1. **Constructing Random Permutations.** We show how to construct a random permutation \( \pi \) on \( [n] = \{1, 2, \ldots, n\} \), given a black box that outputs numbers independently and uniformly at random from \( [k] = \{1, 2, \ldots, k\} \), where \( k \geq n \). If we compute a function \( f : [n] \rightarrow [k] \) with \( f(1), f(2), \ldots, f(n) \) all distinct, this yields a permutation; simply output the numbers \( 1, 2, \ldots, n \) in the order of the \( f(i) \) values. To construct such a function (using the black box), do the following for \( j = 1, 2, \ldots, n \):

Choose \( f(j) \) repeatedly obtaining numbers from the black box and set \( f(j) \) to be the first number found such that \( f(j) \) is different from \( f(1), \ldots, f(j-1) \).

(a) Prove that this approach gives a permutation chosen u.a.r. from all permutations.

(b) Find the expected number of calls to the black box that are needed when \( k = n \) and \( k = 2n \).

(c) For the case \( k = 2n \), argue that for each \( j \), the probability that a single call to the black box assigns a value of \( f(j) \) to \( j \) (that is, the call returns a value that is distinct from the previous assignments is \( f(1), \ldots, f(j-1) \)) is at least 1/2. Use a Chernoff bound to show that the probability that the number of calls to the black box is greater than \( 4n \) is \( 2^{-\Omega(n)} \).

[TIP: Recall the Chernoff bound: Let \( X_1, \ldots, X_n \) be independent 0-1 r.v.'s. Let \( X = X_1 + \ldots + X_n \) and \( E[X] = \mu \). Then, for \( 0 < \delta < 1 \), \( \Pr[X \leq (1 - \delta)\mu] \leq e^{-\mu\delta^2/2} \).]

2. **Routing via Bit-Fixing Can Take Exponential Time.** Consider the bit-fixing routing algorithm for routing a permutation on the \( n \)-cube. (For \( n = 4 \) and to route a packet from 0000 to 1111, the bit-fixing routing algorithm uses the path

\[
0000 \rightarrow 1000 \rightarrow 1100 \rightarrow 1110 \rightarrow 1111
\]

Suppose \( n \) is even. Write each source \( s \) as the concatenation of two binary strings \( a_s \) and \( b_s \), each of length \( n/2 \). Let the destination of \( s \)'s packet be the concatenation of \( b_s \) and \( a_s \). Show that this permutation causes the bit-fixing routing algorithm to take \( \Omega(2^{n/2}) \) steps.