

PERANCANGAN DAN IMPLEMENTASI METODE KRIPTOGRAFI DATA TEKS ADVANCED ENCRYPTION STANDARD (AES) DALAM SISTEM KOMUNIKASI BERBASIS NEAR FIELD COMMUNICATION (NFC)

Johnny Immanuel Budikurniawan Christian

1122016

Program Studi Teknik Elektro, Fakultas Teknik, Universitas Kristen Maranatha

Jl. Prof. Drg. Surya Sumantri 65, Bandung 40164, Jawa Barat, Indonesia

E – Mail : johnnychristian93@gmail.com

ABSTRAK

Penggunaan smart card pada abad ke – 21 semakin dibutuhkan oleh manusia untuk berbagai keperluan, salah satunya adalah untuk mendukung proses transaksi perbankan yang lebih cepat dan aman. Salah satu faktor yang mendukung keamanan penyimpanan data pribadi di dalam smart card adalah dengan menggunakan metode kriptografi data teks. Namun, banyak smart card yang masih menggunakan metode kriptografi data teks tipe lama, yaitu Data Encryption Standard (DES), yang telah usang dan rentan terhadap pencurian data pribadi di dalamnya.

Pada Tugas Akhir ini, akan dirancang aplikasi pengisian data dan aplikasi pembacaan data smart card MIFARE Classic 1K dengan menggunakan metode kriptografi data teks tipe baru, yaitu Advanced Encryption Standard (AES), dalam bahasa pemrograman C++. Proses pertukaran data antara smart card MIFARE Classic 1K dan kedua aplikasi tersebut dilakukan dengan bantuan smart card reader ACR 1252U dalam teknologi komunikasi berbasis Near Field Communication (NFC). Versi metode kriptografi data teks AES yang digunakan adalah AES – 128.

Berdasarkan hasil pengujian, metode kriptografi data teks AES dapat diimplementasikan pada aplikasi pengisian data dan aplikasi pembacaan data smart card MIFARE Classic 1K dengan baik menggunakan dua versi AES, yaitu metode kriptografi AES versi asli dan metode kriptografi AES versi modifikasi.

Kata Kunci : Kriptografi, AES, NFC, MIFARE, C++

DESIGN AND IMPLEMENTATION OF ADVANCED ENCRYPTION STANDARD (AES) TEXT DATA CRYPTOGRAPHY METHOD IN NEAR FIELD COMMUNICATION (NFC) BASED COMMUNICATION SYSTEM

Johnny Immanuel Budikurniawan Christian

1122016

Department of Electrical Engineering, Maranatha Christian University

Prof. Drg. Surya Sumantri St. 65, Bandung 40164, West Java, Indonesia

E – Mail : johnnychristian93@gmail.com

ABSTRACT

The use of smart cards in the 21st century increasingly needed by humans for various purposes, one of which is to support the faster and safer of banking transaction process. One of the factors that support the security of personal data storage in the smart card is by using the text data cryptography methods. However, there are many smart cards that still using the old type of text data cryptography method, namely the Data Encryption Standard (DES), which was outdated and vulnerable to theft of personal data inside it.

In this Final Project, there will be designed data writing application and data reading application of MIFARE Classic 1K smart card using the new type of text data cryptography method, namely the Advanced Encryption Standard (AES), in the C++ programming language. The process of data exchange between MIFARE Classic 1K smart card and both applications is done with the help of ACR 1252U smart card reader in Near Field Communication (NFC) based communication technology. The version of AES text data cryptography method used is AES – 128.

Based on the test results, AES text data cryptography method can be implemented on data writing application and data reading application of MIFARE Classic 1K smart card well using two versions of AES, namely the original version of AES cryptography method and the modified version of AES cryptography method.

