Jurnal Sains Teknologi dan Sistem Informasi
journal.yp3a.org/index.php/satesi
Vol. 1 No. 1 (2021) 26 – 31 ISSN Media Elektronik: 2807–8152

Implementasi Algoritma AES Pada QR-Code Sebagai Parameter Keaslian Data Dalam Pembuatan KTA

Nahar Mardiyantoro[1*], Mefa Listiani[2]

[1,2]Teknik Informatika, Fakultas Teknik dan Ilmu Komputer, Universitas Sains Al-Quran, Wonosobo, Indonesia
Email: [1*]mardziyant@fastikom-unsiq.ac.id, [2]mefalistiani143@gmail.com

ABSTRACT
The process of making KTA at UPT RPH Wonosobo Regency which is still carried out by typing prospective member data in MS Excel and editing it in the form of a card and then be printed, is considered ineffective so that it prolongs the process of making KTA. Besides that there is no guarantee of authenticity, so an application for making KTA is made with added the AES algorithm to speed up the performance of the KTA manufacturing process and guarantee its authenticity. The implementation of the AES Algorithm is included in the KTA checking URL which is converted into a QR-Code for easy scanning. This research is expected to help the process of making KTA at UPT RPH Wonosobo Regency and ensure the authenticity of the KTA made.

Keywords: AES Algorithm, QR-Code, KTA, Security, Authenticity.

ABSTRAK
Proses pembuatan KTA pada UPT RPH kabupaten wonosobo yang masih dilakukan dengan mengetik data calon anggota pada MS Excel dan mengeditnya dalam bentuk kartu kemudian dicetak, proses tersebut dirasa kurang efektif sehingga memperlama proses pembuatan KTA. Selain itu juga tidak ada jaminan keasliannya, maka dibuatlah aplikasi pembuatan KTA dengan menambahkan algoritma AES untuk mempercepat kinerja proses pembuatan KTA dan menjamin keasliannya. Implementasi Algoritma AES dimasukkan ke dalam URL pengecekan KTA yang dikonversi menjadi QR-Code agar mudah dipindai dan mudah dilakukan pengecekan. Penelitian ini diharapkan dapat membantu proses pembuatan KTA di UPT RPH Kabupaten Wonosobo dan menjamin keaslian KTA yang dibuat.

Kata Kunci: Algoritma AES, QR-Code, KTA, Keamanan, Keaslian.

1. Pendahuluan

Rumah Potong Hewan atau yang disebut dengan RPH adalah suatu bangunan yang didesain dengan syarat tertentu digunakan sebagai tempat pemotongan hewan untuk konsumsi masyarakat umum. Berfungsi sebagai sarana untuk melaksanakan pemotongan hewan dengan benar, pemeriksaan hewan sebelum dan sesudah dipotong untuk menghasilkan daging yang aman, sehat, utuh dan halal.

Salah satu syarat diakuinya pekerja pemotong daging di UPT RPH Kabupaten Wonosobo adalah sudah memiliki Kartu Tanda Anggota (KTA). Proses pembuatan KTA yang lebih singkat dapat mempercepat calon anggota untuk segera bekerja dan meningkatkan kinerja UPT RPH Kabupaten Wonosobo.

Pemotongan hewan dilakukan oleh para pekerja pemotong daging yang terdiri dari 39 anggota, diantaranya yang bertugas sebagai penyembelih, pemotong kepala dan kaki, pengulitan, pemisah daging, dan pengeluaran jeroan.

Namun, saat ini pelaksanaan pemotongan hewan masih belum berjalan dengan tertib. Selain itu, proses pembuatan KTA dilakukan dengan cara mendesain KTA dahulu melalui Ms. Excel, kemudian diketik data diri anggotanya lalu mencetaknya. Hal ini akan menyebabkan data anggota pekerja pemotongan hewan tidak tersusun secara terkelompok karena pengetikannya tidak berurutan dan memperlama proses pembuatan KTA. Begitu juga dengan jaminan keaslian KTA tersebut. Dengan mudahnya membuat KTA secara manual, KTA menjadi rawan dengan praktik pemalsuan. Agar pemotongan bisa tertib, cepat, efisien dan aman dibutuhkan suatu aplikasi yang dapat mengolah data secara sistematis dan meng-*enkripsi* KTA dengan aman.

