

SVEUČILIŠTE U ZAGREBU FAKULTET ELEKTROTEHNIKE I RAČUNARSTVA

DIPLOMSKI RAD br. 1445

SIGURNOSNI MEHANIZMI ZA RAD S PAMETNIM KARTICAMA

Aleksander Radovan

Zagreb, rujan 2004.

2

Sadržaj

1. UVOD	5
2. FIZIČKA STRUKTURA I ŽIVOTNI CIKLUS KARTICE	7 2.1.
FIZIČKA STRUKTURA PAMETNE KARTICE	7 2.2.
ŽIVOTNI CIKLUS PAMETNE KARTICE	8
2.2.1. Faza proizvodnje.....	8 2.2.2.
Pripremna faza personalizacije	8 2.2.3. Faza
personalizacije	9 2.2.4. Faza
korištenja.....	9 2.2.5. Završna faza
(faza poništavanja kartice)	9 3. LOGIČKA STRUKTURA I
KONTROLA PRISTUPA	11 3.1. LOGIČKA STRUKTURA
DATOTEKA	11 3.2. KONTROLA
PRISTUPA.....	12 3.2.1 Razine
uvjeta pristupa.....	12 3.3.
PREZENTACIJA PIN-A	13 3.3.1.
Rukovanje PIN-om	13 4.
PROCEDURALNA ZAŠTITA.....	15 4.1.
IDENTIFIKACIJA DOKUMENATA.....	15 4.2.
AUTENTIFIKACIJA KERBEROS SUSTAVOM	16
4.3. KONTROLA PRISTUPA OPERACIJSKOM SUSTAVU	20 4.4. NAPADI NA PAMETNE KARTICE
.....	21 4.4.1. Logički
napadi.....	21 4.4.2. Fizički
napadi.....	21 4.4.3. Probijanje
kriptografskih algoritama.....	21 5. ARHITEKTURA I
VRSTE PAMETNIH KARTICA.....	23 5.1. ARHITEKTURA
PAMETNIH KARTICA.....	23 5.1.1
Mikroprocesor.....	23 5.1.2
Memorija	23 5.1.3.
Ulazno/izlazno sučelje.....	24 5.1.4. Izvor
napajanja	24 5.2. VRSTE
PAMETNIH KARTICA	25 5.2.1.
Memorijske kartice.....	25 5.2.2.
Mikroprocesorske kartice	26 5.2.3. Kartice
s kriptografskim koprocesorom	27 5.2.4. Beskontakne
pametne kartice	27
5.2.4.1. Induktivni spoj.....	28
5.2.4.2. Kapacitivni spoj.....	28
5.2.5. Hibridne pametne kartice	30 5.2.6.
Napredne pametne kartice	30 6.

SIGURNOSNI MEHANIZMI	31	6.1.
ALGORITMI KRIPTIRANJA.....	31	6.1.1.
DES.....	32	6.1.2.
Trostruki DES.....	38	6.2.
ALGORITMI SAŽIMANJA	38	6.2.1.
SHA-1	38	
6.2.1.1. Izračunavanje sažetka poruke	38	
6.3. DIGITALNI POTPIS	41	
6.4. ALGORITMI ZA RAZMJENU KLJUČEVA	41	
6.4.1. RSA	42	
6.4.1.1. Enkripcija.....	42	
3		
6.4.1.2. Dekripcija	42	
6.4.1.3. Digitalno potpisivanje	42	
6.4.1.4. Verifikacija digitalnog potpisa	42	
6.4.1.5. Jednostavan primjer RSA enkripcije.....	43	
6.4.1.6. Složeniji primjer RSA enkripcije	43	
6.4.1.7. Stvarni primjer.....	44	
6.4.1.8. Duljine ključeva i njihov životni ciklus	45	
6.5. DIGITALNI CERTIFIKATI	46	7.
PRAKTIČNI RAD – DEMONSTRACIJA SIGURNOSNIH MEHANIZAMA KORISTEĆI PAMETNE KARTICE...		
..... NAMERNO UKLONJEN DEO TEKSTA		
.....	50	7.2.2. Popunjavanje elektroničke uplatnice.....
.....	51	7.2.3. Provo enje transakcija
.....	52	7.3. IZVORNI TEKSTOVI
PROGRAMA.....	53	7.4. ZAKLJUČAK O
PRAKTIČNOM RADU	53	8.
ZAKLJUČAK.....	55	
PRILOG 1 – NAJVAŽNIJI DIJELOVI PROGRAMSKOG KODA	56	P.1.1.
PROVJERA UNESENOG PIN-A	56	P.1.2.
DOHVAĆANJE CERTIFIKATA S KARTICE	58	
P.1.3. DIGITALNO POTPISIVANJE NALOGA ZA ELEKTRONIČKO PLAĆANJE		
.....	60	P.1.4. PROVJERA DIGITALNOG POTPISA
.....	61	DODATAK A
.....	62	A.1. POPIS
SVIH PAROVA VRIJEDNOSTI CNDN	62	A.2.
POPIS SVIH KLJUČEVA DOBIVENIH PERMUTACIJOM PAROVA CNDN	63	
A.3. POPIS SVIH S-KUTIJA	64	
A.3.1. S1 kutija.....	64	A.3.2.
S2 kutija.....	64	A.3.3. S3
kutija.....	64	A.3.4. S4
kutija.....	64	A.3.5. S5
kutija.....	64	A.3.6. S6
kutija.....	64	A.3.7. S7
kutija.....	65	A.3.8. S8
kutija.....	65	A.4. POPIS
SVIH KORAKA U PETLJI (T = 0 DO 79) U SHA-1 ALGORITMU	65	
LITERATURA	69	

----- OSTATAK TEKSTA NIJE PRIKAZAN. CEO RAD MOŽETE
PREUZETI NA SAJTU. -----

www.maturskiradovi.net

MOŽETE NAS KONTAKTIRATI NA E-MAIL: maturskiradovi.net@gmail.com