Keywords : **Cryptography, AES, NFC, MIFARE, C++**

DAFTAR ISI

LEMBAR PENGESAHAN	
PERNYATAAN ORISINALITAS LAPORAN TUGAS AKHIR	
PERNYATAAN PUBLIKASI LAPORAN TUGAS AKHIR	
PRAKATA	
ABSTRAK	i
ABSTRACT	ii
DAFTAR ISI	iii
DAFTAR TABEL	vii
DAFTAR GAMBAR	viii
DAFTAR RUMUS	xi
DAFTAR LAMPIRAN	xiii
DAFTAR SINGKATAN	xiv
 BAB I PENDAHULUAN	 1
1.1 Latar Belakang Masalah	1
1.2 Identifikasi Masalah	3
1.3 Rumusan Masalah	3
1.4 Tujuan	4
1.5 Pembatasan Masalah	4

1.6	Metodologi Penelitian	5
1.7	Spesifikasi Alat Yang Digunakan	5
1.8	Sistematika Penulisan	6
BAB II LANDASAN TEORI		7
2.1	Kriptografi	7
2.2	Metode Kriptografi Data Teks AES (<i>Advanced Encryption Standard</i>)	10
2.2.1	Proses Enkripsi Menggunakan Metode Kriptografi Data Teks AES (<i>Advanced Encryption Standard</i>)	11
2.2.2	Proses Dekripsi Menggunakan Metode Kriptografi Data Teks AES (<i>Advanced Encryption Standard</i>)	22
2.3	RFID (<i>Radio Frequency Identification</i>)	28
2.3.1	Cara Kerja RFID	29
2.4	NFC (<i>Near Field Communication</i>)	30
2.5	MIFARE Classic 1K	32
2.5.1	Organisasi Memori MIFARE Classic 1K	33
2.5.2	Prinsip Komunikasi Data MIFARE Classic 1K	36
2.6	<i>Contactless Smart Card Reader ACR 1252U</i>	36
2.7	Microsoft Visual Studio 2008 C++ .NET	38

BAB III PERANCANGAN DAN REALISASI 40

3.1	Metode Kriptografi Data Teks AES (<i>Advanced Encryption Standard</i>) Versi Modifikasi	40
3.2	Perancangan Perangkat Keras	41
3.3	Perancangan Perangkat Lunak	43
3.3.1	Aplikasi Pengisian Data <i>Smart Card</i> MIFARE Classic 1K Menggunakan Metode Enkripsi AES	45
3.3.2	Program Enkripsi AES Dalam Aplikasi Pengisian Data <i>Smart Card</i> MIFARE Classic 1K Menggunakan Metode Enkripsi AES	49
3.3.3	Aplikasi Pembacaan Data <i>Smart Card</i> MIFARE Classic 1K Menggunakan Metode Dekripsi AES	52
3.3.4	Program Dekripsi AES Dalam Aplikasi Pembacaan Data <i>Smart Card</i> MIFARE Classic 1K Menggunakan Metode Dekripsi AES	56
3.3.5	APDU (<i>Application Protocol Data Unit</i>)	59
3.3.6	Fungsi hex2bin	61
3.3.7	Fungsi bin2hex	62
3.3.8	Fungsi dec2bin	63
3.3.9	Fungsi bin2dec	64
3.3.10	Fungsi format_biner	65
3.3.11	Fungsi ascii2hex	66

3.3.12	Fungsi ex_or	67
3.3.13	Fungsi sbox dan isbox	68
3.3.14	Fungsi mixcolumns2	69
3.3.15	Fungsi mixcolumns3	70
3.3.16	Fungsi imixcolumns9	71
3.3.17	Fungsi imixcolumns11	72
3.3.18	Fungsi imixcolumns13	73
3.3.19	Fungsi imixcolumns14	74
3.3.20	Fungsi addnull	75
3.3.21	Fungsi clock	76
BAB IV	DATA PENGAMATAN DAN ANALISA	77
4.1	Pengujian Performa Metode Kriptografi Data Teks AES	77
4.2	Analisa Hasil Pengujian Performa Metode Kriptografi Data Teks AES	86
BAB V	SIMPULAN DAN SARAN	87
5.1	Simpulan	87
5.2	Saran	88
DAFTAR REFERENSI		89
LAMPIRAN		

