Implementasi Skema *QR-Code* dan *Digital Signature* menggunakan Kombinasi Algoritma RSA dan AES untuk Pengamanan Data Sertifikat Elektronik

Fitri Nuraeni[1], Yoga Handoko Agustin[2], Dede Kurniadi[3], Imas Dewi Ariyanti[4]
[1,2,3]Sekolah Tinggi Teknologi Garut
Jl. Mayor Syamsu No.1, Jayaraga, Kec. Tarogong Kidul, Kabupaten Garut
e-mail: [1]fitri.nuraeni@sttgarut.ac.id, [2]yoga.handoko@sttgarut.ac.id, [3]dede.kurnadi@sttgarut.ac.id,
[4]imasagalarupa@gmail.com

Abstrak

Maraknya kegiatan webinar dan kursus online saat ini, menambah banyak penggunaan sertifikat elektronik, sebagai bukti partisipasi kegiatan tersebut. File sertifikat elektronik yang disebarkan melalui media internet rentan terhadap ancaman modifikasi dan fabrikasi data oleh pihak yang tidak bertanggung jawab. Sehingga dibutuhkan suatu jaminan keamanan data pada sertifikat elektronik tersebut dengan menerapkan tanda tangan digital pada sertifikat elektronik. Tanda tangan digital yang dirancang pada penelitian ini terdiri dari fungsi hashing SHA-3 dan super enkripsi kombinasi RSA dan AES dengan ukuran blok 128bit dan mode operasi CBC. Penggunaan super enkripsi ini terbukti dapat meningkatkan jaminan keamanan dengan kualitas enkripsi yang bagus yaitu 1) rata-rata waktu proses enkripsi dan dekripsi cepat di bawah 0,1 milisecond; 2) nilai entropi cukup bagus sebesar 4,96 yang lebih mendekati 8; serta nilai avalanche effect 40,61% yang bagus karena mendekati 50% perubahan pada perbedaan 1 bit plainteksnya. Sistem tanda tangan digital ini menjadi lebih mudah digunakan karena disisipkan pada file sertifikat elektronik menggunakan skema QR-code.

Kata kunci: *AES, RSA, SHA-3, sertifikat elektronik, Tanda Tangan digital*

Abstract

The present webinars activity and online courses, increasing the use of electronic certificates, testifies to the participation of the activity. Certificate file electronics propagated through Internet media is susceptible to threats of modification and data fabrication by irresponsible authorities. So, it is needed a data safety guarantee on the electronic certificate by applying digital signature on it. Digital signature designed on this research consisted of a function of hashing SHA-3 and super encryption of combination RSA and AES of a 128bit block and CBC operating mode. The use of these super encryptions had been shown to increase security coverage with the good quality encryption 1) the average time for a fast encryption and decryption process below 0.1 millisecond; 2) the value of entropy was good enough for more than 4.96 approaching 8; and the avalanche value of 40,61% was good because it was close to 50% of the difference between one bit of a playoff. This digital signature system is becoming easier to use because it is inserted into electronic certificate files using QR-code scheme.

Keywords*: AES, Digital signature, e-certificate, RSA, SHA-3*

1. Pendahuluan

Saat pandemi yang terjadi di Indonesia serta negara-negara lain di berbagai belahan dunia pada tahun 2020 ini, banyak kegiatan yang beralih menggunakan teknologi informasi sebagai media untuk berkumpul dan berkomunikasi dalam jaringan (daring/ *online*). Salah satu kegiatan yang cukup popular saat ini di kalangan masyarakat, baik di dunia pendidikan maupun non-pendidikan, yaitu webinar. Istilah webinar ini popular karena kegiatan seminar yang selalu dilaksanakan tiap waktu oleh berbagai pihak, semula menggunakan konsep mengumpulkan orang banyak disuatu tempat tertentu untuk penyampaian informasi secara tatap muka, saat ini beralih dilakukan secara online. Webinar ini memungkinkan orang-orang melakukan tatap muka secara online yang disampaikan melalui media internet dan dihadiri oleh banyak orang di lokasi yang berbeda-beda dan berinteraksi menggunakan media gambar, video dan teks[1]. Selain webinar, saat ini juga banyak lembaga-lembaga yang menyediakan layanan kursus kompetensi tertentu secara online. Pada setiap kegiatan webinar maupun kursus online ini, biasanya pihak penyelenggara memberikan sertifikat sebagai bukti partisipasi kegiatan baik untuk pemateri

maupun pesertanya. Namun, karena kegiatan webinar ini dilakukan secara online, maka sertifikat yang diberikan pun berupa file digital yaitu sertifikat elektronik (*e-certificate*).

Sertifikat elektronik ini tetap menjadi dokumen resmi yang penting layaknya dokumen sertifikat hasil cetak, dan dapat digunakan oleh pemiliknya sebagai syarat pada berbagai kegiatan resmi lainnya. Namun, karena bentuknya berupa file digital yang ditransmisikan melalui internet, sertifikat elektronik rentan adanya pemalsuan, baik fabrikasi maupun modifikasi data, maka perlu adanya suatu upaya untuk mengamankan data asli dari orang pemilik sertifikat (peserta/ pemateri) dan data kegiatan yang mengeluarkan sertifikat tersebut. Untuk menjaga aspek kemananan data dan informasi tersebut, kriptografi menyediakan fasilitas tanda tangan digital yang dapat memberikan jaminan otentifikasi, integritas data dan non-*repudiation*[2], sehingga dapat menghilangkan kekhawatiran adanya sertifikat palsu.

Tanda tangan digital memiliki perbedaan dengan tanda tangan konvensional, dimana tanda tangan digital sangat bergantung pada isi dokumen yang ditanda tanganinya, sehingga setiap dokumen akan menghasilkan tanda tangan digital yang berbeda dengan dokumen lainnya[3]. Dapat dipastikan bahwa setiap sertifikat elektronik yang dihasilkan untuk setiap partisipan kegiatan webinar akan memiliki tanda tangan digital yang unik. Tanda tangan digital ini akan bergantung pada data partisipan selaku pemilik sertifikat, data kegiatan webinar serta data pejabat yang mengesahkan sertifikat, sehingga adanya pembubuhan tanda tangan digital pada sertifikat elektronik dapat menunjukan keaslian dari sertifikat yang terjamin[4]. Selain itu, tanda tangan digital tidak mudah ditiru oleh orang lain, sehingga data asli sertifikat elektronik ini, tidak bisa dengan mudah dimodifikasi[5].

