Question 1)

a) There are 16 generators in Z*_61. 2 and 6 are some of the generators.

b) <9> is a subgroup of Z*_61 with order 5 its generators are [9, 20, 58, 34, 1].

Question 2)

Since p and q are prime phi(n) = phi(p) * phi(q) = p-1 * q-1

By using the right to left algorithm to calculate the modular of a power number we calculate

m =
3025624232311647114337757903685173495659956678495780877790008415934431140334807724330546889390094435679786549374287072364078639802603092317776014730871103745240338942225882488148569284312104218028021195525032789626303267205529411190014107098152321777301565858693092317773271396617297276351007405927094082O416

a) Since the since the gcd of a and n is 2 and b is divisible by 2 then there are 2 incongruent solutions to this congruence.
x = [1632949440937904653800123918, 168551507567775226236841370368]

b) The congruence has no solutions because gcd if a and n does not divide b, so there is no solutions for this congruence.

c) Since the gcd of a and n is 1 then a and n are relatively prime. Hence there is only one incongruent solution for this congruence.
x = 327252728639173874206458501252

Question 4)

For p1(x) it generates the maximum period sequences when the length is greater than 61. P1(x) maximum period is 2^L-1 which is 31.

For p2(x) the maximum period is 2^L - 1 however given the initial state it does not generate the maximum period, it only generates values smaller than 31. It might be because it is not a prime polynomial.

Question 5)

By using the Berlekamp-Massey Algorithm we can conclude that all 3 sequences are predictable. They all have a linear complexity of L(s^n) = 31 and C(x) = [1, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1].

Question 6)

Since we know that the message starts with 'Dear Student', we know the first 84 bits of the plain text and when we XOR it with the cipher text we should be able to find the first 84 keys.

Now we can use Berlekamp-Massey Algorithm to find the length of the polynomial for the LFSR and the first 84 keys.

Let the length of the polynomial coefficients (not including the constant) be L.

To calculate the ith key we take the last L known keys (from i-L-1 to i-1) and we add them and take the modulus of 2.

OR we can simply take the dot product of the last L known keys with the polynomial coefficients and take the modulus of 2.

after that we will have all the keys, we can xor the keys with the cipher text to get our plain text in binary format. Then convert it into ascii to get our message:

Dear Student,

You have worked hard and that paid off:)

You have just earned 20 bonus points. Congrats!

Best,

Erkay Savas