ENKRIPSI DATA PADA KARTU RFID MENGGUNAKAN ALGORITMA AES-128 UNTUK ANGKUTAN UMUM DI KABUPATEN BANDUNG

DATA ENCRYPTION ON RFID USING AES-128 ALGORITHM FOR PUBLIC TRANSPORTATION IN BANDUNG REGENCY

Metris S. Widura[1], Yudha Purwanto[2], Surya M. Nasution[3]

[1,2,3] Prodi S1 Teknik Komputer, Fakultas Teknik Elektro, Universitas Telkom
[1]meetrise@students.telkomuniversity.ac.id, [2]omyudha@telkomuniversity.ac.id, [3]michrandi@telkomuniversity.ac.id

Abstrak

Pengumpulan data angkutan umum di Kabupaten Bandung yang masih menggunakan sistem manual mengarah pada penggunaan kertas yang banyak dan menyebabkan pengolahan data menjadi tidak efektif. Pada penelitian ini dirancang sebuah program RFID pengolahan data digital (paperless) angkutan umum dan proses enkripsi sebagai sistem keamanan data. Algoritma AES-128 dipilih untuk mengenkripsi data tersebut. Kartu RFID tersebut akan diberikan kepada pemilik angkutan umum sebagai tanda bukti kepemilikan dan akan digunakan untuk proses administrasi angkutan umum tahunan. Dengan sistem RFID dan enkripsi AES-128, diharapkan Dinas Perhubungan Kabupaten Bandung tidak lagi kesulitan untuk selalu memastikan data pengoperasian angkutan umum dan bisa menjamin tidak ada pemalsuan data oleh pemilik angkutan umum.

Kata kunci : RFID; enkripsi; Algoritma AES; keamanan data; angkutan umum; ACS Smart Card

Abstract

Manual data collection process of public transportation in Bandung Regency leads to the use of many papers to record data and causes a search of a data becomes less effective. This paper will design a digital data collection program (paperless) of RFID for public transportation and an encryption algorithm as a data security system. RSA algorithm is used to encrypt data. With the RSA encryption system, it is expected the Department of Transportation Bandung Regency no longer hassle to always make sure the public transportation data operation and can ensure there is no falsification of data by the owner of public transportation. This RFID program connected with the information system database managed by the Department of Transportation Bandung Regency, and then the data will be processed for data collection every public transportation.

Keywords : RFID, encryption, AES, RSA, data security, public transport

1. Pendahuluan

Saat sekarang ini, banyak angkutan umum di Kabupaten Bandung yang telah beroperasi di jalan dan terminal. Besarnya jumlah angkutan umum dan pengolahan data yang masih menggunakan sistem manual menyebabkan penggunaan kertas yang banyak di kantor Dinas Perhubungan. Terlalu banyak kertas yang digunakan tersebut menyebabkan pencarian data dan pemrosesan data menjadi lebih lambat dan kurang efektif.

Pihak Dinas Perhubungan Kabupaten Bandung sudah mempunyai sebuah basis data berisi data-data administrasi angkutan umum di Kabupaten Bandung. Akan tetapi basis data tersebut belum dilengkapi dengan sebuah sistem informasi dan masih dikelola secara manual oleh pengelola sehingga membutuhkan banyak kertas. Untuk itu dalam tugas akhir ini dilakukan perancangan sistem RFID untuk pendataan angkutan umum. Sistem RFID yang dirancang berupa kartu RFID yang akan ditambahkan proses enkripsi data di dalamnya. Jenis enkripsi yang digunakan adalah sistem enkripsi AES-128. Sistem enkripsi data pada kartu RFID diharapkan dapat memberikan keamanan bagi pengelola data angkutan umum dalam proses pendataan. Kartu RFID tersebut akan diberikan kepada pemilik angkutan umum sebagai tanda bukti kepemilikan dan akan digunakan untuk proses administras angkutan umum. Dengan adanya kartu RFID untuk angkutan umum yang terenkripsi diharapkan membuat pekerjaan lebih efisien dan mengurangi penggunaan kertas (paperless).

Susunan paper selanjutnya adalah seperti ini: Bagian 2 membahas landasan teori tentang RFID dan algoritma enkripsi. Bagian 3 memperlihatkan perancangan program RFID dan implementasi algoritma. Pada bagian 4 hasil dan analisis. Di bagian 5 kesimpulan.

