УНИВЕРЗИТЕТ У БЕОГРАДУ – ЕЛЕКТРОТЕХНИЧКИ ФАКУЛТЕТ

Павле В. Вулетић, Жарко С. Станисављевић

ЗАШТИТА ПОДАТАКА

АКАДЕМСКА МИСАО
Београд, 2025.

Павле В. Вулетић, Жарко С. Станисављевић

ЗАШТИТА ПОДАТАКА

Рецензенти
др Марија Пунт, ванредни професор
др Маја Вукасовић, доцент

Наставно-научно веће Електротехничког факултета одобрило је објављивање овог уџбеника одлуком број 650/4 од 8. 4. 2025. године.

Издавачи
Универзитет у Београду – Електротехнички факултет
Академска мисао, Београд

Дизајн насловне стране
Борис Поповић

Штампа
Планета принт, Београд

Тираж
300 примерака

ISBN 978-86-6200-049-1

Место и година издања: Београд, 2025.

НАПОМЕНА: Фотокопирање или умножавање на било који начин познат данас или који ће се појавити у будућности или поновно објављивање ове књиге – у целини или у деловима - није дозвољено без претходне изричите сагласности и писменог одобрења издавача.

Садржај

Предговор..... 9

1 Увод.....13
1.1 Заштита података у рачунарским системима.....14
1.2 Напади на сигурност података и механизми заштите.....17
1.3 Модели заштите података.....22
1.4 Стандарди и стандардизација алгоритама заштите података.....25
1.5 Терминологија.....27
1.6 Нотација.....28

2 Симетрични криптографски алгоритми.....31
2.1 Заштита података симетричним криптографским алгоритмима.....32
2.1.1 Супституциони криптографски алгоритми.....35
2.1.1.1 Цезаров алгоритам.....35
2.1.1.2 Моноалфабетски алгоритам.....36
2.1.1.3 Вишесловни супституциони алгоритми.....40
2.1.1.4 Полиалфабетски алгоритми.....44
2.1.2 Транспозициони криптографски алгоритми.....52
2.1.2.1 Rail Fence алгоритам.....53
2.1.2.2 Алгоритам транспозиције редова.....53
2.1.3 Продукциони криптографски алгоритми.....55
2.2 Алгоритми за шифровање блока података.....59
2.2.1 Фајстелова структура.....61
2.2.2 Супституционо-пермутационе мреже.....63
2.2.3 Стандард за шифровање података - DES.....64
2.2.4 Напредни стандард за шифровање података - AES.....68
2.2.5 Режими блоковских симетричних алгоритама.....75
2.2.5.1 ECB режим.....75
2.2.5.2 CBC режим.....76
2.2.5.3 CFB режим.....76
2.2.5.4 OFB режим.....78
2.2.5.5 CTR режим.....79
2.3 Алгоритми за шифровање тока података.....80

2.3.1 Salsa20 алгоритам....82
2.3.2 ChaCha20 алгоритам....82
2.4 Литература....83

3 Асиметрични криптографски алгоритми....87
3.1 Основни концепти криптографије са јавним кључем....88
3.2 RSA алгоритам....94
3.2.1 Сложеност израчунавања RSA алгоритма....97
3.2.2 Напади на RSA алгоритам....99
3.2.2.1 Напади грубом претрагом....99
3.2.2.2 Математички напади....99
3.2.2.3 Временски напади....100
3.2.2.4 Напади на хардвер....101
3.2.2.5 Напад изабраном шифрованом поруком и хомоморфност....101
3.2.3 Препоручене величине кључева....102
3.3 Литература....103

4 Управљање кључевима....105
4.1 Размена тајног кључа помоћу симетричних криптографских алгоритама....106
4.2 Размена тајног кључа помоћу асиметричних криптографских алгоритама....111
4.3 Дистрибуција јавног кључа....114
4.3.1 Јавно објављивање кључа....115
4.3.2 Јавно доступни директоријум....115
4.3.3 Ауторитет за јавне кључеве....116
4.3.4 Сертификати са јавним кључевима....118
4.4 Дифи-Хелман (DH) алгоритам....119
4.4.1 Пример рада Дифи-Хелман алгоритма....122
4.4.2 Други алгоритми за размену кључева....124
4.5 Литература....125

5 Криптографске хеш функције и функције за обезбеђивање веродостојности порука....127
5.1 Начини провере веродостојности порука....127
5.2 Хеш функције....129
5.2.1 Основна примена хеш функција – провера веродостојности....130
5.2.2 Карактеристике криптографских хеш функција....134
5.2.2.1 Слаба и јака отпорност на колизије....136
5.2.2.2 Криптографске и некриптографске хеш функције....138
5.2.3 Основни градивни елементи криптографских хеш функција....139

