Problem 1: Birthday attack

Implement a birthday attack for a hash function with 48 bit output. The python code in birthday.py contains template code, fill in the code for the function find_collision.

Problem 2: One-way functions

Which of the following are one-way functions? For each function that is a one-way function, explain why (no formal proof required). For each function that is not a one-way function, write an attack in Python. (Code for all the functions, including test code is provided in owf.py. You only need to fill in the functions adv i for attacking function f i.)

Hint: Out of the four functions, one is a OWF, the other three are not.

Note: Formally, of course, the question would have to be “is the function a (σ,ε)-OWF?” and σ and ε would have to be specified. I am omitting specific σ and ε, instead, you are to interpret “is an OWF” as “there is no attack in reasonable time and with reasonable success probability”.

Note: You may assume that the RSA assumption holds. And that \(E_{AES}\) is a PRF. (For reasonable σ,ε, again.)

Note: Remember that to break a one-way function, it is sufficient to find some preimage, not necessarily the “true” one that was fed into the one-way function.

(a) \(f_1(x) := 0\) for all \(x \in \{0,1\}^n\).

(b) \(f(N,e,x) := (N,e,x^e \mod N)\) where the domain of \(f\) is the set of all \((N,e,x)\) where \(N\) is an RSA modulus, \(e\) is relatively prime to \(N\), and \(x \in \{0,\ldots,N-1\}\).

(c) \(f(N,e,x) := x^e \mod N\) where the domain of \(f\) is the set of all \((N,e,x)\) where \(N\) is an RSA modulus, \(e\) is relatively prime to \(N\), and \(x \in \{0,\ldots,N-1\}\).

(d) \(f(k,x) := E_{AES}(k,x)\).