IMPLEMENTASI ALGORITMA ADVANCED ENCRYPTION STANDARD (AES) UNTUK KEAMANAN QR-CODE SEBAGAI DIGITAL SIGNATURE PADA APLIKASI E-SURAT

Dhika Maulana Okto Wibowo, Erna Dwi Astuti, Hidayatus Sibyan
Teknik Informatika, Fakultas Teknik dan Ilmu Komputer
Email : dhikamaulana@unsiq.ac.id

ABSTRAK

Proses Surat Menyurat pada Fakultas Ekonomi (FE) UNSIQ masih diketik melalui *Ms. Word*. Banyaknya tahapan yang dilakukan dalam membuat surat menjadikan waktu yang dibutuhkan cukup banyak selain itu keamanan surat juga tidak dapat dijamin. Hal ini akan mengurangi kinerja dan efisiensi pada proses administrasi di Fakultas Ekonomi UNSIQ. Oleh karena itu dibuatlah aplikasi Sistem e-Surat (SERAT) FE UNSIQ yang di dalamnya sudah diimplementasikan Algoritma AES untuk mempercepat kinerja pembuatan surat dan menjamin keasliannya. Implementasi Algoritma AES dimasukkan ke dalam URL pengecekan surat yang dikonversi menjadi *QR-Code* agar mudah dipindai. Penelitian ini diharapkan dapat membantu proses pembuatan surat di Fakultas Ekonomi UNSIQ dan menjamin keaslian surat yang dibuat.

Kata Kunci : surat, keamanan, keaslian, algoritma aes, qr-code.

ABSTRACT

The mailing process at Faculty of Economics (FE) UNSIQ is still typed through Ms. Words. A lot of steps in the making a letter makes the time needed to be quite a lot, besides that the security of the letter cannot be guaranteed. This will reduce the performance and efficiency of the administrative process at the Faculty of Economics, UNSIQ. Therefore, the "Sistem e-Surat (SERAT) FE UNSIQ" application was made in which the AES Algorithm has been implemented to speed up the performance of making letters and guarantee their authenticity. The implementation of the AES Algorithm is included in the mail checking URL which is converted into a QR-Code for easy scanning. This research is expected to help the mailing process at the Faculty of Economics UNSIQ and guarantee the authenticity of the letters made.

Keywords ***:*** *mailing, security, authenticity, aes algorihtm, qr-code.*

1. PENDAHULUAN

Proses surat menyurat pada Fakultas Ekonomi Universitas Sains Al-Qur'an (UNSIQ) masih belum efektif. Proses pengarsipan dan pembuatan surat masih dilakukan secara manual dengan berbagai tahapan yang tidak sedikit. Hal ini akan memperlambat proses. Selain itu juga tidak antisipasi dalam keadaan darurat, seperti saat surat yang harus diedarkan secepat mungkin namun tidak ada pimpinan yang hadir untuk menandatangani surat tersebut. Dalam hal ini biasanya akan menggunakan tandatangan scan untuk mempersingkat pendistribusian surat. Namun, hal ini membuat semua orang bisa membuat surat tanpa adanya persetujuan dari pimpinan asalkan mempunyai file scan tandatangan pimpinan tersebut yang mana akan membuat surat rawan pemalsuan.

Berdasarkan hal di atas maka dibutuhkan suatu sistem keamanan di dalam surat yang telah tercetak dengan membuat sebuah aplikasi "Sistem e-Surat Fakultas Ekonomi UNSIQ (SERAT FE-UNSIQ) yang dapat digunakan untuk mengarsip dan membuat surat, serta dapat memberikan *Digital Signature* atau tandatangan digital berupa *QR-Code* yang dienkripsi menggunakan Algoritma *Advanced Encryption Standard* (AES). Dengan adanya aplikasi, diharapkan dapat meningkatkan efektifitas dalam pengarsipan surat. Sehingga pelayanan pun akan meningkat, dan menjadikan Fakultas Ekonomi UNSIQ menjadi lebih maju.

