

Sistem Pengamanan Pintu Otomatis Berbasis RFID Menggunakan Metode AES

Amelia Pratiwi
Universitas Buana Perjuangan
Karawang, Indonesia
if17.ameliapратиwi@mhs.ubpkarawang.ac.id

Ahmad Fauzi
Universitas Buana Perjuangan
Karawang, Indonesia
afauzi@ubpkarawang.ac.id

Dwi Sulistya Kusumaningrum
Universitas Buana Perjuangan
Karawang, Indonesia
dwi.sulistya@ubpkarawang.ac.id

Abstract—

Tidak sedikit masyarakat yang khawatir saat meninggalkan rumah dan meninggalkan barang berharga-nya agar penghuni rumah merasa aman saat meninggalkan rumah maka dibutuhkan-nya produk teknologi guna menunjang keamanan yang canggih serta meminimalisir pencurian. Dari pernyataan tersebut maka dibuatkannya sistem *doorlock radio frequency identification* (RFID) dan *keypad* 4x4 sebagai alat akses pintu rumah otomatis guna mengganti dari kunci konvensional, tidak hanya itu sistem ini sudah dilengkapi dengan *second security* dengan menggunakan kriptografi *advanced encryption standard* (AES) yang bertujuan untuk mengamankan data dari RFID. Tujuan terbangunnya sistem ini dikarenakan meningkatnya perampokan rumah, dan sebagainya yang mengakibatkan pemilik rumah selalu khawatir meninggalkan rumah. Sistem ini didukung dengan *internet of things* yang dapat melindungi dan mencegah tindakan yang tidak diinginkan. Kriptografi ini cukup aman untuk mengamankan data pada RFID karena butuh waktu yang lama untuk mendapatkan kunci yang benar. dilihat dari sisi lain perangkat ini dapat membuat pintu lebih menarik dan mengikuti perkembangan teknologi dibandingkan dengan kunci konvensional maka dapat disimpulkan hasil dari sistem ini dapat berjalan dengan 2 mode yaitu *mode Offline* dan *online*, serta berhasil mengimplementasikan enkripsi dengan menggunakan metode AES serta hasil dari pengujian RFID bahwa maksimal jarak pada sensor RFID yaitu 5cm.

PENDAHULUAN.

Keamanan rumah merupakan hal penting yang harus diutamakan karena semakin meningkat pencurian dan perampokan membuat kita harus lebih ekstra menjaga keamanan rumah, tidak sedikit masyarakat yang menggunakan kunci manual, yang mudah sekali di duplikat atau di sabotase, selain itu sering terjadi ketinggalan karena bentuk pada kunci tersebut kecil, lupa mengunci pintu, dan sering sekali penghuni rumah mengabaikan aspek penting dalam penjagaan keamanan rumah. alhasil kasus kehilangan barang di luar pengawasan tentu masih sering terjadi, terjadinya pencurian tentu saja tidak bisa dihilangkan, tidak dapat disangkal bahwa tidak ada yang 100% akurat sehingga keamanan perlu berubah (1).Perkembangan teknologi saat ini banyak alat elektronika yang mampu membuat alat canggih salah satunya yaitu membuat sistem keamanan pintu yang canggih, dengan menggunakan sistem keamanan ini maka dapat meningkatkan keamanan rumah. Sistem keamanan rumah ini berbentuk perangkat keras dan berfungsi mengamankan pintu rumah.

