

Handout 4: Definitional Exercises

*Instructor: Silvio Micali**Teaching Assistant: abhi shelat*

These definitional exercises are due in class on **Monday, February 9, 2004**.

You will enjoy Monday's lecture if you turn in a solution to the following two definitional problems. You can refer to Handout 3 for a primer on our notation.

Definitional problem 1

$$\forall I_{ppt}, \forall c > 0, \exists k_c \text{ such that } \forall k > k_c \\ \Pr[x \leftarrow \{0, 1\}^k; y \leftarrow f(x); z \leftarrow I_{ppt}(y) : f(z) = y] < k^{-c}$$

Some of you objected to the fact that the parameter k_c depended on the particular inverting algorithm I_{ppt} (which, however was necessary because this algorithm could have enough states to code the value of f on all inputs of length less than some particular constant).

Try to find a "less objectionable" definition using the following suggestions:

1. An F -family of *non-uniform polynomial time machines* is an infinite sequence of machines, M_1, M_2, \dots where F is a monotonically increasing function from natural number to natural numbers, the description length of M_i is less than $F(i)$, and M_i is only run on inputs of length i and terminates in less than $F(i)$ steps.
2. Make a strong non-uniform assumption about your inverting algorithm, and remember that 2^{300} upper bounds the number of particles in the universe.

Definitional problem 2

Define a trap-door permutation using the notation given in class.