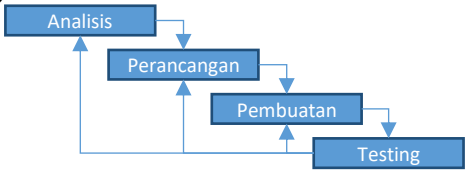
2. METODE

2.1. Metode Pengumpulan Data

Untuk mempermudah proses penelitian, penulis menggunakan beberapa metode pengumpulan data, antara lain Observasi, Studi Literatur dan Wawancara.

2.2. Metode Pengembangan Sistem

Metode yang digunakan untuk membuat aplikasi tersebut adalah menggunakan metode waterfall. Penjelasan metode waterfall dapat dilihat pada gambar di bawah ini (El Rahma, 2021):



Gambar 1. Metode Pembuatan Sistem e-Surat FE UNSIQ

2.3. Penerapan Algoritma AES

Pada Aplikasi Sistem e-Surat Fakultas Ekonomi UNSIQ (SERAT FE-UNSIQ), Algoritma AES merupakan hasil enkripsi Kode Surat dalam Data Base yang digabungkan dengan URL halaman pengecekan surat kemudian dikonversi menjadi QR-Code lalu disisipkan ke dalam surat sebagai sistem keamanannya.

3. HASIL DAN PEMBAHASAN

3.1. Proses enkripsi Algoritma AES

Teks yang akan dienkripsi dalam pembahasan ini adalah "001@srt_keluar". Sedangkan kunci atau *key* yang digunakan adalah "abcdefghijuklmno". Untuk bisa mulai melakukan proses enkripsi sebelumnya ubah dahulu teks menjadi *plaintext* dalam bentuk heksadesimal, sehingga menjadi :
303031407372745F6B656C7561720000
Begitu pula dengan *key* nya, menjadi :
6162636465666768696A756B6C6D6E6F

Proses enkripsi dalam Algoritma AES menggunakan transformasi berupa substitusi dan permutasi yang diulang-ulang sampai dengan 10 putaran. Proses enkripsi secara keseluruhan dapat dilihat pada tabel di bawah ini (Muharram, 2018):

Tabel 1. Proses Enkripsi Algoritma AES

Putaran ke	Proses	Proses di Luar Putaran
1	*Initial Round* *Sub Bytes* *Shift Rows* *Mix Columns* *Add Round Key*	*Key Schedule*
2-9	*Sub Bytes* *Shift Rows* *Mix Columns* *Add Round Key*	
10	*Sub Bytes* *Shift Rows* *Add Round Key*	

Initial Round adalah proses perkalian XOR antara *plaintext* dengan *chiper key*, *SubBytes* adalah substitusi hasil Initial Round dengan tabel S-Box, *ShiftRows* adalah pergeseran bit dalam *array* dari kanan ke kiri dari hasil *SubBytes*, *MixColumns* adalah perkalian hasil *ShiftRows* dengan suatu matrik, dan *AddRoundKey* adalah proses perkalian XOR antara hasil dari *MixColumns* dengan *Round Key* yang didapat dari hasil ekspansi kunci (*key schedule)* (Hasibuan, 2017).

Hasil untuk setiap proses pada setiap putaran dapat dilihat pada gambar di bawah ini:

