SLOVAK UNIVERSITY OF TECHNOLOGY IN BRATISLAVA
FACULTY OF ELECTRICAL ENGINEERING AND INFORMATION TECHNOLOGY

Registration number: FEI-xxxx-xxxx

ELLIPTIC CURVE CRYPTOGRAPHY

BACHELOR'S THESIS

2024 **Erik Ziman**

SLOVAK UNIVERSITY OF TECHNOLOGY IN BRATISLAVA
FACULTY OF ELECTRICAL ENGINEERING AND INFORMATION TECHNOLOGY

Registration number: FEI-xxxx-xxxx

ELLIPTIC CURVE CRYPTOGRAPHY

BACHELOR'S THESIS

Study Programme:	Applied Informatics
Study Field:	Computer Science
Training Workplace:	Institute of Computer Science and Mathematics
Supervisor:	Mgr. Ing. Peter Párker, PhD.
Consultant:	

Bratislava 2024 **Erik Ziman**

SÚHRN

SLOVENSKÁ TECHNICKÁ UNIVERZITA V BRATISLAVE
FAKULTA ELEKTROTECHNIKY A INFORMATIKY

Študijný program:	Aplikovaná informatika
Autor:	Erik Ziman
Bakalárska práca:	Elliptic curve cryptography
Vedúci záverečnej práce:	Mgr. Ing. Peter Párker, PhD.
Konzultant:	
Miesto a rok predloženia práce:	Bratislava 2024

Lorem ipsum dolor sit amet, consectetuer adipiscing elit. Aenean et est a dui semper facilisis. Pellentesque placerat elit a nunc. Nullam tortor odio, rutrum quis, egestas ut, posuere sed, felis. Vestibulum placerat feugiat nisl. Suspendisse lacinia, odio non feugiat vestibulum, sem erat blandit metus, ac nonummy magna odio pharetra felis. Vivamus vehicula velit non metus faucibus auctor. Nam sed augue. Donec orci. Cras eget diam et dolor dapibus sollicitudin. In lacinia, tellus vitae laoreet ultrices, lectus ligula dictum dui, eget condimentum velit dui vitae ante. Nulla nonummy augue nec pede. Pellentesque ut nulla. Donec at libero. Pellentesque at nisl ac nisi fermentum viverra. Praesent odio. Phasellus tincidunt diam ut ipsum. Donec eget est. A skúška mäkčeňov a dĺžnov.

Kľúčové slová: kľúčové slovo1, kľúčové slovo2, kľúčové slovo3

ABSTRACT

SLOVAK UNIVERSITY OF TECHNOLOGY IN BRATISLAVA
FACULTY OF ELECTRICAL ENGINEERING AND INFORMATION TECHNOLOGY

Study Programme:	Applied Informatics
Author:	Erik Ziman
Bachelor's thesis:	Elliptic curve cryptography
Supervisor:	Mgr. Ing. Peter Párker, PhD.
Consultant:	
Place and year of submission:	Bratislava 2024

On the other hand, we denounce with righteous indignation and dislike men who are so beguiled and demoralized by the charms of pleasure of the moment, so blinded by desire, that they cannot foresee the pain and trouble that are bound to ensue; and equal blame belongs to those who fail in their duty through weakness of will, which is the same as saying through shrinking from toil and pain. These cases are perfectly simple and easy to distinguish. In a free hour, when our power of choice is untrammelled and when nothing prevents our being able to do what we like best, every pleasure is to be welcomed and every pain avoided. But in certain circumstances and owing to the claims of duty or the obligations of business it will frequently occur that pleasures have to be repudiated and annoyances accepted. The wise man therefore always holds in these matters to this principle of selection: he rejects pleasures to secure other greater pleasures, or else he endures pains to avoid worse pains.

Keywords: keyword1, keyword2, keyword3

Acknowledgments

I would like to express a gratitude to my thesis supervisor.

Contents

List of Figures and Tables

List of Abbreviations

CDMA	Code Division Multiple Access
GSM	Global System for Mobile communication
HW	Halo Wars
SW	Star Wars

List of Algorithm

List of listings

Introduction

Tu bude krasny uvod s diakritikou atd.
A mozno aj viac riadkovy uvod.