DAFTAR TABEL

Tabel 2.1	Tabel Konversi Karakter ASCII	13
Tabel 2.2	Tabel <i>Substitution Box</i> (S – Box) AES	14
Tabel 2.3	Tabel Nilai <i>Round Constant</i> AES – 128	15
Tabel 2.4	Tabel Kebenaran <i>Exclusive – OR</i> (XOR)	16
Tabel 2.5	Tabel <i>Inverse Substitution Box</i> (IS – Box) AES	25
Tabel 3.1	Tabel <i>Substitution Box</i> (S – Box) AES Versi Modifikasi	40
Tabel 3.2	Tabel <i>Inverse Substitution Box</i> (IS – Box) AES Versi Modifikasi	41
Tabel 4.1	<i>Input</i> Data Percobaan 1	78
Tabel 4.2	<i>Input</i> Data Percobaan 2	79
Tabel 4.3	Hasil Percobaan 1 Metode AES Versi Asli	81
Tabel 4.4	Hasil Percobaan 1 Metode AES Versi Modifikasi	81
Tabel 4.5	Hasil Percobaan 2 Metode AES Versi Asli	82
Tabel 4.6	Hasil Percobaan 2 Metode AES Versi Modifikasi	82
Tabel 4.7	Rata – Rata Hasil Percobaan 1	83
Tabel 4.8	Rata – Rata Hasil Percobaan 2	83

DAFTAR GAMBAR

Gambar 2.1	Diagram Blok Proses Enkripsi AES	12
Gambar 2.2	Urutan Penempatan Data Pada Blok – Blok Matriks	13
Gambar 2.3	Tahapan Pertama Proses <i>Key Expansion</i>	14
Gambar 2.4	Proses Substitusi Menggunakan S – Box AES	15
Gambar 2.5	<i>Left Shift</i> Pada Proses <i>Shift Rows</i>	18
Gambar 2.6	Proses <i>Mix Columns</i>	19
Gambar 2.7	Diagram Proses Enkripsi AES	21
Gambar 2.8	Diagram Blok Proses Dekripsi AES	22
Gambar 2.9	<i>Right Shift</i> Pada Proses <i>Inverse Shift Rows</i>	25
Gambar 2.10	Proses <i>Inverse Mix Columns</i>	27
Gambar 2.11	Contoh <i>Tag</i> RFID	29
Gambar 2.12	Logo NFC	31
Gambar 2.13	<i>Contactless Smart Card</i> MIFARE Classic 1K	32
Gambar 2.14	Desain <i>Smart Card</i> MIFARE Classic 1K	33
Gambar 2.15	Organisasi Memori MIFARE Classic 1K	34
Gambar 2.16	<i>Contactless Smart Card Reader</i> ACR 1252U	37
Gambar 2.17	Spesifikasi <i>Contactless Smart Card Reader</i> ACR 1252U	38
Gambar 2.18	Tampilan Antarmuka Microsoft Visual Studio 2008	39

Gambar 3.1	Proses Komunikasi Sistem	42
Gambar 3.2	Organisasi Memori MIFARE Classic 1K Dalam Pengujian Performa Metode Kriptografi Data Teks AES	43
Gambar 3.3	Aplikasi Pengisian Data <i>Smart Card</i> MIFARE Classic 1K Menggunakan Metode Enkripsi AES	45
Gambar 3.4	<i>Flowchart</i> Aplikasi Pengisian Data <i>Smart Card</i> MIFARE Classic 1K Menggunakan Metode Enkripsi AES	46
Gambar 3.5	<i>Flowchart</i> Program Enkripsi AES (Bagian 1)	50
Gambar 3.6	<i>Flowchart</i> Program Enkripsi AES (Bagian 2)	51
Gambar 3.7	Aplikasi Pembacaan Data <i>Smart Card</i> MIFARE Classic 1K Menggunakan Metode Dekripsi AES	53
Gambar 3.8	<i>Flowchart</i> Aplikasi Pembacaan Data <i>Smart Card</i> MIFARE Classic 1K Menggunakan Metode Dekripsi AES	54
Gambar 3.9	<i>Flowchart</i> Program Dekripsi AES (Bagian 1)	57
Gambar 3.10	<i>Flowchart</i> Program Dekripsi AES (Bagian 2)	58
Gambar 3.11	APDU Fungsi Autentikasi	59
Gambar 3.12	APDU Fungsi Pengisian Data <i>Smart Card</i>	60
Gambar 3.13	APDU Fungsi Pembacaan Data <i>Smart Card</i>	60
Gambar 3.14	<i>Flowchart</i> Fungsi hex2bin	61
Gambar 3.15	<i>Flowchart</i> Fungsi bin2hex	62
Gambar 3.16	<i>Flowchart</i> Fungsi dec2bin	63
Gambar 3.17	<i>Flowchart</i> Fungsi bin2dec	64