	SubBytes				ShiftRows				MixColumns				AddRoundKey				Key Schedule				Round Constant
Round 1	D1	47	77	D7	D1	47	77	D7	D0	BD	2F	BA	8C	84	7F	86	5C	39	50	3C	01
	00	FA	76	C0	FA	76	C0	00	F1	27	76	22	0C	BC	87	BE	FD	9B	F1	9C	00
	00	7D	D4	9F	D4	9F	00	7D	7B	4E	02	BB	B0	E2	DB	0C	CB	AC	D9	B7	00
	36	9A	72	A8	A8	36	9A	72	0D	4C	76	FB	39	10	41	A3	34	5C	37	58	00
Round 2	64	5F	D2	44	64	5F	D2	44	D4	6B	7B	8A	54	D2	92	5F	80	B9	E9	D5	02
	FE	65	17	AE	65	17	AE	FE	74	7A	6D	93	20	B5	53	31	54	CF	3E	A2	00
	E7	98	B9	FE	B9	FE	E7	98	76	99	EC	0F	D7	94	38	6C	A1	0D	D4	63	00
	12	CA	83	0A	0A	12	CA	83	64	2C	AB	B7	BB	AF	1F	5B	DF	83	B4	EC	00
Round 3	20	B5	4F	CF	20	B5	4F	CF	1A	E7	BB	A5	A4	E0	55	9E	BE	07	EE	3B	04
	B7	D5	ED	C7	D5	ED	C7	B7	A1	6E	B1	1C	0E	0E	EF	E0	AF	60	5E	FC	00
	0E	22	07	50	07	50	0E	22	B0	DD	1F	67	DF	BF	A9	B2	6F	62	B6	D5	00
	EA	79	C0	39	39	EA	79	C0	C0	B6	EA	44	1C	E9	01	43	DC	5F	EB	07	00
Round 4	49	E1	FC	0B	49	E1	FC	0B	BD	08	5B	84	BB	09	B4	50	06	01	EF	D4	08
	AB	AB	DF	E1	AB	DF	E1	AB	70	81	82	22	DC	4D	10	4C	AC	CC	92	6E	00
	9E	08	D3	37	D3	37	9E	08	71	EF	18	34	DB	27	66	9F	AA	C8	7E	AB	00
	9C	1E	7C	1A	1A	9C	1E	7C	97	F3	5C	46	A9	92	D6	CB	3E	61	8A	8D	00
Round 5	EA	01	8D	53	EA	01	8D	53	DD	4F	8C	0D	54	C7	EB	BE	89	88	67	B3	10
	86	E3	CA	29	E3	CA	29	86	7D	2B	40	FD	B3	29	D0	03	CE	02	90	FE	00
	B9	CC	33	DB	33	DB	B9	CC	4E	08	1C	57	B9	37	5D	BD	F7	3F	41	EA	00
	D3	4F	F6	1F	1F	D3	4F	F6	CB	AF	82	48	BD	B8	1F	58	76	17	9D	10	00
Round 6	20	C6	E9	AE	20	C6	E9	AE	92	07	7E	AA	80	9D	83	E4	12	9A	FD	4E	20
	6D	A5	70	7B	A5	70	7B	6D	CF	D2	89	01	86	99	52	24	49	4B	DB	25	00
	56	9A	4C	7A	4C	7A	56	9A	A3	CC	8A	B7	9E	CE	C9	1E	3D	02	43	A9	00
	7A	6C	C0	6A	6A	7A	6C	C0	5D	AF	D5	85	46	A3	44	04	1B	0C	91	81	00
Round 7	CD	5E	EC	69	CD	5E	EC	69	87	94	98	8E	EA	63	92	CA	6D	F7	0A	44	40
	44	EE	00	36	EE	00	36	44	84	92	97	7C	1E	43	9D	53	9A	D1	0A	2F	00
	0B	8B	DD	72	DD	72	0B	8B	8F	54	D2	0D	BE	67	A2	D4	31	33	70	D9	00
	5A	0A	1B	F2	F2	5A	0A	1B	80	24	06	42	B4	1C	AF	6A	34	38	A9	28	00
Round 8	87	FB	4F	74	87	FB	4F	74	03	CA	80	82	FB	C5	85	C3	F8	0F	05	41	80
	72	1A	5E	ED	1A	5E	ED	72	FF	12	FB	7D	50	6C	8F	26	AF	7E	74	5B	00
	AE	85	3A	48	3A	48	AE	85	EF	B9	5A	9C	EA	8F	1C	03	05	36	46	9F	00
	8D	9C	79	02	02	8D	9C	79	B6	01	B1	99	99	16	0F	0F	2F	17	BE	96	00
Round 9	0F	A6	97	2E	0F	A6	97	2E	04	57	F7	AC	DE	82	27	3D	DA	D5	D0	91	1B
	53	50	73	F7	50	73	F7	53	66	23	B7	6B	12	29	C9	4E	74	0A	7E	25	00
	87	73	9C	7B	9C	7B	87	73	E6	0A	BC	01	73	A9	59	7B	95	A3	E5	7A	00
	EE	47	76	76	76	EE	47	76	31	3E	5C	BE	9D	85	59	2D	AC	BB	05	93	00
Round 10	1D	13	CC	27	1D	13	CC	27					CE	15	1A	60	D3	06	D6	47	36
	C9	A5	DD	2F	A5	DD	2F	C9					0B	79	F5	36	AE	A4	DA	FF	00
	8F	D3	CB	21	CB	21	8F	D3					82	CB	80	A6	49	EA	0F	75	00
	5E	97	CB	D8	D8	5E	97	CB					F5	C8	04	CB	2D	96	93	00	00
	SubBytes				ShiftRows				MixColumns				AddRoundKey				Key Schedule				Round Constant

