

I deo

Sadržaj

1. UVOD.....	7
2. PRIMENA KRIPTOGRAFSKIH METODA ZAŠTITE U INFORMACIONIM SISTEMIMA	8
3. SIMETRIČNI KRIPTOGRAFSKI ALGORITMI.....	9
3.1 Teorijske osnove simetričnih kriptografskih algoritama	10
3.2 Apsolutno tajni šifarski sistem – Shannon-ova teorema.....	11
3.3 Blok šifarski sistemi	11
3.3.1 DES (Data Encryption Standard)	12
3.3.2 3DES (Triple DES).....	15
3.3.3 IDEA algoritam	17
3.3.4 AES algoritam.....	17
3.4 Kriptografski modovi blok šifarskih algoritama	26
3.4.1 Mod elektronske kodne knjige (<i>ECB – Electronic CodeBook</i>)	26
3.4.2 Mod ulančavanja blokova (<i>CBC – Cipher Block Chaining</i>)	27
3.4.3 Mod povratnog šifrovanja (<i>CFB – Cipher-Feedback Mode</i>).....	29
3.4.4 Izlazni povratni mod (<i>OFB – Output Feedback Mode</i>).....	30
3.4.5 Izbor odgovarajućeg moda rada blok šifarskog sistema	32
3.5 Sekvencijalni šifarski sistemi	32
3.5.1 Klasifikacija sekvencijalnih šifarskih sistema.....	33
3.5.2 Generatori pseudo-slučajnog niza (GPSN).....	34
3.5.3 Sinhroni sekvencijalni šifarski sistemi	35
3.5.4 Samosinhronišući asinhroni šifarski sistemi.....	37
3.5.5 RC4 algoritam.....	38
3.6 Komparativna analiza blok i sekvencijalnih šifarskih sistema	38
3.7 Problemi u primeni simetričnih kriptografskih algoritama	39
4. ASIMETRIČNI KRIPTOGRAFSKI ALGORITMI	40
4.1 Pojam šifarskog sistema sa javnim ključem	40
4.2 Difi-Helmanov protokol	41
4.3 RSA algoritam – Osnovne karakteristike.....	42
4.3.1 Primer jednostavnog zadatka sa RSA algoritmom.....	43
4.4 PKCS#1 standard	44
4.5 PKCS#7 standard Cryptographic Message Syntax.....	47
4.6 RSA algoritam – Teorijske osnove	49
4.7 FIPS 186-4 DSS (<i>Digital Signature Standard</i>).....	57
4.7.1 Inicijalno podešavanje potpisnika.....	60
4.7.2 Kreiranje digitalnog potpisa	62
4.7.3 Verifikacija i validacija digitalnog potpisa	63
4.8 DSA algoritam.....	64
4.8.1 DSA Parametri.....	64
4.8.2 Izbor veličine parametara i hash funkcija za DSA algoritam	65
4.8.3 DSA domenski parametri.....	66
4.8.4 Parovi ključeva	67
4.8.5 Tajni ključ po poruci u DSA algoritmu	68
4.8.6 Kreiranje digitalnog potpisa putem DSA algoritma.....	68
4.8.7 Verifikacija i validacija digitalnog potpisa kreiranog DSA algoritmom.....	69
4.9 RSA algoritam za digitalni potpis	70
4.9.1 Generisanje para ključeva u RSA algoritmu	70
4.9.2 Upravljanje parom ključeva	71
4.9.3 Osiguranja	71

4.9.4 ANSI X9.31	72
4.9.5 PKCS #1	72
4.10 Elliptic Curve algoritam za digitalni potpis (ECDSA)	73
4.10.1 ECDSA domenski parametri	73
4.10.2 Privatni i javni ključevi.....	75
4.10.3 Kreiranje tajnog broja	76
4.10.4 Kreiranje i verifikacija ECDSA digitalnog potpisa	76
4.10.5 Osiguranja	77
5. HASH (MESSAGE DIGEST) ALGORITMI	78
5.1 MD5 algoritam – MessageDigest Algorithm	78
5.2 SHA-1 algoritam	80
5.3 SHA-2 familija hash funkcija	82
5.3.1 SHA-1 algoritam	83
5.3.2 SHA-256 algoritam	84
5.3.3 SHA-224 algoritam	84
5.3.4 SHA-512 algoritam	84
5.3.5 SHA-384 algoritam	85
5.4 Secure Hash Standard FIPS 180-4	85
5.4.1 Parametri algoritma, simboli i izrazi.....	87
5.4.2 Označavanje i konvencije.....	88
5.4.3 Funkcije i konstante.....	90
5.5 Opisi standardnih hash algoritama	99
5.5.1 SHA-1 algoritam	99
5.5.2 SHA-256 algoritam	103
5.5.3 SHA-224 algoritam	105
5.5.4 SHA-512 algoritam	105
5.5.5 SHA-384 algoritam	108
5.5.6 SHA-512/224 algoritam	108
5.5.7 SHA-512/256 algoritam	108
5.5.8 Skraćivanje hash vrednosti	108
5.6 SHA-3 algoritmi.....	109
5.6.1 Sumarni pregled hash algoritama	109
5.6.2 Merkle-Damgard konstrukcija.....	112
5.6.3 Problem u dosadašnjim hash funkcijama.....	113
5.7 NIST FIPS 202 standard.....	117
5.7.1 Rečnik termina.....	119
5.7.2 KECCAK-p permutacije	123
5.7.3 Mapirajući koraci.....	128
5.7.4 KECCAK- $p[b, nr]$ permutacija.....	133
5.7.5 Poređenje sa KECCAK-f	134
5.8 Sponge Konstrukcija	134
5.9 KECCAK	136
5.9.1 Specifikacija pad10*1	136
5.9.2 Specifikacija KECCAK[c].....	136
5.10 Specifikacija SHA-3 funkcija	137
5.10.1 SHA-3 Hash funkcije	137
5.10.2 SHA-3 proširive izlazne funkcije (XOFs)	137
5.10.3 Alternativne definicije za SHA-3 XOF funkcije	138
5.11 Usaglašenost	138
5.12 Bezbednosni aspekti.....	139
A.1 Sumarizovane bezbednosne snage SHA-3 funkcija.....	140
A.2 Dodatno razmatranje XOF funkcija.....	141
B Primeri	142
B.1 Funkcije konverzije.....	142
B.2 Heksadecimalna forma bitova za proširenje poruke.....	144