Gambar 3.18	<i>Flowchart</i> Fungsi format_biner	65
Gambar 3.19	<i>Flowchart</i> Fungsi ascii2hex	66
Gambar 3.20	<i>Flowchart</i> Fungsi ex_or	67
Gambar 3.21	<i>Flowchart</i> Fungsi sbbox dan isbox	68
Gambar 3.22	<i>Flowchart</i> Fungsi mixcolumns2	69
Gambar 3.23	<i>Flowchart</i> Fungsi mixcolumns3	70
Gambar 3.24	<i>Flowchart</i> Fungsi imixcolumns9	71
Gambar 3.25	<i>Flowchart</i> Fungsi imixcolumns11	72
Gambar 3.26	<i>Flowchart</i> Fungsi imixcolumns13	73
Gambar 3.27	<i>Flowchart</i> Fungsi imixcolumns14	74
Gambar 3.28	<i>Flowchart</i> Fungsi addnull	75
Gambar 4.1	Grafik Proses Pengisian Data (Rata – Rata Hasil Percobaan 1)	84
Gambar 4.2	Grafik Proses Pengisian Data (Rata – Rata Hasil Percobaan 2)	84
Gambar 4.3	Grafik Proses Pembacaan Data (Rata – Rata Hasil Percobaan 1) .	85
Gambar 4.4	Grafik Proses Pembacaan Data (Rata – Rata Hasil Percobaan 2) .	85