Diterima Redaksi: 09-09-2021 | Selesai Revisi: 09-09-2021 | Diterbitkan Online: 10-09-2021

Beberapa metode yang dapat digunakan untuk meng-*enkripsi* informasi yang dimuat dalam KTA antara lain Algoritma IDEA, DES, *Blowfish*, dan AES. Namun, berdasarkan pengujian yang telah dilakukan dari segi kecepatan dan ukuran *file* yang dihasilkan, Algoritma AES merupakan algoritma yang terbaik di antara ketiga algoritma tersebut [1].
Cara kerja Algoritma AES menggunakan substitusi dan permutasi dalam orientasi *byte* yang diulang-ulang sehingga hasil enkripsi lebih aman. Algoritma ini mempunya kunci internal yang berbeda-beda di setiap putarannya [2].
Hasil dari Algoritma AES tidak bisa langsung dicantumkan ke dalam KTA karena akan mempersulit seseorang yang akan mengecek keaslian KTA tersebut. Sehingga Algoritma yang dihasilkan di-*enkripsi* lagi ke dalam sebuah *Quick Response Code (QR-Code). QR-Code* merupakan pengembangan dari *Barcode* yang mampu menyimpan informasi agar bisa diolah dengan cepat dan tepat. Dengan di-*enkripsi*-kan ke dalam *QR-Code*, hasil enkripsi bisa diidentifikasi oleh semua orang menggunakan aplikasi pembaca *QR-Code* yang sudah umum digunakan pada *Smartphone* masing-masing [3].
Berdasarkan beberapa hal di atas, penulis berkeinginan untuk merancang suatu aplikasi atau program yang tepat dengan membuat suatu aplikasi yang dapat membantu instansi. Hal ini tentunya akan sangat membantu dalam kelancaran atau kecepatan penyelesaian berbagai pekerjaan apapun. Dengan adanya aplikasi ini instansi dapat lebih maju dan semua data yang diperlukan bisa didapat dengan cepat dan mudah.

2. Metode Penelitian

2.1. Objek Penelitian

Objek penelitian dalam penelitian ini adalah Pembuatan KTA di UPT RPH Kabupaten Wonosobo.

2.2 Jenis Penelitian

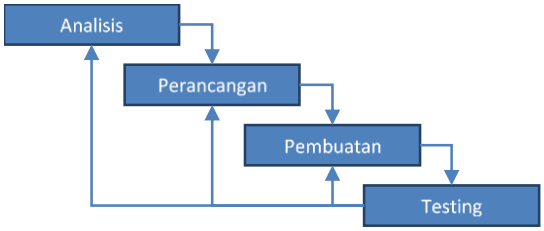
Jenis Penelitian ini merupakan penelitian pengembangan yaitu penelitian yang bertujuan untuk mengembangkan atau menghasilkan suatu produk [4]. Dalam penelitian ini produk yang dihasilkan adalah sebuah aplikasi untuk mempercepat proses pembuatan KTA di UPT RPH Kabupaten Wonosobo.

2.3 Data Penelitian

Data dalam penelitian ini bersumber dari dua jenis data, yaitu data primer dan data sekunder. Data primer yang didapat melalui proses wawancara adalah data mengenai alur pembuatan KTA siapa saja yang berwenang untuk membuat KTA. Sedangkan data sekunder dalam penelitian ini adalah data penunjang yang dikumpulkan berasal dari dokumen-dokumen yang berkaitan dengan KTA dan sistem pengamanan yang dapat diterapkan seperti desain KTA dan biodata para pekerja

2.4 Metode Pengembangan Sistem

Pembuatan aplikasi ini menggunakan metode waterfall. Tahapan yang dilakukan pada metode tersebut dapat dilihat pada gambar di bawah ini :



Gambar 1. Metode Waterfall

2.5 Penerapan Algoritma AES

Penerapan Algoritma AES Pada Aplikasi Pembuatan KTA ada pada enkripsi dari kode anggota yang tersimpan di dalam *Data base* digabungkan dengan URL yang nantinya akan mengarahkan ke dalam halaman pengecekan KTA. URL yang sudah berisi enkripsi kode anggota kemudian dikonversi menjadi bentuk *QR-Code. QR-Code* ini disisipkan ke dalam KTA agar lebih mudah dalam melakukan pengecekan KTA.

3. Hasil dan Pembahasan

3.1. Proses enkripsi Algoritma AES

Untuk penjelasan proses enkripsi Algoritma AES kita ambil contoh pada salah satu kode anggota ditambahkan nama anggota itu sendiri, yaitu "001_Ribudi".
Algoritma AES merupakan algoritma yang menggunakan transformasi substitusi dan permutasi yang diulang-ulang menggunakan kunci pada tiap pengulangannya [5]. Kunci pada proses putaran pertama dapat kita tentukan sendiri. Selanjutnya kunci tersebut akan ditransformasikan ke dalam 10 kunci yang berbeda melalui proses *Key Schedule*. Dalam hal ini kunci yang kita tentukan adalah "abcdefghijuklmno".
Sebelum masuk ke tahap enkripsi, ubah terlebih dahulu teks yang akan dienkripsi dan kunci yang telah ditentukan ke dalam bentuk *Hex* yang kemudian disebut sebagai *Plaintext* dan *Chiper Key*. Sehingga dihasilkan :

Tabel 1. Perubahan pada bentuk *Hex*

Teks/*Key*	Hex
001_Ribudi	3030315F526962756469000000000000
abcdefghijuklmno	6162636465666768696A756B6C6D6E6F

