2.3.2 The A5/1 for GSM

In GSM every conversation consists of sequence of frames, each lasting 4.6 millisecond.

Each frame contains 114 bits for the communication from Alice to Bob and 114 for the communication from Bob to Alice.

Each conversation makes use of a session key K of 64 bits.

For each frame, the session key K and the publicly known frame counter F_n (22 bits long) generate 228 bits that are XOR-ed with the $2 \times 114 = 228$ bits of plaintext.

- **How are the 228 bits generated?**

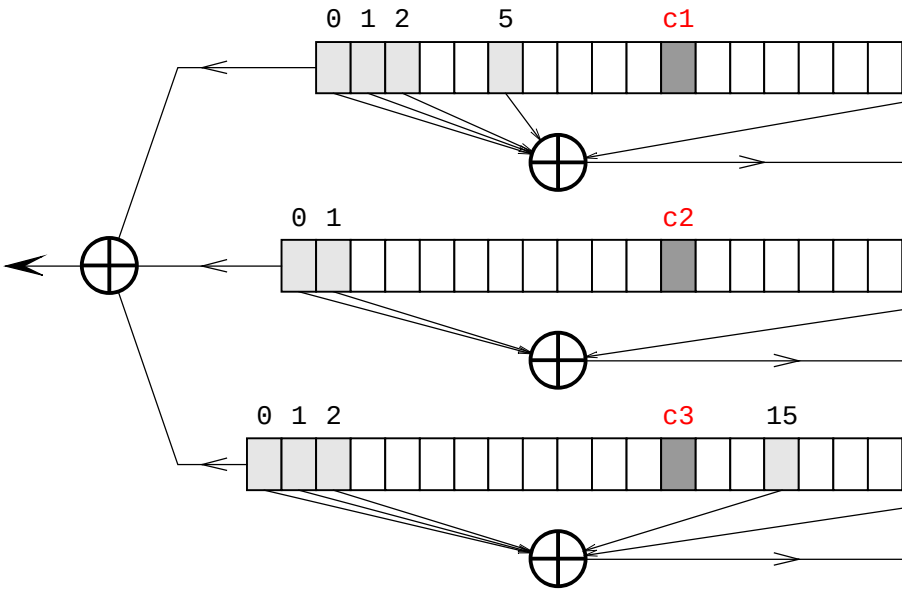
Use the three LFSR's depicted below. Their output is XOR-ed to give the output sequence that is XOR-ed with the plaintext.

The characteristic polynomials of the registers aren given by

$1 + x + x^2 + x^5 + x^{19}$	**for R1**
$1 + x + x^{22}$	**for R2**
$1 + x + x^2 + x^{16} + x^{23}$	**for R3**

However the LFSR's are not always shifted at the same time. Each one has a single "clocking" tap (at positions 8, 10, and 10 for R_1, R_2, resp. R_3). At each clock cycle those registers will shift that agree on their clocking tap with the majority value m of the three clocking taps c1, c2 and c3. This is called the"stop/go" rule.

(Note that always at least 2 LFSR's will shift.)



m=Majority(c1,c2,c3)

The generation of the 228 bits.

Put the LFRS's in their zero-state. Feed in the 64 bits of *K* by clocking 64 times all three LFRS's (so no stop/go rule), each time XOR-ing the next bit of *K* in parallel with the right most cell of each register . **(2.1)**

Continue in exactly the same way 22 more clock cycles to feed in the 22 bits of F_n. **(2.2)**

The three LFRS's are clocked 100 more times with the stop/go rule. No output is generated so far. **(2.3)**

The three LFRS's are clocked 228 more times with the stop/go rule to generate 228 bits of output. **(2.4)**