

**ANALISIS DAN PEMANFAATAN ALGORITMA KRIPTOGRAFI  
UNTUK PENGKODEAN SERIAL NUMBER PADA APLIKASI  
BERBASIS DESKTOP**

**SKRIPSI**



disusun oleh

**Adrianus Adi**

**12.11.6118**

**PROGRAM SARJANA  
PROGRAM STUDI INFORMATIKA  
FAKULTAS ILMU KOMPUTER  
UNIVERSITAS AMIKOM YOGYAKARTA  
YOGYAKARTA  
2017**

**ANALISIS DAN PEMANFAATAN ALGORITMA KRIPTOGRAFI  
UNTUK PENGKODEAN SERIAL NUMBER PADA APLIKASI  
BERBASIS DESKTOP**

**Skripsi**

untuk memenuhi sebagian persyaratan  
mencapai gelar Sarjana  
pada Program Studi **Teknik Informatika**



disusun oleh

**Adrianus Adi**

**12.11.6118**

**PROGRAM SARJANA  
PROGRAM STUDI INFORMATIKA  
FAKULTAS ILMU KOMPUTER  
UNIVERSITAS AMIKOM YOGYAKARTA  
YOGYAKARTA  
2017**

# **PERSETUJUAN**

## **SKRIPSI**

### **ANALISIS DAN PEMANFAATAN ALGORITMA KRIPTOGRAFI UNTUK PENGKODEAN SERIAL NUMBER PADA APLIKASI BERBASIS DESKTOP**

yang dipersiapkan dan disusun oleh

**Adrianus Adi**

**12.11.6118**

telah disetujui oleh Dosen Pembimbing Skripsi  
pada tanggal 1 November 2016

**Dosen Pembimbing,**



**Krisnawati, S.Si, M.T.**  
**NIK. 190302038**

# PENGESAHAN

## SKRIPSI

### ANALISIS DAN PEMANFAATAN ALGORITMA KRIPTOGRAFI UNTUK PENGKODEAN SERIAL NUMBER PADA APLIKASI BERBASIS DESKTOP

yang dipersiapkan dan disusun oleh

**Adrianus Adi**

**12.11.6118**

telah dipertahankan di depan Dewan Penguji  
pada tanggal 25 Februari 2017

#### Susunan Dewan Penguji

**Nama Penguji**

**Tanda Tangan**

**Krisnawati, S.Si, M.T.**  
**NIK. 190302038**



**Mei P Kurniawan, M.Kom**  
**NIK. 190302187**



**Robert Marco, M.T.**  
**NIK. 190302228**



Skripsi ini telah diterima sebagai salah satu persyaratan  
untuk memperoleh gelar Sarjana Komputer  
Tanggal 25 Februari 2017



## PERNYATAAN

Saya yang bertandatangan dibawah ini menyatakan bahwa, Tugas Akhir ini merupakan karya saya (ASLI), dan isi dalam Tugas Akhir ini tidak terdapat karya yang pernah diajukan oleh orang lain untuk memperoleh gelar akademis di suatu institusi pendidikan tinggi manapun, dan sepanjang pengetahuan saya tidak terdapat karya atau pendapat yang pernah ditulis dan/atau diterbitkan oleh orang lain, kecuali yang secara tertulis diacu dalam naskah ini dan disebutkan dalam daftar pustaka.

Segala sesuatu yang terkait dengan naskah dan karya yang telah dibuat adalah menjadi tanggungjawab saya pribadi.