1 Ukážka glossaries

Verzia FEIstyle 1.5 používa glossary[1] balík. Code Division Multiple Access (CDMA) je dlhá skratka, naopak GSM je skratka v krátkej forme.

Ukážka druhého odseku spolu s medzerou a odsadením. Všimnite si, že ten to riadok je odsadený, zatiaľ čo prvý nie je. Je to pretio, lebo prvý riadok je vizuálne oddelený medzerou od nadpisu a nie je potrebné ďalšie oddelenie.

[1] `https://www.ctan.org/pkg/glossaries?lang=en`

2 Recitácia

Citujem všetky zdroje v **bibliography.bib** [1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16].
Good luck.

3 Možnosti anonymizácie

Anonymizácia znamená zmena alebo úprava údajov tak, aby sa podľa nich nedala jednoznačne určiť osoba, ktorej tieto údaje patria [2]. Existuje niekoľko spôsobov, ktorými môžeme dosiahnuť rôznu úroveň anonymizácie na internete: od mazania cookies súborov po ukončení prehliadania webových stránok až po používanie operačných systémov, ktoré sú na anonymite založené; od bezplatných možností až po komerčné verzie.
Nasleduje priblíženie niektorých možnosti anonymizácie.

3.1 Súkromné prehliadanie

Najpoužívanejšie internetové prehliadače súčasnosti majú v sebe zabudovanú funkcionalitu, ktorá dokáže čiastočne anonymizovať prístup na internet. Táto funkcionalita blokuje ukladanie navštívených stránok do histórie a nezaznamenáva súbory, ktoré sa stiahnu z internetu. SW a Halo Wars sú skratky.

3.2 Anonymná sieť

Anonymná sieť je sieť serverov, medzi ktorými dáta prechádzajú šifrované. V anonymných sieťach dáta prechádzajú z počítača používateľa, odkiaľ bola požiadavka poslaná, cez viaceré proxy smerovače, z ktorých každý správu doplní o smerovanie a zašifruje vlastným kľúčom. Cesta od...

3.3 Funkcionalita

Rozšírenie tiež okrem splnenia špecifikácie malo pre prehľadnosť a overenie funkčnosti zobrazovať údaje, ktoré boli na server odoslané. Zoznam údajov odoslaných na server, sa mal ukladať do krátkodobej histórie, aby nemal používateľ k dispozícií len najnovšie údaje, ale aj údaje odoslané v nejakom časovom období. Nejaký listing z príloh C.1.

3.3.1 Funkcionalita2

Samozrejmosťou bolo nastavenie zapnutia rozšírenia pri štarte, prípadne interval zmeny odosielaných údajov.

3.4 Vzhľad

Dôležitou požiadavkou kladenou na rozšírenie bolo príjemné používateľské rozhranie. Z tohto dôvodu malo rozšírenie obsahovať zoznam modifikovaných vlastností a tlačidlo

Table 1: Moduly a ich funkcie pri anonymizácii

	Funkcia													
						Modifikácia								
Modul	zobrazenie hlavičky	blokovanie skriptov	zmena IP	zmena lokalizácie	zmazanie/blokovanie cookies	blokovanie trackerov	popis	používateľský agent	kódové označenie prehliadača	názov prehliadača	verzia prehliadača	platforma	výrobca prehliadača	označenie výrobcu prehliadača
User agent switcher							X	X	X	X	X	X	X	X
Ghostery					X	X								
Better privacy					X									
Anonymox			X	X	X		X	X						
Modify headers					X			X						
Request policy						X								
Live HTTP headers	X													
User agent awitcher							X	X						
Header hacker							X	X	X	X	X	X	X	X
Mod header							X	X	X	X	X	X	X	X
Script no		X												
No script		X												
Proxify it			X	X										
I'm not here				X										
Get edition		X	X	X	X	X								

Table 2: Príklad tabuľky s použitím balíka `booktabs`

Veľkosť (B)	Typ správy
8	Nejaký typ správy

pre prístup k nastaveniam rozšírenia v jednoduchej a praktickej forme. Predpokladaný vzhľad je zobrazený na obrázku č. 1. Dôležitou požiadavkou kladenou na rozšírenie bolo