Selain tanda tangan digital, saat ini otentifikasi dokumen dapat memanfaatkan skema QR-Code (*quick response code*) yang dapat menyimpan data numerik, alphanumerik, binary dan kanji[6], serta memiliki penyimpanan yang jauh lebih besar dibandingkan *barcode*[7]. QR-Code ini dapat digunakan untuk menyembunyikan suatu pesan dibalik sebuah kode yang dapat memberikan jaminan keaman dan privasi terhadap orang yang melakukan pengiriman pesan. Namun pembangkitan QR-code ini belum memiliki kunci yang memberikan parameter perubahan yang dapat menyembunyikan data asli, sehingga untuk keamanan data lebih tinggi, maka kriptografi dapat digunakan untuk mengenkripsi data sebelum dibangkitkan QR-codenya[8].

Konsep tanda tangan digital memiliki 2 proses utama, yaitu penanda-tangan (signing) dan verifikasi. Dalam praktiknya kadang proses *signing* menghasilkan kode yang cukup panjang sehingga diperlukan teknik penyisipan atau pembubuhan tanda tangan digital pada dokumen tersebut[4]. Maka, untuk kemudahan implementasi tanda tangan digital ini, kode yang dihasilkan dari proses *signing* disimpan pada sebuah QR-code. Kemudian QR-code ini akan dengan mudah digunakan untuk melakukan proses verifikasi keaslian sertifikat elektronik[9].

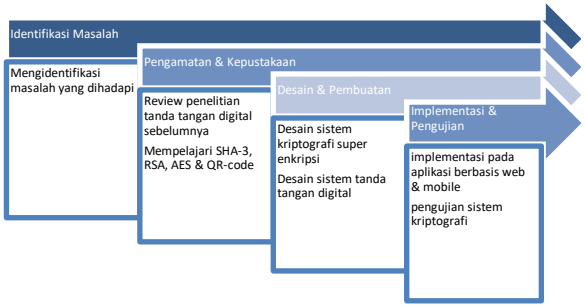
Kekuatan tanda tangan digital tergantung pada metode kriptografi dan panjang kunci yang digunakan[10]. Beberapa algoritma yang digunakan untuk pengembangan tanda tangan digital diantaranya RSA [2][3][4], yang merupakan algoritma kunci asimetris (kunci public dan kunci private). RSA merupakan algoritma yang banyak dipergunakan pada tanda tangan digital, karena algoritma ini proses tidak sederhana juga tidak begitu rumit[11], namun aman karena adanya kerumitan yang terletak pada sulitnya memfaktorkan bilangan prima yang cukup besar menjadi factor-faktor prima yang lebih kecil. Selain itu, ada juga tanda tangan digital yang menggunakan algoritma kunci simetris seperti AES[5] yang merupakan algortima yang lebih aman, efisien dan lebih cepat daripada semua algoritma dengan memungkinkan ukuran kunci 256-bit dan melindungi dari serangan di masa depan[12].

Pada penelitian ini, untuk dapat meningkatkan keamanan dari sistem kriptografi maka dilakukan pengembangan tanda tangan digital dengan menggunakan kombinasi algoritma RSA, yang memiliki kunci *public* dan kunci *private*, dengan algoritma AES, dengan proses enkripsi berbasis blok 256 bit, serta algoritma Keccak, sebagai algoritma *hashing* yang terpilih sebagai fungsi *hash* standar (SHA-3)[3]. Hasil dari penelitian ini adalah didapatnya nilai kualitas enkripsi yang bagus dilihat dari segi waktu proses enkripsi-dekripsi, nilai entropi, nilai korelasi, dan nilai *avalanche effect*. Selain itu, Dari penelitian sebelumnya, penggunaan tanda tangan digital menggunakan RSA menghasilkan kode tanda tangan yang cukup panjang sehingga kode dilampirkan, tidak disisipkan serta menyulitkan proses verifikasi karena kode yang panjang harus diinputkan manual [4]. Dengan adanya skema QR-code, dapat digunaka untuk menampung kode tanda tangan digital yang cukup Panjang sehingga dapat disisipkan pada file sertifikat serta proses verifikasi dapat dilakukan dengan mudah menggunakan fasilitas QR-code reader.

ISSN (Printed) : 2579-7271
ISSN (Online) : 2579-5406

2. Metode Penelitian

Penelitian ini dilakukan dengan menggunakan metode eksperimen dilanjutkan dengan proses pembangunan aplikasi untuk penerapan dari tanda tangan digital ini. Metode eksperimen ini ditujukan untuk menerapkan kombinasi algoritma RSA dan AES pada tanda tangan digital dengan kualitas yang bagus, dilihat dari segi waktu proses enkripsi-dekripsi, nilai entropi, nilai korelasi, dan nilai *avalanche effect*.



Gambar 1. Skema Metode Penelitian yang dilakukan

2.1. Identifikasi Masalah

Tanda tangan digital dianggap handal karena menggunakan sistem kriptografi asimetris yang memiliki pasangan kunci *public* dan kunci *private*, dimana satu kunci pegang oleh pihak yang menerbitkan dokumen secara rahasia dan kunci yang lainnya dapat dipergunakan oleh pihak penerima dokumen untuk proses pengecekan keaslian dokumen. Namun, suatu sistem kriptografi dikatakan aman (*computationally secure*) apabila memenuhi salah satu syaratnya yaitu memiliki operasi algoritma yang sangat kompleks sehingga sulit dipecahkan[13]. Sehingga dibutuhkan suatu upaya untuk meningkatkan keamanan sistem kriptografi pada tanda tangan digital dengan cara menggunakan super enkripsi atau kombinasi antara 2 algoritma atau lebih[14].

