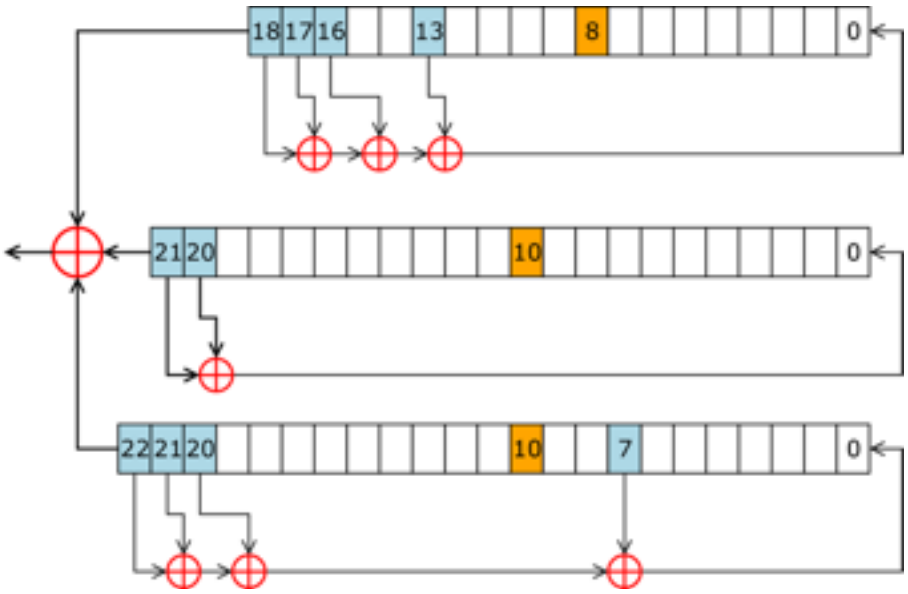
Stream Cipher Exercises

Bad keys for RC4. What RC4 key values will leave the permutation *S* unchanged by the initialization (called the "run-up" in the slides)?

State size for RC4. Using a straightforward implementation of RC4, how many bits are required to store the state (*S, i,* and *j*)? How many "bits of information" are contained in the state? To compute the "bits of information", you need to determine the number *N* of possible values for the state, and then compute $\lg(N) = \log_2(N)$.

Stepping in A5/1. The A5/1 stream cipher uses irregular stepping of the three registers. Each register has a *motion bit* (the orange bits in the diagram), which determine whether a register is stepped or not. The majority vote *m* of the three bits is calculated, and the registers for which the motion bit has the value *m* take one step; registers for which the motion bit is not equal to *m* do not step. How much does each register step *on average*? Simulate the A5/1 algorithm in the programming language of your choice.



A5/1 DIAGRAM (FROM WIKIPEDIA)

One-time Pad. In class, it was mentioned that a *One-time Pad* (OTP) is a secure method of encrypting data, but that because each user must have a copy of a file of random key, it is not practical in most situation. Recall that the random key for OTP must be truly random, typically generated from a hardware entropy source. What other condition must be met for OTP to be secure? When this condition is not met, what situation arises, and why is it a bad thing?