2. Landasan Teori

Dalam penelitian ini digunakan satu set RFID, terdiri dari ACR122U USB NFC Reader sebagai mesin pembaca dan Mifare MFI IC S50 sebagai kartu RFID. Alat tersebut sudah banyak digunakan untuk aplikasi perkantoran di kota besar pada negara maju. Di kota besar, alat tersebut biasa digunakan untuk mempermudah proses transaksi pembayaran secara *cantacless.*

A. ACR122U USB NFC Reader

ACR122U NFC Reader adalah mesin pembaca kartu pintar RFID yang dikembangkan berdasarkan teknologi RFID 13.56 MHz. Mengikuti standard ISO/IEC18092 untuk NFC (Near Field Communication), ACR122U mendukung tidak hanya kartu Mifare ISO 14443 tipe A dan tipe B tetapi juga semua tipe penanda NFC. ACR122U ideal untuk kebutuhan verifikasi identifikasi yang aman dan transaksi micro-payment online. Penerapan yang lain dari ACR122U adalah keperluan akses kontrol, e-payment, e-ticketing untuk beberapa event, pembayaran jalan tol dan autentitikasi jaringan.

B. Mifare MF1 IC S50

Mifare MF1ICS50 adalah kartu pintar RFID yang berdasar pada ISO/IEC 14443 tipe A. Mifare MF1ICS50 IC banyak digunakan untuk sistem tiket dimana banyak kota-kota besar telah menggunakannya sebagai pilihan solusi e-ticketing. Chip dari MF1ICS50 berisi 1 Kbyte EEPROM, antarmuka frekuensi radio dan Unit Kontrol Digital. Energi dan data dikirim lewat antena, yang berisi lilitan dengan berbagai putaran berarah yang terhubung dengan MF1ICS50.

C. Kriptografi Simetris

Kriptografi simetris, juga biasa disebut kriptografi kunci tunggal, adalah sistem kriptografi yang menggunakan satu kunci untuk mengenkripsi suatu informasi. Dalam proses enkripsi ini pengirim dan penerima informasi harus menyetujui satu kunci yang akan digunakan untuk mengenkripsi informasi dan hanya diketahui oleh kedua pihak tersebut. Ada pesan asli (disebut *plaintext*) dan kunci sebesar 16 bit, proses enkripsi menghasilkan data acak (disebut *ciphertext*), yang memliki panjang data yang sama dengan pesan asli (*plaintext*). Dekripsi adalah kebalikan dari enkripsi, dan menggunakan kunci yang sama seperti kunci untuk mengenkripsi.

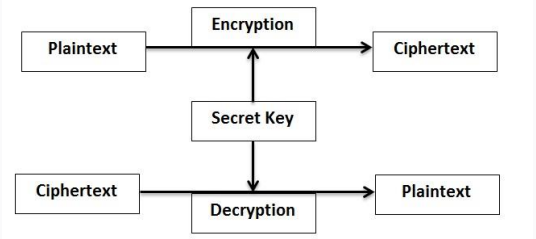

Fig. 1. Proses Kriptografi Kunci Simetris

D. Algoritma Kriptografi AES

AES (Advanced Encryption Standard) merupakan salah satu algoritma enkripsi yang termasuk dalam kriptografi simetris dan merupakan algoritma pengganti dari DES (Data Encryption Standard) yang masa berlakunya sudah selesai dikarenakan faktor keamanan. Pada bulan Maret tahun 2001 NIST (National Institute of Standards and Technology) menetapkan algoritma baru sebagai pengisi AES yaitu Rijndael. Algoritma Rijndael ini sendiri terpilih sebagai algoritma AES setelah mengalahkan 5 finalis lainnya yang diseleksi oleh NIST.

