CS174 Final Exam Spring 99
J. Canny May 19

This is a closed-book exam with 6 questions. You have 3 hours. All questions are worth equal points, so be sure to budget 30 minutes per question. You are allowed to use the 4 sides of notes you brought with you. No other notes are allowed. No calculators please. Write all your answers in this booklet. Good luck!

NAME_____

SID Number_____

NOTE: Please print your name and SID CLEARLY. We can't be responsible for scores for exams without a legible name.

1. Suppose you scheduled N speakers to give training talks on a Monday. Before each speaker gives their talk, they are wrapped up in last-minute preparation, so they always miss the talk of the speaker before them. Now suppose you want to schedule the same talks for the next day (Tuesday), but you want to make sure that no speaker follows the speaker that they followed on Monday. That way, every speaker can listen to every other speaker's talk on one of the two days.

   (a) Suppose you made a random permutation of the N talks on Monday to get the order for Tuesday. What is the probability that no speaker on Tuesday follows the speaker that they followed on Monday? Assume N is large.

   (b) Suppose now that each speaker also requires some time after their talk to collect their materials, so that they always miss the talk of the speaker after them (as well as the one before). What is the probability that a random permutation of the Monday talks leads to no conflicts? i.e. No two talks that were consecutive (in either order) on Monday should be consecutive on Tuesday?

   (c) Assuming a random re-ordering of the talks, what is the expected number of talks that end up in the same time slot on Monday and Tuesday? A talk is in the same time slot if it is the k^{th} talk in the Monday ordering and then the k^{th} talk in the Tuesday ordering.

2. Let X be the number of sixes that occur in N tosses of a fair six-sided die. Give Markov, Chebyshev and Chernoff bounds for the probability of at least $N/4$ sixes, i.e. $Pr[X \geq N/4]$.

   (a) Give the Markov bound for $Pr[X \geq N/4]$:

   (b) Give the Chebyshev bound for $Pr[X \geq N/4]$:

   (c) Give the Chernoff bound for $Pr[X \geq N/4]$:

3. Let G be a graph with N vertices. Initially, G has no edges, then $\binom{N}{2}$ edges are added to G at random with replacement. That is, we do the following step $\binom{N}{2}$ times: choose vertices u and $v \neq u$ at random from the vertices of G, and add edge $\{u, v\}$ (with replacement) to G.

   (a) What is the expected number of edges in G?

   (b) Now suppose we choose a random perfect matching in G (a set of $N/2$ edges with no common vertices), and contract those edges giving a new graph G'. The result will be a graph with $N/2$ vertices. Each of the new vertices represents a contraction of two of the original vertices. What is the expected number of edges in G'?

   (c) Now suppose we repeat the contraction operation above k times, giving a new graph G''. After k such contractions, the graph will have $N/2^k$ vertices, and each new vertex will represent 2^k vertices of G. How large should k be so that there is a high probability that G'' is a complete graph? Hint: think about the coupon collectors problem.

4. Suppose $n = 3^k$

   (a) What is $\phi(n)$, the order of the multiplicative group $\mathbb{Z}_n^*$?

   (b) What are the possible orders of subgroups of $\mathbb{Z}_n^*$?

   (c) Since n is a power of an odd prime, $\mathbb{Z}_n^*$ is a cyclic group, and it has at least one generator. What fraction of the elements in $\mathbb{Z}_n^*$ are generators?

5. Let $F(M, k, n)$ be the RSA encryption/decryption function:

$$F(M, k, n) = M^k (\mathrm{mod}\ n)$$

Suppose we try to use this function as a secure hash function. That is, assume the message $M \gg n$, and that k is a key which is relatively prime to $\phi(n)$. We define the hash function $H(M) = F(M, k, n)$. The desirable characteristics for a secure hash function are:

(a) A hash function $h(x)$ is said to be *one-way* if given y it is hard to find an x such that $h(x) = y$.

(b) A hash function $h(x)$ is said to be *weakly collision-free* if given a message x_1 it is hard to find another message x_2 such that $h(x_1) = h(x_2)$.

(c) A hash function $h(x)$ is said to be *strongly collision-free* if it is hard to find any pair of messages x_1, x_2 such that $h(x_1) = h(x_2)$.

Which of the three properties above does the RSA function $H(M)$ have? Explain briefly.

6. (a) Suppose a person X wants to have their friend Y cash a check at a bank. Using RSA signatures, and assuming both have published RSA public keys, explain how the check could be written so that:

   i. The bank is convinced that X wrote the check.

   ii. The bank is convinced that it was intended to be cashed by Y (and Y didnt simply steal the bits).

   iii. Y agreed to cash the check.

   iv. The person that has the bits (and comes to the bank) is Y.

   (b) Now suppose we want to do the same thing but with Y remaining anonymous. That is, X asks Y to cash a check and to satisfy the properties above, but you cannot use Y's public RSA key, or anything that identifies Y. You should still prove to the bank that the person with the bits (Y) is the same person the check was written for and that they agreed to accept it.