An optional exercise on OWF

A collection of functions $\{f_i : D_i \rightarrow \{0,1\}^*\}_{i \in \bar{I}}$ is called *one-way* if there exist three probabilistic polynomial-time algorithms, I, D and F, so that the following two conditions hold:

- Easy to sample and compute: The output of algorithm I, on input 1^n, is distributed over the set $\bar{I} \cap \{0,1\}^n$ (i.e., is an n-bit long index of some function). The output of algorithm D, on input (an index of a function) $i \in \bar{I}$, is distributed over the set D_i (i.e., over the domain of the function). On input $i \in \bar{I}$ and $x \in D_i$, algorithm F always outputs $f_i(x)$.
- Hard to invert: For every probabilistic polynomial-time algorithm A', every positive polynomial p and all sufficiently large n's,

$$Pr[A'(i, f_i(x)) \in f_i^{-1}(f_i(x))] < \frac{1}{p(n)},$$

  where $i = I(1^n)$ and $x = D(i)$.

1. Show how multiplying two large prime numbers is a special case of this definition.
2. Show that if such a collection exists then OWF exists.