

# Sustav zaštite privatnosti podataka temeljen na AES algoritmu

---

**Babić, Dario**

**Master's thesis / Diplomski rad**

**2014**

*Degree Grantor / Ustanova koja je dodijelila akademski / stručni stupanj:* **Josip Juraj Strossmayer University of Osijek, Faculty of Electrical Engineering / Sveučilište Josipa Jurja Strossmayera u Osijeku, Elektrotehnički fakultet**

*Permanent link / Trajna poveznica:* <https://urn.nsk.hr/urn:nbn:hr:200:879607>

*Rights / Prava:* [In copyright](#)/[Zaštićeno autorskim pravom.](#)

*Download date / Datum preuzimanja:* **2024-09-01**

*Repository / Repozitorij:*

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



**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

1. UVOD .....	1
1.1. Zadatak i struktura rada .....	2
2. KRIPTIRANJE I KRIPTOGRAFIJA .....	3
2.1. Povijest kriptografije .....	3
2.2. Razvoj i potreba za kriptiranjem .....	5
2.3. Podjela kriptografskih postupaka .....	6
3. NAPREDNI ENKRIPCijski ALGORITAM .....	10
3.1. Osnovni pojmovi .....	11
3.2. Matematički model .....	13
3.3. AES kriptiranje .....	17
3.3.1. Ekspanzija ključa .....	18
3.3.2. Zamjena okteta .....	20
3.3.3. Posmak redaka .....	22
3.3.4. Miješanje stupaca .....	23
3.3.5. Dodavanje podključa .....	24
3.4. AES dešifriranje .....	24
3.4.1. Inverzni posmak retka .....	25
3.4.2. Inverzna zamjena okteta i inverzno miješanje stupaca .....	26
4. REALIZACIJA AES POSTUPKA .....	27
4.1. Programski okvir .....	27
4.2. AES aplikacija .....	31
5. VALIDACIJA I REZULTATI ISPITIVANJA .....	37
5.1. Funkcionalna validacija .....	37
5.2. Analiza performansi .....	43
5.3. Sigurnost AES algoritma .....	45
6. ZAKLJUČAK .....	48
LITERATURA .....	49
SAŽETAK .....	50
ABSTRACT .....	51
ŽIVOTOPIS .....	52
PRILOG .....	53

## 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, encrypting 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 than 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, symmetric algorithm, Visual C# 2010 Express.