Dalam *embedded system* terdapat komponen - komponen yang dipasang secara sistematis, adanya *Arduino nano* sebagai *mainboard* untuk pengolahan perintah, ada *radio frequency identification* (RFID) yang terbagi menjadi 2 jenis yaitu, RFID *tag card* yang fungsinya untuk menyimpan data dan RFID *reader* yaitu membaca data dari RFID *tag card*. Desain keamanan rumah semacam ini tidak mengutamakan perangkat sebagai antarmuka, tetapi menggunakan alat elektronik, karena selain pengetahuan yang diperlukan untuk pemrograman dan teknologi informasi, memiliki banyak kunci tentu akan mengganggu kita, *radio frequency identification* (RFID) berfungsi untuk pengambilan data dan mengidentifikasi dengan menggunakan *barcode* atau *magnetic card*. Proses identifikasi *radio frequency identification* (RFID) gelombang elektromagnetik, sehingga RFID membutuhkan 2 perangkat yaitu, RFID *tag* dan *reader* agar dapat beroperasi secara normal metode-nya menggunakan *tag* RFID dengan fungsi menyimpan dan mengambil data (Daulay, Nelly Khairani,2019). Jika ingin mengganti kunci pada pintu tidak perlu membongkar, tetapi hanya perlu mengubah sintaks program yang tertanam di pembaca RFID tanpa harus membongkar, pencatatan data dan pelaporan barang milik perusahaan dalam unit pengiriman barang.

TINJAUAN PUSTAKA

A. Kriptografi

Kriptografi ialah suatu proses untuk mengamankan komunikasi serta informasi lewat penggunaan kode supaya data tertentu dapat dibaca dikirim oleh mereka yang mempunyai akses spesial. Algoritma serta konsep perhitungan matematis ini hendak digunakan di masa depan untuk mengganti pesan yang sulit dijabarkan, terdapat sebagian aspek keamanan dalam kriptografi ialah, *Authority* (Pemalsuan), data *Integrity*, *Authentication*, *Non-repudiation* (Tidak ada penyangkalan).

B. Internet Of Things (IOT)

IoT (*internet of things*) secara dinamis menyesuaikan satu sama lain dengan mengelola informasi dimana fitur raga bisa terhubung ke *internet*. Misalnya, Kulkas, TV, Mesin Cuci serta yang lain bisa dikontrol memakai *smartphone* untuk mematikan, menghidupkan serta aktivis lainnya, tidak hanya itu *IoT* juga mengenali dengan menggunakan *radio frequency identification* (RFID) untuk metode komunikasinya (Yudhanto Yudha. 2015).

C. Advanced Encryption Standard (AES)

Kriptografi AES terbilang cukup aman untuk mengamankan data maupun informasi rahasia, kriptografi ini memiliki kunci dengan panjang yang berbeda yaitu (128 *bit*, 192 *bit*, dan 256 *bit*). Perbedaan dari panjangnya kunci dapat berpengaruh pada saat jumlah *round* yang ingin diterapkan.

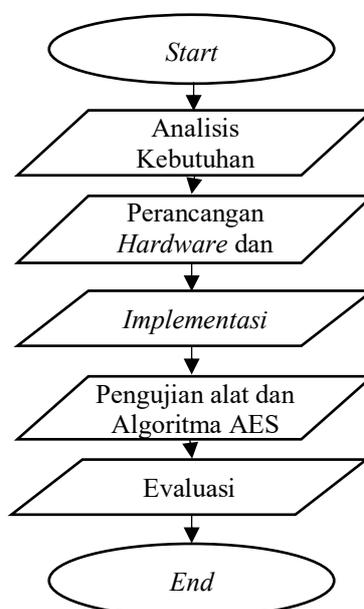
Tabel 1 Kunci Algoritma AES

	<i>Key Length</i>	<i>Block Size</i>	<i>Number of Process</i>
AES-128	4	4	10
AES-192	6	4	12
AES-256	8	4	14

Algoritma AES menerapkan permutasi, substitusi serta beberapa putaran Yang biasa disebut dengan *round key*, untuk setiap *round* memakai kunci berbeda. Sebab algoritma ini beroperasi dalam *byte* kemudian menjadi algoritma yang efektif pada *software* maupun *hardware*. Algoritma ini berfungsi pada blok dan Panjang 128 *bit* adalah sebagai berikut :

