ИЗЈАВА

Студент: Ненад Тофоровић

Број индекса: 77 РН

Студијски програм: рачунарске науке

Наслов мастер рада: Имплементација савремених алгоритама шифровања

Ментор мастер рада: Јелена Ићтовић

Изјављујем да без сагласности ментора резултати мастер рада неће бити публиковани у стручном или научном часопису нити саопштени на научном скупу/конференцији.

У Нишу, 12.12.2023

Потпис

ОБАВЕШТЕЊЕ О ОДБРАНИ МАСТЕР РАДА

Име:	Ненад
Презиме:	Тодоровић
Број индекса:	77 РН
Департман:	рачунарске науке
Тема мастер рада:	Имплементација савремених алгоритама шифровања
Ментор:	Јелена Игнатовић
Датум одбране:	29.12.2023.
Време одбране:	11:30
Место одбране:	Црвена сала

Датум:	**Потпис студента:**
12.12.2023.	НТ

ПРИРОДНО - МАТЕМАТИЧКИ ФАКУЛТЕТ
НИШ

КЉУЧНА ДОКУМЕНТАЦИЈСКА ИНФОРМАЦИЈА

Редни број, **РБР**:	
Идентификациони број, **ИБР**:	
Тип документације, **ТД**:	монографска
Тип записа, **ТЗ**:	текстуални / графички
Врста рада, **ВР**:	мастер рад
Аутор, **АУ**:	Ненад Тодоровић
Ментор, **МН**:	Јелена Игњатовић
Наслов рада, **НР**:	Имплементација савремених алгоритама шифровања
Језик публикације, **ЈП**:	Српски
Језик извода, **ЈИ**:	Енглески
Земља публиковања, **ЗП**:	Р. Србија
Уже географско подручје, **УГП**:	Р. Србија
Година, **ГО**:	2023
Издавач, **ИЗ**:	ауторски репринт
Место и адреса, **МА**:	Ниш, Вишеградска 33.
Физички опис рада, **ФО**: (поглавља/страна/ цитата/табела/слика/графика/прилога)	4, 7, 8, 14, 15, 16, 17, 18, 24, 25, 26, 27, 28, 29, 30, 31, 35, 38, 39, 42, 43 стр. ; граф. прикази
Научна област, **НО**:	рачунарске науке
Научна дисциплина, **НД**:	криптографија
Предметна одредница/Кључне речи, **ПО**:	алгоритам/протокол
УДК	004.056.55
Чува се, **ЧУ**:	Библиотека
Извод, **ИЗ**:	Рад се бави алгоритмима шифровања и протоколима који омогућавају имплементацију тих алгоритама у савременим софтверима. У уводној глави се описују почеци криптографије, а онда и дефинишу основни појмови. Потом се даје објашњење математичких појмова потребних за разумевање алгоритама. Након тога следе DES и AES алгоритми, а потом глава Криптографски протоколи са посебним осврtом на Дифи-Хелман протокол. На крају рада приказују се имплементације DES и CAES алгоритама, као и Дифи-Хелман протокола.
Датум прихватања теме, **ДП**:	

Датум одбране, ДО:		
Чланови комисије, КО:	Председник:	
	Члан:	
	Члан, ментор:	

ПРИРОДНО - МАТЕМАТИЧКИ ФАКУЛТЕТ
НИШ

KEY WORDS DOCUMENTATION

Accession number, **ANO**:	
Identification number, **INO**:	
Document type, **DT**:	**monograph**
Type of record, **TR**:	**textual / graphic**
Contents code, **CC**:	master degree thesis
Author, **AU**:	Nenad Todorovic
Mentor, **MN**:	Jelena Ignjatovic
Title, **TI**:	Implementation of modern encription algoritms
Language of text, **LT**:	**Serbian**
Language of abstract, **LA**:	**English**
Country of publication, **CP**:	**Republic of Serbia**
Locality of publication, **LP**:	**Serbia**
Publication year, **PY**:	2023
Publisher, **PB**:	**author's reprint**
Publication place, **PP**:	**Niš, Višegradska 33.**
Physical description, **PD**: (chapters/pages/ref./tables/pictures/graphs/appendixes)	4, 7, 8, 14, 15, 16, 17, 18, 24, 25, 26, 27, 28, 29, 30, 31, 35, 38, 39, 42, 43 p. ; graphic representations
Scientific field, **SF**:	computer science
Scientific discipline, **SD**:	cryptography
Subject/Key words, **S/KW**:	algorithm/protocol
UC	004.056.55
Holding data, **HD**:	**library**
Note, **N**:	
Abstract, **AB**:	Topics of this paper are encryption algorithms and cryptographic protocols that enable implementation of those algorithms in modern software. In opening chapter we describe beginnings of cryptography and give definitions of basic terms. After that we give an explanation of mathematical concepts needed for better understanding of algorithms. In next two chapters we describe DES and AES algorithms, and after that cryptographic protocols, with emphasis on Diffie-Hellman protocol. In the end of the paper, we show implementations of DES, SAES and Diffie-Helman protocol.

Accepted by the Scientific Board on, **ASB**:		
Defended on, **DE**:		
Defended Board, **DB**:	President:	
	Member:	
	Member, Mentor:	