

# Pregled kriptografije koja se koristi u računalskim sustavima

---

**Perić, Marina**

**Undergraduate thesis / Završni rad**

**2015**

*Degree Grantor / Ustanova koja je dodijelila akademski / stručni stupanj:* **Josip Juraj Strossmayer University of Osijek, Faculty of Electrical Engineering, Computer Science and Information Technology Osijek / Sveučilište Josipa Jurja Strossmayera u Osijeku, Fakultet elektrotehnike, računarstva i informacijskih tehnologija Osijek**

*Permanent link / Trajna poveznica:* <https://um.nsk.hr/um:nbn:hr:200:838169>

*Rights / Prava:* [In copyright](#)

*Download date / Datum preuzimanja:* **2021-04-11**

*Repository / Repozitorij:*

[Faculty of Electrical Engineering, Computer Science and Information Technology Osijek](#)



**SVEUČILIŠTE JOSIPA JURJA STROSSMAYERA U OSIJEKU**

**ELEKTROTEHNIČKI FAKULTET**

**Sveučilišni studij**

**KRIPTOGRAFIJA U RAČUNALSKIM SUSTAVIMA**

**Završni rad**

**Marina Perić**

**Osijek, 2015.**

## SADRŽAJ:

<b>1. UVOD</b> .....	<b>1</b>
1.1. Zadatak završnog rada.....	1
<b>2. KLASIČNA KRIPTOGRAFIJA</b> .....	<b>2</b>
2.1. Osnovni pojmovi .....	2
2.2. Povijest kriptografije .....	3
2.3. Supstitucijske šifre .....	5
2.4. Vigenèreova šifra .....	8
2.5. Transpozicijske šifre .....	9
<b>3. RAČUNALNA KRIPTOGRAFIJA</b> .....	<b>11</b>
3.1. Simetrični sustavi za kriptografiju .....	11
3.1.1. DES algoritam .....	11
3.1.2. AES algoritam .....	13
3.1.3. IDEA algoritam .....	15
3.2. Asimetrični sustavi za kriptografiju .....	15
3.2.1. Kriptosustavi s javnim ključem .....	16
3.2.2. RSA kriptosustav .....	17
3.2.3. Ostali sustavi s javnim ključem.....	19
3.3. Funkcije za izračunavanje sažetka poruke .....	19
3.3.1. MD5.....	19
3.3.2. SHA .....	21
3.4. Digitalni potpis.....	21
3.5. Kvantna kriptografija .....	23
<b>4. PRIMJENA KRIPTOGRAFIJE U ELEKTRONSKOJ POŠTI</b> .....	<b>24</b>
4.1. PGP .....	25
4.2. S/MIME .....	27
<b>5. ZAKLJUČAK</b> .....	<b>30</b>
<b>6. LITERATURA</b> .....	<b>31</b>
<b>7. SAŽETAK</b> .....	<b>32</b>
<b>8. ŽIVOTOPIS</b> .....	<b>33</b>

## **7. SAŽETAK**

Glavni problem kojim sam se bavila u ovome radu bila je primjena kriptografije u računalskim sustavima i u sustavu elektronske pošte. U radu je dan i pregled povijesti kriptografije, a opisani su i principi klasične kriptografije. Računalna kriptografija podjeljena je i opisana kroz simetričnu i asimetričnu, a opisane su i hash funkcije i digitalni potpis. Na kraju, postavljen je problem primjene kriptografije u elektronskoj pošti te je njegovo rješenje dano kroz objašnjenja programa koji se koriste.

### **CRYPTOGRAPHY IN COMPUTER SYSTEMS**

The main problem in this thesis has been the cryptography application in computer and email systems. Besides the usage of cryptography throughout the history, its classical principles have also been described. Two types of cryptography have been portrayed, symmetrical and asymmetrical, as well as the hash functions and digital signature. Finally, the usage of cryptography in the emails has been explained through the applications of different softwares.