Jurnal Infosecure Vol.5 No.1, April 2024
p-ISSN: 2087-1023
MTI-UNLA

Implementasi QR Code dan Algoritma *Advanced Encryption Standard* (AES) Pada Pengesahan Surat

Liman Megi Setiawan[1], Hadi Prasetya Utomo[2], Aisyah Nuraeni[3]

Program Studi Informatika, Fakultas Teknik, Universitas Langlangbuana[1,2,3]

[1]setiawan.liman76@gmail.com

[2]aisyahnuraeni20@gmail.com

[3]hadi@informatika.unla.ac.id

Abstrak— Proses pengesahan surat pada Fakultas Teknik yang menggunakan tanda tangan manual, walaupun pembuatan surat didukung sistem terkomputerisasi. Metode manual ini memiliki kelemahan dalam aspek keamanann dan rawan pemalsuan. Penelitian ini bertujuan untuk mengatasi permasalahan tersebut dengan mengimplementasikan teknologi QR Code dan algoritma enkripsi *Advanced Encryption Standard* (AES) 256-bit yang menjaga aspek *confidentiality*, *integrity*, dan *Availability* sesuai prinsip CIA dalam pengesahan surat. QR Code digunakan untuk menyimpan informasi terkait surat, sedangkan algoritma AES mengenkripsi ID surat dalam URL hasil pemindaian QR Code. Metode yang digunakan adalah *Enhaced Re-Enginerring*, yang mencakup tahapan analisis sistem, restrukturisasi spesifikasi kebutuhan sistem, *design to code*, dan evaluasi sistem. Metodologi ini kemudian di terapkan melalui tahapan pengembangan sistem *Extreme Programming* (XP), yang mencakup tahapan *planning, design, coding dan testing*. Hasilnya, implementasi QR Code dan AES terbukti meningkatkan keamanan dan efektif dalam pengesahan surat, mengurangi risiko pemalsuan, serta mempercepat verifikasi dokumen.

Kata kunci— QR Code, *Advanced Encryption Standard* (AES), Pengesahan Surat, *Enhaced Re-Engineering, Extreme Programming* (XP).

I. PENDAHULUAN

Perkembangan teknologi digital telah memberikan dampak besar pada efisiensi dan keamanan di berbagai bidang, termasuk dalam pengelolaan surat di institusi pendidikan. Pada Fakultas Teknik pembuatan surat kini dapat dapat di akses melalui sistem pengajuan surat, meskipun sistem telah dikembangkan, proses pengesahan surat masih menggunakan tanda tangan manual. Proses ini memiliki kelemahan dalam aspek keamanan dan rentan terhadap risiko pemalsuan.

E-surat adalah layanan berbasis internet yang dapat mengirim dan menerima pesan dalam bentuk teks maupun gambar yang terus berkembang menggantikan penggunan surat fisik (Andani, *et al*., 2023).

Menurut (Saputra, *et al*., 2023) CIA *Triad* adalah model standar yang digunakan dalam keamanan informasi untuk mengatur serta mengevaluasi sebuah organisasi atau perusahaan dalam menangani data saat disimpan, dikirim atau diproses. Setiap elemen dalam CIA Triad (*Confidentiality*, *Integrity*, dan *Availability*). *Confidentiality* ini berfungsi melindungi informasi atau data, *integrity* ini berfungsi dalam menjaga agar infommasi atau data tidak dirubah tanpa izin pihak yang berwenang, dan *availability* berfokus pada penyediaan data saat dibutuhkan. Berdasarkan studi dari Saputra, *et al*., 2023 implementasi QR Code dan algoritma AES dalam konteks CIA *Triad* termasuk dalam aspek berikut:

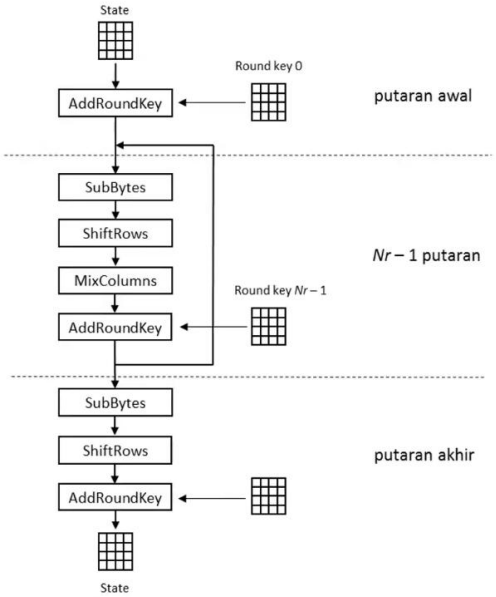
1. *Confidentiality*: algoritma AES melindungi kerahasiaan data dalam QR Code dengan mengenkripsi ID surat.
2. *Integrity*: QR Code mendukung integritas dengan memastikan bahwa informasi yang dibaca sesuai dengan yang di inputkan dan belum diubah atau dipalsukan.
3. *Availability*: QR Code mudah diakses dan dapat dipindai menggunakan perangkat standar, sehingga data tetap tersedia selama QR Code masih dapat dipindai.

Beberapa penelitian menunjukkan bahwa QR Code terbukti lebih efektif dan mengurangi risiko pemalsuan. Studi yang dilakukan oleh Kamila, *et al*. (2020) menemukan bahwa penggunaan QR Code membuat proses tanda tangan lebih efeisien, efektif, dan sulit untuk dipalsukan. Penelitian yang dilakukan oleh Adri dn Suni (2020) mengungkapkan bahwa QR Code menyimpan data secara rahasia dengan baik. Seperti ID pengguna yang digunakan untuk verifikasi kehadiran pegawai. Penelitian lainnya oleh Agustiono, *et al*. (2021) menunjukan bahwa aplikasi e-surat menghasilkan dokumen dengan QR Code yang unik, yang dapat menjaga keamanan dan validasi surat.