Yogyakarta, 25 Februari 2017

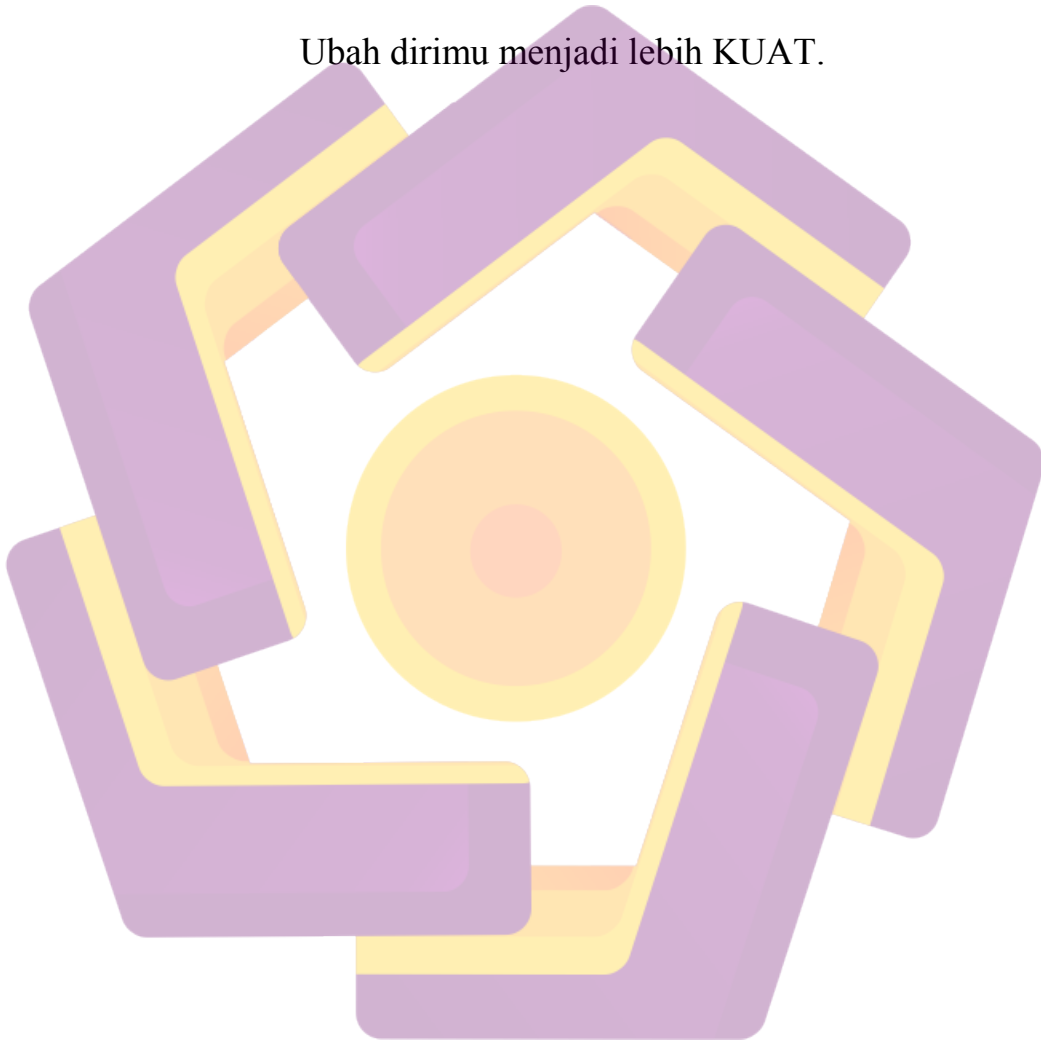


Adrianus Adi  
NIM. 12.11.6118

## **MOTTO**

Ketika kehidupan berubah menjadi lebih SULIT

Ubah dirimu menjadi lebih KUAT.



## PERSEMBAHAN

Dengan mengucapkan rasa syukur yang tak terhingga atas karunia Tuhan yang maha kuasa. Skripsi ini dipersembahkan kepada mereka yang telah berjasa dan menginspirasi penulis.

1. Tuhan yang maha kuasa yang terus menyertai dan memberi kekuatan dalam menghadapi rintangan-rintangan yang penulis hadapi.
2. Kedua orang tua yang senantiasa bersabar dalam mendukung, berdoa, dan memberi semangat untuk penulis.
3. Keluarga besar yang selalu mendoakan dan memberi nasihat-nasihat bagi penulis.
4. Seluruh teman-teman kelas 12 S1TI 06 yang telah memberi kenangan yang tak terlupakan semasa kuliah dan saling bahu-membahu dalam menyelesaikan setiap *final project*.
5. Serta seluruh pihak yang telah banyak membantu dan tidak bisa disebutkan satu per satu, dengan penuh rasa bahagia penulis ucapkan terima kasih banyak.

## KATA PENGANTAR

Puji dan syukur penulis persembahkan kepada Tuhan yang maha kuasa yang telah meyertai penulis dalam menyelesaikan skripsi yang berjudul Analisis dan Pemanfaatan Algoritma Kriptografi untuk Pengkodean Serial Number pada Aplikasi berbasis Desktop dapat terselesaikan.

