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

DAFTAR TABEL

DAFTAR GAMBAR

DAFTAR RUMUS

DAFTAR LAMPIRAN

DAFTAR SINGKATAN

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

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