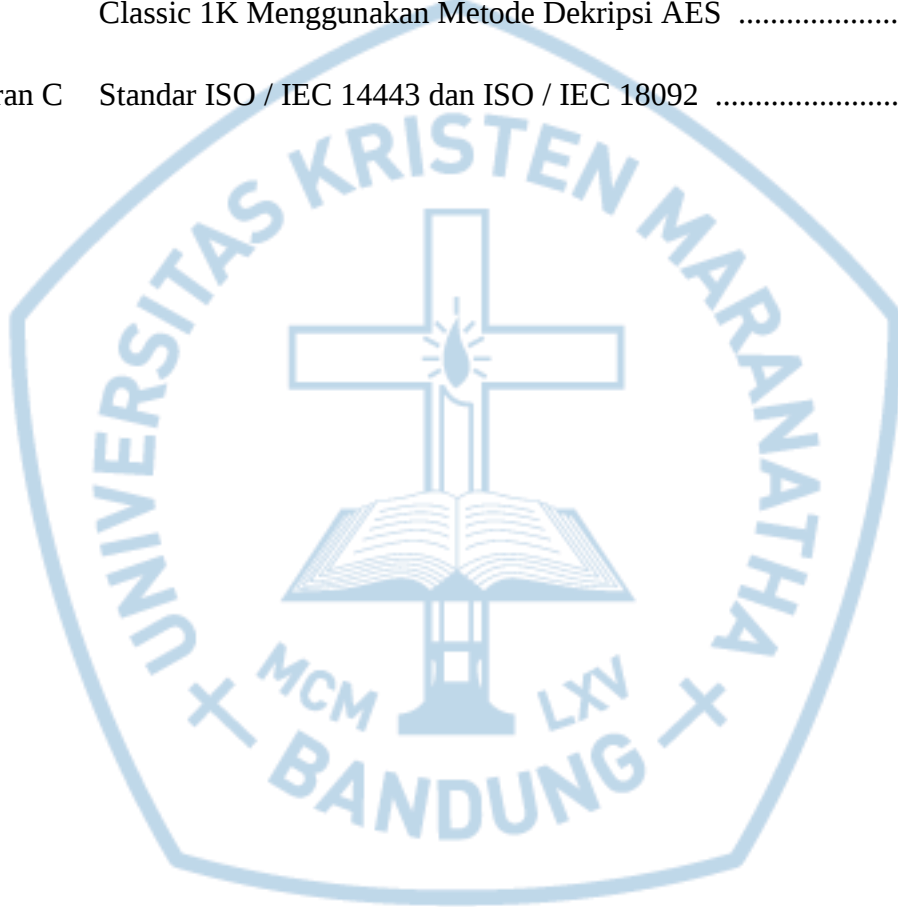
DAFTAR RUMUS

Rumus 2.1	Rumus Perhitungan Kolom Pertama <i>Round Key</i> Pada Tahapan Keempat Langkah Proses <i>Key Expansion</i>	16
Rumus 2.2	Rumus Perhitungan Kolom Kedua, Ketiga dan Keempat <i>Round Key</i> Pada Tahapan Keempat Langkah Proses <i>Key Expansion</i>	16
Rumus 2.3	Rumus Perhitungan Langkah Proses <i>Add Round Key Round – 0 / Initial Transformation</i>	17
Rumus 2.4	Rumus Perhitungan Langkah Proses <i>Substitute Bytes</i>	18
Rumus 2.5	Rumus Perhitungan Langkah Proses <i>Mix Columns</i>	19
Rumus 2.6	Rumus Perhitungan Perkalian Dot Matriks Baris Pertama Pada Langkah Proses <i>Mix Columns</i>	19
Rumus 2.7	Rumus Perhitungan Perkalian Dot Matriks Baris Kedua Pada Langkah Proses <i>Mix Columns</i>	19
Rumus 2.8	Rumus Perhitungan Perkalian Dot Matriks Baris Ketiga Pada Langkah Proses <i>Mix Columns</i>	19
Rumus 2.9	Rumus Perhitungan Perkalian Dot Matriks Baris Keempat Pada Langkah Proses <i>Mix Columns</i>	20
Rumus 2.10	Rumus Perhitungan Langkah Proses <i>Add Round Key</i>	20
Rumus 2.11	Rumus Perhitungan Langkah Proses <i>Inverse Add Round Key Round – 0 / Inverse Initial Transformation</i>	24

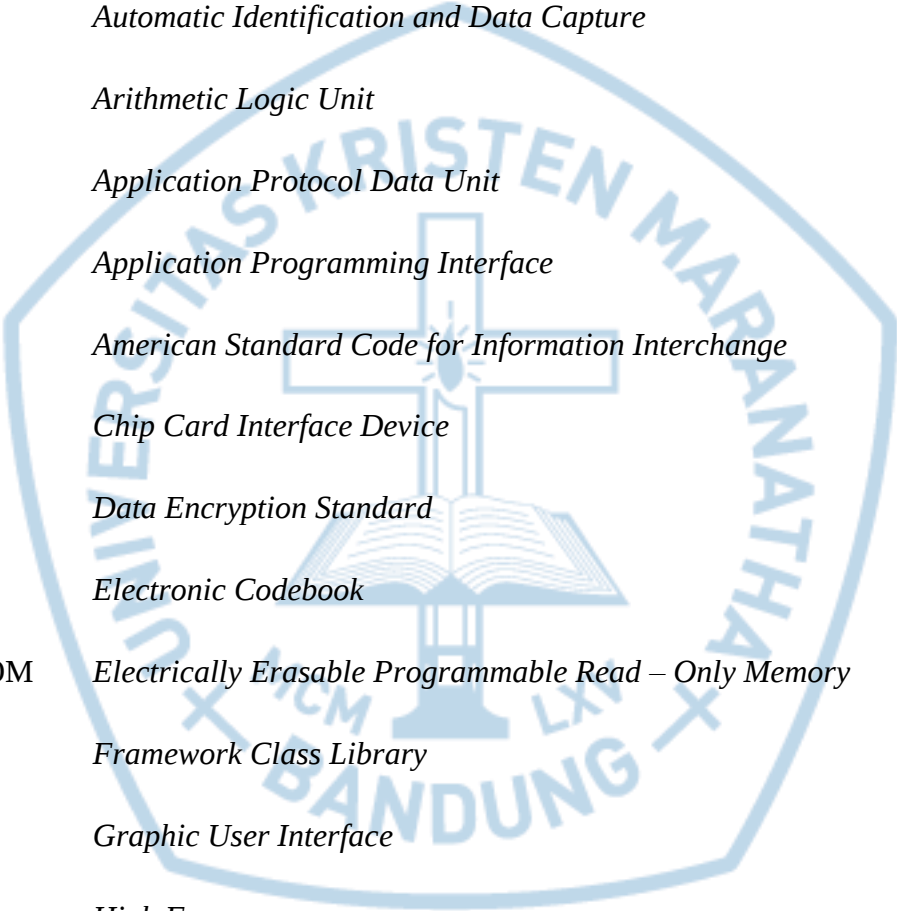
Rumus 2.12	Rumus Perhitungan Langkah Proses <i>Inverse Substitute Bytes</i>	26
Rumus 2.13	Rumus Perhitungan Langkah Proses <i>Inverse Add Round Key</i>	26
Rumus 2.14	Rumus Perhitungan Langkah Proses <i>Inverse Mix Columns</i>	27
Rumus 2.15	Rumus Perhitungan Perkalian Bilangan Heksadesimal 09 Pada Langkah Proses <i>Inverse Mix Columns</i>	28
Rumus 2.16	Rumus Perhitungan Perkalian Bilangan Heksadesimal 0B Pada Langkah Proses <i>Inverse Mix Columns</i>	28
Rumus 2.17	Rumus Perhitungan Perkalian Bilangan Heksadesimal 0D Pada Langkah Proses <i>Inverse Mix Columns</i>	28
Rumus 2.18	Rumus Perhitungan Perkalian Bilangan Heksadesimal 0E Pada Langkah Proses <i>Inverse Mix Columns</i>	28
Rumus 4.1	Rumus Perhitungan Waktu Proses Total	80
Rumus 4.2	Rumus Perhitungan Rata – Rata	80