5.2.3.1 Компресионе функције које користе симетричне криптографске алгоритме ... *141*
5.2.3.2 SHA-2 алгоритми ... *143*
5.2.3.3 Сунђер функција ... *147*
5.2.3.4 SHA3 алгоритми ... *149*
5.2.3.5 Перформансе тренутно коришћених хеш функција ... *152*
5.2.4 Примене хеш функција ... 153
5.2.4.1 Чување лозинки у рачунарским системима ... *153*
5.2.4.2 Заштита од спам мејла – hashcash механизам ... *155*
5.2.4.3 Мерклеово стабло ... *157*
5.3 Функције за обезбеђивање веродостојности порука (MAC) ... 160
5.3.1 Обезбеђивање веродостојности поруке MAC функцијама ... 161
5.3.2 Сигурност MAC функција ... 162
5.3.3 HMAC – MAC функције засноване на хеш функцијама ... 163
5.3.4 CMAC – MAC функције засноване на алгоритмима шифровања ... 164
5.3.5 Примена MAC – вишефакторска аутентикација и TOTP ... 166
5.3.6 Примена MAC - Генерисање псеудослучајних бројева ... 169
5.3.6.1 Извођење псеудослучајних низова из лозинки ... *171*
5.4 Енкрипција са обезбеђивањем веродостојности порука ... 172
5.4.1 CCM – Бројач са CBC режимом рада симетричног алгоритма ... 173
5.4.2 Галоа/бројачки режим - GCM ... 174
5.4.3 Ascon алгоритам за уређаје скромних хардверских карактеристика ... 176
5.5 Литература ... 178

6 Генератори псеудослучајних бројева ... 181
6.1 Врсте генератора случајних вредности ... 181
6.2 Псеудослучајне и једносмерне функције ... 184
6.3 Алгоритми за генерисање псеудослучајних вредности ... 186
6.3.1 Генератори засновани на модуларној аритметици ... 187
6.3.1.1 Линеарни конгруентни генератор ... *187*
6.3.1.2 Блам-Блам-Шаб генератор ... *188*
6.3.1.3 Блам-Микали генератор ... *188*
6.3.2 Генератори који користе симетричне алгоритме за шифровање ... 189
6.3.2.1 Генератор који користи OFB режим рада ... *189*
6.3.2.2 Генератор који користи бројачки режим рада ... *190*
6.3.3 Генератори који користе хеш и HMAC функције ... 191
6.3.3.1 Генератори који користе хеш функције ... *191*
6.3.3.2 Генератори који користе HMAC функције ... *193*
6.4 Тестови псеудослучајности ... 194
6.5 Литература ... 198

7 Дигитални потписи.....201
7.1 Дигитални потпис – модел сигурности, ентитети.....202
7.2 Елгамал дигитални потпис.....205
7.2.1 Дигитално потписивање Елгамаловом шемом.....205
7.2.2 Верификација Елгамаловог дигиталног потписа.....206
7.3 DSA алгоритам и DSS стандард.....208
7.3.1 Дигитално потписивање DSA алгоритмом.....209
7.3.2 Верификација дигиталног потписа DSA алгоритмом.....210
7.4 RSA PSS.....210
7.4.1 EMSA-PSS енкодовање и дигитални потпис.....211
7.4.2 Провера RSA-PSS дигиталног потписа.....212
7.5 Дигитални потпис у Србији.....213
7.6 Пост-квантни дигитални потписи засновани на хеш функцијама.....215
7.6.1 Лампорт-Дифи једнократни механизам за дигитално потписивање 216
7.6.1.1 Формирање кључева за дигитално потписивање.....216
7.6.1.2 Дигитално потписивање.....217
7.6.1.3 Верификација дигиталног потписа.....218
7.6.1.4 Мане Лампорт-Дифијеве шеме за дигитално потписивање. .219
7.6.2 Винтерницов једнократни механизам за дигитално потписивање..220
7.6.2.1 Формирање кључева за дигитално потписивање.....220
7.6.2.2 Дигитално потписивање.....222
7.6.2.3 Верификација дигиталног потписа.....223
7.6.3 Мерклеова шема за дигитално потписивање.....223
7.6.3.1 Дигитално потписивање Мерклеовом шемом.....225
7.6.3.2 Верификација дигиталног потписа Мерклеовом шемом.....225
7.6.3.3 Мане дигиталног потписивања Мерклеовом шемом.....226
7.6.3.4 XMSS: eXtended Merkle Signature Scheme.....227
7.6.3.5 WOTS+ шема дигиталног потписивања.....228
7.6.4 SPHINCS+ шема дигиталног потписивања.....230
7.6.4.1 Мерклеово хиперстабло.....231
7.6.4.2 SPHINCS+ дигитални потписи.....233
7.6.4.3 Шеме за дигитално потписивање неколико пута: HORS и FORS.....234
7.7 Литература.....236

