Pregled kriptografije koja se koristi u računalskim sustavima

Perić, Marina

SVEUČILIŠTE JOSIPA JURJA STROSSMAYERA U OSIJEKU

ELEKTROTEHNIČKI FAKULTET

Sveučilišni studij

KRIPTOGRAFIJA U RAČUNALSKIM SUSTAVIMA

Završni rad

Marina Perić

Osijek, 2015.

SADRŽAJ:

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.