Menurut beberapa studi, penggunaan algoritma AES dapat mengamankan ID surat dalam URL dengan menyamarkan *plaintext* menjadi *ciphertext*. Penelitian oleh Wijaya (2020) menyimpulkan bahwa pengamanan URL dapat mengatasi serangan yang mengancam data dari metode SQL *Injcetion*. Penelitian oleh Andriyanto, *et al.*

(2020) menyimpulkan bahwa URL terenkripsi meningkatkan keamanan sistem dengan menampilkan *ciphertext,* meskipun waktu *load* sistem sedikit lebih lama. Penelitian oleh Indriati (2023) menyimpulkan bahwa dengan enkripsi menggunakan algoritma AES, informasi yang dikirmkan melalui URL dapat disamarkan, sehingga meningkatkan kerahasiaan data akademik mahasiswa.

Algoritma *Advanced Encryotion Standard* (AES) adalah algoritma kriptografi simetris yang dikembangkan oleh *National Institute of Standards and Technology* (NIST) sebagai pengganti *Data Encryption Standard* (DES), dengan panjang kunci 128, 192, dan 256-bit, yang menentukan jumlah putaran enkripsi. Operasi pada blok AES 256-bit dengan kunci 32-byte, diluar proses pembangkitan *round key*, adalah sebagai berikut, seperti yang ditunjukan pada Gambar 1*:*



Gambar. 1 Proses Algoritma AES Sumber: youtube Munir (2020).

Proses tahapan dari enkripsi AES pada Gambar. 1 di atas, berikut adalah penjelasan dari setiap tahapannya:

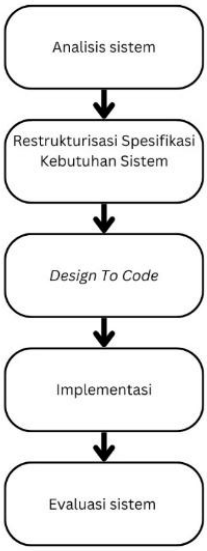
1. AddRoundKey, melakukan XOR antara *state* awal (*plaintext*) dengan *Cipher Key*, tahap ini disebut dengan *initial round*.
2. Putaran sebanyak NR-1 kali. Proses yang dilakukan pada setiap putaran:
   a. *SubBytes*: subtitusi byte dengan menggunakan tabel subtitusi (S-box).
   b. *ShiftRows:* pergeseran baris-baris *array state* secara *wrapping.*
   c. *MixColumns*: mengacak data masing-masing kolom *arraay state*.
   d. *AddRoundKey*: melalukan XOR antara *state* sekarang dengan *roundkey.*
3. Final Round: proses untuk putaran terakhir yaitu *SubBytes*, *ShiftRows*, dan *AddRoundKey* (Munir, 2020).

Untuk mengatasi permasalahan tersebut, penelitian ini menerapkan QR Code dan algoritma *Advanced Encryption Standard* (AES) 256-bit. Enkripsi AES memungkinkan ID surat dienkripsi dalam URL yang disematkan ke dalam QR Code, sehingga keamanan dan keaslian data dapat lebih terjaga. Penelitian ini bertujuan untuk merancang sistem pengesahan surat berbasis QR Code yang aman, dan efektif bagi Fakultas Teknik dengan menggabungkan fitur enkripsi untuk melindungi ID surat yang disematkan ke dalam URL hasil pemindaian QR Code. Adapun metode penelitian yang digunakan adalah *Enhanced Re-Engineering*, yang meliputi analisis sistem, restrukturisasi spesifikasi kebutuhan sistem, *design to code*, implementasi, dan evaluasi sistem.

Sedangkan untuk pengembangan sistem pengesahan surat berbasis QR Code dengan enkripsi AES 256-bit. Tahapan pengembangan *Extreme Programming* (XP) diterapkan sebagai pendekatan utama. XP menekankan pengkodean sebagai aktivitas utama di setiap tahap pengembangan, dengan keunggulan menghasilkan *output* secara cepat dan memungkinkan pengulangan pada bagian tertentu sesuai dengan tujuan pengembangan (Ahmad, *et al*., 2020). Pada Tahap pengujian, metode *black box testing* digunakan untuk menguji fungsionalitas sistem tanpa mengakses desain atau kode program. Metode ini memvalidasi kesesuaian *input* dan *output* sesuai spesifikasi serta mendeteksi kelemahan, sehingga memastikan data yang dihasilkan akurat dan mencegah kesalahan pada aplikasi sebelum digunakan (Febriyanti, *et al*., 2021).

II. METODE

Re-Engineering adalah proses perbaikan perangkat lunak yang memanfatkan teknik dari *forward* dan *reverse engineering* dengan melalui beberapa langkah, termasuk analisis kelayakan dan kebutuhan, restrukturisasi spesifikasi kebutuhan sistem, *design to code*, implementasi dan evaluasi sistem (Naufal, 2022). Metode penelitian yang digunakan dalam penelitian ini yaitu adaptasi dari penelitian (Naufal, 2022) adaptasi pada penelitian ini meliputi analisis sistem, restrukturisasi spesifikasi kebutuhan sistem, *design to code*, implementasi, dan evaluasi sistem. Adaptasi dari penelitian ini menjadi tahapan yang lebih sesuai denga penelitian yang sedang di kembangkan. Adaptasi ini mengubah tahapan studi kelayakan dan kebutuhan menjadi analisa sistem yang berfokus pada pada aspek teknik dan spesifikasi sistem yang ada. Selain itu, evaluasi performa sistem diubah menjadi evaluasi sistem yang memungkinkan evaluasi lebih luas, tidak terbatas pada performa sistem.