Dari penelitian sebelumnya, penggunaan tanda tangan digital menggunakan RSA menghasilkan kode tanda tangan yang cukup panjang sehingga kode dilampirkan, tidak disisipkan serta menyulitkan proses verifikasi karena kode yang panjang harus diinputkan manual[4]. Dengan adanya skema QR-*code*, dapat digunaka untuk menampung kode tanda tangan digital yang cukup Panjang sehingga dapat disisipkan pada file sertifikat serta proses verifikasi dapat dilakukan dengan mudah menggunakan fasilitas *QR-code reader*.

2.2. Algoritma yang digunakan

2.2.1. Algoritma Keccak (SHA-3)

Keccak merupakan salah satu algoritme fungsi hash yang dirancang oleh Guido Bertoni, Joan Daemen, Michaël Peeteres, dan Gilles Van Assche, yang diperkenalkan sebagai *secure hash algoritm* (SHA-3). Perbedaan utama antara Keccak dengan SHA-1, SHA-2, ataupun MD5 adalah Keccak menggunakan konstruksi *spons function* pada pembentukan nilai hash-nya, sedangkan tiga algoritme tersebut menggunakan skema *Merkle-Damgård*[3]. Algoritma ini juga memiliki kinerja yang lebih baik dari pada algortima SHA-1 dengan kehandalan dan keamanannya[15]. Algoritma SHA-3 mempunyai keluaran beragam, beragam mulai dari 224, 256, 384, dan 512 bit[16]. Konstruksi *spons* didasarkan pada fungsi acak yang luas atau permutasi acak, dan memungkinkan memasukkan ("menyerap" dalam terminologi *spons*) sejumlah data, dan mengeluarkan ("memeras") sejumlah data, sementara bertindak sebagai fungsi *pseudorandom* berkaitan dengan semua masukan sebelumnya. Ini mengarah pada fleksibilitas yang tinggi.

2.2.2. Algortima RSA

RSA merupakan algortima yang menggunakan sistem kriptografi kunci publik yang dapat memberikan jaminan keamanan pada jalur transmisi distribusi kunci serta mendukung tanda tangan digital yang memverifikasi pesan yang diterima merupakan pesan asli yang dikirim oleh pengirim pesan. RSA dikatakan aman, karena sulitnya memfaktorkan bilangan n, dimana $n = pxq$, p dan q adalah bilangan prima yang sangat besar[3].

RSA membangkitkan kunci privat dan kunci publik-nya, dengan langkah-langkash sebagai berikut:

a) Membangkitkan nilai *p* dan *q* secara sembarang, dimana *p* dan *q* ini adalah bilangan prima yang besar.
b) Menghitung n

$$n = p \,.\, q \quad (1)$$

c) Menghitung $\varphi(n)$ yaitu

$$\varphi(n) = (p-1)(q-1) \quad (2)$$

d) Memilih kunci public e yang relative prima terhadap $\varphi(n)$. $GCD(\varphi(n), e) = 1$
e) Membangkitkan kunci private *d* menggunakan rumus (3)

$$e.d = k.\varphi(n) + 1 \quad (3)$$

f) Dihasilkanlah pasangan kunci public (e,n) dan kunci private (d,n).

Sedangkan untuk proses enkripsi dan dekripsi, RSA melakukan langkah-langkah seperti berikut:

a) Enkripsi suatu pesan (m) menggunakan kunci public (e, n)

$$c = m^e \ mod\, n \quad (4)$$

b) Dekripsi suatu cipherteks (c) menggunakan kunci privat (d,n)

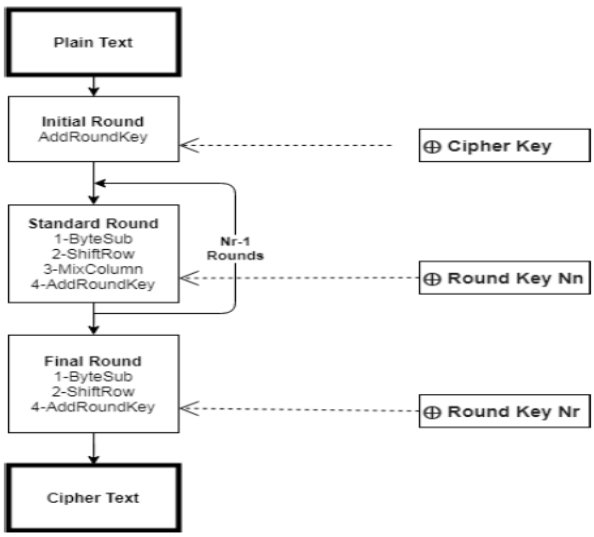
$$m = c^d \ mod\, n \quad (5)$$

2.2.3. Algortima AES

Advanced Encryption Standard (AES) merupakan algoritma kriptografi yang dapat digunakan untuk mengamankan data. Algoritma AES adalah blok chipertext simetrik yang dapat mengenkripsikan (encipher) dan dekripsi (decipher) informasi. Enkripsi merubah data yang tidak dapat lagi dibaca disebut ciphertext, sebaliknya dekripsi adalah merubah ciphertext data menjadi bentuk semula yang kita kenal sebagai plaintext. Algoritma AES ini menggunakan kunci kriptografi 128, 192, dan 256 bits untuk mengenkrip dan dekrip data pada blok 128 bits.

