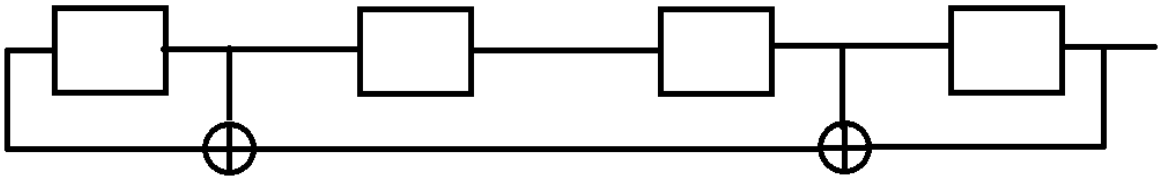
ITEC345 assignment 3 name_____
Spring 2024 historical crypto, LFSR

to turn this in, hand it to me in class, or leave under my door by the due date/time stated on the class website

1. 2**pts** You have a 4 bit linear feedback shift register:



It has an initial seed of **0011.**

a) Show one full cycle of key bits.

b) what is the maximum possible length of a cycle of key bits from an LFSR with 3 flip flops?

ITEC345 assignment 3

Let the alphabet A = { a, b, c, d, e, f, g, h, I, j, k, l, m, n, o, p, q, r, s, t, u, v, w, x, y, z} and the key K = “history”; consider a == 1 & z ==26 (not 0/25); ignore spaces

1pt . What is the Vigenere ciphertext for the message: where is the flag ?

1pt. Show the cipher text which results when you use the Playfair cipher to encrypt the cipher text:

math is real, but physics is true

The key is: “petey stands for part time cat”

Ignore spaces and punctuation, left to right, top to bottom, leave out ‘J’, just like in class.