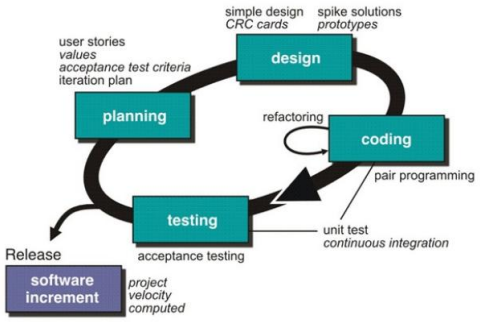


Gambar. 2 Metode *Enhanced Re-Engineering*

Brdasarkan Gambar. 2 tahapan dari metode *Enhaced Re-Engineering* di atas, berikut adalah penjelasan dari setiap tahapnya:

1. Analisis Sistem: analisa sistem pengesahan surat manual untuk mengidentifikasi kelemahan dalam efisiensi dan keamanan.
2. Restrukturisasi Spesifikasi Kebutuhan Sistem: Menyusun ulang kebutuhan sistem berdasarkan analisis, termasuk penambahan fitur QR Code dan enkripsi AES 256-bit.
3. *Design to Code*: Merancang arsitektur sistem baru yang mampu menghasilkan QR Code terenkripsi untuk tiap surat yang disahkan.
4. Implementasi: Menerapkan fitur QR Code dan enkripsi AES pada sistem pengesahan surat.
5. Evaluasi Sistem: Pengujian menggunakan metode *black box testing* untuk menilai keakuratan dan keamanan sistem yang telah diperbarui.

Metode Pengembangan sistem dalam penelitian ini menggunakan pengembangan sistem *Extreme Programming*. Metode ini digunakan karena melibatkan klien secara langsung dalam pengembangan dan pembangunan *interface*. Adapun tahapan *extreme programming* tersebut adalah *planning*, *design*, coding, dan *testing*.



Gambar. 3 Tahapan *Extreme Programming* sumber: Ahmad, et al., (2020)

Berdasarkan Gambar. 3 tahapan pengembangan *Extreme Programming* di atas, berikut adalah penjelasan dari setiap tahapnya:

1. *Planning* (Perencanaan): tahap pertama melalakukan identifikasi alur proses, fitur dan fungsi perangkat lunak yang akan dikembangkan serta merencanakan keseluruhan fungsionalitas.
2. *Design* (Perancangan): merancang sistem menggunakan UML, terutama *use case* diagram untuk memvisualisasikan interaksi aktor dan perangkat lunak.
3. Coding (Pengkodean): mengimplementasikan desain menjadi kode yang dapat dikenali oleh komputer.
4. *Testing* (Pengujian): menguji perangkat lunak dengan metode *black box* untuk memastikan fungsi berjalan dengan baik dan mendeteksi kesalahan.

III. HASIL DAN PEMBAHASAN

Pada implementasi sistem pengesahan surat menggunakan QR Code dan algoritma AES 256-bit, beberapa tahapan dan pengujian telah dilakukan untuk memastikan keamanan dan efisiensi sistem. Berikut ini adalah hasil utama dari implementasi tersebut:

A. Identifikasi Masalah

Sistem informasi pengajuan surat pada Fakultas Teknik masih mengandalkan metode manual. Dalam upaya untuk meningkatkan efektivitas dan keamanan, sistem baru yang memanfaatkan teknologi QR Code dan enkripsi id surat telah dirancang. Berikut adalah identifikasi masalah yang ditemukan dalam proses pengesahan surat yang dijelaskan pada Tabel I.

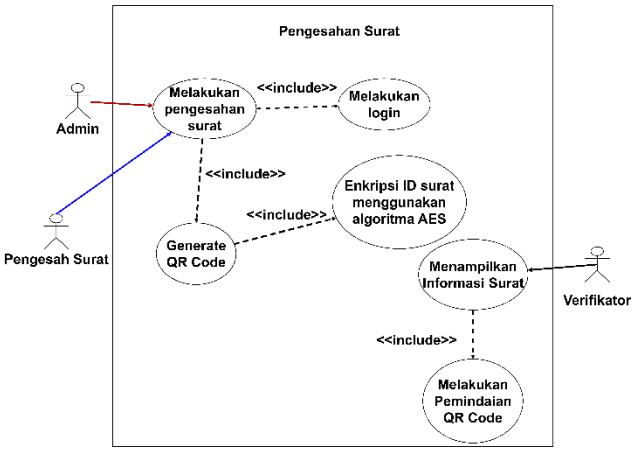
TABEL I
Tabel I Identifikasi Masalah

No	Identifikasi Masalah	Dekripsi Masalah	Dampak
1.	Tanda Tangan Manual	Tanda tangan di simpan dalam bentuk image di dalam publik sistem.	Tanda tangan bisa diunduh, dipalsukan oleh pihak tidak bertanggung jawab.

2.	Peoses validasi yang lemah	Tanda tangan tidak memiliki proses validasi yang kuat.	Sulit memastikan apakah tanda tangan berasal dari pihak berwenang.
3.	Keamanan data	Tidak ada keamanan terhadap tanda tangan manual.	Surat yang disahkan dapat dengan mudah dipalsukan, diubah atau di duplikasi oleh pihak tidak bertanggung jawab.
4.	Proses verifikasi surat	Tanda tangan tidak memiliki metadata yang memudahkan pelacakan atau verifikasi.	Proses verifikasi surat menjadi rumit dan memerlukan pemeriksaan manual.

B. *Use Case* Diagram

Use Case Diagram merupakan pemodelan untuk kelakuan (*behavior*) sistem informasi yang akan dibuat. *Use Case* diagram mendefinisikan sebuah interaksi antara satu atau lebih aktor dengan sistem infrormasi yang dibuat.