Berikut ini adalah operasi Rijndael (AES) yang m enggunakan 128 bit kunci :

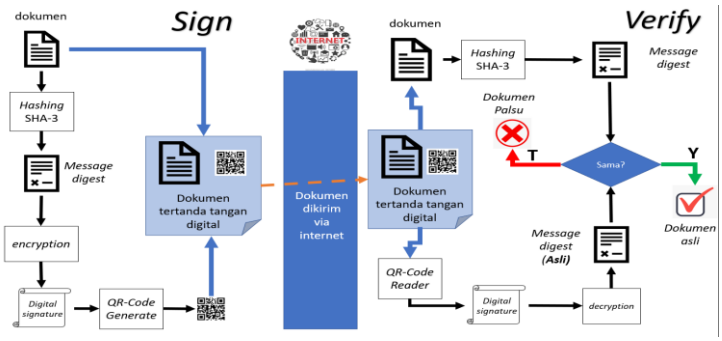
1) Ekspansi kunci utama (dari 128 bit menjadi 1408 bit);
2) *Initial Round,* Pencampuran state awal plainteks dengan *cipher key*
3) Ulang dari i=1 sampai i=10 lakukan Transformasi :
   a. *ByteSub* (subtitusi per byte)
   b. *ShiftRow* (pergeseran byte perbaris)
   c. *MixColumn* (Operasi perkalian GF(2) per kolom);
   d. *AddRoundKey*, XOR dengan *roundKey* ke-i
4) *Final Round*, sama seperti transformasi sebelumnya namun tidak memasukan *MixColumn* saja.



Gambar 2. Algortima AES [17]

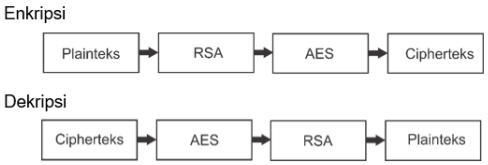
ISSN (Printed) : 2579-7271
ISSN (Online) : 2579-5406

2.3. Desain Tanda Tangan Digital



Gambar 3. Skema Proses *Sign* dan *Verify* Tanda Tangan Digital pada Dokumen Elektronik

Tanda tangan digital memiliki 2 proses utama terlihat pada gambar 1, yaitu *sign* dan *verifiy*, yang dimana pada proses tersebut memerlukan algoritma kriptografi untuk memproses data dari dokumen. Proses penanda-tanganan (*sign*) diawali dengan proses *hashing*, yaitu data asli dari dokumen diambil intisarinya (*message digest*) menggunakan fungsi *hash* seperti MD5, SHA-1, SHA-256 maupun SHA-512[18]. Fungsi *hash* digunakan untuk mendapatkan nilai *hash* dari data yang ada pada pesan/ dokumen, dan biasanya hanya proses satu arah, dimana hasil *hashing* tidak dapat diproses kembali untuk mendapatkan data aslinya seperti proses dekripsi pada sistem kriptografi. Fungsi *hash* ini memiliki kelemahan yaitu memungkinkan untuk menghasilkan nilai *hash* yang sama dari data yang berbeda (*collision*/ tumbukan). Keccak merupakan pemenang kompetisi SHA-3 *Cryptographic Hash Algorithm Competition* dan dijadikan standar algoritma fungsi *secure hash algoritmn* (SHA-3) yang terbaru[3].



Gambar 4. Proses Super Enkripsi RSA-AES untuk menghasilkan Tanda Tangan Digital

Selanjutnya *message digest* (md0) dari dokumen masuk proses enkripsi menggunakan kunci *private* yang dihasilkan dari algoritma RSA. Algoritma RSA ini merupakan sistem kriptografi asimestris yang dapat digunakan untuk memberikan layanan *privacy* dan keaslian data digital sehingga banyak digunakan untuk mengamankan lalu lintas dokumen elektronik melalui internet[3]. Untuk meningkatkan keamanan pada penelitian ini dilakukan proses enkripsi sebanyak dua kali seperti pada gambar 2. Setelah *message digest* dienkripsi mengunakan RSA lalu dienkripsi kembali menggunakan algoritma AES. *Advance Encryption Standard* (AES) cukup berbeda dengan RSA, karena merupakan kriptografi kunci simetris, yaitu sistem kriptografi menggunakan kunci yang sama untuk proses enkripsi dan dekripsinya. AES merupakan algoritma yang memproses data dalam ukuran blok 128, 256 atau 512 bit. Algoritma ini juga memiliki tingkat keamanan dan performa yang bagus[12]. Proses enkripsi AES ini lah yang menghasilkan kode tanda tangan digital. Kode tanda tangan digital selanjutnya masuk proses pembangkitan kode QR, untuk memudahkan proses penyisipannya pada dokumen. Gambar dari QR-code kemudian dimasukan pada dokumen sertifikat elektronik yang kemudia dikirimkan pada pihak-pihak yang berhak menerimanya.

Sedangkan untuk kebutuhan pengecekan otentifikasi sertifikat elektronik tersebut, maka proses *verify* pada tanda tangan digital dilakukan. Proses ini dilakukan dengan membaca QR-code terlebih dahulu untuk mendapatkan kode tanda tangan digital. Kemudia kode tersebut masuk proses dekripsi berganda, yaitu dekripsi dengan AES dan dekripsi menggunakan kunci public pada RSA. Proses enkripsi ini akan mengembalikan *message digest* asli(md0) yang dibuat pada proses *sign*. Sedangkan untuk memverifikasi keaslian dokumen, diperlukan adanya inputan data yang tercantum pada dokumen sertifikat elektronik. Data tersebut masuk proses *hashing* untuk mendapatkan *message digest* (md1). Jika message digest yang didapat dari sertifikat elektronik (md1) ini sama dengan *message digest* asli (md0), maka dapat dipastikan sertifikat tersebut asli (integritas data terjamin). Namun jika dihasilkan *message digest* (md1) yang berbeda, maka patut dicurigai adanya modifikasi data pada sertifikat tersebut.

2.4. Implementasi & Pengujian

Setelah desain tanda tangan digital dengan superenkripsi telah dibuat, kemudia dibangun aplikasi yang merupakan perwujudan dari rancangan tersebut dengan menggunakan HTML dan PHP untuk versi webnya. Sedangkan untuk kemudahan proses verifikasi dibangun aplikasi berbasis mobile dengan tambahan fasilitas untuk membaca QR-code.

Untuk dapat menguji peningkatan keamanan dari superenkripsi yang dirancang, dilakukan perhitungan waktu proses enkripsi dna dekripsi untuk sistem kriptografi dengan RSA saja dan superenkripsi RSA-AES, kemudian dibandingkan hasil penghitungan keduanya. Selanjutnya dihitung nilai entropi untuk melihat keacakan hasil enkripsinya[13] dari sistem kriptografi dengan RSA saja dan superenkripsi RSA-AES, kemudian dibandingkan hasil penghitungan keduanya. Dan terakhir untuk mengukur tingkat perubahan cipherteks dari plainteks yang berbeda 1 bit, dilakukan uji *avalanche effect* karena superenkripsi ini menggunakan mode blok.

