

**TANDA TANGAN DIGITAL MENGGUNAKAN QR CODE
DENGAN METODE ADVANCED ENCRYPTION STANDARD**

TESIS



Oleh :

ABDUL GANI PUTRA SURATMA

1411600727

**PROGRAM STUDI: MAGISTER ILMU KOMPUTER (MKOM)
PROGRAM PASCA SARJANA
UNIVERSITAS BUDI LUHUR
JAKARTA
2016**

TANDA TANGAN DIGITAL MENGGUNAKAN QR CODE DENGAN METODE ADVANCED ENCRYPTION STANDARD

TESIS

Diajukan untuk memenuhi salah satu persyaratan
memperoleh gelar Magister Ilmu Komputer



Oleh :

ABDUL GANI PUTRA SURATMA

1411600727

**PROGRAM STUDI: MAGISTER ILMU KOMPUTER (MKOM)
PROGRAM PASCA SARJANA
UNIVERSITAS BUDI LUHUR
JAKARTA
2016**



PROGRAM STUDI MAGISTER ILMU KOMPUTER
PROGRAM PASCASARJANA
UNIVERSITAS BUDI LUHUR

LEMBAR PERNYATAAN

Saya yang bertanda tangan dibawah ini,

Nama : Abdul Gani Putra Suratna

Nim : 1411600727

Program Studi : Magister Ilmu Komputer

Fakultas : Program Pascasarjana

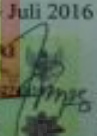
Menyatakan bahwa Tesis yang berjudul :

Aplikasi tanda tangan digital menggunakan QRCode dengan metode advanced encryption standard.

1. Merupakan hasil karya tulis ilmiah sendiri dan bukan merupakan hasil karya yang pernah diajukan untuk memperoleh gelar akademik oleh pihak lain.
2. Saya izinkan untuk dikelola oleh Universitas Budi Luhur sesuai dengan norma hukum dan etika yang berlaku.

Pernyataan ini saya buat dengan penuh tanggung jawab dan saya bersedia menerima konsekuensi apapun sesuai aturan apabila di kemudian pernyataan ini tidak benar.

Jakarta, 25 Juli 2016



(Abdul Gani Putra Suratna)

CERDAS BERBUDI LUHUR

i

PROGRAM STUDI MAGISTER ILMU KOMPUTER
PROGRAM PASCASARJANA
UNIVERSITAS BUDI LUHUR

LEMBAR PENGESAHAN

Nama : Abdul Gani Putra Suratma
NIM : 1411600727
Program Studi : Magister Ilmu Komputer
Konsentrasi : Rekayasa Komputasi Terapan
Jenjang Studi : Strata Dua (S2)
Judul Tesis : Tanda tangan digital menggunakan QRCode dengan metode advanced encryption standard

Jakarta, 25 Juli 2016

Tim Penguji :

Ketua,
(Ir. Wendi Usino, MM, M.Sc, Ph.D)

Anggota,
(Rusdah, M.Kom)

Pembimbing,
(Dr., Ir.Nazori Az, M.T)

Tanda Tangan :

Ketua Program Studi
(Dr. M. Syafrullah, M.Kom, M.Sc)

ABSTRAK

Tanda tangan digital (*digital signature*) adalah sebuah skema matematis yang secara unik mengidentifikasi seorang pengirim, sekaligus untuk membuktikan keaslian dari pemilik sebuah pesan atau dokumen digital, sehingga sebuah tanda tangan digital yang *otentik* (sah), sudah cukup menjadi alasan bagi penerima untuk percaya bahwa sebuah pesan atau dokumen yang diterima adalah berasal dari pengirim yang telah diketahui. Perkembangan teknologi memungkinkan adanya tanda tangan digital yang dapat digunakan untuk melakukan pembuktian secara matematis, sehingga informasi yang didapat oleh satu pihak dari pihak lain dapat diidentifikasi untuk memastikan keaslian informasi yang diterima. Tanda tangan digital merupakan mekanisme otentikasi yang memungkinkan pembuat pesan menambahkan sebuah kode yang bertindak sebagai tanda tangannya. Tujuan dari penelitian ini menerapkan *QR Code* atau yang dikenal dengan istilah *QR (Quick Respon)* dan Algoritma yang akan ditambahkan yaitu *AES (Advanced Encryption Standard)* sebagai tanda tangan digital sehingga hasil dari penelitian penerapan *QR Code* menggunakan algoritma *Advanced Encryption Standard* sebagai tanda tangan digital dapat berfungsi sebagai otentikasi tanda tangan pimpinan serta verifikasi dokumen pengambilan barang yang sah. dari penelitian ini akurasi klasifikasi *QR Code* dengan menggunakan *naïve bayes classifier* sebesar 90% dengan *precision* positif sebesar 80% dan *precision* negatif sebesar 100%.