METODE PENELITIAN

Prosedur pada *project* ini memiliki empat tahapan sesuai dengan kebutuhan dari peneliti. Empat tahapan tersebut adalah analisis kebutuhan, Perancangan *hardware* dan *software*, pengujian, implementasi, dan evaluasi. Analisa pada sistem *radio frequency identification* dan *keypad 4x4* kemudian agar sistem lebih aman maka menggunakan metode kriptografi *advanced encryption standard* (AES) dengan tujuan mengamankan data sehingga data asli tidak dapat terlihat. Analisa ini hanya membahas implementasi sistem RFID sedangkan *keypad 4x4* pada akses pintu rumah hanya objek akses kedua, sistem ini tidak membahas keamanan data pada alat *keypad 4x4* tersebut, Sistem *Website* ini hanya untuk laporan data keluar masuk melalui pintu rumah tidak membahas laporan keamanan dari sudut lain selain objek pada pintu tersebut, sistem hanya meningkatkan keamanan akses pintu dan meminimalisirkan kejahatan bukan menghilangkan kejahatan 100%. objek pada penelitian ini hanya pintu dan *system* RFID.



Gambar 1 Tahapan penelitian

A. Analisis Kebutuhan

Pada aktivitas ini peneliti melakukan identifikasi masalah, serta mengumpulkan data yang masih berkaitan dari topik yang diangkat pada *project* ini. Studi pustaka dari penelitian ini didapatkan dari berbagai sumber, yaitu buku dan jurnal. untuk mencari informasi tentang RFID dan mempersiapkan alat dan bahan yang akan digunakan pada saat membuat sistem tersebut. Kemudian melakukan verifikasi alat dan bahan agar produk yang dibuat dengan melakukan perbandingan dari penelitian sebelumnya. Pada penelitian ini, dibutuhkan alat dan bahan sebagai kebutuhan utama dan kebutuhan penunjang. beberapa alat dan bahan yang dibutuhkan dapat dilihat pada tabel 3.2.

Tabel 2 Peralatan perangkat keras

No	Hardware	Keterangan
1	Laptop	Spesifikasi 2.3 GHz intel core i3, RAM 4GB HDD 1Tb
2	PCB IoT	Board IOT doorlock
3	LCD 20X4	Tegangan 3.3v / 5v, dimensi 98x60x12mm
4	RFID RC-M22	Frekuensi Operasi 13.56Hz, Dimensi 40mm x 60mm, DC 3.3v, 10-13mA
5	Node MCU V3 Lolin	Transfer rate 110-460800bps, 4Mbyte, wifi at 2.4GHz, Wpa/ wpa2 security, 4.5v – 9v
6	Solenoid Door lock	Mosfet IRF520N
7	Keypad 4x4	Keypad 4x4 matrix 16 tombol
8	Limit Switch Sensor	Dimensi PCB (mm) 15x21, 3.3v / 5vDC, Led Signal (Ya)

- 9 Adaptor 12v *Power supply* 12v 2A 100-240v AC, Diameter Jack 5.5mm x 2.1mm
- 10 Kabel Jumper Kabel jumper *female to female*
- 11 Jack DC *Female* DC 5v 2A , Ukuran 5.5mm x 2.1mm

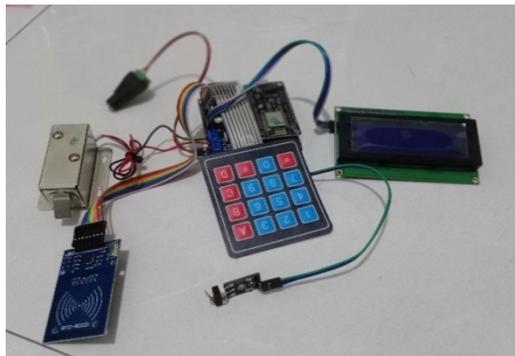
Kemudian perangkat lunak yang dibutuhkan pada saat membangun sistem dapat dilihat pada tabel 3.3.