DAFTAR LAMPIRAN

Lampiran A	Program Aplikasi Pengisian Data <i>Smart Card</i> MIFARE	
	Classic 1K Menggunakan Metode Enkripsi AES	A - 1
Lampiran B	Program Aplikasi Pembacaan Data <i>Smart Card</i> MIFARE	
	Classic 1K Menggunakan Metode Dekripsi AES	B - 1
Lampiran C	Standar ISO / IEC 14443 dan ISO / IEC 18092	C - 1



DAFTAR SINGKATAN



3DES	<i>Triple Data Encryption Standard</i>
ACS	<i>Advanced Card Systems</i>
AES	<i>Advanced Encryption Standard</i>
AIDC	<i>Automatic Identification and Data Capture</i>
ALU	<i>Arithmetic Logic Unit</i>
APDU	<i>Application Protocol Data Unit</i>
API	<i>Application Programming Interface</i>
ASCII	<i>American Standard Code for Information Interchange</i>
CCID	<i>Chip Card Interface Device</i>
DES	<i>Data Encryption Standard</i>
ECB	<i>Electronic Codebook</i>
EEPROM	<i>Electrically Erasable Programmable Read – Only Memory</i>
FCL	<i>Framework Class Library</i>
GUI	<i>Graphic User Interface</i>
HF	<i>High Frequency</i>
IBM	<i>International Business Machines Corporation</i>
ICC	<i>Integrated Circuit Card</i>
IDE	<i>Integrated Development Environment</i>
IEC	<i>International Electrotechnical Commission</i>

IS – Box	<i>Inverse Substitution Box</i>
ISO	<i>International Organization for Standardization</i>
LF	<i>Low Frequency</i>
NFC	<i>Near Field Communication</i>
NIST	<i>National Institute of Standards and Technology</i>
NSA	<i>National Security Agency</i>
NVM	<i>Non – Volatile Memory</i>
PC / SC	<i>Personal Computer / Smart Card</i>
PICC	<i>Proximity Integrated Circuit Card</i>
PoR	<i>Power – on Reset</i>
RFID	<i>Radio Frequency Identification</i>
S – Box	<i>Substitution Box</i>
SDK	<i>Software Development Kit</i>
UHF	<i>Ultra High Frequency</i>
UID	<i>Unique Identifier</i>
USB	<i>Universal Serial Bus</i>