Kata kunci : *Digital Signature, QR Code, Kriptografi, AES, Security Validation*

ABSTRACT

Digital signature is a schematic mathematically that uniquely identifies a sender , as well as to prove the authenticity of the owner of a message or document digitally, so that a digital signature is authentic (valid), is reason enough for the recipient to believe that a message or documents received are coming from unknown senders. The development of technology enabling their digital signature that can be used to prove mathematically, so that the information obtained by one party from the other party can be identified to ensure the authenticity of the information received. The digital signature is an authentication mechanism that allows the manufacturer to add a code message that acts as a signature. The purpose of this study apply the QR Code or which is known as QR (Quick Response) and algorithms to be added , namely AES (Advanced Encryption Standard) as a digital signature so that the results of the research application of the QR Code using Advanced Encryption Standard algorithm as a signature can function as a digital signature authentication and verification of document retrieval leaders legitimate goods . This research classification accuracy of the QR Code using a naïve Bayes classifier with a precision of 90% positive and 80% negative precision of 100% .

Keywords : Digital Signature, QR Code, Kriptografi, AES, Security Validation

PENGANTAR

Puji dan syukur penulis panjatkan kepada Allah SWT atas segala karunia-Nya sehingga penulis dapat menyelesaikan penulisan penelitian ini. Penelitian ini disusun sebagai syarat mendapat gelar Magister Ilmu Komputer. Penulis sadar bahwa masih terdapat kekurangan dalam penulisan ini yang harus diperbaiki. Penulis sangat mengharapkan kritik dan saran yang membangun untuk memperbaiki penulisan tesis ini sehingga nantinya akan menghasilkan penelitian yang lebih baik. Penulis banyak sekali mendapatkan bantuan dan bimbingan dalam penulisan tesis ini dan dengan segala kerendahan hati saya mengucapkan terimakasih sebesar-besarnya kepada ;

1. Kedua orang tua.
2. Dr., Ir.Nazori Az, M.T selaku Pembimbing, yang memberikan dorongan, masukan kepada penulis.
3. Teman-teman Pasca Sarjana Universitas Budi Luhur.

Penulis menyadari, bahwa masih banyak terdapat kekurangandari penelitian ini, karena itu penulis mengharapkan kritik dan saran yang bersifat membangun untuk kesempurnaan penelitian tesis ini. Semoga penelitian tesis ini dapat memberikan manfaat dalam perkembangan Teknologi Informasi di Indonesia khususnya di Universitas Budi Luhur.

Jakarta, 25 Juli 2016

Abdul Gani Putra Suratma

DAFTAR ISI

Halaman

ABSTRAK	ii
ABSTRACT	iv
PENGANTAR	v
DAFTAR ISI	vi
DAFTAR GAMBAR	viii
DAFTAR TABEL	x
DAFTAR LAMPIRAN	xi
BAB I PENDAHULUAN	1
1.1 Latar Belakang	1
1.2 Identifikasi Masalah	2
1.3 Rumusan Masalah	2
1.4 Batasan Masalah	2
1.5 Tujuan dan Manfaat Penelitian	3
1.6 Tata Urut Penulisan	3
BAB II LANDASAN TEORI DAN KERANGKA KONSEP	4
2.1 Tinjauan Pustaka	4
2.1.1. Pengertian Quick Response Code	4
2.1.2. Pengertian Advanced Encryption Standard (AES)	10
2.1.3. Visual Studio	18
2.1.4. ASP.NET	18
2.1.5. Bahasa Pemrograman C Sharp (C#)	19
2.1.6. SQL Server	19
2.1.7. Confusion Matrix	20
2.1.8. FlowChart	22
2.2 Tinjauan Studi	25

2.3	Tinjauan Obyek Penelitian	27
2.4	Kerangka Konsep /Pola Pikir Pemecahan Masalah	30
2.5	Hipotesis.....	31
BAB III METODOLOGI DAN RANCANGAN PENELITIAN		32
3.1	Metode Penelitian.....	32
3.2	Instrumentasi	32
3.3	Teknik Perancangan dan Pengujian Sistem	33
3.3.1.	Teknik Perancangan	33
3.3.2.	Teknik pengujian.....	38
3.3.3.	Langkah – langkah penelitian	38
3.4	Jadwal penelitian	39
BAB IV PEMBAHASAN HASIL PENELITIAN.....		41
4.1	Analisa Algoritma Kriptografi	41
4.2	Perancangan Sistem.....	41
4.3	Hasil Implementasi.....	41
4.4	Pengujian Sistem	46
BAB V PENUTUP.....		52
DAFTAR PUSTAKA		53
DAFTAR LAMPIRAN.....		54