Gambar. 4 *Use Case* Diagram

Berdasarkan Gambar. 4, berikut ini adalah uraian dari setiap *use case* yang digunakan:

1. Melakukan login: aktor melakukan login terlebih dahulu sebelum melakukan pengesahan surat.
2. Melakukan pengesahan surat: aktor melakukan pengesahan surat melalui sistem.
3. Enkripsi ID surat: sistem akan mengambil ID surat dan mengenkripsi menggunakan algoritma AES 256-bit.
4. *Generate* QR Code: sistem akan menghasilkan QR Code berdasarkan ID surat yang telah terekripsi.
5. Memindai QR Code: verifikator dapat memindai QR code tersebut untuk memastikan keaslian dari surat.
6. Menampilkan informasi surat: sistem akan menampilkan informasi surat sesuai dengan data yang di ambil di dalam sistem.

C. Enkripsi *Advanced Encryption Standard* (AES)

Proses enkripsi ID surat pada sistem informasi pengajuan surat mahasiswa menggunakan algoritma AES 256-bit. Tahapan enkripsi meliputi *AddRoundkey*, *SubBytes*, *ShiftRows*, dan *MixColumns*. Proses dari enkripsi adalah sebagai berikut:

PlainText: 123

KeyText: Xka7z9UeF6rL2mQvP1q2W3E4R5T6Y7U2

Dari hasil *plaintext* dan *keytext* tersebut, langkah awal dari proses enkripsi adalah memasukan ke dalam matrix 4x4 sebagai berikut:

Plaintext				
	1	2	3	x
	x	x	x	x
	x	x	x	x
	x	x	x	x

Key				
	x	k	A	7
	z	9	U	e
	F	6	R	L
	2	m	Q	v

	P	1	Q	2
	W	3	E	4
	R	5	T	6
	Y	7	U	2

Pdes				
	49	50	51	120
	120	120	120	120
	120	120	120	120
	120	120	120	120

Kdes				
	120	107	65	55
	122	57	85	101
	70	54	82	76
	50	109	81	118

	80	49	81	50
	87	51	69	52
	82	53	84	54
	89	55	85	50

Gambar. 5 Proses Konversi Ke Dalam Bilangan Desimal

Berdasarkan pada Gambar. 5 di atas, berikut adalah penjelasan dari setiap tahapannya:

1. langkah awal dari proses enkripsi adalah memasukan blok data ke dalam matriks 4x4.
2. Jika plaintext kurang dari 32 byte, *padding* akan ditambahkan menggunakan metode *addpadding* agar memenuhi *standard* dari AES 256-bit.
3. Setelah *plaintext* memenuhi *standard* AES 256-bit, *plaintext* dikonversi ke dalam bilangan desimal.
4. Pada bagian *cipherkey*, blok data dibagi menjadi dua matriks, karena standard AES menggunakan ukuran 128-bit, meskipun *key* yang digunakan berbeda.
5. Setelah dibagi menjadi dua matriks, *cipherkey* kemudian dikonversikan ke dalam bilangan desimal.

Pada proses pembentukan *key schedule* dalam algoritma aes, *key* awal sepanjang 256-bit di olah memalui serangkaian tranformasi untuk menghasilkan *subkey* yang akan digunakan pada setiap putaran yang terdiri dari 14 putaran.

	Key Pertama			
k0	78	6B	41	37
	7A	39	55	65
	46	36	52	4C
	32	6D	51	76

	Key Kedua			
	50	31	51	32
	57	33	45	34
	52	35	54	36
	59	37	55	32

	Kolom 4	ROT WORD	SUB BYTE	XOR SUB BYTE	RCON 1
k1	32	34	18	48	01
	34	36	5	52	00
	36	32	23	71	00
	32	32	23	7A	00

	49	78	29	1B
	52	61	24	10
	71	44	10	26
	7A	4D	18	2A

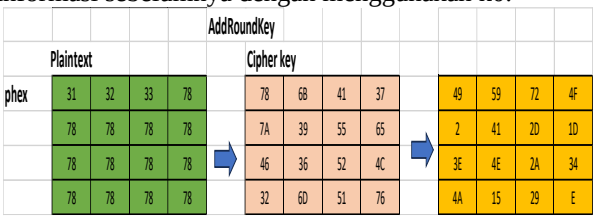
Gambar. 6 Proses *Key Schedule*

Berdasarkan pada Gambar. 6 di atas, berikut adalah penjelasan dari setiap tahapannya:

1. Langkah awal dari proses *key schedule*, menggunakan k0 untuk melakukan *AddRoundKey* antara *state* awal, yang di-XOR-kan dengan k0.

2. *Key* kedua akan digunakan untuk membentuk *key schedule* selama 14 putaran.
3. Proses pertama pada kolom ke empat akan akan digeser satu baris ke atas, menghasilkan blok data *Rot Word*.
4. Blok data *Rot Word* kemudian menjalani proses subtitusi menggunakan table S-*Box*.
5. Hasil subtitusi kemudian di-XOR-kan dengan nilai pada baris pertama dan kolom pertama dari *key* kedua.
6. Hasil dari proses XOR *SubByte* tersebut kemudian di-XOR-kan kembali dengan nilai *rcon*, sehingga menghasilkan nilai pada k1 di baris pertama, kolom pertama.

Proses pertama dari algoritma aes adalah *Addroundkey* merupakan proses penambahan (XOR) antara blok data *plaintext* yang dirubah menjadi *hexadecimal* dengan hasil tranformasi sebelumnya dengan menggunakan k0.

