



**ANALISIS PENGAMANAN DATA TELEMETRI DENGAN
ALGORITMA RIJNDAEL DAN TWOFISH PADA SISTEM
KOMUNIKASI SERIAL**

SKRIPSI

I DEWA GEDE ADHYATMA YASA GUANG

1410511060

UNIVERSITAS PEMBANGUNAN NASIONAL “VETERAN”

JAKARTA

FAKULTAS ILMU KOMPUTER

PROGRAM STUDI INFORMATIKA

2019



**ANALISIS PENGAMANAN DATA TELEMETRI DENGAN
ALGORITMA RIJNDAEL DAN TWOFISH PADA SISTEM
KOMUNIKASI SERIAL**

SKRIPSI

**Diajukan Sebagai Salah Satu Syarat Untuk Memperoleh Gelar
Sarjana Komputer**

I DEWA GEDE ADHYATMA YASA GUANG

1410511060

UNIVERSITAS PEMBANGUNAN NASIONAL “VETERAN”

JAKARTA

FAKULTAS ILMU KOMPUTER

PROGRAM STUDI INFORMATIKA

2019

PERNYATAAN ORISINALITAS

Skripsi ini adalah hasil karya sendiri, dan semua sumber yang dikutip maupun yang dirujuk telah saya nyatakan dengan benar.

Nama : I Dewa Gede Adhyatma Yasa Guang
NIM : 1410511060
Tanggal : 10 Januari 2019

Bilamana di kemudian hari ditemukan ketidaksesuaian dengan pernyataan saya ini, maka saya bersedia dituntut dan diproses sesuai dengan ketentuan yang berlaku.

Jakarta, 10 Januari 2019

Yang Menyatakan,



(I Dewa Gede Adhyatma Yasa Guang)

PERNYATAAN PERSETUJUAN PUBLIKASI SKRIPSI UNTUK KEPENTINGAN AKADEMIS

Sebagai civitas akademik Universitas Pembangunan Nasional "Veteran" Jakarta, saya yang bertanda tangan di bawah ini:

Nama : I Dewa Gede Adhyatma Yasa Guang
NIM : 1410511060
Fakultas : Ilmu Komputer
Program Studi : Informatika

Demi pengembangan ilmu pengetahuan, menyetujui untuk memberikan kepada Universitas Pembangunan Nasional "Veteran" Jakarta Hak Bebas Royalti Non eksklusif (*Non-exclusive Royalty Free Right*) atas karya ilmiah saya yang berjudul:

**"Analisis Pengamanan Data Telemetry Dengan Algoritma Rijndael Dan
Twofish Pada Sistem Komunikasi Serial"**

Beserta perangkat yang ada (jika diperlukan). Dengan Hak Bebas Royalti ini Universitas Pembangunan Nasional "Veteran" Jakarta berhak menyimpan, mengalih media/formatkan, mengelola dalam bentuk pangkalan data (*database*), merawat, dan mempublikasikan Skripsi saya selama tetap mencantumkan nama saya sebagai penulis/pencipta dan sebagai pemilik Hak Cipta.

Demikian pernyataan ini saya buat dengan sebenarnya.

Dibuat di : Jakarta

Pada tanggal : 10 Januari 2019

Yang menyatakan,



(I Dewa Gede Adhyatma Yasa Guang)

PENGESAHAN

Dengan ini dinyatakan bahwa Tugas Akhir berikut:

Nama : I Dewa Gede Adhyatma Yasa Agung

NIM : 1410511006

Program Studi : Informatika

Judul Tugas Akhir : Analisa Pengamanan Data Telemetri Dengan Algoritma Rijndael Dan Twofish Pada Sistem Komunikasi Serial

Telah berhasil dipertahankan di hadapan Tim Penguji dan diterima sebagai bagian persyaratan yang diperlukan untuk memperoleh gelar Sarjana Komputer pada Program Studi Informatika, Fakultas Ilmu Komputer, Universitas Pembangunan Nasional "Veteran" Jakarta.