Penulisan skripsi ini di ajukan untuk memenuhi salah satu syarat kelulusan dalam jenjang perkuliahan Strata 1 Universitas AMIKOM Yogyakarta, penulis menyadari bahwa dalam penyelesaian penulisan skripsi ini juga berkat dukungan, dorongan, dan bimbingan dari berbagai pihak, untuk itu penulis ucapkan terima kasih kepada:

1. Bapak Prof. Dr. M. Suyanto, MM selaku Ketua Universitas AMIKOM Yogyakarta.
2. Ibu Krisnawati, S.Si., M.T. selaku dosen pembimbing yang telah membantu dalam pembuatan skripsi ini.
3. Segenap Staf Pengajar di Universitas AMIKOM Yogyakarta yang telah memberi ilmu dan pemahaman tentang dunia informatika.
4. Keluarga besar yang selalu memberikan doa dan dukungan selama kuliah.
5. Teman-teman yang telah banyak membantu dalam menyelesaikan skripsi ini.

Disadari bahwa dalam penyusunan laporan skripsi ini masih jauh dari kata sempurna. Oleh karna itu kritik dan saran yang bersifat membntu sangat di butuhkan.

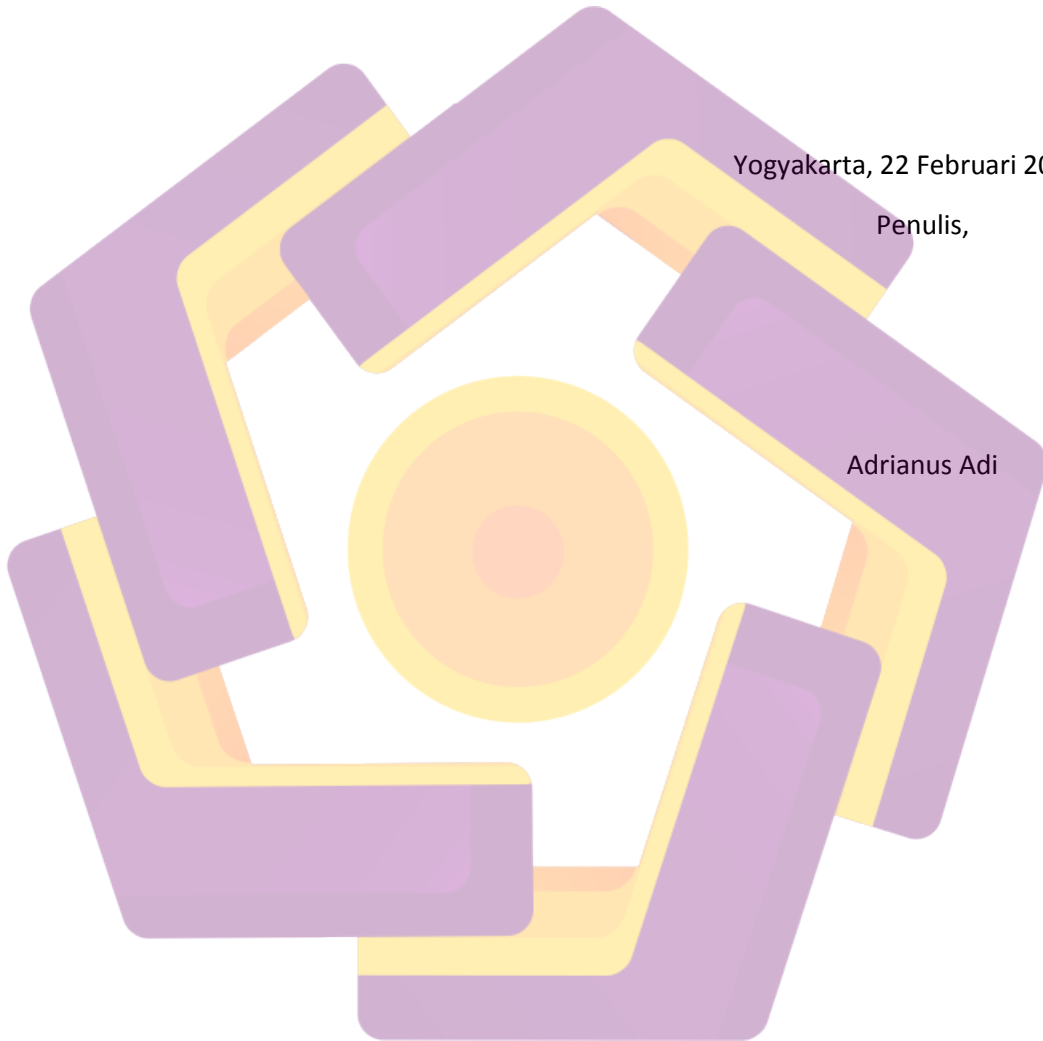