3. Hasil dan Pembahasan

Sistem yang dibangun merupakan aplikasi berbasis web yang dapat diakses oleh petugas dari pihak yang menerbitkan sertifikat elektronik. Sistem ini memiliki fasilitas input data sertifikat, proses penandatangan dan verifikasi keaslian sertifikat. Selain itu, dibangun juga aplikasi verifikator sertifikat yang dibangun berbasis mobile. Aplikasi mobile ini dapat digunakan oleh siapa saja yang akan mengecek keaslian sertifikat elektronik untukk berbagai keperluan lainnya.

3.1. Proses Tanda Tangan Digital

Alur pada sistem tanda tangan digital ini, pada proses dimulai dengan menginput plainteks terlebih dahulu, lalu plainteks tersebut pertama-tama diambil message digestnya menggunakan fungsi SHA-3. Kemudian message digest diproses oleh RSA dan menghasilkan Cipherteks. Selanjutnya Cipherteks di proses kembali oleh AES dan menghasilkan Cipherteks lalu disimpan. Jika ingin menghasilkan dekripsi atau bentuk yang semula maka lakukan kembali tetapi dengan kebalikannya.

Proses Super Enkripsi dengan penggabungan dua Cipher untuk menghasilkan hasil cipherteks yang sulit untuk dipecahkan, pertama dengan memasukan plainteks lalu di proses dengan algoritma RSA sehingga menghasilkan sebuah Cipherteks, selanjutnya Cipherteks tersebut di proses kembali oleh AES dan menghasilkan sebuah Cipherteks dan langsung tersimpan ke database yang tersedia.

Data yang perlu dimasukan adalah data-data yang tercantum pada sertifikat yaitu nomor sertifikat, nama peserta yang akan menerima sertifikat, nama kegiatan atau kursus, nama pejabat pengesah sertifikat dan tanggal diterbitkan sertifikat. Contoh proses superenkripsi dapat dilihat pada tabel 1 berikut:

Tabel 1. Hasil Enkripsi dan pembangkitan QR-code

Data Sertifikat	Data no.sertifikat : 001/WEBINAR/II/2020 Nama peserta : Dilah Nur Padilah Jenis pelatihan : Webinar Kupas Tuntas Pemrograman Web Pejabat pengesah: Dr. Sipuan ,M.Sc Tanggal diterbitkan : 1 Januari 2019
Plaintext	001/WEBINAR/II/2020|DilahNurFadilah|WebinarTips&TrikSeputarPemrogramanWeb|01/01/2019|Dr.Sipuan,M.Sc
Message Digest (SHA-3)	5f4d45f0eabfd403b8b0416a6f310ebf5bf213d953821e000eec3c1123a71e6b (512 bit)
Superenkripsi: - RSA - AES-128-CBC	MIsipjlgP3kHVc/rWRtN03v7HnMZRWaX94U+7fCv8vx/Euej0LHcQdBcCmMB5/4PVbDd Zn3eNt7d61qL6FeqDUxD9teFUNGqencA46CLaJtSNinzt0HReZVe92O/VKFy (1024 bit)
QR-code	

3.2. Arsitektur Sistem

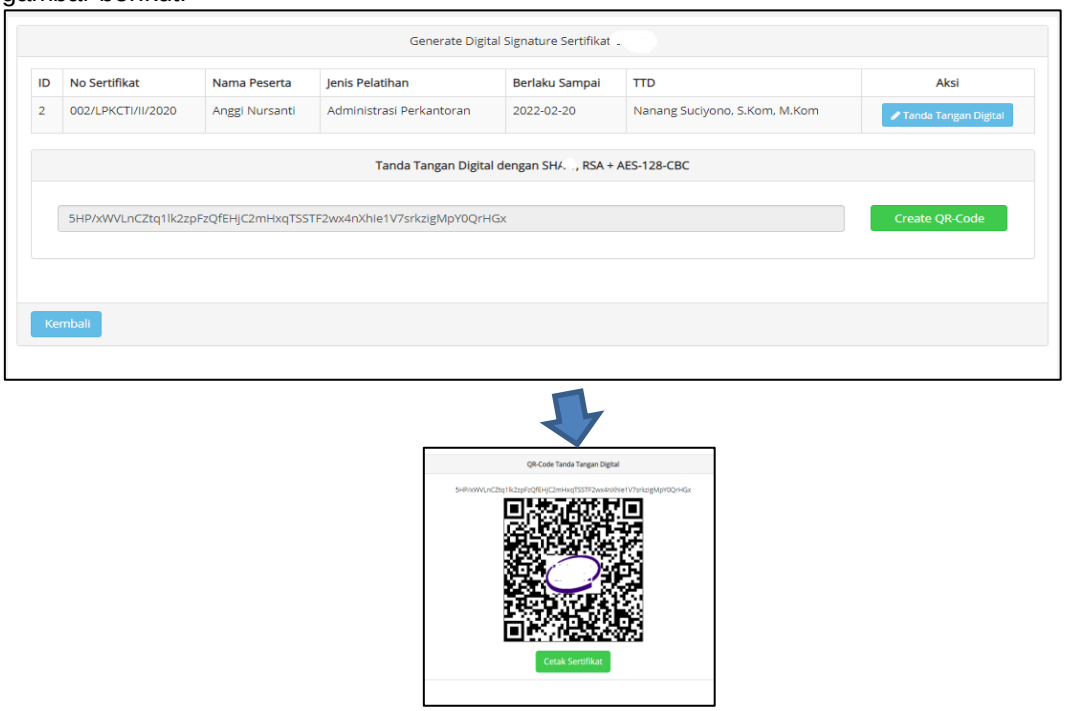
Sistem ini memiliki 2 proses utama yaitu: 1) input data sertifikat yang didalamnya dilakukan proses membangkitan kode tanda tangan digital dan QRcode; dan 2) proses verifikasi

ISSN (Printed) : 2579-7271
ISSN (Online) : 2579-5406

dengan membaca QR-code, input data pada sertifikat dan pencocokan data sesuai kode tanda tangan digital asli yang tersembunyi dibalik QR-code.