Tabel 3 Perangkat Lunak

No	Software	Keterangan
1	IDE Arduino	<i>Text Editor</i>
2	<i>Fritzing</i>	Untuk membuat skema
3	C, C++	Sebagai bahasa pemrograman
4	<i>Flowchart</i>	Untuk membuat <i>Flowchart</i>
5	Xampp	Sebagai server (<i>localhost</i>)
6	<i>Microsoft Word</i>	Untuk Membuat laporan

E. Perancangan hardware dan software

Pada tahap perancangan ini terdapat dua bagian penting pada proses pembuatan produk, yaitu perancangan *hardware* dan *software*.



Gambar 2 Perancangan Hardware

Penjelasan terkait komponen – komponen pada perancangan *hardware* adalah :

1. PCB *IoT door lock*, sebuah alat yang dirancang sederhana untuk uji coba rangkaian elektronik.
2. RFID RC-522, RFID mempunyai 2 jenis yaitu RFID Card dan Tag.
3. Keypad 4x4, Alat yang mempunyai 16 tombol yang digunakan untuk memasukkan 5 digit password.
4. Kabel jumper digunakan sebagai penghubung antar komponen dalam membuat *Hardware*.
5. Solenoid door lock 5V, sebuah alat untuk mengunci pintu secara elektronik.
6. LCD 20X4, pada penelitian, digunakan LCD untuk menampilkan informasi yang sedang di proses mikrocontroller sedangkan untuk perancangan *software* di desain dengan melibatkan beberapa item.

Flowchart sistem keamanan pintu yang ditampilkan pada gambar 3 memiliki penjelasannya masing masing :

1. Start

Langkah awal pada sistem ini akan terlihat pada tampilan LCD apakah sistem masuk kedalam *mode online* atau *offline*.

2. Memasukkan password offline.

Jika sistem masuk ke *mode offline* maka input password yang sudah di setting, RFID tidak bisa digunakan jika sistem dalam *mode offline*.

3. Tampilan LCD pada mode online

Jika sistem masuk ke dalam *mode online* maka dapat menggunakan RFID dan keypad 4x4.

7. RFID card & tag ataupun keypad 4x4 Tervalidasi

Apabila data sudah tervalidasi maka mikrocontroller akan mengaktifkan solenoid selama 5 detik (waktu bisa disetting sesuai keinginan).

8. Gagal tervalidasi

Jika gagal tervalidasi kemungkinan RFID belum terdaftar, maka lakukan registrasi terlebih dahulu pada Website.

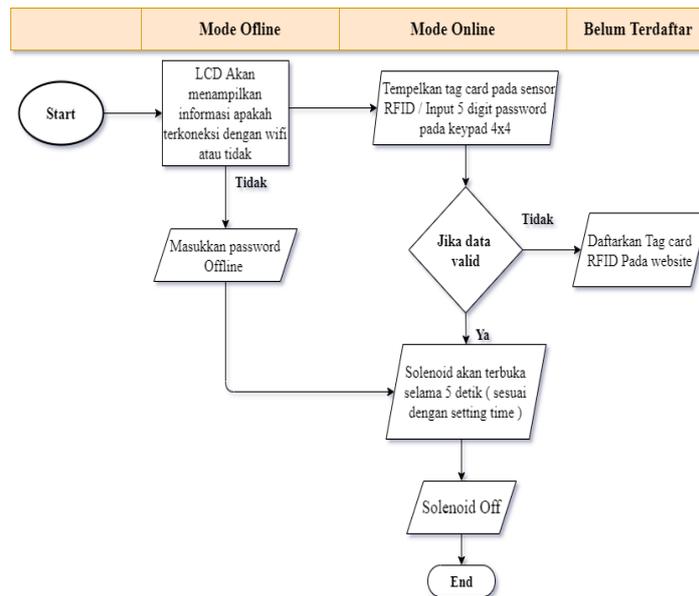
9. Solenoid off

Setelah 5 detik solenoid door lock (off) pengunci akan tertutup.

10. End

End merupakan dimana seluruh pengoperasian akan kembali ke posisi inisialisasi.