Proses pertama dalam meng-enkripsi menggunakan Algoritma AES adalah *Initial Round* yaitu pengkalian XOR antara *plaintext* dengan *chiper key*. Kemudian

DOI: 10.54259/satesi.v1i1.5

hasil pengkalian tersebut disubsitusikan dengan tabel S-Box. Proses ini dinamakan *SubBytes.* Setelah itu lakukan proses *ShiftRows*, yaitu pergeseran ke kiri masing-masing baris pada hasil *SubBytes* sejauh n kolom sesuai dengan letak barisnya. Proses selanjutnya yaitu *MixColumns.* Pada proses ini dilakukan perkalian hasil sebelumnya dengan sebuah matrik. Kemudian lanjut ke proses *AddRoundKey*, yaitu perkalian XOR antara hasil *MixColumns* dengan *RoundKey* (hasil *Key Schedule)* pertama.

Keempat proses tersebut kemudian diulang sampai 9 kali. Dan di perulangan yang ke 10 lakukan proses yang sama kecuali proses *MixColumns.* Ilustrasi proses enkripsi Algoritma AES dapat dilihat pada gambar di bawah ini :

	SubBytes	ShiftRows	MixColumns	AddRoundKey	Key Schedule	Round Constant
Round 0				51 37 0D 6C 52 0F 03 6D 52 05 75 6E 3B 1D 6B 6F	61 65 69 6C 62 66 6A 6D 63 67 75 6E 64 68 6B 6F	
Round 1	D1 9A D7 50 00 76 7B 3C 00 6B 9D 9F E2 A4 7F A8	D1 9A D7 50 76 7B 3C 00 9D 9F 00 6B A8 E2 A4 7F	16 DF 55 B4 29 34 0B 92 65 F9 1C 07 C8 8E 0D 65	4A E6 05 88 D4 AF FA 0E AE 55 C5 B0 FC D2 3A 3D	5C 39 50 3C FD 9B F1 9C CB AC D9 B7 34 5C 37 58	01 00 00 00
Round 2	D6 8E 6B C4 48 79 2D AB E4 FC A6 E7 B0 B5 80 27	D6 8E 6B C4 79 2D AB 48 A6 E7 E4 FC 27 B0 B5 80	BD 27 61 37 F2 56 A4 CB 91 BD D7 F4 F0 38 83 F8	3D 9E 88 E2 A6 99 9A 69 30 B0 03 97 2F BB 37 14	80 B9 E9 D5 54 CF 3E A2 A1 0D D4 63 DF 83 B4 EC	02 00 00 00
Round 3	27 0B C4 98 24 EE B8 F9 04 E7 7B 88 15 EA 9A FA	27 0B C4 98 EE B8 F9 24 7B 88 04 E7 FA 15 EA 9A	E6 58 6D 3A 97 F6 CB 78 2A 87 10 DC 13 07 65 5F	58 5F 83 01 38 96 95 84 45 E5 A6 09 CF 58 8E 58	BE 07 EE 3B AF 60 5E FC 6F 62 B6 D5 DC 5F EB 07	04 00 00 00
Round 4	6A CF EC 7C 07 90 2A 5F 6E D9 24 01 8A 6A 19 6A	6A CF EC 7C 90 2A 5F 07 24 01 6E D9 6A 8A 6A 19	31 70 26 31 57 12 8A 1B 0C 62 D1 F9 DE 6E CA 68	37 71 C9 E5 FB DE 18 75 A6 AA AF 52 E0 0F 40 E5	06 01 EF D4 AC CC 92 6E AA C8 7E AB 3E 61 8A 8D	08 00 00 00
Round 5	9A A3 DD D9 0F 1D AD 9D 24 AC 79 00 E1 76 09 D9	9A A3 DD D9 1D AD 9D 0F 79 00 24 AC D9 E1 76 09	A8 50 4F 1D F2 03 E6 21 05 36 92 8E 78 8A 29 C1	21 D8 28 AE 3C 01 76 DF F2 09 D3 64 0E 9D B4 D1	89 88 67 B3 CE 02 90 FE F7 3F 41 EA 76 17 9D 10	10 00 00 00
Round 6	FD 61 34 E4 EB 7C 38 9E 89 01 66 43 AB 5E 8D 3E	FD 61 34 E4 7C 38 9E EB 66 43 89 01 3E AB 5E 8D	3D 62 06 79 91 7F CD A7 0F 39 41 81 7A 95 F7 DC	2F F8 FB 37 D8 34 16 82 32 3B 02 28 61 99 66 5D	12 9A FD 4E 49 4B DB 25 3D 02 43 A9 1B 0C 91 81	20 00 00 00
Round 7	15 41 0F 9A 61 18 47 13 23 E2 77 34 EF EE 33 4C	15 41 0F 9A 18 47 13 61 77 34 23 E2 4C EF EE 33	39 90 E6 5D F0 7C A2 56 37 44 73 71 C8 75 E6 50	54 67 EC 19 6A AD A8 79 06 77 03 A8 FC 4D 4F 78	6D F7 0A 44 9A D1 0A 2F 31 33 70 D9 34 3B A9 28	40 00 00 00
Round 8	20 85 CE D4 02 95 C2 B6 6F F5 7B C2 B0 E3 84 BC	20 85 CE D4 95 C2 B6 02 7B C2 6F F5 BC B0 E3 84	23 3E CA C4 20 F7 EB 50 9C 13 98 B0 ED EF 4D 83	DB 31 CF 85 8F 89 9F 0B 99 25 DE 2F C2 F8 F3 15	F8 0F 05 41 AF 7E 74 5B 05 36 46 9F 2F 17 BE 96	80 00 00 00
Round 9	B9 C7 8A 97 73 A7 DB 2B EE 3F 1D 15 25 41 0D 59	B9 C7 8A 97 A7 DB 2B 73 1D 15 EE 3F 59 25 41 0D	DF D3 DD 92 92 70 B4 3D CF 59 A5 8D D8 D6 C2 F4	05 06 0D 03 E6 7A CA 18 5A FA 40 F7 74 6D C7 67	DA D5 D0 91 74 0A 7E 25 95 A3 E5 7A AC BB 05 93	1B 00 00 00
Round 10	6B 6F D7 7B 8E DA 74 AD BE 2D 09 68 92 3C C6 85			B8 69 01 3C 74 D0 77 71 40 82 B1 58 A8 04 AF C6	D3 06 D6 47 AE A4 DA FF 49 EA 0F 75 2D 96 93 00	36 00 00 00
	SubBytes	ShiftRows	MixColumns	AddRoundKey	Key Schedule	Round Constant

