

Q. Compute the first two output bytes of the LFSR of degree 8 and the feedback polynomial is $x^8+x^4+x^3+x+1$.

The initialization vector will have the value of FF in hexadecimal format.

A. $(FF)_{16} \Rightarrow (11111111)_2$

Therefore, the sequence that would appear is as follows:

s_7	s_6	s_5	s_4	s_3	s_2	s_1	s_0	Output
1	1	1	1	1	1	1	1	1
0	1	1	1	1	1	1	1	1
0	0	1	1	1	1	1	1	1
0	0	0	1	1	1	1	1	1
0	0	0	0	1	1	1	1	1
1	0	0	0	0	1	1	1	1
0	1	0	0	0	0	1	1	1
0	0	1	0	0	0	0	1	1
1	0	0	1	0	0	0	0	0
1	1	0	0	1	0	0	0	0
1	1	1	0	0	1	0	0	0
0	1	1	1	0	0	1	0	0
0	0	1	1	1	0	0	1	1
1	0	0	1	1	1	0	0	0
0	1	0	0	1	1	1	0	0
0	0	1	0	0	1	1	1	1

From here, when the entire input of the input value process will we have to the next set of binary values waiting to be processed. From the table above, it can be seen that the next output byte to be processed will be $(10010000)_2$.

Therefore, the resulting first two output bytes will be $(1001000011111111)_2 \Rightarrow (90FF)_{16}$