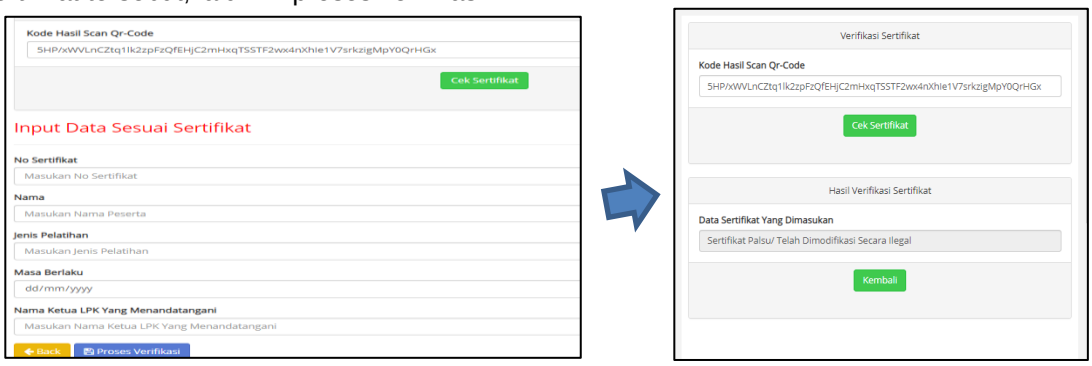
Pada implementasinya, sistem pembangkitan tanda tangan digital berbasis web memiliki prosedur login bagi user yang akan menggunakannya. User disini adalah petugas yang ditunjuk oleh pihak penerbit sertifikat digital untuk mengelola data sertifikat seperti pada gambar 6, membuat sertifikat elektronik sampai mengirimkan sertifikat tersebut melalui email pada masing-masing partisipan kegiatan.

Untuk rangkaian proses pembubuhan tanda tangan digital user memilih data sertifikat, kemudian memproses pembangkitan kode tanda tangan digital. Setelah kode didapat, masuk proses *generate* QR-code, lalu pilih cetak sertifikat elektronik. Secara detailnya dapat dilihat pada gambar berikut.



Gambar 5. Proses Pembangkitan Tanda Tangan Digital

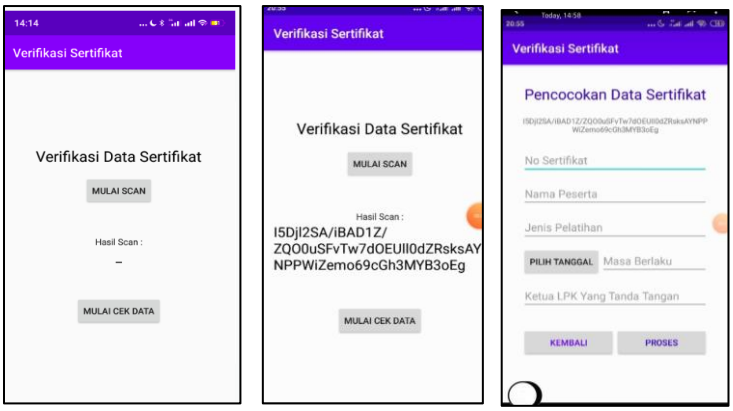
Sedangkan untuk proses verifikasi, user memiliki fasilitas verifikasi pada website ini dengan menambahkan alat pembaca QR-Code. Mula-mula user menggunakan alat membaca QR-code yang tertera pada sertifikat, kemudian menginputkan data-data yang tercantum pada sertifikat tersebut, lalu klik proses verifikasi.



Gambar 6. Proses Verifikasi Keaslian Sertifikat pada *Website User*

Selain verifikasi oleh user melalui *website*, proses ini juga disediakan aplikasi khusus berbasis mobile untuk dapat digunakan oleh penerima sertifikat untuk mengecek keaslian data sertifikat elektronik dengan tampilan seperti pada gambar di bawah ini. Karena verifikator ini berjalan pada *smartphone* yang sudah dilengkapi kamera, sehingga tidak memerlukan alat tambahan sebagai pembaca QR-*code*nya.

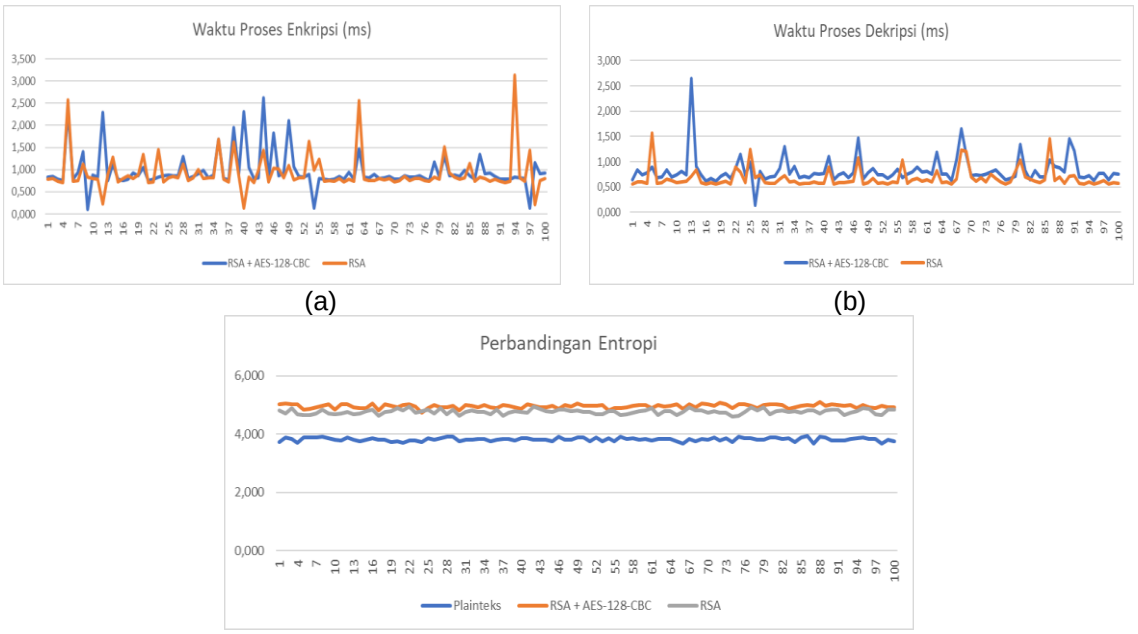
ISSN (Printed) : 2579-7271
ISSN (Online) : 2579-5406