F. Implementasi



Gambar 3 *Flowchart* cara kerja

Setelah produk telah teruji keakuratannya maka langkah selanjutnya adalah implementasi yang dikembangkan membutuhkan sosialisasi yang cukup lama dan panjang. Implementasi produk juga dilakukan untuk mengidentifikasi dua hal penting dalam produk, yaitu fungsi alat dan daya tahan alat.

- Keberfungsian alat

aktivitas ini dilakukan dengan cara mengoperasikan alat sesuai dengan fungsinya yaitu untuk sistem *security* atau keamanan akses pintu. Aktivitas ini bertujuan untuk mengetahui apakah komponen yang ada berfungsi dengan baik.

- Ketahanan alat

Untuk menguji ketahanan alat, maka yang dilakukan adalah dengan memberikan pembebanan maksimal. Waktu pengujian dilakukan selama 24 jam *non-stop* dalam waktu 4 minggu. Pengujian ini bertujuan untuk mengetahui kemampuan alat dalam menahan beban maksimal.

- Implementasi metode AES

Pada tahap ini yaitu mengimplementasikan metode AES pada data RFID fungsi dari implementasi metode ini yaitu agar keamanan data tetap terjaga.

G. Pengujian

Pada tahap ini peneliti melakukan observasi secara intensif kemudian mencatat hal penting untuk dijadikan bahan saat penyempurnaan proyek awal. Sebelum melakukan pengujian ini maka diperlukan teknis analisis data yang bertujuan untuk membedakan komponen sistem dengan kriteria yang telah ditetapkan, pada tahap ini peneliti melakukan pengujian dengan bertahap. Pengujian keakuratan RFID, Keypad 4x4 serta pengujian rangkaian dan keamanan data lainnya. Prosedur teknik pengambilan data pada tahap ini adalah sebagai berikut :

- Data Sensor dari *Radio Frequency Identification* (RFID)

Pengambilan data pada sensor RFID ini bertujuan untuk mengamati kecepatan pembacaan dari sebuah modul *Radio Frequency Identification* (RFID) RC522 pada *id card*. Pengujiannya memiliki 2 jenis yaitu RFID *tag* dan *card* didekatkan pada *reader* maka katup *solenoid door lock* akan terbuka, jika RFID tersebut tidak sesuai atau belum didaftarkan maka *solenoid* tidak terbuka.

- Pengujian pada Keypad 4x4

- Implementasi dengan menggunakan Metode AES untuk melakukan proses *Enkripsi* pada UID RFID *Tag* dan *card*

H. Evaluasi

Evaluasi menilai dan mengoreksi pada suatu kegiatan dengan mengumpulkan dan membandingkan data dengan hasil yang dicapai. Tujuan evaluasi adalah mengetahui kesesuaian rencana dan realisasi. Sehingga apabila terdapat kekurangan dapat diperbaiki sedangkan pelaksanaan yang sudah tepat dapat dipertahankan dan dikembangkan

HASIL DAN PEMBAHASAN

A. Hasil Analisis & Kebutuhan

Pada tahap analisis kebutuhan ini peneliti menyiapkan alat dan bahan dengan sumber informasi yang didapatkan dari studi Pustaka dan *Literature*. Analisis kebutuhan juga mempertimbangkan latar belakang masalah, sehingga alat dan bahan yang digunakan untuk menciptakan produk akan disesuaikan spesifikasinya. Tahap ini sangat penting sebelum merancang perangkat keras dan perangkat lunak yang dibutuhkan pada saat pembuatan *project* guna menunjang kelancaran pada sistem yang terdapat 2 mode yaitu *Mode Offline* dan *Mode Online*.

B. Hasil Perancangan Perangkat Keras

Hasil Perancangan dapat di lihat dibawah ini dimana semua alat yang digunakan guna membantu kinerja penelitian dijadikan didalam sebuah *prototype* sehingga hasilnya seperti dibawah ini.