Gambar 2. Enkripsi Algoritma AES

Hasil keluaran (*output*) dari proses enkripsi di atas adalah :

B87440A869D082040177B1AF3C7158C6

Yang selanjutnya disebut dengan *Chiper Text.*

3.2. Proses Dekripsi Algoritma AES

Pada proses dekripsi, langkah yang dilakukan sama seperti dengan enkripsi, hanya saja prosesnya dibalik. RoundKey yang digunakan juga dibalik urutannya untuk masing-masing putaran, mulai dari *RoundKey* ke 10 untuk putaran pertama, kemudian mundur sampai ke *Chiper* Key [6].

Proses pertama pada Dekripsi AES adalah *AddRoundKey*, yaitu perkalian XOR antara *Chiper Text* dengan *Round Key* ke 10. Kemudian *InvShiftRows* yaitu pergeseran ke kanan masing-masing baris pada hasil *AddRoundKey.* Setelah itu konversi hasil *InvShiftRows* dengan Tabel Invers S-Box. Proses ini dinamakan *InvSubBytes.* Langkah berikutnya yaitu melakukan *AddRoundKey* putaran ke 2, dilanjutkan dengan *InvMixColumns*, yaitu perkalian hasil *AddRoundKey* dengan matrik khusus, kemudian lakukan proses *InvShiftRows* putaran ke 2 lalu proses *InvSubBytes* putaran ke 2. Keempat Langkah ini diulang sampai dengan 9 kali. Langkah terakhir pada proses dekripsi yaitu *AddRoundKey* yang merupakan perkalian XOR antara hasil sebelumnya dengan *Chiper Key* yang telah dibuat sebelumnya.

Berikut adalah Ilustrasi proses dekripsi Algoritma AES untuk setiap langkahnya :