Gambar 2. Hasil transformasi pada setiap proses dan putaran proses enkripsi

Setelah dilakukan beberapa proses dalam enkripsi Algoritma AES maka hasil yang diperoleh untuk teks "001@srt_keluar" adalah : *CE0B82F51579CBC81AF580046036A6CB*

Hasil ini disebut dengan *chipertext.*

3.2. Proses Dekripsi Algoritma AES

Proses Dekripsi Algoritma AES hamper sama dengan proses enkripsinya, hanya saja untuk dekripsi setiap proses yang ada pada enkripsi dibalik urutannya. Begitu juga dengan *round key* yang didapat dari proses *key schedule*, penggunaannya pada setiap putaran dalam proses dekripsi dibalik urutanya, dengan putaran pertama menggunakan *round key* ke 10, putaran kedua menggunakan *round key* ke 9 dan seterusnya. Proses dekripsi menggunakan Algoritma AES secara keseluruhan dapat dilihat pada tabel di bawah ini (Prameshwari, 2018):

Tabel 2. Proses Dekripsi Algoritma AES

Putaran ke	Proses	Proses di Luar Putaran
1	*Add Round Key* *Inv Shift Rows* *Inv Sub Bytes*	*Key Schedule*
2-9	*Add Round Key* *Inv Mix Columns* *Inv Shift Rows* *Inv Sub Bytes*	
10	*Add Round Key* *Inv Mix Columns* *Inv Shift Rows* *Inv Sub Bytes* *Add Round Key*	

Chipertext yang akan didekripsi pada pembahasan ini adalah teks hasil dari proses enkripsi sebelumnya, yaitu :
CE0B82F51579CBC81AF580046036A6CB

AddRoundKey adalah proses perkalian antara *chipertext* dengan *round key*, *InvShiftRows* adalah pergeseran bit dalam *array* dari kiri ke kanan, *InvSubBytes* adalah substitusi hasil *InvShiftRows* dengan tabel Invers S-Box, dan *InvMixCoumn* adalah perkalian hasil proses sebelumnya dengan sebuah matrik. Berikut ini adalah hasil dari setiap proses dan setiap putaran pada dekripsi Algoritma AES (Permana, 2018):