Bayu Hananto, S.Kom, M.Kom.
Ketua Penguji



Indra Permana S., S.Kom, M.Kom.
Anggota Penguji



Ridwan Raafi'udin, S.Kom, M.Kom.
Pembimbing I



Henki Bayu S., S.Kom., M.T.I.
Pembimbing II



Dr. Ermatita, M.Kom
Dekan



Anita Muliawati, S.Kom., MTI
Ketua Program Studi

Ditetapkan di : Jakarta

Tanggal Ujian : 10 Januari 2019

ANALISIS PENGAMANAN DATA TELEMETRI DENGAN ALGORITMA RIJNDAEL DAN TWOFISH PADA SISTEM KOMUNIKASI SERIAL

I Dewa Gede Adhyatma Yasa Guang

ABSTRAK

Perkembangan teknologi terutama pada penggunaan alat-alat elektronik kini sudah memasuki tahap baru dimana alat-alat tersebut mulai menggunakan telemetri dengan ataupun tanpa kabel sebagai media komunikasi terutama pada teknologi robotika. Salah satu cara komunikasi pada teknologi robotika yaitu dengan serial data yang menggunakan komputer sebagai media untuk memberikan perintah hingga memberikan informasi-informasi yang diperlukan untuk memenuhi suatu kebutuhan. Dari kepentingan inilah serial data perlu diamankan dan dengan didasari komunikasi pemberian perintah untuk melakukan atau mendapat sesuatu yang diinginkan tentu dibutuhkan sebuah media untuk mengamankan komunikasi ini, yaitu Kriptografi. Kriptografi bekerja dengan menyandikan pesan atau informasi yang dikirim lalu menetralkannya kembali menjadi sebuah informasi, dengan sistem inilah pengiriman dan penerimaan informasi dapat diamankan dari orang-orang yang tidak diinginkan. Beberapa pengamanan Kriptografi yang kini banyak digunakan yaitu algoritma *Advanced Encryption Standard (AES)* Rijndael dan Twofish, dan dengan dilandasi kebutuhan atas pengamanan pada komunikasi maka penganalisaan untuk menemukan algoritma yang baik dan sesuai diperlukan.

Kata Kunci : Robotika, Telemetri, Komunikasi Serial, Kriptografi, Rijndael, Twofish

ANALYSIS OF TELEMETRY DATA SECURITY WITH RIJNDAEL AND TWOFISH ALGORITHM IN SERIAL COMMUNICATION SYSTEM

I Dewa Gede Adhyatma Yasa Guang

ABSTRACT

Technology development, especially in the use of electronic devices, has now entered a new phase where tools start using telemetry with or without cables as a communication media, especially in robotics technology. One way of communication in robotics technology is serial data that uses computers as a medium to give commands to provide information needed to fulfill a need. From this interest, the serial data needs to be secured and based on the communication of giving orders to do something or get something certainly the media needed to be secured, namely Cryptography. Cryptography works by encoding messages or information sent and then neutralizes them back into information, with this system sending and receiving information can be secured from unwanted people. Cryptographic security which is now widely used, namely the algorithm *Advanced Encryption Standard (AES)* Rijndael and Twofish, and based on the need for security in communication, analyzing to find a good and appropriate algorithm is needed.

Keywords : Robotics, Telemetry, Serial Communication, Cryptography, Rijndael, Twofish

KATA PENGANTAR

Pertama-tama penulis panjatkan puji syukur kehadirat Tuhan Yang Maha Esa atas segala rahmat, hidayah, dan karunia-Nya kepada penulis sehingga proposal Tugas Akhir dengan judul "Analisis Pengamanan Data Telemetry Dengan Algoritma Rijndael Dan Twofish Pada Sistem Komunikasi Serial" dapat terselesaikan dengan baik. Penulis ingin mengucapkan terimakasih kepada:

1. Bapak Ridwan Ra'afiudin., S.Kom., M.Kom, dan Bapak Henki Bayu Seta., S.Kom., M.Kom, selaku dosen pembimbing skripsi, terima kasih untuk ilmunya yang diberikan dan telah memberikan saran dan masukan yang bermanfaat untuk menyelesaikan laporan ini.
2. Ibu Dr. Ermatita, M.Kom. Selaku Dekan Fakultas Ilmu Komputer Universitas Pembangunan Nasional "Veteran" Jakarta.
3. Ibu Anita Muliawati, S.Kom., M.T.I. Selaku Ketua Program Studi Informatika Universitas Pembangunan Nasional "Veteran" Jakarta.
4. Kedua orang tua dan keluarga yang telah memberikan semangat dan doa kepada penulis agar dapat menyelesaikan skripsi ini dengan baik.
5. Teman-teman Teknik Informatika angkatan 2014, KSM Robotika, dan seluruh rekan mahasiswa, terima kasih atas saran dan bantuannya serta semangat yang diberikan selama ini.

Akhir kata penulis menyadari bahwa dalam penulisan skripsi ini masih jauh dari kesempurnaan. Karena itu, penulis memohon saran dan kritik yang sifatnya membangun demi kesempurnaan dan semoga bermanfaat bagi kita semua.