Akhir kata, semoga penyusunan skripsi ini bermanfaat di kemudian hari, khususnya bagi penulisan dan umumnya bagi kita semua dalam rangka menambah wawasan pengetahuan dan pemikiran kita.

Yogyakarta, 22 Februari 2017

Penulis,

Adrianus Adi



## DAFTAR ISI

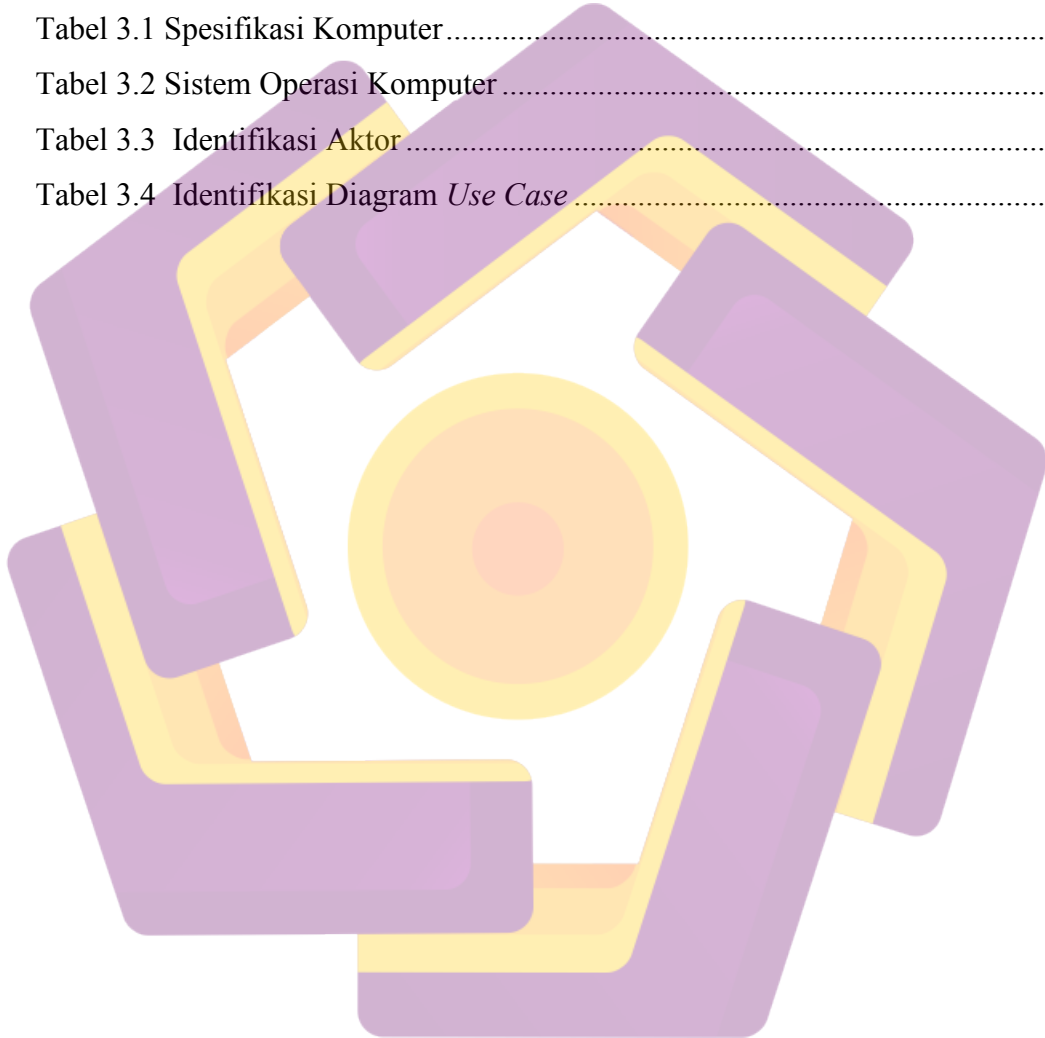
JUDUL .....	i
PERSETUJUAN .....	ii
PENGESAHAN .....	iii
PERNYATAAN.....	iv
MOTTO .....	v
PERSEMBAHAN.....	vi
KATA PENGANTAR.....	vii
DAFTAR ISI.....	viii
DAFTAR TABEL.....	xii
DAFTAR GAMBAR.....	xiii
INTISARI.....	xiv
<i>ABSTRACT</i> .....	xv
BAB I PENDAHULUAN.....	1
1.1 Latar Belakang Masalah .....	1
1.2 Rumusan Masalah.....	3
1.3 Batasan Masalah .....	3
1.4 Maksud dan Tujuan Penelitian.....	4
1.5 Metode Penelitian .....	4
1.5.1 Metode Pengumpulan Data.....	4
1.5.2 Metode Analisis .....	5
1.5.3 Metode Perancangan.....	5
1.5.4 Metode Pengembangan.....	5
1.5.5 Metode Testing .....	5
1.6 Sistematika Penulisan .....	6
BAB II LANDASAN TEORI.....	7
2.1 Tinjauan Pustaka.....	7
2.2 Konsep Kriptografi .....	8
2.2.1 Pengertian Kriptografi .....	8
2.2.2 Algoritma Kriptografi .....	9