Panjang kunci algoritma Rijndael memiliki panjang kunci antara 128 bit sampai dengan 256 bit. Namun dalam penerapannya AES menetapkan panjang kunci yang dibutuhkan adalah 128 bit, 192 bit dan 256 bit sehingga kemudian dikenal dengan sebutan AES-128, AES-192, dan AES-256 walaupun pada penggunaanya paling banyak menggunakan AES-128 dan AES-256 dikarenakan AES-192 sangatlah jarang digunakan. Untuk lebih jelasnya dapat dilihat pada tabel dibawah ini :

TABLE I. TABEL JUMLAH PROSES AES

	Key Length (Nk words)	**Block Size** (Nb words)	**Number of Process** (Nr)
AES-128	4	4	10
AES-192	6	4	12
AES-256	8	4	14

[a.] Jumlah putaran tergantung jumlah bit blok dan panjang kunci

Algoritma Rijndael menggunakan permutasi dan substitusi dan sejumlah putaran. Untuk setiap putarannya, Rijndael menggunakan kunci yang berbeda. Kunci pada setiap putaran algoritma ini disebut dengan round key. Dikarenakan algoritma Rijndael beroprasi dalam byte sehingga memungkinkan untuk diimplementasikan menjadi algoritma yang efisien ke dalam software maupun hardware. Algoritma Rijndael yang beroperasi pada blok 128-bit dengan panjang kunci 128-bit adalah sebagai berikut:

1) SubBytes()

Transformasi substitusi byte non-linear yang dioperasikan secara independen pada setiap byte dengan menggunakan tabel substitusi S-box dimana S-box tersebut juga memiliki invers yang digunakan untuk proses deskripsi. Tabel S-box untuk transformasi SubBytes AES dapat dilihat pada table 3.

2) ShiftRows()

Pada transformasi *shiftRows*, state *byte* pada tiga baris terakhir secara siklik digeser dengan jumlah pergeseran yang berbeda (offset). Hal ini memiliki pengaruh terhadap pergerakan byte dari posisi rendah di dalam baris.

3) MixColumns()

Transformasi MixColumns beroperasi pada state kolom per kolom, dengan memperlakukan setiap kolom sebagai 4 buah polynomial. Kolom tersebut dianggap sebagai polynomial pada GF(2^8) dan dikalikan modulo $x^4 + 1$ dengan polynomial tetap $a(x) = \{03\} x^3 + \{01\} x^2 + \{01\} x + \{02\}$.

4) AddRoundKey()

Pada transformasi *AddRoundKey* sebuah *round key* ditambahkan kepada state dengan operasi bitwise sederhana XOR. Setiap round key terdiri dari Nb word dari hasil key schedule. Dengan demikian masing-masing ditambahkan ke dalam kolom dari state. Aplikasi dari transformasi AddRoundKey pada Nr round dari proses penyandian terjadi ketika $1 \leq$ round $\geq$ Nr. Untuk lebih jelasnya dapat dilihat pada Gambar 4 dimana L = round * Nb alamat byte dalam word dari key schedule.

Ditemukan dalam [3] bahwa algoritma AES mengkonsumsi lebih sedikit waktu enkripsi dibandingkan dengan DES dan RSA. Penggunaan memori algoritma AES dan DES adalah yang paling sedikit untuk semua ukuran file teks. Ketika ukuran data meningkat maka algoritma asimetris manjadi lebih lambat dibandingkan dengan algoritma simetris.

Disimpulkan dalam [4] bahwa kriptografi simetris memiliki penggunaan memori yang sangat kecil dibandingkan dengan algoritma asimetris. Hal ini juga disimpulkan bahwa kriptografi simetris lebih cepat untuk mengenkripsi data untuk array byte dibandingkan dengan kriptografi asimetris. Algoritma simetris dapat melindungi data RFID lebih baik dari beberapa algoritma asimetris karena memungkinkan untuk implementasi yang kompleks Pada penelitian tersebut alat yang digunakan sebagai perangkat RFID adalah perangkat dengan ISO 18000. Pada penelitian serupa [7], telah didapatkan performansi AES dalam perhitungan *clock cycle* dan konsumsi daya.

Penelitian ini memperkenalkan algoritma AES sebagai algoritma kriptografi sistem keamanan pada RFID menggunakan RFID ISO 14443 tipe A. Dari perspektif penulis, ada yang diperlukan untuk membuat AES menjadi lebih aman dengan menggunakan karakter yang unik sebagai kunci privat. Kunci privat hanya diketahui oleh petugas dan tidak akan dibagikan kepada orang lain.