SubBytes	ShiftRows	MixColumns	AddRoundKey	Key Schedule	Round Constant	
			30 52 64 00 30 69 69 00 31 62 00 00 5F 75 00 00	61 65 69 6C 62 66 6A 6D 63 67 75 6E 64 68 6B 6F		Round 10
51 37 0D 6C 52 0F 03 6D 52 05 75 6E 3B 1D 6B 6F	D1 9A D7 50 00 76 7B 3C 9D 9F 00 6B A8 E2 A4 7F	D1 9A D7 50 76 7B 3C 00 65 F9 1C 07 E2 A4 7F A8	16 DF 55 B4 29 34 0B 92 CB AC D9 B7 34 5C 37 58	5C 39 50 3C FD 9B F1 9C CB AC D9 B7 34 5C 37 58	01 00 00 00	Round 9
4A E6 05 88 D4 AF FA 0E AE 55 C5 B0 FC D2 3A 3D	D6 8E 6B C4 48 79 2D AB E4 FC A6 E7 B0 B5 80 27	D6 8E 6B C4 79 2D AB 48 A6 E7 E4 FC 27 B0 B5 80	BD 27 61 37 F2 56 A4 CB 91 BD D7 F4 F0 38 83 F8	80 B9 E9 D5 54 CF 3E A2 A1 0D D4 63 DF 83 B4 EC	02 00 00 00	Round 8
3D 9E 88 E2 A6 99 9A 69 30 B0 03 97 2F BB 37 14	27 0B C4 98 24 EE B8 F9 B0 B5 80 27 15 EA 9A FA	27 0B C4 98 EE B8 F9 24 7B 88 04 E7 FA 15 EA 9A	E6 58 6D 3A 97 F6 CB 78 2A 87 10 DC 13 07 65 5F	BE 07 EE 3B AF 60 5E FC 6F 62 B6 D5 DC 5F EB 07	04 00 00 00	Round 7
58 5F 83 01 38 96 95 84 45 E5 A6 09 CF 58 8E 58	6A CF EC 7C 90 2A 5F 07 6E D9 24 01 8A 6A 19 6A	6A CF EC 7C 31 70 26 31 24 01 6E D9 6A 8A 6A 19	31 70 26 31 57 12 8A 1B 0C 62 D1 F9 DE 6E CA 68	06 01 EF D4 AC CC 92 6E AA C8 7E AB 3E 61 8A 8D	08 00 00 00	Round 6
37 71 C9 E5 FB DE 18 75 A6 AA AF 52 E0 0F 40 E5	9A A3 DD D9 0F 1D AD 9D 24 AC 79 00 E1 76 09 D9	9A A3 DD D9 1D AD 9D 0F 79 00 24 AC D9 E1 76 09	A8 50 4F 1D F2 03 E6 21 05 36 92 8E 78 8A 29 C1	89 88 67 B3 CE 02 90 FE F7 3F 41 EA 76 17 9D 10	10 00 00 00	Round 5
21 D8 28 AE 3C 01 76 DF F2 09 D3 64 0E 9D B4 D1	FD 61 34 E4 EB 7C 38 9E 89 01 66 43 AB 5E 8D 3E	FD 61 34 E4 7C 38 9E EB 66 43 89 01 3E AB 5E 8D	3D 62 06 79 91 7F CD A7 0F 39 41 81 7A 95 F7 DC	12 9A FD 4E 49 4B DB 25 3D 02 43 A9 1B 0C 91 81	20 00 00 00	Round 4
2F F8 FB 37 D8 34 16 82 32 3B 02 28 61 99 66 5D	15 41 0F 9A 18 47 13 61 77 34 23 E2 4C EF EE 33	15 41 0F 9A 47 13 61 F0 34 23 E2 37 EF EE 33 4C	39 90 E6 5D 7C A2 56 6A 44 73 71 06 C8 75 E6 50	6D F7 0A 44 9A D1 0A 2F 31 33 70 D9 34 38 A9 28	40 00 00 00	Round 3
54 67 EC 19 6A AD A8 79 06 77 03 A8 FC 4D 4F 78	20 85 CE D4 95 C2 B6 02 6F F5 7B C2 B0 E3 84 BC	20 85 CE D4 95 C2 B6 02 7B C2 6F F5 BC B0 E3 84	23 3E CA C4 20 F7 EB 50 9C 13 98 B0 ED EF 4D 83	F8 0F 05 41 AF 7E 74 5B 05 36 46 9F 2F 17 BE 96	80 00 00 00	Round 2
DB 31 CF 85 8F 89 9F 0B 99 25 DE 2F C2 F8 F3 15	B9 C7 8A 97 A7 DB 2B 73 1D 15 EE 3F 25 41 0D 59	B9 C7 8A 97 92 70 B4 3D CF 59 A5 8D 59 25 41 0D	DF D3 DD 92 74 0A 7E 25 95 A3 E5 7A D8 D6 C2 F4	DA D5 D0 91 00 00 AC BB 05 93	1B 00 00 00	Round 1
05 06 0D 03 E6 7A CA 18 5A FA 40 F7 74 6D C7 67	6B 6F D7 7B 8E DA 74 AD BE 2D 09 68 92 3C C6 85		6B 6F D7 7B DA 74 AD 8E 09 68 BE 2D 85 92 3C C6	D3 06 D6 47 AE A4 DA FF 49 EA 0F 75 2D 96 93 00	36 00 00 00	Round 0
SubBytes	ShiftRows	MixColumns	AddRoundKey	Key Schedule	Round Constant	

Gambar 3. Dekripsi Algoritma AES

Berdasarkan proses dekripsi di atas, Output yang dihasilkan adalah :

3030315F526962756469000000000000

Hasil ini masih berupa *Plaintext* yang berbentuk *Hex.* Apabila diubah ke dalam teks maka akan menghasilkan :

"001_Ribudi"