2.2.3	<i>Advanced Encryption Standard (AES)</i> .....	12
2.2.4	MD-5 .....	15
2.2.5	Tujuan Kriptografi .....	17
2.3	Konsep Analisis .....	18
2.3.1	Analisis SWOT .....	19
2.3.2	Analisis Kebutuhan .....	19
2.3.3	Analisis Keleyakan .....	20
2.4	Konsep Sistem Berorientasi Objek .....	21
2.5	<i>Unified Modeling Language (UML)</i> .....	22
2.5.1	<i>Use Case Diagram</i> .....	24
2.5.2	<i>Activity Diagram</i> .....	25
2.5.3	<i>Class Diagram</i> .....	26
2.5.4	<i>Sequence Diagram</i> .....	27
2.6	Konsep Testing .....	30
<b>BAB III ANALISIS DAN PERANCANGAN</b> .....		<b>32</b>
3.1	Tujuan Aplikasi .....	32
3.2	Analisis SWOT .....	32
3.2.1	Analisis kekuatan ( <i>Strength</i> ) .....	32
3.2.2	Analisis Kelemahan ( <i>Weaknesses</i> ) .....	33
3.2.3	Analisis Peluang ( <i>Opportunity</i> ) .....	33
3.2.4	Analisis Ancaman ( <i>threats</i> ) .....	34
3.3	Analisis Kebutuhan Sistem .....	34
3.3.1	Kebutuhan Fungsional .....	34
3.3.2	Kebutuhan Non Fungsional .....	35
3.4	Analisis Kelayakan Sistem .....	36
3.4.1	Kelayakan Teknologi .....	36
3.4.2	Kelayakan Operasional .....	36
3.4.3	Kelayakan Hukum .....	36
3.4.4	Kebutuhan Pengguna .....	37
3.5	Perancangan Sistem .....	37
3.5.1	Perancangan UML .....	38

3.5.1.1	<i>Use Case Diagram</i> .....	38
3.5.1.2	<i>Activity Diagram</i> .....	40
3.5.1.3	<i>Class Diagram</i> .....	42
3.5.1.4	<i>Sequence Diagram</i> .....	43
3.5.2	Perancangan <i>Interface</i> .....	44
3.5.2.1	Perancangan Form Register .....	44
3.5.2.2	<i>Splash Screen</i> .....	44
BAB IV IMPLEMENTASI DAN PEMBAHASAN .....		45
4.1	IMPLEMENTASI .....	45
4.1.1	IMPLEMENTASI AES 128 .....	45
4.1.1.1	S-Box .....	45
4.1.1.2	Proses <i>Sub Byte</i> .....	47
4.1.1.3	Proses <i>Shift Row</i> .....	48
4.1.1.4	Proses <i>Mix Column</i> .....	49
4.1.1.5	Proses <i>Add Round Key</i> .....	51
4.1.1.6	Proses Enkripsi .....	52
4.1.2	Implementasi Menu Register .....	53
4.1.3	Implementasi <i>Splash Screen</i> .....	53
4.2	Pembahasan .....	54
4.2.1	Sistem .....	54
4.2.2	Form Register .....	55
4.2.3	<i>Splash Screen</i> .....	55
4.2.4	Pengujian Sistem .....	55
BAB V PENUTUP .....		61
5.1	KESIMPULAN .....	61
5.2	SARAN .....	62
DAFTAR PUSTAKA .....		63
LAMPIRAN		

