Exercise sheet 3, 26 November 2015

This exercise sheet takes you on a trip to investigate RC4. You can do it with a simple implementation of it in sage or python but it will be much faster (and thus your results will be more meaningful) if you work with a faster implementation, e.g. in C.

1. Take 128 bits as keylength; vary the key, and plot the distribution of the second output byte over all 256 possible values of that byte.
2. What happens to the output if $S[2] = 0$ at the end of the key-setup stage?
3. Take 128 bits as keylength; vary the key but keep the first byte of it fixed and plot the first output byte.
4. Take 128 bits as keylength; vary the first three key bytes and keep the remaining ones constant. Plot the distribution of the third output byte + key[0] + key[1] + key[2] + key[3].
5. Read the specification of WEP (the protocol to connect to routers). How can you use the knowledge from the first three parts to likely break it?
6. Check out the documentation and explanation of Aircrack-ng.