Gambar 4 Hasil *prototype* tampak depan

C. Hasil Pengujian Jarak RFID

Pada tahap pengujian ini bertujuan untuk mengetahui kemampuan sensor pada kartu RFID dengan RFID reader.

Tabel 4 Pengujian RFID

UID	Username	Access	Jarak	Response Time
B3136F15	User 1	Berhasil	1 cm	0,65 Detik
5432CBEC	User 2	Berhasil	2 cm	0,70 Detik
5AD9AC1A	User 3	Berhasil	3 cm	0,60 Detik
CC1AE637	User 4	Berhasil	4 cm	1 detik
5432CBEC	User 5	Berhasil	4,5 cm	1 detik
B3136F15	User 6	Gagal	5 cm	3 detik
CC1AE637	User 7	Berhasil	1 cm	0,60 detik
5AD9AC1A	User 8	Berhasil	2 cm	0,65 detik
5432CBEC	User 9	Berhasil	2,5 cm	1 detik
CC1AE637	User 10	Gagal	3 cm	2 detik

Berdasarkan hasil pengujian diatas untuk RFID tag kemampuan jarak yang dapat ditangkap pada RFID Reader yaitu maksimal 2,5 cm namun pada jarak 3 cm tag RFID tidak terjangkau, sedangkan pada RFID card kemampuan jarak yang dapat dijangkau oleh RFID reader maksimal 4,5 cm ketika mencapai 5 cm maka tidak dapat dijangkau oleh RFID reader. maka dapat disimpulkan bahwa RFID card mempunyai kemampuan sensor lebih unggul dibandingkan dengan RFID tag.

D. Pengujian AES

Dibawah ini terdapat simulasi perhitungan manual sesuai dengan tahap metode AES.

1. Initial Round

Plainteks : AMELIAPRATIWIAES
Key : 5AD9AC1A

Tabel 5 Initial Round

Plainteks				Chiper Key			
A	M	E	L	5	A	D	9
I	A	P	R	A	C	1	A
A	T	I	W	Nul	Nu	Nul	Nul
I	A	E	S	Nul	Nul	Nul	Nul

Pada Tabel di atas akan dirubah terlebih dahulu menjadi Nilai Hexa Seperti gambar dibawah ini :

Tabel 6 Output Initial Round

Output Plaintext				XOR	Output Chiper Key			
41	40	45	4c		35	41	44	39
49	41	50	52		41	43	31	41
41	54	49	57		00	00	00	00
49	41	45	53		00	00	00	00

Jika sudah mendapatkan hasil hexa kemudian hasil dari plaintext dengan chiper key akan di XOR dan hasilnya seperti dibawah ini :

Tabel 7 Hasil XOR initial round

BLOK			
74	01	01	75

08	02	61	13
41	54	49	57
49	41	45	53

2. Pembangkitan Kunci

Pada tahap ini akan melakukan pembangkitan kunci setelah data *initial round* di dapatkan. Data yang akan di ambil terlebih dahulu yaitu data *chipper key* yang akan di Xor kan dengan tabel rcon .

Tabel 8 Tabel rcon

Tabel rcon									
01	02	04	08	10	20	40	80	1b	36
00	00	00	00	00	00	00	00	00	00
00	00	00	00	00	00	00	00	00	00
00	00	00	00	00	00	00	00	00	00

Tabel 9 Chiper key

Chiper key			
35	41	44	39
41	43	31	41
00	00	00	00
00	00	00	00

Tabel 10 Substisi chiper key

Chiper key					
39		41		83	01
41	Rootword	00	Sub-byte	63	XOR
00		00		63	00
00		39		12	00

Dari proses di atas kolom ke-4 dari *chipper key* di *rootword* terlebih dahulu kemudian di *sub-byte* dan di XOR kan pada kolom pertama tabel rcon hasil setiap kolomnya. Langkah di atas dapat di lakukan sampai 10 *round* sehingga hasilnya seperti dibawah ini.

