CSE441: Project Proposal
Cryptanalysis of Hash Functions

Cole Johnson: cole.johnson.@student.nmt.edu
John Runyon: john.runyon@student.nmt.edu

September 11, 2024

Introduction and Outline of Project

0.1 The Basics of Hash Functions

Hashing, as an overall process, is a function that maps plaintext data of any length into a fixed-length ciphertext output–often called a digest. Hash functions, unlike encryption, destroy information encoded in the plaintext, which means the function is one-way and cannot be reversed to obtain the plaintext again.

Hash functions are a widely used cryptographic algorithm. They can be used for a variety of purposes, such as data integrity verification, password storage, and digital fingerprint/signatures, and data indexing (often called hash-tables). Since hash functions serve vital purposes in modern cryptography and computer science, knowing the important mathematical properties of a hash function (and how these can be implemented in programs) is critical to understanding their function. Once the function and real-world implementation

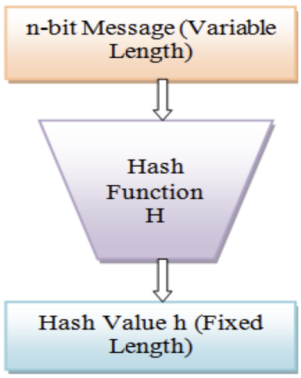

Figure 1: Basic diagram of a hash function

0.2 Outline of Project

Here is the sections of the project, along with a small description of what each of the sections would cover:

(a.) Introduction to Hash Functions

(a) Basics of Hash Functions

(b) Modern and Classic Applications of Hash Functions

(c) Hash Functions Examples (MD5, SHA-256, Tornado)

(b.) Properties of Hash Functions

(a) One-way Function (Pre-Image Resistance)

(b) Target Collision Resistance (2nd Pre-Image Resistance)

(c) Deterministic

(d) Avalanche Effect

(e) Computational Speed

(c.) Cryptanalysis and Attacks on Cryptographic Hash Functions

(a) Brute-Force Attacks

(b) One-way Function Inversion

(c) 2nd Pre-Image Resistance Attack

(d) Collision Attack