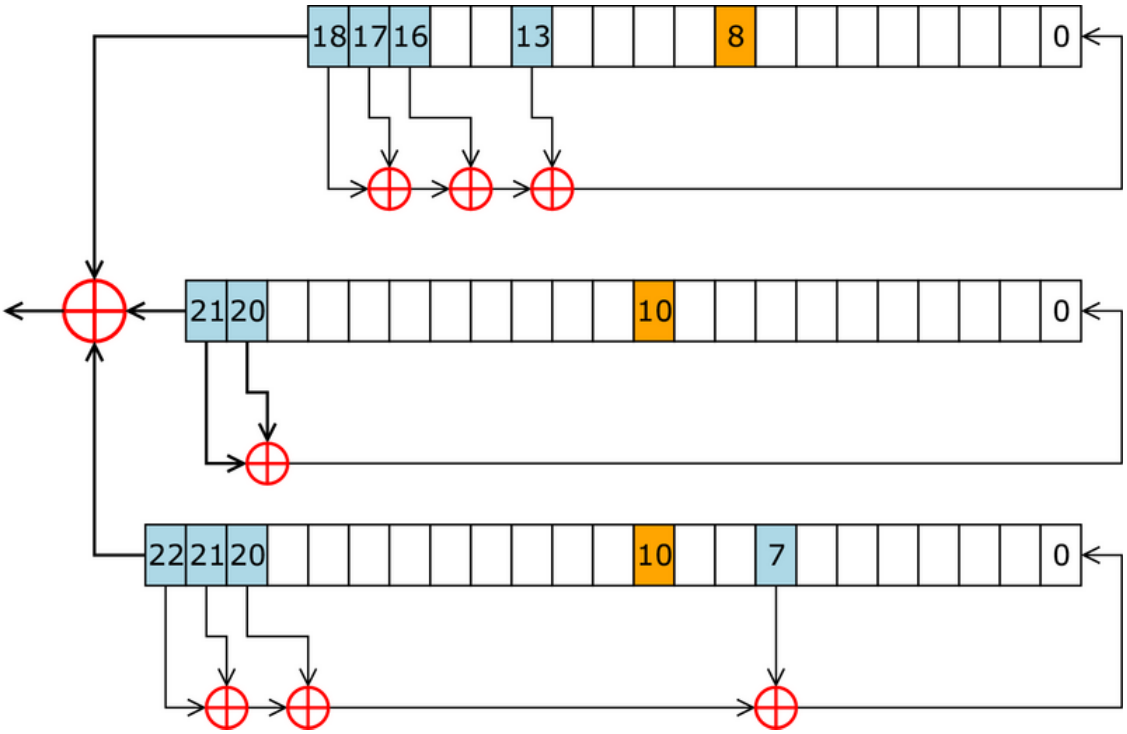
GSM A5/1 cipher

3 different LFSR are initialized with 64 bits

and their output is xored to produce 114 bits at a time

these bits are xored with 114 bits of the data stream and sent every 4.615 msec



pic from Matt Crypto - Wikipedia

In [1]:
```
lfsr1:x^19+x^18+x^17+x^14+1
```

Out[1]: $x^{19} + x^{18} + x^{17} + x^{14} + 1$

In [2]:
```
gf_primitive_poly_p(lfsr1,2)
```

Out[2]: **true**

In [3]:
```
lfsr2:x^22+x^21+1
```

Out[3]: $x^{22} + x^{21} + 1$

In [4]:
```
gf_primitive_poly_p(lfsr2,2)
```

Out[4]: **true**

In [5]:
```
lfsr3:x^23+x^22+x^21+x^8+1
```

Out[5]: $x^{23} + x^{22} + x^{21} + x^{8} + 1$

In [6]:
```
gf_primitive_poly_p(lfsr3,2)
```

Out[6]: **true**

In [ ]:
```

```