

Střední průmyslová škola Třebíč

Maturitní práce

Hashtesting

Profilová část maturitní zkoušky

Studijní obor: Informační technologie

Třída: ITA4

Školní rok: 2024/2025 Kamil Franek

Zadání práce

ABSTRAKT

Maturitní práce na téma hashování, jeho využití a typy hashovacích algoritmů. Zabývá se problematikou spojenou s hashováním a vysvětlení použití hashování v IT. Tento dokument popisuje použitou technologii, praktiky a vytváření samotného programu a všeho okolo. Výsledný program disponuje základními i rozšířenými funkcemi práce s hashem a soubory pro zvýšení efektivity práce. Dále disponuje okénkem pro informace, vysvětlení rozdílů mezi hashovacími algoritmy, rozdíl mezi použitím a nepoužitím soli a dále za účelem zvýšení chápání daného téma pro uživatele.

KLÍČOVÁ SLOVA

Maturitní práce, Password JailBreak, Výuka, Hash

ABSTRACT

\*abstrakt anglicky\*

KEYWORDS

Graduation thesis, Password JailBreak, Teaching, Hash

PODĚKOVÁNÍ

Děkuji Ing. Ladislavu Havlátu a oponentu Ing. Drahomíru Škárkovi za cenné připomínky a rady, které mi poskytli při vypracování maturitní práce.

V Třebíči dne 10. října 2024 podpis autora

PROHLÁŠENÍ

Prohlašuji, že jsem tuto práci vypracoval/a samostatně a uvedl/a v ní všechny prameny, literaturu a ostatní zdroje, které jsem použil/a.

V Třebíči dne 10. října 2024

podpis autora

Obsah

[Úvod 6](#_Toc147495618)

[1 Struktura maturitní práce 7](#_Toc147495619)

[1.1 Titulní list 7](#_Toc147495620)

[1.2 Zadání maturitní práce 7](#_Toc147495621)

[1.3 Abstrakt 7](#_Toc147495622)

[1.4 Klíčová slova 7](#_Toc147495623)

[1.5 Poděkování a prohlášení 8](#_Toc147495624)

[1.5.1 Poděkování 8](#_Toc147495625)

[1.5.1 Prohlášení 8](#_Toc147495626)

[2 Textová část 9](#_Toc147495627)

[2.1 Styly 9](#_Toc147495628)

[2.1.1 Řádkování 9](#_Toc147495629)

[2.1.2 Zvýrazňování textu 9](#_Toc147495630)

[2.1.3 Členění textu 9](#_Toc147495631)

[2.1.4 Číslování stran 9](#_Toc147495632)

[2.2 Vytvoření obsahu 10](#_Toc147495633)

[2.3 Psaní úvodu 10](#_Toc147495634)

[2.4 Struktura odstavců 11](#_Toc147495635)

[2.5 Obrázky, tabulky a rovnice 11](#_Toc147495636)

[2.6 Řazení a struktura kapitol 13](#_Toc147495637)

[2.7 Závěr 13](#_Toc147495638)

[2.8 Seznam použitých zdrojů 13](#_Toc147495639)

[2.9 Seznam použitých symbolů a zkratek 13](#_Toc147495640)

[2.10 Seznamy použitých obrázků a tabulek 14](#_Toc147495641)

[2.11 Seznam příloh 14](#_Toc147495642)

[Závěr 15](#_Toc147495643)

[Seznam použitých zdrojů 16](#_Toc147495644)

[Seznam použitých symbolů a zkratek 17](#_Toc147495645)

[Seznam obrázků 18](#_Toc147495646)

[Seznam tabulek 19](#_Toc147495647)

[Seznam příloh 20](#_Toc147495648)

Úvod

Cílem této práce a programu je zjednodušení práce s hashema, ukázku rozdílů mezi hashovacími algoritmy, použití a nepoužití soli, postupné hashování pomocí mezikroků, silné a slabé stránky hashů a kde a proč se používají. Dále program obsahuje test prolomení hesla (jailbreak) pomocí hrubého útoku. V dokumentu jsou popsány použité programy a technologie, jak jsou použité a proč jsou použité. V praktické části je popsána celá cesta dělání programu, hlavní problémy, trable a vysvětlení fungování celého programu s ukázkami samotného kódu, testování a různé obrázky z pracovního postupu. V závěru jsou popsány moje pocity z práce na projektu a spokojenost s finální verzí programu.