	SubBytes				ShiftRows				MixColumns				AddRoundKey				Key Schedule				Round Constant
Round 0													30	73	6B	61	61	65	69	6C	
													30	72	65	72	62	66	6A	6D	
													31	74	6C	00	63	67	75	6E	
													40	5F	75	00	64	68	6B	6F	
Round 1	51	16	02	0D	D1	47	77	D7	D1	47	77	D7	D0	BD	2F	BA	5C	39	50	3C	01
	52	14	0F	1F	00	FA	76	C0	FA	76	C0	00	F1	27	76	22	FD	9B	F1	9C	00
	52	13	19	6E	00	7D	D4	9F	D4	9F	00	7D	7B	4E	02	BB	CB	AC	D9	B7	00
	24	37	1E	6F	36	9A	72	A8	A8	36	9A	72	0D	4C	76	FB	34	5C	37	58	00
Round 2	8C	84	7F	86	64	5F	D2	44	64	5F	D2	44	D4	6B	7B	8A	80	B9	E9	D5	02
	0C	BC	87	BE	FE	65	17	AE	65	17	AE	FE	74	7A	6D	93	54	CF	3E	A2	00
	B0	E2	DB	0C	E7	98	B9	FE	B9	FE	E7	98	76	99	EC	0F	A1	0D	D4	63	00
	39	10	41	A3	12	CA	83	0A	0A	12	CA	83	64	2C	AB	B7	DF	83	B4	EC	00
Round 3	54	D2	92	5F	20	B5	4F	CF	20	B5	4F	CF	1A	E7	BB	A5	BE	07	EE	3B	04
	20	B5	53	31	B7	D5	ED	C7	D5	ED	C7	B7	A1	6E	B1	1C	AF	60	5E	FC	00
	D7	94	38	6C	0E	22	07	50	07	50	0E	22	B0	DD	1F	67	6F	62	B6	D5	00
	BB	AF	1F	5B	EA	79	C0	39	39	EA	79	C0	C0	B6	EA	44	DC	5F	EB	07	00
Round 4	A4	E0	55	9E	49	E1	FC	0B	49	E1	FC	0B	BD	08	5B	84	06	01	EF	D4	08
	0E	0E	EF	E0	AB	AB	DF	E1	AB	DF	E1	AB	70	81	82	22	AC	CC	92	6E	00
	DF	BF	A9	B2	9E	08	D3	37	D3	37	9E	08	71	EF	18	34	AA	C8	7E	AB	00
	1C	E9	01	43	9C	1E	7C	1A	1A	9C	1E	7C	97	F3	5C	46	3E	61	8A	8D	00
Round 5	BB	09	B4	50	EA	01	8D	53	EA	01	8D	53	DD	4F	8C	0D	89	88	67	B3	10
	DC	4D	10	4C	86	E3	CA	29	E3	CA	29	86	7D	2B	40	FD	CE	02	90	FE	00
	DB	27	66	9F	B9	CC	33	DB	33	DB	B9	CC	4E	08	1C	57	F7	3F	41	EA	00
	A9	92	D6	CB	D3	4F	F6	1F	1F	D3	4F	F6	CB	AF	82	48	76	17	9D	10	00
Round 6	54	C7	EB	BE	20	C6	E9	AE	20	C6	E9	AE	92	07	7E	AA	12	9A	FD	4E	20
	B3	29	D0	03	6D	A5	70	7B	A5	70	7B	6D	CF	D2	89	01	49	4B	DB	25	00
	B9	37	5D	BD	56	9A	4C	7A	4C	7A	56	9A	A3	CC	8A	B7	3D	02	43	A9	00
	BD	B8	1F	58	7A	6C	C0	6A	6A	7A	6C	C0	5D	AF	D5	85	1B	0C	91	81	00
Round 7	80	9D	83	E4	CD	5E	EC	69	CD	5E	EC	69	87	94	98	8E	6D	F7	0A	44	40
	86	99	52	24	44	EE	00	36	EE	00	36	44	84	92	97	7C	9A	D1	0A	2F	00
	9E	CE	C9	1E	0B	8B	DD	72	DD	72	0B	8B	8F	54	D2	0D	31	33	70	D9	00
	46	A3	44	04	5A	0A	1B	F2	F2	5A	0A	1B	80	24	06	42	34	38	A9	28	00
Round 8	EA	63	92	CA	87	FB	4F	74	87	FB	4F	74	03	CA	80	82	F8	0F	05	41	80
	1E	43	9D	53	72	1A	5E	ED	1A	5E	ED	72	FF	12	FB	7D	AF	7E	74	5B	00
	BE	67	A2	D4	AE	85	3A	48	3A	48	AE	85	EF	B9	5A	9C	05	36	46	9F	00
	B4	1C	AF	6A	8D	9C	79	02	02	8D	9C	79	B6	01	B1	99	2F	17	BE	96	00
Round 9	FB	C5	85	C3	0F	A6	97	2E	0F	A6	97	2E	04	57	F7	AC	DA	D5	D0	91	1B
	50	6C	8F	26	53	50	73	F7	50	73	F7	53	66	23	B7	6B	74	0A	7E	25	00
	EA	8F	1C	03	87	73	9C	7B	9C	7B	87	73	E6	0A	BC	01	95	A3	E5	7A	00
	99	16	0F	0F	EE	47	76	76	76	EE	47	76	31	3E	5C	BE	AC	BB	05	93	00
Round 10	DE	82	27	3D	1D	13	CC	27					1D	13	CC	27	D3	06	D6	47	36
	12	29	C9	4E	C9	A5	DD	2F					A5	DD	2F	C9	AE	A4	DA	FF	00
	73	A9	59	7B	8F	D3	CB	21					CB	21	8F	D3	49	EA	0F	75	00
	9D	85	59	2D	5E	97	CB	D8					D8	5E	97	CB	2D	96	93	00	00
	SubBytes				ShiftRows				MixColumns				AddRoundKey				Key Schedule				Round Constant