Tabel 11 Hasil substitusi

Round 1				Round 10			
B7	F6	B2	8b	A5	46	7A	FD
22	61	50	11	F6	6D	15	E0
63	63	63	63	98	3D	A0	57
12	12	12	12	CA	F0	E3	6F

3. Sub-byte

Pada tahap ini hasil *plaintext* dan *chipper key* yang telah di XOR kan akan di *Sub-byte* dengan tabel s-box sebagai berikut:

Tabel 12 Sub-byte

Blok					After sub-byte			
74	01	01	75		92	7C	7C	9D
08	02	61	13	Sub-byte	30	77	EF	7D
41	54	49	57		83	20	3B	5B
49	41	45	53		3B	83	6E	ED

4. Shift-rows

Pada tahap ini hasil dari *Sub-byte* akan di *shift rows* yaitu pergeseran baris hanya pada baris 2 – 4 tetapi untuk baris Pertama tidak digeser hasil nya akan tetap.

Tabel 13 Shift-rows

Hasil Sub-byte					Output			
92	7C	7C	9D		92	7C	7C	9D
30	77	EF	7D	Sub-	77	EF	7D	30

				<i>byte</i>					
83	20	3B	5B		3B	5B	83	20	
3B	83	6E	ED		ED	3B	83	6E	

5. *Mix-coloumns*

Setelah melakukn 3 tahap maka kemudian dapat melakukan tahap *mix coloumns* yang dikalikan dengan matrix

Tabel 14 *Mix coloumns*

Hasil Shift rows				•	Matrix				After mix coloumns			
92	7C	7C	9D		02	03	01	01	72	BF	7F	3D
77	EF	7D	30		01	02	03	01	DF	6F	9C	F3
3B	5B	83	20		01	01	02	03	B2	6B	81	5A
ED	3B	83	6E		03	01	01	02	B5	40	61	6D

6. *Add round key*

Perhitungan *add round key* merupakan perhitungan hasil dari *mix coloumns* di XOR kan dengan hasil *round 1* dari pembangkit kunci, Proses ini dapat dilakukan hingga *round 9* pada tahap akhir tidak perlu melakukan *mix coloumns*. Sehingga hasil dari *round 10* Yaitu :

Tabel 15 *Add round key*

Hasil mix coloumns				XOR	Round 1				Output round 10			
72	BF	7F	3D		B7	F6	B2	8B	58	69	A8	FC
DF	6F	9C	F3		22	61	50	11	20	16	CF	31
B2	6B	81	5A		63	63	63	63	0C	A2	B4	3B
B5	40	61	6D		12	12	12	12	6A	FA	36	20

7. Hasil Akhir Metode AES

Hasil dari *add round key* diubah ke dalam hexa sehinga meghasilkan nilai *chipertext*.

Tabel 16 Hasil akhir proses AES

Hexa	58	20	0c	6A	69	16	A2	FA	A8	CF	B4	36	FC	31	3B	20
Dec	88	32	12	106	105	22	162	250	168	207	180	54	252	49	59	32
Chipertext	X	Space	FF	J	I	SYN	ó	-	ı	±	†	6	„	1	;	Space

II. Hasil Pengujian AES

Pada tampilan dibawah ini merupakan hasil dari UID yang telah di enkripsi dengan menggunakan kriptografi AES, tampilan di bawah ini hanya menunjukkan keberhasilan pada proses enkripsi karena pada dasarnya tujuan kriptografi untuk mengamankan data, pada tampilan sebenarnya tidak terlihat hasil enkripsi data tersebut. Masing – masing pada UID mempunyai UID yang berbeda tentu saja hasil enkripsinya pun akan berbeda.

III. Tampilan hasil enkripsi AES

Tampilan dibawah ini merupakan hasil keberhasilan dari proses enkripsi dengan menggunakan AES berikut hasil sebelum dan sesudah di enkripsi.

