Problem 8. Write out the addition and a multiplication table for \(\mathrm{GF}(2^3)\), the field with 8 elements. Represent points using the irreducible polynomial of \(m(x) = x^3 + x^2 + 1\), putting the most significant bit on the left, and then naming field elements \(\{0,1,\ldots,7\}\) in the natural way.

Problem 9. Let’s go back to problem 6, from the last problem set. For a PRG \(G\) : \(\{0,1\}^n \rightarrow \{0,1\}^N\), let’s define the multiquery PRG advantage of an adversary \(A\) as

\[
\text{Adv}_G^{\text{prg}*}(A) = \Pr[A^G \rightarrow 1] - \Pr[A^\$ \rightarrow 1]
\]

where the first oracle answers any query by \(G(K)\), for a freshly chosen \(K \leftarrow \{0,1\}^n\), and the second oracle answers any query by returning \(N\) uniformly random bits. Consider \(G = \text{RC4}\), thought of as a map from 16 bytes to two (or more) bytes.

Assume, as your experiments suggested, that the second byte of RC4 output is the zero byte with probability \(1/128\). Design an adversary that breaks the security of RC4 with \(\text{prg}^*\) advantage at least 0.99. For your analysis, you can use the following tool:

**Hoeffding’s inequality.** (See the Wikipedia entry with this name for more information.)

Let \(X_1, \ldots, X_n\) be independent and identically distributed random variables, each in \(\{0,1\}\) and each taking on the value 1 with probability \(p\). Let \(\overline{X} = \frac{1}{n} \sum X_i\) be the “empirical mean” of the observations, which has an expected value of \(E[\overline{X}] = p\). Then for all real numbers \(t \geq 0\),

\[
\Pr[|\overline{X} - p| \geq t] \leq 2e^{-2nt^2}.
\]

Problem 10. In class we quantified the unpredictability of a blockcipher \(E : K \times \{0,1\}^n \rightarrow \{0,1\}^n\) by way of

\[
\text{Adv}_E^{\text{unp}}(A) = \Pr[K \leftarrow K; (X,Y) \leftarrow A^{E_K(\cdot)} : E_K(X) = Y \text{ and } A \text{ never queried } X].
\]

Prove that prp-security implies unp-security.