# Struktura maturitní práce

Práce se předkládá ve formátu A4 na výšku, psaná textovým editorem v elektronické podobě. Součástí práce je titulní strana a obsah. Okraje se volí širší levý okraj, tedy vlevo 4 cm, nahoře a dole 3 cm, vpravo 2,5 cm, zápatí pro číslování stránek 1,25 cm, což odpovídá přibližně rozsahu 80 znaků na řádek včetně mezer a 30 řádků na stránku.

Záhlaví je prázdné. Zápatí obsahuje číslování stránek zarovnané na střed. První číslovanou stranou je stránka s úvodem.

## Titulní list

Titulní list maturitní práce změňte. Obsahuje název školy s logem, text Maturitní práce, název práce, Profilová část maturitní zkoušky, studijní obor, třídu, školní rok, jméno a příjmení autora.

## Zadání maturitní práce

Zadání maturitní práce autorů je k nalezení v Moodle. Stáhněte si ho ve formátu pdf. Převeďte ho do formátu obrázku jpg nebo png. A vložte na dané místo v dokumentu, je změněno obtékání textu obrázku na obdélníkové (popřípadě odškrtnuto posouvání s textem) a obrázek je roztažen přes celou první stranu.

## Abstrakt

## Klíčová slova

Klíčová slova jsou slova či sousloví vystihující danou problematiku. Běžný počet klíčových slov je okolo pěti. Není vhodné používat příliš mnoho klíčových slov. Snažte se využít co nejvýstižnější klíčová slova. Klíčová slova se píšou malými písmeny, která jsou odděleny čárkami, za posledním slovem není čárka ani tečka Abstrakt a klíčová slova včetně anglické verze překladu jsou umístěny na jedné straně.

## Poděkování a prohlášení

Poděkování se píše v horní části stránky a prohlášení v dolní části stejné stránky.

### Poděkování

Tato část není povinná (lze ji zcela odstranit), nicméně je doporučeno poděkovat vedoucímu práce. Lze také uvést jména členů rodiny nebo obecně kohokoliv, kdo významným způsobem napomohl v řešení práce. Ručně psaný podpis je pouze v tištěné podobě.

### Prohlášení

Tuto část není nutné upravovat. Pouze část *vypracoval/a, uvedl/a, použil/a* může být autory upravena tak, aby gramaticky korespondovala s jejich pohlavím.

# Textová část

Celý text je psán fontem Times New Roman. Použitá velikost písma je 12pt kromě nadpisů a je užito řádkování 1,5. K tomu je v této šabloně určen styl *Normální*. Minimální rozsah maturitní práce (úvod, vlastní text práce a závěr) je 15 stran. Jednou stranou je myšlena jedna normostrana, jež má 1800 znaků včetně mezer (tj. přibližně 250 slov). Minimální rozsah maturitní práce je tedy přibližně 3750 slov. [2]

## Styly

Normální velikost 12pt

Nadpis 1 velikost 20pt, tučně

Nadpis 2 velikost 16pt, tučně

Nadpis 3 velikost 14pt, tučně

### Řádkování

Pro vizuální rozdělení nadpisu kapitol a textu se doporučuje před nadpisy kapitol vložit 12 bodů, za nadpisy kapitol 6 bodů, mezi jednotlivé odstavce v textu se vkládá 6 bodů. Mezi odstavce se tedy nevkládá prázdný řádek prostřednictvím ENTERu, ale prostřednictvím odsazení odstavce. Řádkování v základním textu (styl normální) velikost 1,5 bodů.

### Zvýrazňování textu

Důležité myšlenky zvýrazňovat pomocí **tučného** písma nebo *kurzívou* nepoužívat podtržení. Používat jednotnou barvu písma, doporučuje se černá.