UID	USERNAME
4A28E781	Irvan
5AD9AC1A	Ratna
B3136F15	Amelia
B91A1CBA	Antonie
C0122332	Erika
CC1AE637	Nelly

Showing 1 to 6 of 6 entries

Gambar 5 Tampilan sebelum di enkripsi

UID	USERNAME
2Kf3IbAnSypv1cM/0X2G7w==	ZRALeu/m4GQqU5w5R0p/Gg==
AHc9LTi0Jg42P0ziqpxxQg==	Hw1gPyYSusvtTclKodmjxg==
M/uhY/bPymFgpMMF5h3TA==	AVRik88Js8N06TJwNjnfWw==
nh/PRufkbnZGsluE/nnJ2g==	j4EKf1gGKnMuK8JA1Ak+g==
SfzG5rXKanYoXKhEojrqJA==	4QtG6ZdQrj5IDPMkvtZWDw==
SsYg9HXeH6w7ammzzXweRw==	9CS3cDdPM7GDxSk1vlvcYw==

Showing 1 to 6 of 6 entries

Gambar 6 Tampilan setelah di enkripsi pada Website AES

KESIMPULAN DAN SARAN

A. Kesimpulan

Berdasarkan sistem yang dikembangkan dan pengembangan yang telah dilakukan dapat diperoleh beberapa kesimpulan, antara lain :

1. Sistem ini berhasil enkripsi data dengan mengimplementasikan metode AES dan alat RFID dan telah di uji bahwa RFID dapat digunakan dengan maksimal 5cm.
2. Sistem ini berhasil mengimplementasikan sistem RFID dan *Keypad* 4x4 pada prototype pintu yang digunakan untuk sistem akses keluar masuk serta.

B. Saran

Untuk meningkatkan dan mengembangkan hasil sistem ini ada beberapa saran yang dapat dilakukan sebagai berikut:

1. Sistem ini dapat dikembangkan lebih baik lagi.
2. Sistem ini dapat menambahkan *button alarm* agar setiap ada interaksi yang tidak sesuai dengan aturannya *alarm* akan memberikan tanda.

DAFTAR PUSTAKA

- [1] Abroruddin Misbah Perancangan Sistem Pengaman Pintu Rumah menggunakan Sidik Jari berbasis Arduino [Journal]. - 01 Mei 2020. - Vol. Vol.5 No.1. -ISSN 2502-1613 E-ISSN 2541-3740.
- [2] Daulay Nelly Khairani *Monitoring* sistem keamanan pintu menggunakan RFID dan *Fingerprint* berbasis *Website* dan *Database* [Journal] Jasikom : Jurnal Sistem Komputer Musi rawas. - 02 Desember 2019. - Vols. Vol.04, No.2.
- [3] Efendi Ilham Pengertian arduino [Journal] It-Jurnal.Com.
- [4] Ekayana Anak Agung Gde Implemenasi sistem keamanan pintu menggunakan RFID *Mifare Frequency* 13.56MHZ Dengan *Multi Access* [Journal] Jurnal Pendidikan Teknologi dan Kejuruan. - Juli 2018. - Vol. Vol.15 No.2. - p. 244. - P-ISSN : 0216-3241 ; E-ISSN : 2541-0652.
- [5] Immersa Lab Teknologi *smart home* dan manfaatnya [Journal]. - maret 2018.
- [6] Kurniawan Muhammad Irfan *Internet of Things* : Sistem Keamanan Rumah berbasis *Raspberry Pi* dan *Telegram Messenger* [Journal] ELKOMIKA. - Januari 2018. - Vol. Vol.6 No.1. - pp. 1-15. - ISSN-2338-8323.
- [7] Luluk Elvitaria, M. H. (2017). Smk Analisis Kesehatan Abdurrah Menggunakan Algoritma. (*Jurnal Teknologi Dan Sistem Informasi Univrab*, 2(2), 220–233.
- [8] Ramadhan Ade Surya Rancang Bangun Sistem Keamanan Rumah Berbasis Arduino Mega 2560 [Journal] Jurnal Teknologi Informasi. - Mei 2016. - Vol. Vol.15. - e-issn : 2356-2579.