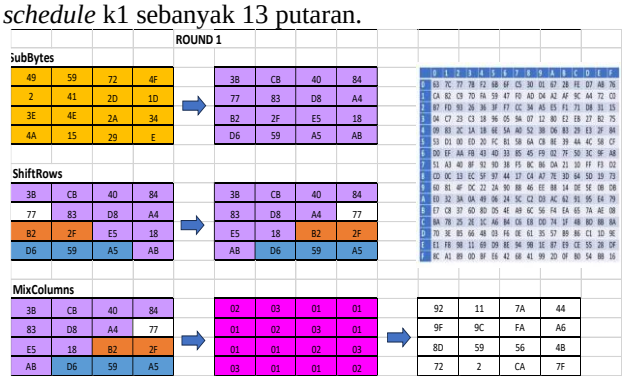


Gambar. 7 Proses *AddRoundKey*

Berdasarkan pada Gambar. 7 di atas, berikut adalah penjelasan dari setiap tahapannya:

1. Langkah awal dari proses enkripsi adalah mengubah nilai *plaintext* ke dalam format hexadesimal, kemudian melakukan *AddRoundKey*, di mana state awal akan di-XOR-kan dengan *cipherkey* pertama.
2. Hasil dari XOR Pada baris pertama dan kolom pertama adalah hasil XOR antara nilai pada *plaintext* di baris pertama, kolom pertama dengan nilai pada cipherkey di baris pertama dan kolom pertama.

Pada putaran pertama algoritma aes, data blok *plaintext* pertama kali mengalami operasi *SubBytes*, *ShifRows*, *Mixcolumns* dan *AddRoundKey* dengan menggunakan *key schedule* k1 sebanyak 13 putaran.

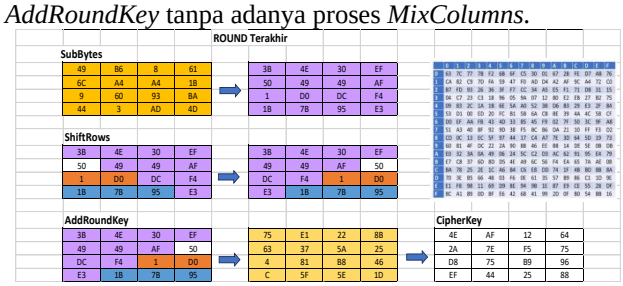


Gambar. 8 Proses *SubBytes*, *ShiftRows*, *MixColumns*, Dan *AddRoundKey*.

Berdasarkan pada Gambar. 8 di atas, berikut adalah penjelasan dari setiap tahapannya:

1. Langkah selanjutnya dari proses enkripsi adalah *SubBytes*, pada putaran pertama data blok *plaintext* mengalami operasi *SubBytes*, di mana setiap byte dari state akan digantikan dengan nilai yang sesuai dari tabel S-*Box*.
2. Setelah operasi *SubBytes*, langkah berikutnya adalah *ShiftRows*. Dalam operasi ini, setiap baris pada state akan digeser ke kiri sesuai dengan indeks barisnya. Baris pertama tidak mengalami pergeseran, baris kedua digeser satu kolom, baris ketiga digeser dua kolom, dan baris keempat digeser tiga kolom.
3. Setelah *ShiftRows*, proses dilanjutkan dengan *MixColumns*. Di sini, setiap kolom dari state akan diperlakukan sebagai *polinomial* derajat tiga dan dikalikan dengan *polinomial* tetap untuk menghasilkan kolom baru.
4. Setelah *MixColumns*, operasi terakhir pada putaran pertama adalah *AddRoundKey*, di mana state yang telah dimodifikasi akan di-XOR-kan dengan *key* dari *key schedule*, yaitu k1.
5. Dalam putaran pertama ini, *key schedule* k1 diterapkan sebanyak 13 kali, memastikan bahwa setiap putaran memiliki kunci yang berbeda untuk meningkatkan kerumitan enkripsi.

Pada putaran terakhir algoritma AES, blok data mengalami transformasi *SubBytes*, *ShiftRows*, dan *AddRoundKey* tanpa adanya proses *MixColumns*.



Gambar. 9 Proses *SubBytes*, *ShiftRows*, Dan *AddRoudKey*.

Berdasarkan pada Gambar. 9 di atas, berikut adalah penjelasan dari setiap tahapannya:

1. Langkah terakhir dari proses enkripsi adalah *SubBytes*, pada putaran pertama data blok *plaintext* mengalami operasi *SubBytes*, di mana setiap byte dari *state* akan digantikan dengan nilai yang sesuai dari tabel S-*Box*.
2. Setelah operasi *SubBytes*, langkah berikutnya adalah *ShiftRows*. Dalam operasi ini, setiap baris pada state akan digeser ke kiri sesuai dengan indeks barisnya. Baris pertama tidak mengalami pergeseran, baris kedua digeser satu kolom, baris ketiga digeser dua kolom, dan baris keempat digeser tiga kolom.
3. Setelah *ShiftRows*, operasi terakhir pada putaran pertama adalah *AddRoundKey*, di mana *state* yang

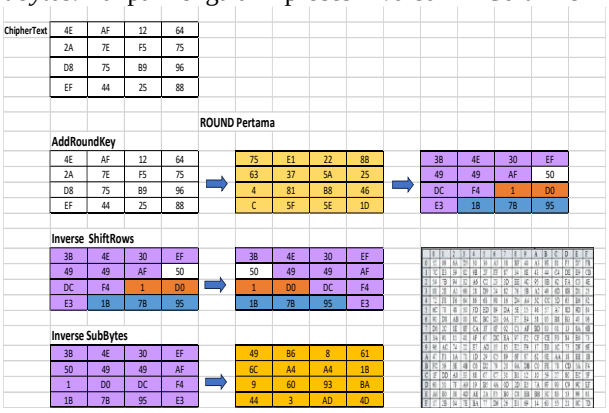
telah dimodifikasi akan di-XOR-kan dengan *key* dari *key schedule*, yaitu k14. Sehingga menghasilkan *ciphertext*.

