Homework 1

1. (10 + 10 + 5 points) Let $\Omega_{n,k}$ be the experiment where we sample k balls numbered $\{1, 2, \ldots, n\}$ (with replacement) uniformly and independently at random. Given a sample of k balls, we say that a *collision has occurred* if there exist two balls with identical numbers in this sample. Let $p(n, k)$ represent the probability that *no collisions* have occurred when a sample is drawn in the experiment $\Omega_{n,k}$.

   (a) Plot $p(n, k)$ for $k = 1, \ldots, n$, where $n = 100$. The X-axis should represent k and the Y-axis should represent $p(n, k)$. Using this graph, find the value k_0 such that k_0 is the largest value with $p(n, k_0) \geqslant 0.99$, and the value k_1 such that k_1 is the smallest value with $p(n, k_1) \leqslant 0.01$.

   (b) Perform the same experiment as above with $n = 10,000$.

   (c) Find the values of k_0^2/n and k_1^2/n in the above two experiments.

   (Hint: Use arbitrary precision arithmetic of `sage` to perform the probability computations and to obtain the data. Next, use the `tikz` package to plot this data in LaTeX.)

2. (15 + 10 points) We consider a new definition of security for encryption schemes.

   (a) Formally describe a security experiment where an adversary gets to choose two messages $m^{(0)}, m^{(1)}$ of its choice. The honest challenger picks a uniformly random bit $b \xleftarrow{\$} \{0, 1\}$, and samples $\mathsf{sk} \sim \mathsf{Gen}(1^\lambda)$, where λ is the length of the messages being encrypted. Next, the honest challenger picks a random message $m \xleftarrow{\$} \mathcal{M}$, and samples $c \sim \mathsf{Enc}_{\mathsf{sk}}(m^{(b)})$ and $d \sim \mathsf{Enc}_{\mathsf{sk}}(m)$. The honest challenger sends (c, m, d) to the adversary and asks it to predict the bit b.

   (b) Show that the one-time pad encryption scheme is *completely* insecure for this definition. What is the advantage that you are able to obtain?