Gambar 3. Hasil transformasi pada setiap proses dan putaran proses dekripsi

Setelah dilakukan beberapa proses dalam dekripsi Algoritma AES, maka hasil yang diperoleh untuk *chipertext* :

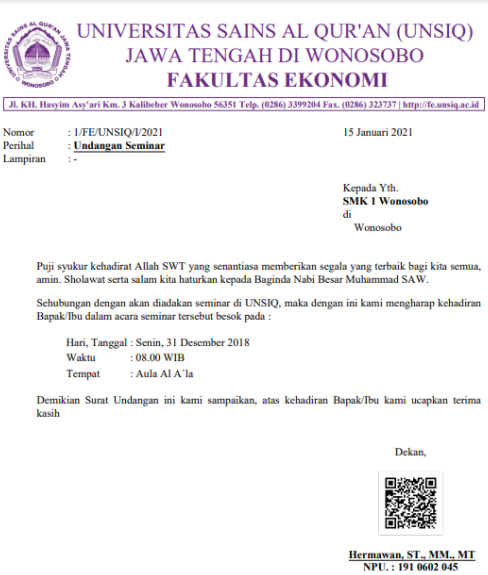
CE0B82F51579CBC81AF580046036A6CB
Adalah :
303031407372745F6B656C7561720000
Hasil tersebut masih dalam bentuk heksadesimal, oleh karena itu kita ubah ke dalam bentuk teks, sehingga menjadi "001@srt_keluar".

3.3. Implementasi Algoritma AES pada Aplikasi SERAT FE-UNSIQ

Algoritma AES pada Aplikasi SERAT FE-UNSIQ dimasukkan dalam URL pengecekan surat yang dikonversi menjadi bentuk *QR-Code*. Dalam pembahasan ini URL pengecekan surat yaitu http://suratfe.rf.gd/surat_detail.php?id=ce0b82f51579cbc81af580046036a6cb. Setelah itu konversi ke dalam bentuk *QR-Code menjadi*

Gambar 4. Hasil konversi *QR-Code*

QR-Code yang sudah jadi dimasukkan ke dalam surat dibagian tandatangan pimpinan untuk menggantikan tandatangan konvensional dengan tandatangan digital agar bisa dilakukan pengecekan surat dengan mudah. Berikut adalah contoh surat yang sudah diberi tandatangan digital berupa *QR-Code* :



UNIVERSITAS SAINS AL QUR'AN (UNSIQ)
JAWA TENGAH DI WONOSOBO
FAKULTAS EKONOMI
Jl. KH. Hasyim Asy'ari Km. 3 Kalibeber Wonosobo 56351 Telp. (0286) 3399204 Fax. (0286) 323737 | http://fe.unsiq.ac.id

Nomor : 1/FE/UNSIQ/I/2021
Perihal : Undangan Seminar
Lampiran : -

15 Januari 2021

Kepada Yth.
SMK 1 Wonosobo
di
Wonosobo

Puji syukur kehadirat Allah SWT yang senantiasa memberikan segala yang terbaik bagi kita semua, amin. Sholawat serta salam kita haturkan kepada Baginda Nabi Besar Muhammad SAW.