6.	PRIMENA KRIPTOGRAFSKIH ALGORITAMA U INFORMACIONIM SISTEMIMA	145
7.	AUTENTIFIKACIJA KORISNIKA	148
7.1	Upravljanje identitetom – Osnovne funkcije	148
7.1.1	Identifikacija	148
7.1.2	Elektronski identitet (e-ID)	148
7.1.3	Autentifikacija	148
7.1.4	Sistemi autentifikacije korisnika.....	148
7.1.5	Jaka autentifikacija korisnika	148
7.1.6	Multifaktorska autentifikacija korisnika	149
7.1.7	Autorizacija	149
7.2	Elementi koji se koriste za multifaktorsku autentifikaciju	149
7.2.1	Element identiteta.....	149
7.2.2	Element posedovanja	150
7.2.3	Element znanja.....	152
7.3	Kod za autentifikaciju poruke	152
7.3.1	CBC-MAC algoritam	153
7.3.2	HMAC algoritam	153
7.4	One-time password.....	154
7.4.1	Lampportova šema.....	154
7.4.2	HMAC bazirani One-time password	154
7.4.3	Time-Based One-Time Password	156
7.4.4	Challenge-response autentifikacija	157
7.4.5	OATH Challenge-Response Algorithm.....	160
7.4.6	Challenge-response autentifikacija bazirana na asimetričnoj kriptografiji	162
7.4.7	Zero-knowledge autentifikacija.....	168
8.	EMV AUTENTIFIKACIJA.....	170
8.1	Osnovne karakteristike EMV specifikacije.....	170
8.2	Mehanizmi EMV zaštite – autentifikacija kartice.....	170
8.3	Mehanizmi EMV zaštite – Odnos SDA i DDA.....	172
8.4	Mehanizmi EMV zaštite – DDA.....	172
8.5	Razvoj čip infrastrukture i servisa	175
8.6	Multiaplikativne smart kartice.....	176
8.7	MasterCard CAP aplikacija.....	177
8.7.1	MasterCard CAP application – Osnovne karakteristike	177
8.7.2	Korišćenje CAP tokena.....	178
8.7.3	Generisanje CAP tokena.....	179
8.7.4	Validacija CAP tokena	180
8.7.5	Zahtevi za validaciju CAP tokena i aplikacijskog kriptograma	180
9.	3-D SECURE SISTEM.....	183
9.1	3-D Secure model.....	183
9.2	Postupak Autentifikacije korisnika u 3D Secure sistemu.....	187
9.3	Verified-by-Visa.....	190
9.4	MasterCard Secure Code	190
9.5	Pregled SecureCode rešenja.....	191
10.	UPRAVLJANJE PRISTUPOM	193
10.1	Autentifikacija.....	193
10.2	Autentifikacioni server.....	195
10.3	Kerberos	195
10.3.1	Osnovne karakteristike Kerberos autentifikacionog servera.....	196
10.3.2	Pregled Kerberos protokola.....	198
10.3.3	Kerberos – Verzija 4	200
10.3.4	Kerberos – Verzija 5	201
10.4	Windows smart card logon	202

10.5 SSO (Single-Sign-On)	204
10.6 SAML 2.0	205
11. KRIPTOGRAFSKI ASPEKTI DLT/BLOCKCHAIN TEHNOLOGIJE	208
11.1 Uvodne napomene	208
11.2 Povezanost sa digitalnim valutama	212
11.3 Blokovi in DLT/Blockchain mrežama	213
11.4 Ključna bezbednosna obeležja DLT/Blockchain tehnologije	214
11.4.1 Distribuirana priroda DLT/Blockchain sistema	215
11.4.2 Konsenzus mehanizam	215
11.4.3 Kriptografski mehanizmi	216
12. LITERATURA	219
Recenzenti	223