Tristan Erney
December 1st, 2021
Intro to Cryptology
Hands On Exercise 14

1)

$h(x) = a^x \pmod p$ is not a good hash function since it can be seen that collisions can take place. For instance,

$2^3 \bmod 5 = 3 \pmod 5$
$3^5 \bmod 5 = 3 \pmod 5$

2)

a)

$h(x) = x^2 \pmod n$ is preimage resistant because this function has the properties of a one-way function where given x, there is no x` we can use to give us x back.

Suppose x = 8, n = 5
$8^2 \pmod 5 = 64 \pmod 5 = 4$

$4^2 \pmod 5 = 16 \pmod 5 = 1$

Even with n, we cannot determine a way using this function to get our original x value.

b)

$h(x) = x^2 \pmod n$ is not strongly collision-free because it is possible to find message m_1 and m_2 where $h(m_1) = h(m_2)$.

suppose n = 13
2 ^ 2 mod 13 = 4
3 ^ 2 mod 13 = 9
4 ^ 2 mod 13 = 3
5 ^ 2 mod 13 = 12
6 ^ 2 mod 13 = 10
7 ^ 2 mod 13 = 10
8 ^ 2 mod 13 = 12
9 ^ 2 mod 13 = 3
10 ^ 2 mod 13 = 9
11 ^ 2 mod 13 = 4
12 ^ 2 mod 13 = 1
13 ^ 2 mod 13 = 0
14 ^ 2 mod 13 = 1
15 ^ 2 mod 13 = 4
16 ^ 2 mod 13 = 9
17 ^ 2 mod 13 = 3
18 ^ 2 mod 13 = 12
19 ^ 2 mod 13 = 10
20 ^ 2 mod 13 = 10

As we can see here just from x = 2 to x = 20 there are lots of collisions

3)

This hash function satifies properties 1 and 2 since the function can be calculated quickly, and you cannot find an m` such that h(m`) = y. It does not fit category 3 since there is a chance that collisions may occur.

Suppose the block length was 8
m = “disk”
m = ‘d’ | ‘i’ | ‘s’ | ‘k’
m = 100 | 105 | 115 | 107
h(m) = 21

m = “item”
m = ‘i’ | ‘t’ | ‘e’ | ‘m’
m = 105 | 116 | 101 | 109
h(m) = 21

As we can see from the above example, from two different messages we get the same hash. Therefore, we know that property 3 doesn’t apply and collisions can still occur.