3. Perancangan Sistem

Bagian ini menjelaskan kerangka yang diusulkan, yang terdiri dari dua tahap utama, pemetaan blok RFID dan implementasi algoritma enkripsi AES. Sistem akan dibagi menjadi 2 proses utama yaitu enkripsi dan dekripsi. Proses enkripsi berlangsung saat pemilik mendaftarkan kartu Mifare RFID baru. Untuk proses dekripsi terjadi ketika petugas ingin memperbaharui data pada kartu Mifare RFID. Diagram alir proses enkripsi dan dekripsi adalah sebagai berikut:

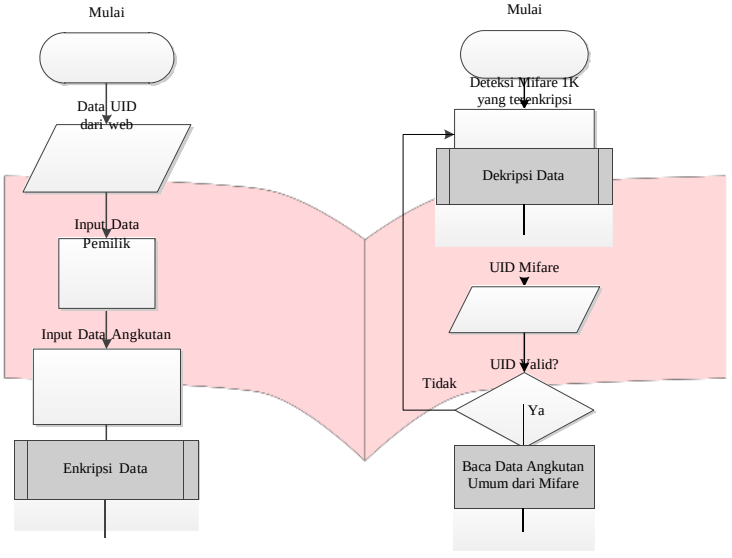

Fig. 2. Flow Diagram Proses Enkripsi

Fig. 3. Flow Diagram Proses Dekripsi

A. Pemetaan Blok pada Mifare

Memori EEPROM 1 Kbyte dari kartu RFID terdiri dari 16 sektor dengan masing-masing sector berisi 4 blok dan setiap blok berisi 16 byte data karakter. Setiap blok akan diisi oleh 1 *attribute* data. Gambaran pemetaan blok Mifare 1 Kbyte dapat dilihat pada gambar berikut:

TABLE II. PEMETAAN BLOK MIFARE RFID

Sektor	Data	Size
0	-	3 blok
1, 2	Data Pemilik	6 blok
3, 4, 5	Data Angkutan 1	9 blok
6, 7, 8	Data Angkutan 2	9 blok
9, 10, 11	Data Angkutan 3	9 blok
12, 13, 14	Data Angkutan 4	9 blok
15	-	3 blok

B. Algoritma AES

TABLE III. TABEL JUMLAH PUTARAN AES-128

Panjang blok (Nb)	128 bits (16 *byte*/karakter)
Panjang kunci (Nk)	128 bits (16 *byte*/karakter)
Jumlah Putaran (Nr)	10 proses

Plain Text (ASCII) = METRIS SOVIAN

Kode ASCII dibagi manjadi beberapa karakter untuk membantu menjadi lebih mudah:

TABLE IV. TABEL ASCII KE HEXADESIMAL

Bytes	Char	Hexadecimal
m_0	M	4D
m_1	E	45
m_2	T	54
m_3	R	52
m_4	I	49
m_5	S	53
m_6	(space)	20
m_7	S	73
m_8	O	4F
m_9	V	56
m_{10}	I	49
m_{11}	A	41
m_{12}	N	4E
m_{13}	Null	0D
m_{14}	Null	0D
m_{15}	Null	0D

[a.] Plain Text to decimal table

Plain Text (Hex) = 4d455452495320734f5649414e000000
Key (ASCII) = ini adl key16bit
Key (Hex) = 696e692061646c206b65793136626974

Output/ciphertext (Hex) = 38f037daed7943d8a9f7b093c5c9509a
Output/ciphertext (ASCII) = ã;¤➧&” ÒÝ– Š Æ¾CQû

4. Hasil Pengujian dan Analisis

Pengujian yang dilakukan adalah pengujian jarak Mifare, pengujian kecepatan enkripsi dan dekripsi, pengujian *Avalanche Effect.* Setelah diuji kemudian dilakukan analisis. Berikut daftar table pengujian :

TABLE V . JARAK MIFARE KE PEMBACA RFID

Percobaan	Jarak
1	6,5cm
2	6,7 cm
3	6,4 cm
4	6,6 cm
5	6,6 cm
6	6,7 cm
7	6,5 cm
Rata-rata	**6,51cm**

Hasil eksperimen untuk jarak yang harus ditempatkan Mifare pembaca ke RFID ditunjukkan pada tabel 5. Dengan menganalisis tabel 5, jarak efektif untuk Mifare ditempatkan ke pembaca adalah 6,4 cm.