Sehubungan dengan akan diadakan seminar di UNSIQ, maka dengan ini kami mengharap kehadiran Bapak/Ibu dalam acara seminar tersebut besok pada :

Hari, Tanggal : Senin, 31 Desember 2018
Waktu : 08.00 WIB
Tempat : Aula Al A`la

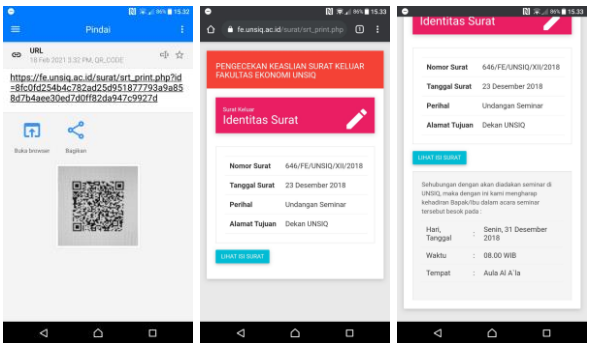
Demikian Surat Undangan ini kami sampaikan, atas kehadiran Bapak/Ibu kami ucapkan terima kasih

Dekan,

Hermawan, ST., MM., MT
NPU. : 191 0602 045

Gambar 5. Surat bertandatangan digital

Pengecekan surat dilakukan dengan memindai *QR-Code* yang ada di dalam surat menggunakan *Barcode Scanner*, kemudian URL yang memuat enkripsi algoritma AES dan mengarahkan ke halaman pengecekan akan muncul.



Gambar 6. Tampilan pemindaian *QR-Code* dan pengecekan surat

Jika kita bandingkan, informasi yang ada pada halaman pengecekan sama dengan yang ada pada surat aslinya.

4. PENTUTUP

4.1. Kesimpulan

Berdasarkan hasil penelitian yang telah dilakukan pembuatan Aplikasi SERAT FE-UNSIQ berjalan dengan baik. Begitu juga dengan implementasi Algoritma AES di dalamnya. Sehingga dapat disimpulkan bahwa dengan adanya Aplikasi SERAT FE-UNSIQ ini dapat mempercepat kinerja pembuatan surat serta dapat menjamin keaslian surat itu sendiri.

4.2. Saran

Meskipun Aplikasi SERAT FE-UNSIQ bisa berjalan dengan baik, tetapi dari pihak Fakultas Ekonomi UNSIQ masih belum secara penuh menggunakan aplikasi ini. Karena untuk saat ini di sana masih dilakukan proses adaptasi menggunakan aplikasi. Oleh karena itu diharapkan pihak fakultas segera menyelesaikan proses adaptasinya sehingga aplikasi dapat digunakan secara penuh.

Untuk Aplikasi SERAT FE-UNSIQ masih dapat dikembangkan lagi seperti menambahkan beberapa menu baru yang berkaitan dengan Surat Menyurat yang belum bisa dibuat menggunakan aplikasi.

5. DAFTAR PUSTAKA

El Rahma, R., Asmarajati, D., Hasanah, N., & Sibyan, H. (2021). PENENTUAN KONKLUSI NOTIFIKASI PADA CHATBOT RESERVASI WISATA DENGAN METODE FORWARD CHAINING. Device, 11(1), 19-24.

Muharram, F., Aziz, H., & Manga, A. R. (2018, September). Analisis Algoritma pada Proses Enkripsi dan Dekripsi File Menggunakan Advanced Encryption Standard (AES). In Prosiding SAKTI (Seminar Ilmu Komputer dan Teknologi Informasi) (Vol. 3, No. 2, pp. 112-115).

Hasibuan, A. M. (2017). Rancang Bangun Aplikasi Keamanan Data Menggunakan Metode AES Pada Smartphone. MEANS (Media Informasi Analisa dan Sistem), 2(1), 29-35.

Prameshwari, A., & Sastra, N. P. (2018). Implementasi Algoritma Advanced Encryption Standard (AES) 128 Untuk Enkripsi dan Dekripsi File Dokumen. Jurnal Eksplora Informatika, 8(1), 52-58.

Permana, A. A., & Nurnaningsih, D. (2018). Rancangan Aplikasi Pengamanan Data Dengan Algoritma Advanced Encyption Standard (AES). Jurnal Teknik Informatika, 11(2), 177-186.