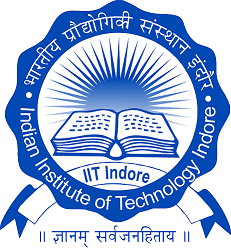
- Ishan GOEL 160001023

BITAN PAUL 160001016



CS:254 ALGORITHM DESIGN PROJECT

STUDY AND COMPARISON OF VARIOUS HASHING ALGORTIHMS

February 18, 2018

# CS:254 ALGORITHM DESIGN PROJECT

## INTRODUCTION

Since bitcoin has become the current rage, people are gravitating towards cryptocurrency which involves trading of billions of dollars and hence, security is a major issue. So, to ensure security, hash functions are extensively used.

So, it's evident from all these facts that cryptography, hashing in particular is gaining lots of ground and peaking people's interest, which makes it important for us to understand what hashing is in its true sense.

This project aims at doing the exact thing in a systematic way by studying hashing algorithms.

## PROJECT OUTLINE

The current objectives for our project are:

### OBJECTIVE 1

To study and analyse the current hashing algorithms extensively.

Analysis includes understanding the algorithm and its various aspects, advantages over previous algorithms, degree of security particular algorithm offers and any shortcomings due to which the algorithm was rendered obsolete for any outdated algorithms.

### OBJECTIVE 2

To compare the various studied algorithms in detail to understand how secure each one is, how difficult it is to one of them. /\* and understand how drawbacks are overcome for our next objective.\*/

### OBJECTIVE 3

To synthesize a hashing algorithm using the knowledge acquired from the case study of all our algorithms which will be as close to the currently used algorithm as possible after our understanding of what makes or breaks a hashing algorithm.