### Členění textu

Zarovnání textu do bloku (vpravo i vlevo). Nepoužívat odsazení textu. Číslování kapitol od čísla 1. Za nadpisy kapitol se neuvádí dvojtečka, ani tečka, ani zdroj. Hlavní kapitoly začínají na nové stránce. Ostatní podkapitoly se oddělují od konce předcházející kapitoly mezerou o velikosti 12 bodů.

### Číslování stran

Strany číslovat dole uprostřed. Strany se počítají od titulního listu, uvádějí se však až od vlastního textu (počínaje úvodem) – tedy první uváděné číslo může být např. 6.

## Vytvoření obsahu

Obsah se tvoří automaticky dle užitých stylů. Styly *Nadpis 1*, *Nadpis 2* a *Nadpis 3* slouží k víceúrovňovému vrstvení kapitol. Styl *NadpisBezObs* se v obsahu nezobrazí (viz strana 4, 5 – nadpisy nejsou v obsahu). Z hlediska přehlednosti není doporučeno využívat více než tři úrovně nadpisů. Pro projevení změn je nutné obsah ručně aktualizovat.



Obr. 2.1 Obsah

Text obsahu se píše od jednotné svislice (se zřetelem k nejdelšímu číselnému označení).

## Psaní úvodu

Úvod může být osobitějšího rázu. První odstavec by měl obsahovat motivaci či důvod, který autora přiměl k volbě daného tématu s ohledem na přínos práce. V dalších odstavcích může být popsán obsah jednotlivých kapitol.

## Struktura odstavců

V případě, že věta vychází se spojkou na konci řádku, je spojka vždy přesunuta pomocí Shift + Enter na následující řádek. Hodnoty s jednotkami musí mít mezi číslem a označením jednotky jednu mezeru. To lze uskutečnit pomocí Shift + Ctrl + Mezerník (tzv. pevná mezera).

Text práce by měl být napsán v neutrální formě, tj. ve 3. osobě v trpném rodě. V textu by se neměli objevovat slangové výrazy, citově zabarvená slova ani podmiňovací způsob (s výjimkou je-li, uvažujeme-li apod.). Autor by se měl vyhnout přílišnému opakování slov či užívání nadbytečných výrazů.

Forma textu:

* v neurčité formě (bylo zjištěno, navrhuje se…);
* v 1.  osobě jednotného čísla (zjistil jsem, navrhuji …) – zvláště vhodné v kapitolách, které jsou vlastní prací autora.

## Obrázky, tabulky a rovnice

Popisek obrázku a tabulky se vkládá kliknutím pravého tlačítka myši na objekt a výběrem možnosti *Vložit titulek*. Následně je vybrán typ objektu (*Tab.* nebo *Obr.*) a jeho poloha (obrázky pod objekt, tabulky nad objekt). Styl popisku je Times New Roman 11 kurzíva uprostřed. Seznamy obrázků a tabulek na konci dokumentu jsou automaticky vygenerovány. Obrázky a tabulky mají vždy i slovní popis a rovnice jsou bez slovního popisu. Za titulek obrázku nepatří tečka. [3] Číslování obrázků, tabulek a rovnic je provedeno dle **hlavní kapitoly**, v níž se vyskytují a jejich pořadí v této kapitole. Nástroj *Vložit Titulek* čísluje popisky obrázků a tabulek automaticky. V případě že dojde k editaci, odstranění nebo přesunu již existujícího popisku je nutné dokument aktualizovat. Pro samotné vkládání rovnic je užit nástroj *Rovnice* v záložce *Vložení* (rovnice jsou vždy psány kurzívou).

|  |  |
| --- | --- |
|  |  |

Vzorec pro měření entropie. Rovnice jsou bez slovního popisu.



Obr. 2.2 Příklad umístění legendy obrázku

Titulek ke grafu a obrázku se píše pod objekt.

Tab. 2.1 Legenda k tabulce

|  |  |  |  |
| --- | --- | --- | --- |
| Jméno | Příjmení | Body | Známka |
| Petr | Novák | 25 | 4 |
| Karel | Kolář | 36 | 3 |
| Martin | Pokorný | 89 | 1 |

Titulek tabulky se píše nad tabulku.

Vložený objekt musí být vždy okomentován. Je nutné napsat před a za objekt alespoň jeden odstavec textu.

