Problem Set 3 – Dew Thu, 18 Apr 2024

Problem 6. Alice wants to deal a one-byte secret to shareholders 1, 2, and 3 such that any two of them can reconstruct the secret, but no single player knows anything about it. She decides to use Shamir secret sharing over the smallest prime field that will work for this situation. She represents bytes and points in this field in the natural way. Players 1 and 2 end up with shares of $209 = 0\text{xD1}$ and $34 = 0\text{x22}$, respectively. What secret was shared? What was player 3's share?

Problem 7. 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 8.[1] 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 from truly random bits. Estimate your adversary's advantage, defined as the probability that it outputs 1 when given truly random bits minus the probability that it outputs 1 when given pseudorandom (RC4-generated) bits.

[1] This problem requires a little programming, and it requires you to lookup a definition of RC4.