Sustav zaštite privatnosti podataka temeljen na AES algoritmu

Babić, Dario

SVEUČILIŠTE JOSIPA JURJA STROSSMAYERA U OSIJEKU

ELEKTROTEHNIČKI FAKULTET

Sveučilišni studij

Sustav zaštite privatnosti podataka temeljen na AES algoritmu

Diplomski rad

Dario Babić

Osijek, 2014.

SADRŽAJ

SAŽETAK

Zadatak ovog rada jest objasniti postupak AES kriptiranja i dekriptiranja podataka, te razraditi postupak i izgraditi testni sustav za ovakvo kriptiranje sa raznim duljinama ključeva. Potrebno je provesti kvalitativnu i analizu performansi.

AES algoritam nudi zaštitu informacija kriptirajući ih ključevima duljina od 128, 192 i 256 bita. Koraci algoritma osmišljeni su na takav način da onemoguće poznate napade. Napadi „primjenom sile“ su nepraktični, jer zbog veličine ključa, vrijeme koje je potrebno za razbijanje ključa višestruko prelazi životni vijek čovjeka. Testni sustav je izgrađen u C# programskom jeziku i Visual C# 2010 Express programski alat.

Ključne riječi: AES algoritam, C# programski jezik, kriptiranje blokova, kriptografija, simetrični algoritam, , Visual C# 2010 Express.

ABSTRACT

System for data privacy protection based on AES algorithm

The task of this thesis is to explain AES encryption and decryption process, to elaborate the process and build a test system for encryption with different length of keys. It is necessary to conduct a qualitative and performance analysis.

AES algorithm offers information protection, encrypthing them with keys length of 128, 192 and 256 bits. Algorithm steps are made in such way, so the algorithm can resist known attacks. Brute force attacks are not practical because of size of the key, time needed to „break“ the key is multiple times longer then a lifetime of one person. Test system is built in C# programming language, using Visual C# 2010 Express development environment.

Keywords: AES algorithm, block encryption, Cryptography, C# programming language, symetric algorithm, Visual C# 2010 Express.