Fixed Length Collision Resistant Hash function

n=16

q=35381

g=7

h=3

Input: Two bit sequence seed (x1,x2) of length n.

Output: Returns the hash of the input string.

Algorithm:

Calculate $g^{x1}.h^{x2}$ mod q and return the hash.