4. Dalam putaran terakhir ini, proses *MixColumns* tidak diterapkan.

D. Dekripsi *Advanced Encryption Standard* (AES)

Proses dekripsi menggunakan algoritma AES yang merupakan kebalikan dari proses enkripsi. Dekripsi dilakukan untuk mengembalikan *ciphertext* menjadi *plaintext* dengan menggunakan *key* yang sama selama proses enkripsi. Proses dekripsi adalah sebagai berikut:

Pada putaran pertama dekripsi algoritma AES, proses dimulai dengan *AddRoundKey*, *ciphertext* akan di-XOR dengan *key round* terakhir, *Inverse shiftRows*, *Inverse Subytes*. Tanpa mengalami proses *Inverse MixColumns*

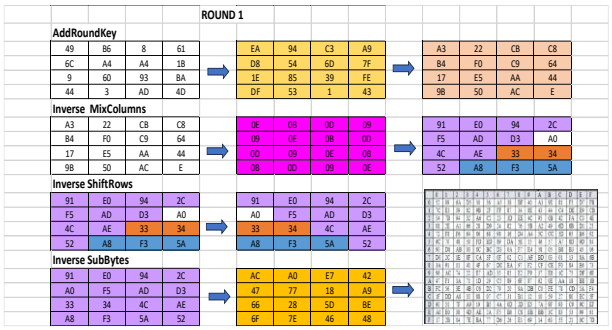


Gambar. 10 Proses *AddRoundKey*, *Inverse ShiftRows*, Dan *Invers SubBytes*.

Berdasarkan pada Gambar. 10 di atas, berikut adalah penjelasan dari setiap tahapannya:

1. Langkah pertama dari proses dekripsi adalah *AddRoundKey*, pada putaran pertama di mana *cipherkey* akan di-XOR-kan dengan *key* dari *key schedule*, yaitu k14.
2. Setelah operasi *AddRoundKey*, langkah berikutnya adalah *Inverse ShiftRows*. Dalam operasi ini, setiap baris pada *state* akan digeser ke kanan sesuai dengan indeks barisnya. Baris pertama tidak mengalami pergeseran, baris kedua digeser satu kolom ke kanan, baris ketiga digeser dua kolom ke kanan, dan baris keempat digeser tiga kolom ke kanan.
3. Setelah *Inverse ShiftRows*, operasi terakhir pada putaran pertama adalah *Inverse SubByte*, di mana setiap byte dari *state* akan digantikan dengan nilai yang sesuai dari tabel S-*Box* invers.
4. Dalam putaran pertama ini, proses *Inverse MixColumns* tidak diterapkan.

Pada proses pertama, *ciphertext* pertama kali di oprasikan dengan *AddRoundKey*, *Inverse MixColumns*, *Inverse ShiftRows*, dan *Inverse SubBytes* sebanyak 13 putaran.

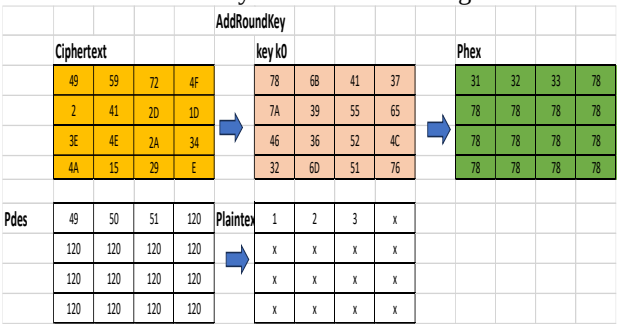


Gambar. 11 Proses AddRoundKey, Inverse MixColums, Inverse ShiftRows, Dan Inverse SubBytes.

Berdasarkan pada Gambar. 11 di atas, berikut adalah penjelasan dari setiap tahapannya:

1. Langkah selanjutnya dari proses dekrip adalah *AddRoudKey*, pada putaran pertama di mana ciphertext akan di-XOR-kan dengan *key* dari *key schedule*, yaitu k13.
2. Setelah operasi *AddRoundKey*, langkah berikutnya adalah *Inverse MixColumns*. Dalam operasi ini, setiap kolom dari *state* akan diperlakukan sebagai *polinomial* derajat tiga dan dikalikan dengan polinomial tetap untuk menghasilkan kolom baru.
3. Setelah *Inverse MixColumns*, proses dilanjutkan dengan *Inverse ShiftRows*. Dalam operasi ini, setiap baris pada state akan digeser ke kanan sesuai dengan indeks barisnya. Baris pertama tidak mengalami pergeseran, baris kedua digeser satu kolom ke kanan, baris ketiga digeser dua kolom ke kanan, dan baris keempat digeser tiga kolom ke kanan.
4. Setelah *Inverse ShiftRows*, operasi terakhir pada putaran pertama adalah *Inverse SubBytes*, di mana setiap byte dari state akan digantikan dengan nilai yang sesuai dari tabel S-*Box invers*.
5. Dalam putaran pertama ini, *key schedule* k14 sampai k1 diterapkan sebanyak 13 kali, memastikan bahwa setiap putaran memiliki kunci yang berbeda untuk meningkatkan kerumitan enkripsi.

Pada putaran terakhir algoritma AES, blok data dari hasil transformasi sebelumnya akan di-XOR dengan k0.



Gambar. 12 Proses AddRoundKey.

Berdasarkan pada Gambar. 12 di atas, berikut adalah penjelasan dari setiap tahapannya:

1. langkah terakhir dari proses dekripsi adalah *AddRoundKey*, pada putaran terakhir di mana *ciphertext* akan di-XOR-kan dengan *key* dari *key schedule*, yaitu k0
2. Setelah operasi *AddRoundKey*, *state* yang dihasilkan dapat dikonversikan dari format byte ke dalam bilangan desimal.
3. Setelah mendapatkan hasil dari *AddRoundKey*, state tersebut kemudian akan dikembalikan ke format teks asli atau *plaintext*.