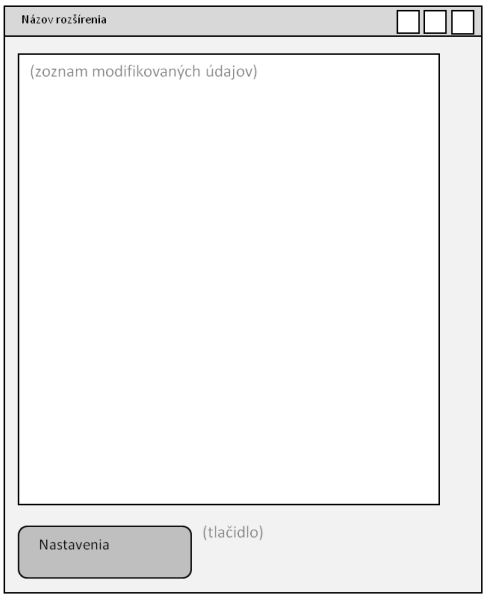

Figure 1: Predpokladaný vzhľad rozšírenia.

príjemné používateľské rozhranie [1]. Z tohto dôvodu malo rozšírenie obsahovať zoznam modifikovaných vlastností a tlačidlo pre prístup k nastaveniam rozšírenia v jednoduchej a praktickej forme. Predpokladaný vzhľad je zobrazený na obrázku č. 1.

```
/* Hello World program */

#include<stdio.h>

struct cpu_info {
    long unsigned utime, ntime, stime, itime;
    long unsigned iowtime, irqtime, sirqtime;
};

main()
{
    printf("Hello World");
}
```

Listing 1: Ukážka výpisu programového kódu

Algorithm 1 Ukážka príkazov pre algorithmic

```
  <text>
  if <condition> then
    <text>
  else
    <text>
  end if
  if <condition> then
    <text>
  else if <condition> then
    <text>
  end if
  for <condition> do
    <text>
  end for
  for <condition> to <condition> do
    <text>
  end for
  for all <condition> do
    <text>
  end for
  while <condition> do
    <text>
  end while
  repeat
    <text>
  until <condition>
  loop
    <text>
  end loop
Require: <text>
Ensure: <text>
  return <text>
  print <text> {<text>} and , or , xor , not , to , true, false
```

Conclusion

Conclusion is going to be where?

Here.

Bibliography

1. BRATKOVÁ, Eva (comp.). *Metody citování literatury a strukturování bibliografických záznamů podle mezinárodních norem ISO 690 a ISO 690-2: metodický materiál pro autory vysokoškolských kvalifikačních prací* [online]. Verze 2.0, aktualiz. a rozšíř. Praha: Odborná komise pro otázky elektronického zpřístupňování vysokoškolských kvalifikačních prací, Asociace knihoven vysokých škol ČR, 2008-12-22 [visited on 2011-02-02]. Available from: `http://www.evskp.cz/SD/4c.pdf`.
2. BORGMAN, Christine L. *From Gutenberg to the global information infrastructure: access to information in the networked world*. First. Cambridge (Mass): The MIT Press, 2003. ISBN 0-262-52345-0.
3. GREENBERG, David. Camel drivers and gatecrashers: quality control in the digital research library. In: HAWKINS, B.L and BATTIN, P (eds.). *The mirage of continuity: reconfiguring academic information resources for the 21st century*. Washington (D.C.): Council on Library and Information Resources; Association of American Universities, 1998, pp. 105–116.
4. LYNCH, C. Where do we go from here?: the next decade for digital libraries. *DLib Magazine* [online]. 2005, vol. 11, no. 7/8 [visited on 2005-08-15]. ISSN 1082-9873. Available from: `http://www.dlib.org/dlib/july05/lynch/07lynch.html`.
5. DĚŤA, Hugh and RYCHLÍK, Tomáš. *A big paper: Podtitul* [online]. 2nd ed. Praha: Academia, 1991 [visited on 2011-01-12]. Pokusná edice. ISBN 978-80-8149-080-4. Available from: `http://pokus.cz`.
6. DĚŤA, Hugh, RYCHLÍK, Tomáš, DALŠÍ, Pepa, SPOUSTA, Pepa, SKORO, Moc, ALE, Nestačí and HODNĚ. *Úplně úžasná knížka*. 3rd ed. Praha, 1991.
7. DĚŤA, Hugh, RYCHLÍK, Tomáš, DALŠÍ, Pepa, SPOUSTA, Pepa, SKORO, Moc, ALE, Nestačí and HODNĚ. *Úplně úžasná knížka*. 3rd ed. Praha: MIT Press, 1991.
8. FREELY, I.P. A small paper: Podtitulek. *The journal of small papers*. 1997, vol. 1, no. 3, pp. 2–5. to appear.
9. JASS, Hugh. A big paper. *The journal of big papers*. 1991, vol. 23.
10. Titulek. *The journal of big papers*. 1991, vol. 12, no. 2, pp. 22–44. Available from DOI: `10.112.22/jkn`.

