Spring 2023 - ICSI 526
Homework 4

Written by Jacob Clouse

May 11, 2023

Contents

1 Question 1

1.1 Hash function A (n = p x q)

Properties:

- One Way Property: This does satisfy the One Way Property even if we know n. We because of the Modulus, we don't know how many times the original function has 'wrapped around' so to speak. We can't predict the output.

- Weak Collision Resistance: This is NOT Weak Collision Resistant, it is possible to generate the same hash value for two different inputs. We can use -2 and 2 as our input x values and p = 107 and q = 127 for our primes. Because of the x**2, they will be the same value N = 13589 when being fed into the mod function and will output the same hash. Because for any two inputs x1 and x2, if x1 ≠ x2, then there exists a possibility that h1(x1) = h1(x2) which means that this is false.

- Strong Collision Resistance: This is NOT Strong Collision Resistant. The reason is that for any two inputs x1 and x2, the hash function h1(x) produces the same output if x1 = -x2 (mod n). That is, h1(x1) = h1(x2) if x1 ≡ -x2 (mod n). An attacker who knows the primes p and q can easily find two inputs x1 and x2 such that x1 ≡ -x2 (mod n) and then generate a collision by computing h1(x1) and h1(x2).

1.2 Hash function B ($h2(m) = M1 \oplus M2 \ldots \oplus Mn.$)

Properties:

- One Way Property: This does satisfy the One Way Property. The hash function h2(x) is one-way because given an input message m, it is computationally infeasible to determine the message m from the hash value h2(m). This is because the hash function uses the bitwise XOR operation to combine the blocks of the message, which is a one-way function.
- Weak Collision Resistance: This is Weak Collision Resistant.The hash function h2(x) is weak-collision resistant because it is computationally infeasible to find two messages m1 and m2 such that h2(m1) = h2(m2). This is because any change to the input message, no matter how small, will result in a completely different hash value due to the bitwise XOR operation.
- Strong Collision Resistance: This is NOT Strong Collision Resistant. This is because it is possible to find two messages m1 and m2 that have the same hash value h2(m1) = h2(m2) with a brute-force attack. For example, if we take the message M1 = M2 = ... = Mn = 0, then h2(m) will always be 0. Which means it is not secure for applications where strong collision resistance is required, such as in digital signatures.

2 Question 2

2.1 Design and implement a PRNG using AES (OFB mode)

Design Algo...

2.2 Calculate the Fraction of One Bits

Calculate FOOB...