

Bachelor Thesis

Hash-Funktions

Marco Bellmann

May 8, 2023

Reviewers:

Professor Coja-Oghlan

Arnab Chatterjee

Technische Universität Dortmund

Fakultät für Informatik

LEHRSTUHL 2 (LS 2)

<https://eac.cs.tu-dortmund.de//>

Inhaltsverzeichnis

1	Introduction	2
2	Implementation of MD5	3
A	Weitere Informationen	4
	Abbildungsverzeichnis	5
	Algorithmenverzeichnis	7
	Literaturverzeichnis	9
	Erklärung	9

Kapitel 1

Introduction

1. Introduction
2. about hashfunctions
3. about md5
4. about collisions
5. goals and motivation
6. notation explained
7. Definition of md5
8. impelmentation of md5
 - (a) padding (difficulties, missing by stevens)
 - (b) processing
 - (c) md5compress
 - (d) representation
 - (e) potential for improvement
 - (f) difficulties
9. attack of md5

Kapitel 2

Implementation of MD5

Anhang A

Weitere Informationen

Abbildungsverzeichnis

Algorithmenverzeichnis

Literaturverzeichnis

Hiermit versichere ich, dass ich die vorliegende Arbeit selbstständig verfasst habe und keine anderen als die angegebenen Quellen und Hilfsmittel verwendet sowie Zitate kenntlich gemacht habe.

Dortmund, den 8. Mai 2023

Muster Mustermann