## DAFTAR TABEL

Tabel 2.1 Simbol-Simbol <i>Use Case diagram</i> .....	24
Tabel 2.2 Simbol-Simbol <i>Activity Diagram</i> .....	25
Tabel 2.3 Simbol-Simbol <i>Class Diagram</i> .....	26
Tabel 2.4 Simbol-Simbol <i>Sequence Diagram</i> .....	27
Tabel 3.1 Spesifikasi Komputer .....	35
Tabel 3.2 Sistem Operasi Komputer .....	35
Tabel 3.3 Identifikasi Aktor .....	38
Tabel 3.4 Identifikasi Diagram <i>Use Case</i> .....	39



## DAFTAR GAMBAR

Gambar 2.1 Proses Enkripsi AES 128 bit .....	15
Gambar 2.2 Proses Enkripsi MD-5 .....	17
Gambar 3.1 <i>Use Case</i> diagram.....	40
Gambar 3.2 <i>Activity Diagram</i> .....	41
Gambar 3.3 <i>Class Diagram</i> .....	42
Gambar 3.4 <i>Sequence Diagram</i> .....	43
Gambar 3.5 Form Register.....	44
Gambar 3.6 <i>Splash Screen</i> .....	44
Gambar 4.1 Tampilan Menu Register.....	53
Gambar 4.2 Tampilan <i>Splash Screen</i> .....	53
Gambar 4.3 Register form .....	56
Gambar 4.4 Get Code.....	57
Gambar 4.5 Generate form.....	58
Gambar 4.6 <i>Generate Process</i> .....	58
Gambar 4.7 <i>Register Process</i> .....	59
Gambar 4.8 <i>Warning Registration Complete</i> .....	59
Gambar 4.9 <i>Splash Screen</i> .....	60

## INTISARI

Di jaman sekarang perusahaan-perusahaan rekayasa perangkat lunak bersaing ketat dalam membuat dan menjual program. Program yang dibuat dapat mempunyai harga jual yang tinggi, sehingga dibutuhkan konsep yang dapat mengamankan program tersebut agar tidak mudah untuk diduplikasi.

Pada penelitian ini dilakukan analisa dan menerapkan algoritma kriptografi pada sistem yang akan dibuat untuk mengeneralisasi serial number dimana nantinya dapat diterapkan pada program yang akan dibuat. Sistem ini menyandikan serial number menggunakan algoritma kriptografi *Advanced Encryption Standard* 128 bit (AES128) agar serial number yang dibuat tidak dengan mudah dibaca. Dalam penelitiannya, program berbasis desktop dipilih sebagai objek penelitian. Namun tidak menutup kemungkinan sistem ini dapat diterapkan pada perangkat lain seperti aplikasi mobile, dan lain-lain.

Hasil dari penelitian ini berupa potongan serial number dari produk program yang diproduksi. Ketika program sudah diinstal maka komputer secara otomatis akan melakukan proses pengecekan terhadap serial number yang telah diregistrasikan.

**Kata Kunci:** Keamanan Program, Algoritma Kriptografi, Serial Number, Berbasis Dekstop.

## ***ABSTRACT***

*Nowadays companies competing software engineering in making and selling the program. The program created can have a high price. So it takes the concept to secure the program that are not easily to duplicate.*

*In this research, analysis and implement cryptographic algorithms in the system that will be made to generate the serial number which can then be applied to the program that will be made. These systems encode the serial number cryptographic algorithm using 128 bit Advanced Encryption Standard (AES128) so that the serial number that is made is not easily decrypted.*

*In his research, desktop-based programs have been selected as research objects. But there are possibilities of this system can be applied to other devices such as mobile applications, and others.*

*The results of this research is a piece of program serial number of the product being produced. When the program is installed, the computer will automatically do the process of checking the serial number that has been registered.*

***Keywords:*** *Program Security, Cryptographic Algorithms, Serial Number, Desktop Based.*