Jakarta, 10 Januari 2019

Penulis



I Dewa Gede Adhyatma Yasa Guang

DAFTAR ISI

PERNYATAAN ORISINALITAS	ii
PERNYATAAN PERSETUJUAN PUBLIKASI SKRIPSI UNTUK KEPENTINGAN AKADEMIS	iii
PENGESAHAN	iii
ABSTRAK.....	v
ABSTRACT	vi
KATA PENGANTAR.....	vii
DAFTAR ISI	viii
DAFTAR TABEL.....	xi
DAFTAR GAMBAR	xii
DAFTAR LAMPIRAN	xiii
BAB I PENDAHULUAN	1
1.1 Latar Belakang	1
1.2 Rumusan Masalah.....	2
1.3 Ruang Lingkup	2
1.4 Tujuan Penelitian	3
1.5 Manfaat Penelitian	3
1.6 Sistematika Penulisan.....	4
BAB II LANDASAN TEORI.....	6
2.1 Kriptografi dan Penyandian.....	6
2.1.1 Kriptografi Klasik	8
2.1.2 Kriptografi Modern.....	10

2.1.3	Sistem Kriptografi.....	12
2.2	Kriptografi AES: Rijndael.....	15
2.2.1	Enkripsi AES: Rijndael.....	17
2.2.2	Dekripsi AES: Rijndael.....	22
2.3	Kriptografi <i>Twofish</i>	25
2.4	Telemetry	30
2.5	Arduino.....	30
2.5.1	<i>Board</i> Arduino Mega 2560.....	31
2.6	Studi Litelatur	32
BAB III METODOLOGI PENELITIAN.....		34
3.1	Kerangka Pikir	34
3.1.1	Identifikasi Masalah.....	35
3.1.2	Studi Literatur.....	35
3.1.3	Perancangan Sistem	36
3.1.4	Pengujian Sistem	36
3.1.5	Dokumentasi.....	36
3.2	Komponen Alat dan Bahan Penelitian	36
3.3	Waktu dan Tempat Penelitian.....	36
3.4	Jadwal Penelitian	37
BAB IV HASIL DAN PEMBAHASAN.....		38
4.1	Rancangan Proses Enkripsi Dan Dekripsi.....	38
4.1.1	Perancangan Enkripsi dan Dekripsi Data.....	38
4.2	Rancang Program Rijndael.....	39
4.2.1	Perhitungan Manual Rijndael	40
4.3	Rancang Program Twofish.....	73

4.4	Hasil Enkripsi dan Dekripsi Data	85
4.4.1	Hasil Enkripsi dan Dekripsi Data Dengan Rijndael	85
4.4.2	Hasil Enkripsi dan Dekripsi Data Dengan Twofish.....	87
4.5	Implementasi Alat Peraga	88
4.5.1	Rancangan Bangun Sistem Arduino	88
4.5.2	Rancang Program Rijndael Pada Arduino	90
4.5.3	Hasil Rancang Program Rijndael Pada Arduino	92
BAB V PENUTUP.....		93
5.1	Kesimpulan.....	93
5.2	Saran.....	93
DAFTAR PUSTAKA		
RIWAYAT HIDUP		
LAMPIRAN		

DAFTAR TABEL

Tabel 2.1. Hubungan Antara Heksadesimal, Desimal, dan Biner	11
Tabel 2.2. Operasi XOR	11
Tabel 2.3. Tiga jenis AES berdasarkan jumlah kunci	16
Tabel 2.4. Rijndael S-Box	18
Tabel 2.5. Inverse S-box.....	23
Tabel 2.6. Tabel Spesifikasi Arduino Mega 2560	31
Tabel 3.1. Jadwal Penelitian	37
Tabel 4.1. Hasil Enkripsi dan Dekripsi Data Dengan Rijndael	85
Tabel 4.2. Hasil Enkripsi dan Dekripsi Data Dengan Twofish	85

DAFTAR GAMBAR

Gambar 2. 1 Area bidang kriptologi	6
Gambar 2. 2 Substitusi Caesar Chiper (n+3)	7
Gambar 2. 3 Mekanisme kriptografi kunci simetrik	14
Gambar 2. 4 Mekanisme kriptografi kunci asimetrik	15
Gambar 2. 5 Diagram proses enkripsi AES: Rijndael	17
Gambar 2. 6 Transformasi <i>SubBytes</i>	19
Gambar 2. 7 Proses <i>ShiftRows</i>	19
Gambar 2. 8 Transformasi <i>MixColumns</i>	20
Gambar 2. 9 Transformasi <i>AddRoundKey</i>	21
Gambar 2. 10 Diagram proses dekripsi algoritma AES Rijndael	22
Gambar 2. 11 Transformasi <i>InversShiftRows</i>	23
Gambar 2. 12 Struktur Algoritma Twofish	25
Gambar 3. 1 Flowchart Kerangka Pikir	34
Gambar 4. 1 Arsitektur Proses Enkripsi Dan Dekripsi	38
Gambar 4. 2 Rancang Bangun Sistem Alat Peraga	88
Gambar 4. 3 Model Bangun Sistem Alat Peraga	89
Gambar 4. 4 Model Bangun Sistem Alat Peraga (2)	89
Gambar 4. 5 Implementasi Algoritma Kriptografi Pada Arduino	92

DAFTAR LAMPIRAN

Lampiran 1. Surat Riset Peneliiian

Lampiran 2. Tabel ASCII (*American Standard Code of Information Interchange*)

Lampiran 3. Contoh Perhitungan Manual Twofish