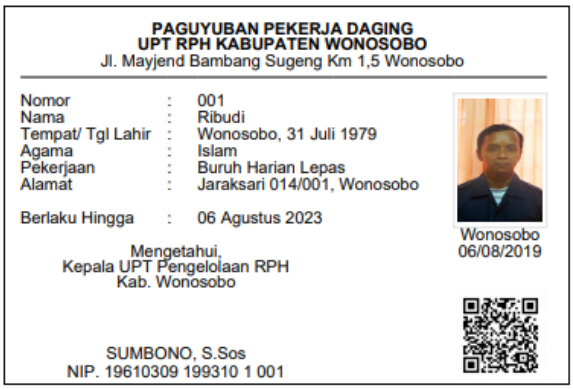
3.3. Implementasi Algoritma AES pada Aplikasi Pembuatan KTA

DOI: 10.54259/satesi.v1i1.5

Penerapan Algoritma AES pada aplikasi pembuatan KTA ada pada *QR-Code* yang berisi URL halaman pengecekan KTA yang sudah digabung dengan hasil enkripsi kode anggota menggunakan Algoritma AES. URL halaman pada pembahasan ini adalah :

http://ktarph.rf.gd/kta_detail.php?id=
b87440a869d082040177b1af3c7158c6

Berikut ini adalah contoh KTA yang sudah disispkan *QR-Code* yang berisi URL dan enkripsi Algoritma AES :


PAGUYUBAN PEKERJA DAGING
UPT RPH KABUPATEN WONOSOBO
Jl. Mayjend Bambang Sugeng Km 1,5 Wonosobo

Nomor : 001
Nama : Ribudi
Tempat/ Tgl Lahir : Wonosobo, 31 Juli 1979
Agama : Islam
Pekerjaan : Buruh Harian Lepas
Alamat : Jaraksari 014/001, Wonosobo

Berlaku Hingga : 06 Agustus 2023

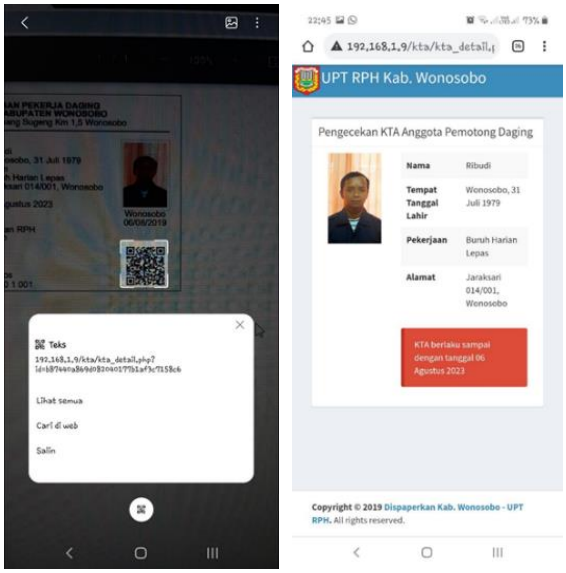
Wonosobo
06/08/2019

Mengetahui,
Kepala UPT Pengelolaan RPH
Kab. Wonosobo

SUMBONO, S.Sos
NIP. 19610309 199310 1 001

Gambar 4. Contoh KTA

Untuk pengecekan KTA dilakukan dengan memasuki halaman pengecekan KTA yang didapat dari hasil pemindaian *QR-Code*. Berikut adalah tampilan pemindaian *QR-Code* dan halaman pengecekan KTA :



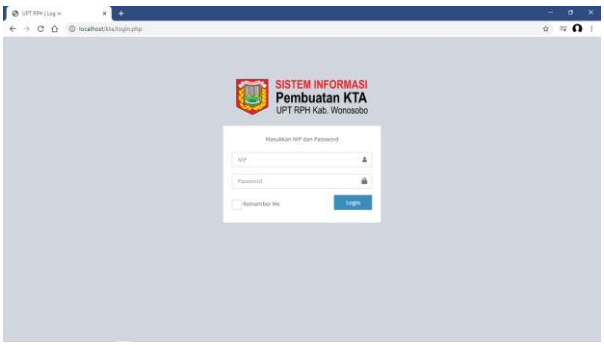
Gambar 5. Tampilan proses pengecekan KTA

Berdasarkan hasil pada halaman pengecekan dapat disimpulkan bahwa data yang tertera pada halaman pengecekan sama dengan data yang tertera pada KTA aslinya.

Selain itu bisa juga ditambahkan beberapa fitur baru seperti pendaftaran secara *online* atau bahkan pembayaran biaya pendaftaran secara *online*.

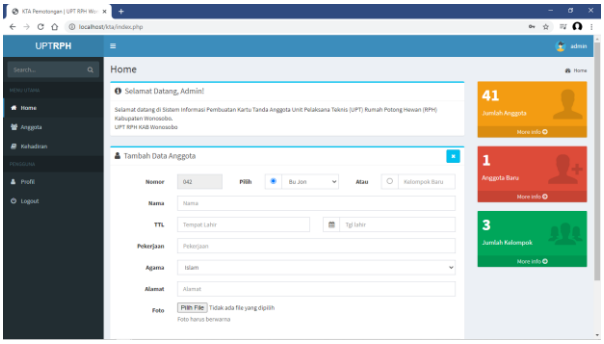
3.4. Implementasi *User Interface* Aplikasi

Sebelum mengakses Sistem Informasi Pembuatan KTA UPT RPH Kabupaten Wonosobo, pengguna / admin diwajibkan melakukan login terlebih dahulu untuk memastikan bahwa pengguna / admin tersebut benar-benar merupakan petugas resmi dari UPT RPH Kabupaten Wonosobo.