E. Implementasi *User Interface*

YAYASAN PENDIDIKAN TRI BHAKTI LANGLANGBUANA
UNIVERSITAS LANGLANGBUANA
TERAKREDITASI "B"
FAKULTAS T E K N I K
Jalan Karapitan No. 116 Telp. 022 – 4218086 Fax. 022 – 4237144 Bandung 40261

Nomor : 1902/AB/11B/26
Lampiran :
Hal : Permohonan Izin Survey Lokasi

Yth, **universitas langlangbuana**
jalan karapitan
KOTA BANDUNG

Dengan hormat,
Bersama ini kami hadapkan Mahasiswa Prodi Teknik Informatika Fakultas Teknik Universitas Langlangbuana Bandung :

N a m a : Daffa Fitrah Akbar
N p m : 41155050200002

Bermaksud mengajukan permohonan **Izin Survey Lokasi** di Instansi/Perusahaan yang Bapak/Ibu pimpin.

Sehubungan dengan hal tersebut di atas, maka dengan ini kami mohon Bapak/Ibu berkenan memberikan izin kepada Mahasiswa kami untuk dapat melaksanakannya.

Atas bantuan dan kerjasamanya kami ucapkan terimakasih.

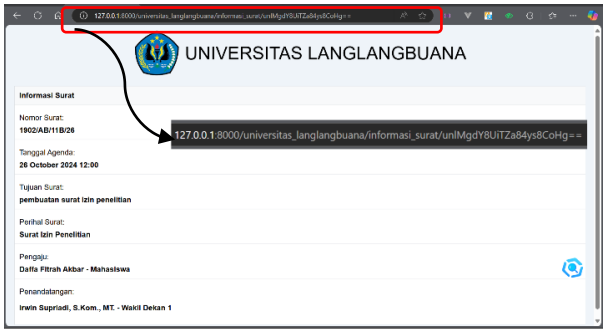
Bandung, 26 Oktober 2024
An. Dekan
Wakil Dekan 1,

Irwin Supriadi, S.Kom., MT.
NIDN. 0414048305

Tembusan :
1. Arsip.

Gambar. 13 *User Interface Generate* QR Code

Implementasi *user interface* untuk penambahan QR Code, telah berhasil dikembangkan seperti yang ditunjukan pada Gambar. 13. Dimana fungsi dari QR Code adalah sebagai pengganti tanda tangan manual menjadi berbasis digital.



Gambar. 14 *User Interface* Enkripsi ID Surat

Implementasi *user interface* untuk enkripsi ID surat, telah berhasil dikembangkan seperti yang di tunjukan pada Gambar. 14. Dimana fungsi pada enkripsi ID surat adalah untuk meningkatkan keamanan ID surat pada URL hasil pemindaian. Hasil dari pemindaian QR code akan menampilkan informasi surat, seperti: Nomor Surat, Tanggal Agenda, Tujuan Surat, Perihal Surat, Pengaju, dan Penandatangan.

F. Pengujian Sitem

Pengujian dilakukan pada proses pengesahan surat untuk memastikan fungsionalitas pada pengesahan berfungsi dengan baik dan sesuai dengan desain yang dibuat. Berikut ini penjelasan mengenai pengujian yang tercantum pada Table II:

TABEL II
Tabel II Rencana Pengujian

No	Aspek Pengujian	Kebutuhan Fungsional	Skenario Pengujian	Kesimpulan
1.	Metode pengesahan surat	Pengesahan surat berbasis QR Code.	-Aktor mengesahkan surat. - Sistem membuat QR Code pada surat	Hasil pengujian menunjukan sistem berhasil menghasilkan QR Code sebagai pengganti tanda tangan manual, yang rentan dipalsukan jika di unduh oleh pihak tidak bertanggung jawab.
3.	Keamanan pada ID surat	Enkripsi ID surat	-sistem mengenkripsi ID surat pada proses pengesahan surat -ID surat terenkripsi dalam URL hasil pemindain QR Code.	Hasil pengujian meujukan sistem berhasil mengenkripsi ID surat dalam url untuk meningkatkan keamanan.
2.	Proses Validasi QR Code	Validasi QR Code	-Aktor memindai QR Code.	Hasil pengujian meunjukan

			-Sistem membaca dan mendekripsi ID surat. -Sistem menampilkan informasi surat. -terdapat pesan kesalahan jika QR Code tidak valid	sistem berhasil mendekripsi ID surat untuk menampilkan informasi surat saat QR Code dipindai, dan memebrikan pesan kesalahan jika QR Code tidak Valid.
4.	Proses Verifikasi ID surat	Verifikasi ID surat	-Aktor memindai QR Code. -Sistem mendekripsi dan memverifikasi ID surat untuk memastikan informasi yang ditampilkan sesuai dengan data surat pada sistem.	Hasil pengujian meunjukan sistem berhasil menampilkan informasi surat sesuai data pada sistem.

IV. SIMPULAN

Penelitian ini berhasil mengimplementasikan teknologi QR Code dan algoritma *Advanced Encryption Standard* (AES) 256-bit dalam sistem pengesahan surat di Fakultas Teknik. Hasil penelitian menunjukkan bahwa sistem baru ini mampu meningkatkan keamanan dan efektif dalam proses pengesahan surat, mengurangi risiko pemalsuan, dan mempercepat verifikasi dokumen. Penggunaan QR Code untuk menyimpan informasi surat dan enkripsi AES 256-bit untuk mengamankan ID surat pada URL hasil pemindaian terbukti efektif dalam menjaga keaslian dan kerahasiaan data. Dengan demikian, penerapan sistem ini diharapkan dapat menjadi solusi yang andal dan aman untuk proses pengesahan surat.

REFERENSI

[1] Abdurrachman, T., & Suteja, B. R. (2021). Pengembangan Sistem Informasi Asosiasi Jasa Konstruksi dengan Menerapkan Tanda Tangan Digital. Jurnal Teknik Informatika dan Sistem Informasi, 7(1).

