 0001 1111. Do not use the key schedule; use the same 16-bit key each time that you need key. Use the key 0010 0001 0110 0101.