11. KOLLMANNOVÁ, Ludmila, BUBENÍKOVÁ, Libuše and KOPECKÁ, Alena. *Angličtina pro samouky*. 5th ed. Praha: Státní pedagogické nakladatelství, 1977. Učebnice pro samouky, no. 4. ISBN 80-04-25663-5.

12. NOVOTNÁ, Pepina. Podkapitola. In: KOLLMANNOVÁ, Ludmila, BUBENÍKOVÁ, Libuše and KOPECKÁ, Alena. *Angličtina pro samouky*. 5th ed. Praha: Státní pedagogické nakladatelství, 1977, chap. 2., pp. 22–29. Učebnice pro samouky, no. 4. ISBN 80-04-25663-5.

14. KNUTH, Donald. Journeys of TEX. *TUGBoat*. 2003– , vol. 17, no. 3, pp. 12–22. ISSN 1222-3333. Available also from: `http://tugboat.tug.org/kkk.pdf`.

15. GENIÁLNÍ, Jiří (ed.). *Mimořádně užitečný sborník*. Praha: Academia, 2007. ISBN 978-80-8149-080-4.

16. VLAŠTOVKA, Josef. Velmi zajímavý článek. In: GENIÁLNÍ, Jiří (ed.). *Mimořádně užitečný sborník*. Praha: Academia, 2007, pp. 22–45. ISBN 978-80-8149-080-4.

Appendix

A Štruktúra elektronického nosiča

/CHANGELOG.md

· file describing changes made to FEIstyle

/example.tex

· main example *.tex* file for diploma thesis

/example_paper.tex

· example *.tex* file for seminar paper

/Makefile

· simply Makefile – build system

/fei.sublime-project

· is project file with build in Build System for Sublime Text 3

/img

· folder with images

/includes

· files with content

/bibliography.bib

· bibliography file

/attachmentA.tex

· this very file

B Algoritmus

Algorithm B.1 Vypočítaj $y = x^n$

Require: $n \geq 0 \vee x \neq 0$

Ensure: $y = x^n$

```
y ⇐ 1
if n < 0 then
    X ⇐ 1/x
    N ⇐ −n
else
    X ⇐ x
    N ⇐ n
end if
while N ≠ 0 do
    if N is even then
        X ⇐ X × X
        N ⇐ N/2
    else {N is odd}
        y ⇐ y × X
        N ⇐ N − 1
    end if
end while
```

C Výpis sublime

```
{
    "folders":
    [
        {
            "path": ".",
            "folder_exclude_patterns": [".build", ".aux"],
            "follow_symlinks": true
        }
    ],
    "settings" : {
        "TEXroot": "example.tex",
        "tex_file_exts": [".tex"],
        "use_biblatex": true,
        "glossary_auto_trigger": true,
        "aux_directory": "./.aux",
        "output_directory": "./.build",
        "builder_settings": {
            "program": "pdflatex",
            "options": "--shell-escape"
        }
    },
    "build_systems":
    [
        {
            "name": "FEI - LaTeX",
            "working_dir": "${folder}",
            "shell_cmd": "make",
            "variants": [
                {
                    "name": "clean",
                    "shell_cmd": "make clean",
                }
            ]
        }
    ]
}
```

Listing C.1: Ukážka sublime-project