Problem Set 3 – Due Wed, 30 Jan 2019 at 12 pm

Instructions: Same instructions as before, but we're back to a Wednesday schedule.

Problem 9. Suppose you'd like to k-out-of-n secret share a 5-gigabyte DVD M among $n \geq 3$ shareholders, obtaining shares $S_1, \ldots, S_n$. Obviously it would be highly inefficient to regard M as a point from a (truly gigantic) finite field. Describe two simpler/faster approaches, and argue informally that they should work. The first should involve use of the field $\mathbb{F}_{2^8}$ and no complexity assumptions. The second should involve using Shamir's secret-sharing scheme on no more than 16 bytes.

Problem 10. The RC4 algorithm maps a key $K \in \textsc{Byte}^k$ to an infinite string $\text{RC4}(K)$, where $k \in [1..256]$. Investigate empirically the probability p_i that the second byte of RC4 output is $i \in \{0, \ldots, 9\}$ (written as a byte). For concreteness, assume a key length of $k = 16$ bytes. Now describe a simple adversary to distinguish RC4 output (with a random 16-byte key) from truly random bits. Estimate your adversary's advantage.