## Řazení a struktura kapitol

Z hlediska přehlednosti každá nová kapitola (Nadpis 1) začíná na novém listu. První kapitola bývá zaměřena na rešeršní část, tedy definice pojmů, vymezení studované oblasti apod. Druhá a následující kapitoly jsou zaměřeny na řešení samotného problému.

## Závěr

Závěr obsahuje stručné shrnutí získaných poznatků, uvedení dalších možných postupů či řešení, hodnocení dostupné odborné literatury, ze které bylo čerpáno. Závěr by měl obsahovat kritické porovnání záměru práce a dosažených výsledků, srovnání dosažených výsledků s dosud známými poznatky a popis odlišností od doposud známých skutečností. Závěr může naznačit praktické uplatnění výsledků práce.

## Seznam použitých zdrojů

Účelem této části je zaznamenání publikací, jež byly využity v maturitní práci.

Citace se řídí normou ČSN ISO 690 Bibliografické citace. [1] V případě doslovné citace je potřebné citovaný text graficky odlišit od ostatního textu, ohraničit apostrofem, případně ještě kurzívou. Odkaz na citovaný zdroj, jehož plná citace bude uvedena v soupisu literatury na konci práce, se uvede přímo za doslovně citovaný text.

Citování zdrojů se provádí v hranatých závorkách, používá se metoda číselných odkazů. Tento seznam je vždy seřazen dle výskytu citací v textu práce. Necitování použité literatury je považováno za plagiátorství.

## Seznam použitých symbolů a zkratek

Seznam symbolů a zkratech je vytvořen pomocí tabulky. Zkratky a názvy veličin jsou psány stylem *Normální* a jednotky jsou vytvořeny pomocí nástroje *rovnice*. Pro přidání řádku je potřeba kliknout pravým tlačítkem myši do posledního řádku tabulky a z nabídky *vložit* vybrat možnost *vložit pod*. Pro odstranění pak obdobně vybrat možnost *odstranit celý řádek*.

## Seznamy použitých obrázků a tabulek

Tyto seznamy se vytvářejí automaticky dle použitých stylů. Seznamy je potřeba aktualizovat kliknutím pravého tlačítka myši na první položku seznamu a následným výběrem možnosti aktualizovat pole (nebo kliknutím na první položku seznamu a stiskem F9).

## Seznam příloh

Seznam příloh je nutné vyplnit ručně.

Závěr

Vytvořená šablona maturitních prací obsahuje formální požadavky maturitních prací na SPŠT Třebíč. Jedná se zejména o upravené styly v dokumentu, podrobný popis jednotlivých částí maturitní práce a jejího obsahu, snadno editovatelné záhlaví a zápatí s automatickým číslováním stránek a propojení stylů se seznamy a obsahem.

Seznam použitých zdrojů

1. Citace.com. *Výklad normy ČSN ISO 690*. Online. Brno: Citace.com, 2023. Dostupné z: <https://www.citace.com/Vyklad-CSN-ISO-690-2022.pdf>. [cit. 2023-10-04].
2. Didacticus. *Normostrana: kolik má znaků, jak zjistit jejich počet a další důležité informace.* Online. Praha: Didacticus, c2011-2020. Dostupné z: <https://didacticus.cz/normostrana>. [cit. 2023-09-11].
3. Ústav pro jazyk český AV ČR. *Tečka.* Online. Internetová jazyková příručka. Praha: Ústav pro jazyk český AV ČR, 2008-2023. Dostupné z: <https://prirucka.ujc.cas.cz/>. [cit. 2023-10-04].

Seznam použitých symbolů a zkratek

|  |  |  |
| --- | --- | --- |
| Symbol | Veličina | Jednotka |
| S | Entropie |  |
| Q | Teplo |  |
| T | Termodynamická teplota |  |
| t | Čas |  |
|  |  |  |

Seznam obrázků

[Obr. 2.1 Obsah 10](#_Toc147493921)

[Obr. 2.2 Příklad umístění legendy obrázku 12](#_Toc147493922)

Seznam tabulek

[Tab. 2.1 Legenda k tabulce 12](#_Toc147493615)

Seznam příloh

Prázdná šablona maturitní práce