Gambar 5. Halaman Login

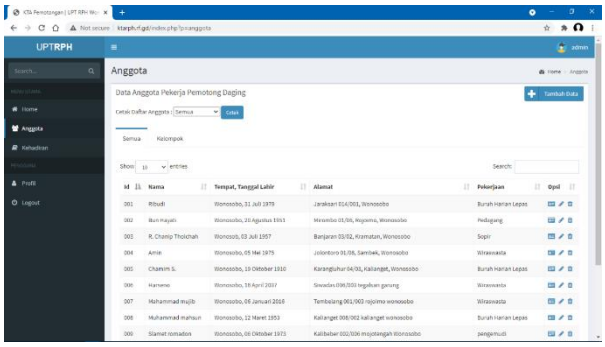
Halaman utama sistem informasi ini menampilkan informasi mengenai jumlah anggota yang sudah ada maupun anggota yang baru ditambahkan. Untuk menambahkan anggota baru juga bisa langsung dilakukan pada halaman ini, termasuk mencetak KTA-nya.



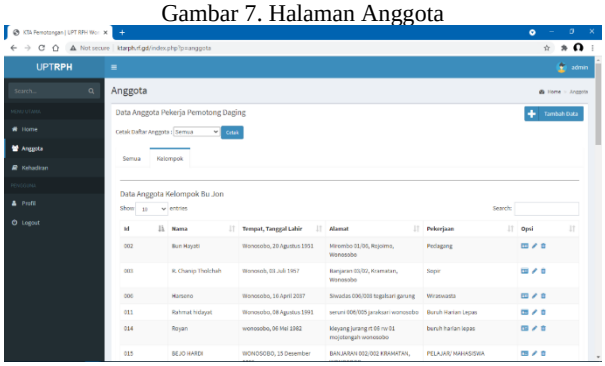
Gambar 6. Halaman Utama

Halaman Anggota menampilkan data anggota secara keseluruhan mapupun kelompok. Di sini juga terdapat tombol untuk menambahkan data anggota, edit data anggota, hapus anggota, dan cetak KTA. Dari halaman ini pula terdapat tombol untuk mencetak data anggota.

DOI: 10.54259/satesi.v1i1.5



Gambar 7. Halaman Anggota

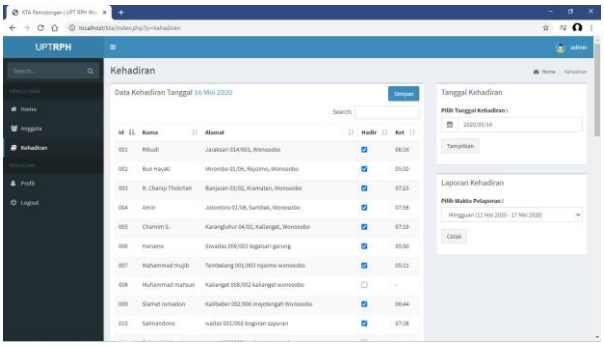


Gambar 8. Halaman Anggota per Kelompok

Halaman Cetak Anggota menampilkan pratinjau daftar anggota yang sudah ada secara keseluruhan, per kelompok, maupun untuk kelompok tertentu saja. Halaman ini berformat .pdf, sehingga bisa langsung dicetak ataupun diunduh ke komputer.

Gambar 9. Halaman Cetak Anggota

Pada Halaman Kehadiran terdapat form untuk mengisi kehadiran anggota.pada tanggal sekarang maupun tanggal tertentu (untuk perubahan data). Pada halaman ini juga ta terdapat tombol untuk mencetak laporan kehadiran bulanan ataupun mingguan.



Gambar 10. Halaman Kehadiran

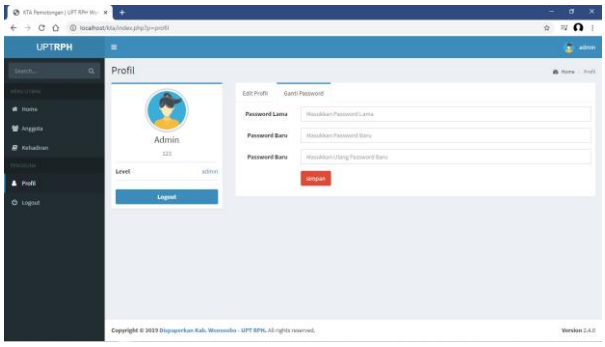
Halaman Cetak Kehadiran menampilkan pratinjau laporan kehadiran bulanan maupun mingguan yang akan dicetak. Untuk memudahkan penyampaian informasi, tiap kolom kehadiran terdapat warna tertentu untuk membedakan status kehadiran anggota. Warna hijau mewakili kehadiran, sedangkan warna merah mewakili ketidakhadiran. Halaman ini berformat .pdf, sehingga bisa langsung dicetak ataupun diunduh ke komputer.

