COMP 754 — Cryptography & Security — Aj. Phillip Rogaway
Problem Set #1 — Out: 2 July 02 — Due: 11 July 02 (in class)

For this problem set I want to see that you can write mathematically rigorous definitions. Make your English correct and precise. You may not consult any books, notes, or the web to do this assignment. Remember that you must turn in one problem set per group.

Problem 1 Give a mathematically rigorous definition for the following notions. (I am describing something only by giving a name in English; you are figuring out what I mean and telling me a mathematically precise way to fill in the "...".)

1. Let A be a finite set and let $\pi : A \to A$ be a permutation and let $x \in A$. Then *the cycle containing* x, denoted $C^\pi(x)$ is ...
2. Let A be a finite set and let $\pi : A \to A$ be a permutation and let $x \in A$. Then *the length of the cycle containing* x, denoted $c^\pi(x)$, is ...
3. Let A be a finite set and let $\pi : A \to A$ be a permutation and let $x \in A$. Then π is a *single cycle* if ...
4. Let A be a finite set and let $\pi : A \to A$ be a permutation. Then the *number of cycles of* π, denoted ncycles(π), is ...
5. Let $f : \mathbb{N} \to \mathbb{R}^+$ and $g : \mathbb{N} \to \mathbb{R}^+$ be functions and let $c \in \mathbb{R}^+$. Then $f + g$ is the function from $\mathbb{N}$ to $\mathbb{R}^+$ defined by ..., while cf is the function from $\mathbb{N}$ to $\mathbb{R}^+$ defined by ... (Note: $\mathbb{N}$ is the positive integers and $\mathbb{R}^+$ is the positive real numbers.)
6. A function $f : \mathbb{N} \to \mathbb{R}^+$ is said to be *eventually smaller than the inverse of any polynomial* (the function is *negligible*) if ...

Problem 2 Answer the following **True** or **False**, giving a proof or counterexample in each case.

1. Every $\pi \in \text{Perm}(n)$ is a single cycle.
2. If you choose a random permutation π from Perm(n) then the probability that π is a single cycle is $1/2^n$.
3. Let $x, y \in \{0,1\}^n$, $x \neq y$. If you choose a random element π from Perm(n) and a random element π' from Perm(n) then $\Pr[\pi(x) = \pi'(x)] = 1/2^n$ and $\Pr[\pi(y) = \pi'(y)] = 1/2^n$ and $\Pr[\pi(x) = \pi'(x) \text{ and } \pi(y) = \pi(y')] = 1/2^{2n}$.
4. If $f, g : \mathbb{N} \to \mathbb{R}^+$ are negligible then $f + g$ is negligible.
5. If $f : \mathbb{N} \to \mathbb{R}^+$ is negligible then $5f$ is negligible.