8 X.509 дигитални сертификати.....241
8.1 Примена сертификата.....241
8.2 Начин коришћења сертификата.....243
8.3 Садржај сертификата.....245
8.4 Хијерархија сертификационих ауторитета.....248

8.5 Екстензије сертификата....253
8.6 Повлачење сертификата....257
8.7 Инфраструктура за рад са јавним кључевима....259
8.8 Литература....261

9 Провера веродостојности корисника....263
9.1 Проблеми провере веродостојности корисника у савременим интернет услугама....263
9.1.1 Проблем великог броја корисничких креденцијала....264
9.1.2 Напад понављањем на протоколе за проверу веродостојности корисника....266
9.1.3 Пример напада понављањем на размену кључева....267
9.2 Начини провере веродостојности корисника....269
9.3 Керберос....270
9.3.1 Једноставни дијалог за доделу приступа серверу....271
9.3.2 Сложенији дијалог за доделу приступа серверу....273
9.3.3 Керберос верзија 4....275
9.3.4 Керберос верзија 5....277
9.4 Федерације идентитета....278
9.4.1 Провера веродостојности корисника у федерацији идентитета....280
9.4.2 SAML језик....281
9.4.3 OpenID Connect....284
9.5 OAuth протокол за ауторизацију....284
9.5.1 Елементи OAuth архитектуре....286
9.5.2 Интеграција веб услуга OAuth ауторизацијом....288
9.5.3 Логовање OAuth ауторизацијом....291
9.6 Верификација идентитета корисника мрежних уређаја....291
9.6.1 RADIUS протокол....292
9.6.2 EAP протокол....293
9.6.3 Провера веродостојности корисника из других домена - *eduroam*. 295
9.7 Литература....296

10 Заштита података приликом преноса....299
10.1 Заштита података на мрежном слоју....302
10.1.1 IPsec....302
10.1.1.1 Аутентикационо заглавље - AH....303
10.1.1.2 Заглавље за сигурну енкапсулацију података - ESP....305
10.1.1.3 Размена кључева - Internet Key Exchange (IKE)....308
10.1.1.4 Креирање кључева након размена....312
10.1.2 WireGuard виртуелна приватна мрежа....313
10.1.2.1 WireGuard размена кључева....314

10.1.2.2 WireGuard заштита података у пакетима.....317
10.2 Заштита података на транспортном слоју.....318
10.2.1 Заштита података у веб апликацијама.....318
10.2.1.1 Делови TLS протокола.....320
10.2.1.2 Протокол за аутентикацију и размену криптографског материјала.....321
10.2.1.3 Креирање кључева за TLS сесију.....326
10.2.1.4 Протокол за заштиту података који се преносе између веб сервера и прегледача.....328
10.2.2 Виртуелна приватна мрежа на транспортном слоју - OpenVPN...329
10.2.3 Сигурни приступ командној линији - SSH.....332
10.2.3.1 SSH Transport Layer Protocol.....332
10.2.3.2 SSH User Authentication Protocol.....334
10.2.3.3 SSH Connection Protocol.....334
10.3 Заштита података на апликативном слоју.....334
10.3.1 Заштита електронске поште.....334
10.3.1.1 S/MIME механизам.....336
10.3.1.2 PGP механизам.....338
10.3.2 Заштита DNS упита и одговора.....341
10.3.2.1 Механизам DNSSEC.....342
10.3.2.2 DNS преко HTTPS и „несвесни“ DNS преко HTTPS.....342
10.4 Литература.....344

11 Заштита података у употреби.....349
11.1 Хомоморфна енкрипција.....350
11.2 Извршно окружење од поверења.....351
11.3 Удаљена атестација.....352
11.4 Пример употребе.....353
11.5 Пример начина рада извршног окружења од поверења.....354
11.6 Пример начина атестације.....355
11.6.1 Верификовање ланца сертификата.....357
11.6.2 Генерисање главне тајне.....358
11.6.3 Заштита података.....359
11.6.4 Мерење.....360
11.7 Литература.....361

12 Биткоин блокчејн.....365
12.1 Централизоване и децентрализоване базе података.....365
12.2 Принцип функционисања биткоин блокчејна.....367
12.2.1 Новчаник.....368
12.2.2 Трансакције.....370

12.2.3 Принцип функционисања уланчане листе блокова.....372
12.2.4 Потврђивање блокова и „рударење” биткоина.....374
12.2.5 Гранање блокчејна.....376
12.3 Сигурност података у блокчејну.....378
12.4 Литература.....380

13 Списак често коришћених скраћеница.....381