Gambar 11. Halaman Cetak Kehadiran Mingguan

Gambar 12. Halaman Cetak Kehadiran Bulanan

Halaman ini menampilkan form edit untuk mengubah profil pengguna / admin

DOI: 10.54259/satesi.v1i1.5



Gambar 13. Halaman Edit Profil

Pengujian sistem berguna untuk memastikan bahwa sistem dapat berjalan sesuai dengan harapan. Pengujian yang dipakai pada penelitian ini adalah Pengujian Black Box.

Pengujian Black Box merupakan pengujian yang mengutamakan kesesuaian program. Pengujian ini tidak memerlukan pengetahuan mengenai struktur internal pada program [7]. Dengan begitu semua orang dapat melakukan pengujian ini.

Pengujian untuk penerapan Algoritma AES pada *QR-Code* dalam penelitian ini dapat dilihat pada tabel di berikut :

3.5. Pengujian Sistem

Tabel 2. Pengujian *Blackbox*

No	Pengujian	Aktivitas Pengujian	Hasil Pengujian	Kesimpulan
1.	Pembuatan *QR-Code*	Cetak KTA menggunakan aplikasi, *Scan QR-Code* dengan *Barcode Scanner*	Muncul *link* pengecekan KTA	OK
2.	Enkripsi Algoritma AES	Cek enkripsi *link* yang diperoleh dari *Barcode Scanner* dengan hasil enkripsi secara manual. Hasil enkripsi dari perhitungan manual : **b87440a869d082040177b1af3c7158c6**	*link* diperoleh : http://192.168.1.9/kta/kta_detail.php?id= **b87440a869d082040177b1af3c7158c6** Enkripsi menggunakan aplikasi maupun perhitungan secara manual menghasilkan *chipertext* yang sama	OK
3	Dekripsi Algoritma AES	Klik *link* yang muncul setelah memindai *QR-Code*	*Link* mengarahkan ke halaman pengecekan KTA. Data yang ditampilkan sama dengan data KTA yang dipindai *QR-Code* nya	OK

4. Kesimpulan

Setelah dilakukan penelitian, dapat disimpulkan bahwa Algoritma AES sanggup mengenkripsi dan menjamin informasi yang ada di dalam KTA dengan baik karena aplikasi yang dibuat bisa berjalan sesuai dengan hasil yang diharapkan. Hal ini dapat dibuktikan dengan sama persisnya data yang tertera pada halaman pengecekan KTA dengan KTA asli. Sehingga proses pembuatan KTA dapat dilakukan dengan mudah dan cepat serta

Referensi

[1] Raharjo, Tri. “Aplikasi Pengamanan Pesan Teks Menggunakan RC6 dan AES Berbasis Android”. Diss. Universitas Mercu Buana Yogyakarta, 2018.

[2] Musabbihah, Diana. “Perencanaan Sistem Keamanan pada Jaringan Komunikasi ITS (Intelligent Transport System) Antara OBU dan TMC Server”. Diss. Institut Teknologi Sepuluh Nopember, 2018.

[3] Baihaqy, Muhammad Alif Muwafiq, Muhamad Fuat Asnawi, and Siti Fatimah. "Rancang Bangun Mobile Verifikator Hewan Layak Qurban Menggunakan Qr Code Berbasis Library Zxing." Jurnal Penelitian dan Pengabdian Kepada Masyarakat UNSIQ 7.2 pp. 194-201, 2020.

[4] Muyaroah, Siti, and Mega Fajartia. "Pengembangan Media Pembelajaran Berbasis Android dengan menggunakan Aplikasi Adobe Flash CS 6 pada Mata Pelajaran Biologi." Innovative Journal of Curriculum and Educational Technology 6.2, pp. 22-26, 2017.

[5] Permana, Angga Aditya, and Desi Nurnaningsih. "Rancangan Aplikasi Pengamanan Data Dengan Algoritma Advanced Encyption Standard (AES)." Jurnal Teknik Informatika 11.2 , pp. 177-186, 2018.

[6] Sodikin, Luthfia, and Taufik Hidayat. "Analisa Keamanan E-Commerce Menggunakan Metode AES Algoritma." Teknokom 3.2, pp. 8-13, 2020.

[7] Latif, Agustan. "Implementasi Kriptografi Menggunakan Metode Advanced Encryption Standar (AES) Untuk Pengamanan Data Teks." MUSTEK ANIM HA 4.2, pp. 163-172, 2015.

DOI: 10.54259/satesi.v1i1.5