[2] Ahmad, I., Borman, R. I., Fakhrurozi, J., & Caksana, G. G. (2020). Software development dengan Extreme Programming (XP) pada aplikasi deteksi kemiripan judul skripsi berbasis Android. Jurnal Inovtek Polbeng Seri Informatika, 5(2), 297-307.

[3] Andini, M., Rozi, F., & Syam, A. M. (2022). PERSEPSI MAHASISWA ILMU KOMUNIKASI STAMBUK 2018 UINSU TENTANG APLIKASI SI-SELMA (SISTEM INFORMASI SURAT EEKTRONIK MAHASISWA). JISOS: JURNAL ILMU SOSIAL, 1(11), 1041-1050.

[4] Andani, S., Christian, A., & Muchlis, M. (2023). Rancang Bangun Sistem E-Surat Pada Desa Jungai Kecamatan Rambang Kapak Tengah. JURNAL PENELITIAN SISTEM INFORMASI (JPSI), 1(4), 92-104.

[5] Ariska, A., & Wahyuddin, W. (2022). Penerapan Kriptografi Menggunakan Algoritma Des (Data Encryption Standard). Jurnal Sintaks Logika, 2(2), 9-19.

[6] Arifin, R., & Latif, N. (2020). Sistem Informasi Pengelolaan Surat Menyurat Berbasis Web Pada Kantor Balai Latihan Masyarakat Makassar. Inspiration: Jurnal Teknologi Informasi dan Komunikasi, 10(1), 68-76.

[7] Bik, Z. A., Murti, A. C., & Latubessy, A. (2023). APLIKASI STUDIO MUSIK BERBASIS QR CODE DI OMT MUSIK STUDIO. Jurnal Dialektika Informatika (Detika), 4(1), 26-32.

[8] CODE, U. Q. (2021). Desain layanan e-surat untuk desa waru barat, pamekasan, madura menggunakan qr code. Jurnal teknologi informasi dan ilmu komputer (JTIIK), 8(6).

[9] Effendy, E., Siregar, E. A., Fitri, P. C., & Damanik, I. A. S. (2023). Mengenal Sistem Informasi Manajemen Dakwah (Pengertian Sistem, Karakteristik Sistem). Jurnal Pendidikan dan Konseling (JPDK), 5(2), 4343-4349.

[10] Febriyanti, N. M. D., Sudana, A. K. O., & Piarsa, I. N. (2021). Implementasi Black Box Testing pada Sistem Informasi Manajemen Dosen. Jurnal Ilmiah Teknologi Dan Komputer, 2(3), 535-544.

[11] Kinaswara, T. A. (2019, October). Rancang Bangun Aplikasi Inventaris Berbasis Website pada Kelurahan Bantengan. In Prosiding Seminar Nasional Teknologi Informasi dan Komunikasi (SENATIK) (Vol. 2, No. 1, pp. 71-75).

[12] Manullang, A. H., Aritonang, M., & Purba, M. J. (2021). Sistem Informasi Bimbingan Belajar Number One Medan Berbasis Web. TAMIKA: Jurnal Tugas Akhir Manajemen Informatika & Komputerisasi Akuntansi, 1(1), 44-49.

[13] Mayana, R. F., & Santika, T. (2021). Legalitas tanda tangan elektronik: posibilitas dan tantangan notary digitalization di Indonesia. ACTA DIURNAL Jurnal Ilmu Hukum Kenotariatan, 4(2), 244-262.

[14] Nurhareza, I. K., & Siswanto, S. (2022, September). Penerapan Algoritme Kriptografi AES 256 Untuk Mengamankan Dokumen Berbasis Web Pada Kelurahan Belendung. In Prosiding Seminar Nasional Mahasiswa Fakultas Teknologi Informasi (SENAFTI) (Vol. 1, No. 1, pp. 302-309).

[15] Novianti, H. D., & Hidayat, A. T. (2023). Implementasi Kriptografi Advanced Encryption Standard 128 Bit dalam Pengamanan Data Keuangan Kas:(Studi Kasus: Masjid Al-ikhlas Trini Sleman Di Yogyakarta). Jurnal Komputer dan Teknologi, 27-34.

[16] Oper, N., Balafif, S., & To'o Fathonah Al-Khaliq, Z. (2022). MODIFIKASI ALGORITMA KRIPTOGAFI CAESAR CIPHER MENJADI ALGORITMA KRIPTOGRAFI ASIMETRIS DENGAN METODE AGILE. Jurnal Informatika Teknologi dan Sains (Jinteks), 4(3), 179-184.

[17] Rinaldi Munir, "Kripto 20: Advanced Encryption Standard (AES)", https://youtu.be/4q3bA0W7UHg?si=e7QcP6L4lrqU_VRv.

[18] Saputra, A. D., Dione, F., & Uluputty, I. (2023). Pengelolaan Keamanan Informasi dan Persandian di Dinas Komunikasi dan Informatika Provinsi Kalimantan Timur. Jurnal Teknologi dan Komunikasi Pemerintahan, 5(2), 159-187.

[19] SINTA, Y. S. (2021). Pengembangan Modul Pemelajaran Pjok Berbasis Qr-Code (Barcode Scanner) Pada Tema Gerak Dasar Untuk Peserta Didik Kelas I SD/MI.

[20] Trizaka, H., Rusdianto, D. S., & Brata, A. H. (2019). Pengembangan sistem aplikasi persuratan elektronik berbasis web di fakultas ilmu komputer (FILKOM) Universitas Brawijaya. Jurnal Pengembangan Teknologi Informasi dan Ilmu Komputer, 3(5), 5115-5121.

[21] Umami, I., Adam, M. T., & Winarti, W. (2022). Perancangan sistem informasi pengelolaan surat menyurat berbasis web Desa Sumberkarang. ULIL ALBAB: Jurnal Ilmiah Multidisiplin, 1(9), 2880-2885.