Gambar 7. Verifikasi pada Aplikasi Berbasis *Mobile*

3.3. Pengujian kualitas enkripsi RSA-AES

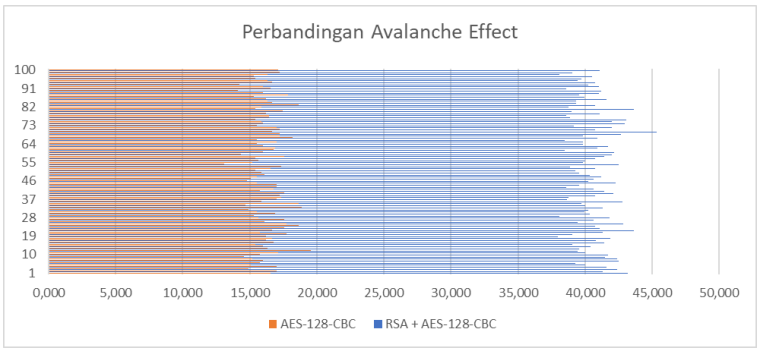
Dilakukan pengujian pada 100 data sertifikat suatu kegiatan workshop online, dengan mengukur waktu proses enkripsi, proses dekripsi, nilai entropi, dan nilai dari *avalanche effect*.



Gambar 8. Grafik Perbandingan Kualitas Enkripsi Sistem Kriptografi Kombinasi RSA-AES dengan Sistem Kriptografi RSA

Pengujian kualitas enkripsi pertama dilihat dari segi kecepatan proses enkripsi dan dekripsi, serta nilai entropi dari cipherteks yang dihasilkan. Sistem kriptografi untuk tangan digital yang hanya menggunakan RSA saja dibandingkan dengan penggunaan super enkripsi (kombinasi) RSA – AES. Dari data waktu proses RSA dan Super Enkripsi, dapat dilihat pada gambar 8 (a) diatas, dilakukan percobaan pada 100 plainteks dengan variasi ukuran file yang berbeda didapatkan rata-rata waktu proses enkripsi RSA 0,92 milisecond sedangkan enkripsi super enkripsi 0,96 milisecond. Dengan perbedaan 0,04 milisecond tidak akan begitu terasa, sehingga kualitas super enkripsi ini dapat dianggap bagus. Begitu juga dengan waktu proses dekripsi berdasarkan gambar 8 (b), hasil rata-rata yang didapat dari algoritma RSA adalah 0,67 milisecon dan hasil rata-rata waktu dekripsi dari super enkripsi adalah 0,83 milisecond. Dengan perbedaan 0,16 milisecond tidak akan begitu terasa, sehingga kualitas super enkripsi ini dapat dianggap bagus.Sedangkan dari segi entropi, dari gambar 8 (c) diatas dapat ditentukan bahwa nilai entropi cipherteks hasil Super Enkripsi 4,96 lebih unggul dibanding entropi cipherteks hasil RSA 4,77. Nilai entropi yang ideal adalah mendekati 8 dengan demikian sistem enkripsi yang dirancang aman dari serangan[19].

ISSN (Printed) : 2579-7271
ISSN (Online) : 2579-5406



Gambar 9. Grafik Perbandingan Kualitas Enkripsi Sistem Kriptografi Kombinasi RSA-AES dengan Sistem Kriptografi AES

Gambar 9 memperlihatkan hasil pengujiaan avalanche effect pada proses enkripsi AES dan super enkripsi RSA-AES. Plainteks yang digunakan untuk menguji avalanche effect dalam menentukan jumlah putaran yang akan digunakan dalam proses enkripsi, jumlah perubahan bit karakter dari plainteks awal ke plainteks yang baru menghasilkan 1 bit perubahan saja. Pengujian *avalanche effect* dilakukan untuk mencari seberapa besar pengaruh perubahan plainteks terhadap cipherteks biasanya digunakan pada sistem kriptografi cipher blok seperti AES. Secara visual dari pengujian yang dilakukan peningkatan avalanche effect AES dengan nilai rata-rata 16,31% sementara avalanche effect Super Enkripsi dengan nilai rata-rata 40,61%. Dari data diatas dapat ditentukan bahwa nilai avalanche effect Super Enkripsi lebih bagus karena nilai dari *avalanche effect* mendekati 50%.

4. Kesimpulan

Berdasarkan hasil penelitian yang didapat, maka dapat disimpulkan bahwa:

1) Penggunaan QR-code pada sertifikat elektronik dapat bermanfaat untuk mempermudah membubuhan tanda tangan digital yang memungkinkan memiliki kode yang cukup panjang, serta proses verifikasi sertifikat menjadi lebih simple karena cukup menggunakan QR-code reader untuk mendapatkan kode tanda tangan digital dari sertifikatnya.
2) Untuk peningkatan keamanan, penggunaan SHA-3 dan superenkripsi RSA-AES menunjukan tingkat kualitas enkripsi yang bagus, dimana:
   a. Waktu proses masih relatif sama dibandingkan waktu proses satu kali enkripsi RSA saja
   b. Nilai entropi 4,96 yang mendekati 8 membuktikan bahwa persebaran karakter pada kode cipherteks yang merata tidak menumpuk pada karakter-karakter tertentu sehingga akan sulit diserang menggunakan analisis frekuensi
   c. Nilai *avalanche effect* 40,61% membuktikan perubahan kode *chiperteks* sudah sangat acak.