TABLE VI. WAKTU ENKRIPSI

Percobaan	Waktu Enkripsi	Waktu Dekripsi
1	0,249 s	0,312 s
2	0,265 s	0,28 s
3	0,359 s	0,28 s
4	0,266 s	0,281 s
5	0,25 s	0,297 s

Tabel 6 menunjukkan waktu rata-rata yang digunakan untuk mengenkripsi data pada kartu adalah 0,277 detik dan dekripsi 0,29 detik. Pengujian menunjukkan waktu enkripsi lebih cepat dari dekripsi, yaitu dengan selisih sekitar 0,013 detik.

TABLE V. AVALANCHE EFFECT

Ciphertext	Biner Ciphertext	Perbedaan Bit
...	10000101	3
·	10110111	6
	00010011	5
Ô	11010100	4
Ÿ	11111111	4
ç	10100010	2
I	01101001	4
K	01101011	5
}	01111101	4
•	10001101	4
”	10010100	4
:	00111010	6
	00010110	5
Í	11101101	4
Ò	11110010	8
¹	10111001	4

Dari hasil di atas terlihat bahwa perbedaan bit pada posisi yang sama sebanyak 68 bit, jadi nilai *Avalanche Effect*-nya adalah sebagai berikut:

$$\frac{\text{jumlah bit yang berbeda}}{\text{jumlah bit yang dibandingkan}} \times 100\% = \frac{68}{128} \times 100\% = 53{,}13\%$$

5. Kesimpulan dan Pekerjaan Selanjutnya

Enkripsi sangat berperan penting dalam keamanan data dimana tingkat keamanan dan waktu enkripsi adalah masalah utamanya. Efektifitas penggunaan algoritma AES terletak pada kecepatan proses data dan penggunaan memori. AES mengkonsumsi waktu enkripsi paling efektif dan penggunaan memori juga sangat rendah bila dibandingkan dengan algoritma asimetris. Pada penelitian ini implementasi enkripsi data pada kartu RFID berhasil dilakukan dan mengsailkan nilai *Avalanch Effect* yang baik karena nilai masih mendekati 50% yaitu 53,13%. Penggunaan kartu RFID berhasil membantu pekerjaan petugas untuk pencatatan data perizinan angkutan umum di Kabupaten Bandung Untuk pekerjaan selanjutnya diperlukan percobaan menggunakan metode enkripsi lainnya yang bisa menghasilkan nilai AE yang lebih baik.

REFERENSI

[1] Thakur J., & Kumar N., "DES, AES and Blowfish: Symmetric Key Cryptography Algorithms Simulation Based Performance Analysis," International Journal of Emerging Technology and Advanced Engineering, 1(2), 6-12. 2011.

[2] P. Priteshkumari, P. Nehal, M. Robinson, K. Nisarg, S. Parth, "Comparative Analysis of DES, AES, RSA Encryption Algorithms," International Journal of Engineering and Management Research, Vol.4, Issue-1, February-2014, ISSN No.: 2250-0758.

[3] Shashi M. Seth, Rajan Mishra, "Comparative Analysis Of Encryption Algorithms For Data Communication," International Journal Computer Science and Technology, Vol.2, Issue 2, June 2011.

[4] M. Aigner, M. Feldhofer, "Secure Symmetric Authentication for RFID Tags," Telecommunacation and Mobile Computing TCMC 2005 Workshop, Graz, Austria, 2005.

[5] ASCII Code - The extended ASCII table. www.ascii-code.com

[6] NXP B.V., "MF1ICS50 Functional specification," Product data sheet, 001056, November 2010.

[7] Feldofer, M., Dorminikus S., Wolkerstorfer J. "Strong Authentication for RFID Systems Using the AES Algorithm," Cryptographic Hardware and Embedded Systems-CHES 2004. Springer Berlin Heidelberg, 2004. 357-370.