**1.** (**Of Monkey and Apes.**)

A monkey types on a 26-letter keyboard. At each keystroke, each of the 26 letters is equally likely to be hit. The monkey types $2^{20}$ letters. What is the expected number of times the sequence "ape" appears in this text? [HINT: Let $X$ be the number of occurrences. Write $X$ as the sum of indicator random variables and use linearity of expectation. This should be a very simple calculation!]

**2.** **(Much Ado About Min-Cuts.)**

Here are some problems based on the randomized min-cut algorithm discussed in class (MU Section 1.4).

(a) A graph may have more than one minimum cut. Using the analysis of the error probability of the randomized min-cut algorithm, show that the number of distinct minimum cuts is at most $\frac{n(n-1)}{2}$.

(b) Suppose that the algorithm is modified as follows. Rather than picking an *edge* uniformly at random and merging its endpoints, the algorithm picks a pair of vertices (not necessarily adjacent) u.a.r. and merges them. Give a family of connected graphs $G_n$ (where $G_n$ has $n$ vertices for each $n$) such that when the modified algorithm is run on $G_n$ the probability that it finds a minimum cut is *exponentially* small in $n$. [NOTE: By "exponentially small" we mean that the probability is less than $c^{-n}$ for some constant $c < 1$ and all sufficiently large $n$.]

(c) Show that an exponential number of repeated trials of the algorithm of part (b) would be needed in order to reduce the error probability to $\frac{1}{2}$.

**3.** **(Fixing a Broken Table.)**

We are given a function $F : \{0, \ldots, n-1\} \to \{0, \ldots, m-1\}$ with the property that all $0 \leq x, y \leq n-1$, $F((x+y) \bmod n) = (F(x) + F(y)) \mod m$. The only way we have for evaluating $F$ is to use a lookup table that stores the values of $F$. Unfortunately, an Evil Adversary has modified the values for a $1/5$ fraction of the entries in the lookup table.

[NOTE: This problem may seem a little contrived, but it is actually a very simple illustration of techniques that are used to establish the celebrated PCP Theorem!]

(a) Describe a randomized algorithm that given an input $z$, uses (at most) two lookups, and outputs a value that equals $F(z)$ with probability more than $1/2$. Your algorithm should work for every input $z$, regardless of which values the Adversary has modified.

[HINT: Your algorithm should output the correct answer as long as neither of the two entries it looks up has been modified. It should be easier to bound the probability that the algorithm makes a mistake. In addition, the following "union bound" should come in handy in the analysis: for any events $E_1, E_2$ not necessarily independent, $\Pr[E_1 \cup E_2] \leq \Pr[E_1] + \Pr[E_2]$.]

(b) Suppose you are allowed to repeat your initial algorithm three times in order to reduce the error probability. How should you combine the three values into a single output, and what is the probability that your enhanced algorithm returns the correct answer?