Untuk pengembangan penelitian selanjutnya disarankan untuk melakukan perbaikan dari sisi waktu proses enkripsi dan dekripsi yang lebih cepat dan besar file hasil yang lebih kecil, dengan memilih pasangan algoritma kriptografi lainnya, sehingga proses *sign* dan *verify* menjadi lebih cepat dan mudah.

Daftar Pustaka

[1] R. M. K. Anaway Irianti Mansyur, Rif'ah Purnamasari, "Webinar Sebagai Media Bimbingan Klasikal Sekolah Untuk Pendidikan Seksual Berbasis Online (Meta Analisis Pedagogi Online)," *J. Bimbing. Konseling Univ. Syiah Kuala*, Vol. 4, No. 1, Pp. 26–30, 2019.
[2] Y. Anshori, A. Y. Erwin Dodu, and D. M. P. Wedananta, "Implementasi Algoritma Kriptografi Rivest Shamir Adleman (RSA) pada Tanda Tangan Digital," *Techno.Com*, vol. 18, no. 2, pp. 110–121, 2019, doi: 10.33633/tc.v18i2.2166.
[3] R. A. Azdy, "Tanda tangan Digital Menggunakan Algoritme Keccak dan RSA," *J. Nas. Tek. Elektro dan Teknol. Inf.*, vol. 5, no. 3, pp. 184–191, 2016, doi: 10.22146/jnteti.v5i3.255.
[4] F. Nuraeni, Y. H. Agustin, and I. M. Muharam, "Implementasi Tanda Tangan Digital Menggunakan RSA dan SHA-512 Pada Proses Legalisasi Ijazah," *Knsi 2018*, pp. 864–869, 2018.
[5] A. G. P. Suratma and A. Azis, "Tanda Tangan Digital Menggunakan Qr Code Dengan Metode Advanced Encryption Standard," *Techno*, vol. 18, no. 1, pp. 59–68, 2017.

[6] S. 18004, "Information Technology Automatic Identification and Data Capture Techniques Bar Code Symbology QR Code," *Switzerland : International Standard*, 2000.
[7] E. Ardhianto and N. Wakhidah, "Pengembangan Metode Otentikasi Keaslian Ijasah Dengan Memanfaatkan Gambar Qr Code," *J. Transform.*, vol. 13, no. 2, p. 35, 2016, doi: 10.26623/transformatika.v13i2.325.
[8] L. Kartika and Yudi, "Rancang Bangun Aplikasi Penyembunyian Pesan QRCode Dengan Menggunakan Metode Caesar Cipher Berbasis Android," *J. FTIK*, vol. 1, no. 1, pp. 511–518, 2020.
[9] A. Farissi and M. Fachrurrozi, "Algoritma RSA Kombinasi dan Skema QR Code untuk Mengamankan Data Penjualan Tiket Online," *Pros. Annu. Res. Semin. 2017 Comput. Sci. ICT*, vol. 3, no. 1, pp. 3–7, 2017.
[10] A. E. Mezher, "Enhanced RSA Cryptosystem based on Multiplicity of Public and Private Keys.," *Int. J. Electr. Comput. Eng.*, vol. 8, 2018.
[11] E. C. Prabowo and I. Afrianto, "Penerapan Digital Signature Dan Kriptografi Pada Otentikasi Sertifikat Tanah Digital," *Komputa J. Ilm. Komput. dan Inform.*, vol. 6, no. 2, pp. 83–90, 2017, doi: 10.34010/komputa.v6i2.2481.
[12] U. Thirupalu, R. Scholar, and E. K. Reddy, "Performance Analysis of Cryptographic Algorithms in the Information Security," *Int. J. Eng. Res. Technol.*, vol. 8, no. 2, pp. 1–6, 2020, [Online]. Available: www.ijert.org.
[13] E. Setyaningsih, *Kriptografi & Implementasinya Menggunakan Matlab*. Yogyakarta: ANDI, 2015.
[14] E. Setyaningsih, C. Iswahyudi, and N. Widyastuti, "Konsep Super Enkripsi untuk Meningkatkan Keamanan Data Citra," in *Prosiding Seminar Nasional Sistem & Teknologi Informasi (SNASTI) 2011*, 2011, p. ISLP 7-ISLP 10.
[15] F. Kurniawan, A. Kusyanti, and H. Nurwarsito, "Analisis dan Implementasi Algoritma SHA-1 dan SHA-3 pada Sistem Autentikasi Garuda Training Cost," *J. Pengemb. Teknol. Inf. dan Ilmu Komput.*, vol. 1, no. 9, pp. 803–812, 2017, [Online]. Available: http://j-ptiik.ub.ac.id/index.php/j-ptiik/article/view/247.
[16] H. A. Kartika, A. Kusyanti, and M. Data, "Implementasi Algoritme SPECK dan SHA-3 Pada Database Rekam Medik," *J. Pengemb. Teknol. Inf. dan Ilmu Komput. Univ. Brawijaya*, vol. 2, no. 12, pp. 6942–6951, 2018.
[17] F. Nuraeni, Y. H. Agustin, and A. E. Purnama, "Implementasi Caesar Cipher & Advanced Encryption Standar (Aes) Pada Pengamanan Data Pajak Bumi Bangunan," *J. Ilm. Matrik*, Vol. 22, No. 2, Pp. 187–194, 2020, [Online]. Available: Http://Journal.Binadarma.Ac.Id/Index.Php/Jurnalmatrik/Article/View/949.
[18] H. F. Isnaini And K. Karyati, "Penerapan Skema Tanda Tangan Schnorr Pada Pembuatan Tanda Tangan Digital," *Pythagoras J. Pendidik. Mat.*, Vol. 12, No. 1, P. 57, 2017, Doi: 10.21831/Pg.V12i1.11631.
[19] P. Irfan, "Aplikasi Enkripsi Citra Menggunakan Algoritma Kriptografi Arnold Cat Map Dan Logistic Map," *J. Matrik*, Vol. 16, No. 1, Pp. 96–104, 2016.