DAFTAR GAMBAR

Gambar	Halaman
Gambar II-1 Contoh <i>QR Code</i>	4
Gambar II-2 <i>Anatomi QR Code</i>	5
Gambar II-3 Codeword Data.....	9
Gambar II-4 Proses Input Bytes, State Array, dan Output.....	11
Gambar II-5 Proses Input Bytes, State Array, dan Output.....	13
Gambar II-6 Pemetaan pada Setiap Byte dalam State.	15
Gambar II-7 Transformasi ShiftRows.....	15
Gambar II-8 Ilustrasi Proses Dekripsi <i>AES</i>	16
Gambar II-9 Transformasi <i>InvShiftRows</i>	17
Gambar II-10 Flowchart.....	24
Gambar II-11 Struktur Organisasi.....	28
Gambar II-12 Prosedur Penanda Tanganan.	30
Gambar II-13 Kerangka pemikiran	30
Gambar III-1 Proses tanda tangan digital.	33
Gambar III-2 Proses Enkripsi pada <i>QR Code</i>	34
Gambar III-3 Proses Dekripsi pada <i>QR Code</i>	34
Gambar III-4 Teknik Penerapan Tanda tangan digital.....	35
Gambar III-5 Proses Enkripsi dan Dekripsi	35
Gambar III-6 Proses pembuatan Plaintext	36
Gambar III-7 Proses pembuatan <i>QR Code</i>	36
Gambar III-8 Proses Scan Dokumen.....	37
Gambar III-9 Proses Dekripsi Chiphertext	37
Gambar III-10 Proses Verifikasi Dokumen	38
Gambar III-11 Langkah –langkah penelitian	38
Gambar IV.1 Alur sistem	42
Gambar IV-2 Login.....	42
Gambar IV-3 Transfer.....	43
Gambar IV-4 Halaman Home Pimpinan.....	43

Gambar IV-5 Transfer departmen.....	44
Gambar IV-6 Transfer detail sebelum approved.....	44
Gambar IV-7 Transfer detail setelah approved.....	45
Gambar IV-8 Scanner.	45
Gambar IV-9 Proses Scan dokumen.	46



DAFTAR TABEL

Tabel	Halaman
Tabel II-1 Spesifikasi QR Code.	8
Tabel II-2 Perbandingan Jumlah Round dan Key.	11
Tabel II-3 S-Box SubBytes.	14
Tabel II-4 Inverse S-Box:	17
Tabel II.5 Tabel matrik	21
Tabel II.6 Simbol <i>Flowchart</i>	22
Tabel II- 7 Tinjauan Studi.	26
Tabel III.1 Jadwal Penelitian.....	39
Tabel IV.1 Pengujian Akurasi Klasifikasi <i>QR Code</i>	47
Tabel IV.2 Confusion matrix:	50
Tabel IV.3 Perhitungan Confusion Matrix.....	50

DAFTAR LAMPIRAN

Lampiran	Halaman
Lampiran 1: Dokumen Approved	54
Lampiran 2 : Dokumen tidak disetujui	55



DAFTAR PUSTAKA

- Ashford, R., (2010). QR Codes and Academic Libraries. *College & Research Libraries News*, Vol.71, No.10, 526 – 530.
- Ariadi, 2011, Analisis dan Perancangan Kode Matriks Dua Dimensi Quick Response (QR) Code. <http://repository.usu.ac.id/bitstream/123456789/29816/4/Chapter%20II.pdf> (diakses pada tanggal 21 April 2016).
- Denso Wave Inc. 2016. About QR Code.
<http://www.denso-wave.com/qrcode/aboutqr-e.html> (diakses 21 April 2016)
- Dennis, A., Wixon B.H., dan Tegarden, D., 2009, *Sistem Analysis and Design with UML 3rd Edition*, John Wiley & Sons, Inc
- Hartanto, B. 2008, *Memahami Visual C#.NET secara mudah*, Penerbit ANDI, Yogyakarta.
- Jamaludin, ST. 2006, *Belajar sendiri .net dengan visual C# 2005*, Penerbit ANDI, Yogyakarta.
- Lianty dan Venynova, 2014, *Pengembangan Sistem Informasi Manajemen E-Pengadaan Langsung (SIMPEL) Berbasis Web Application : Studi Kasus Pusat LPSE Kementerian Keuangan*, Hal 47, Tesis, Jakarta: Universitas Budi Luhur.
- Noertjahya dan Agustinus 2002, *Studi Analisis Rapid Application Development sebagai salah satu alternative metode pengembangan perangkat lunak*, Universitas Kristen Petra, Jakarta, Indonesia.
- Setiawan, Ade, Deden dan Endrawan, 2011, *Rapid Application Development, Sistem Informasi*, Universitas Gunadarma, Jakarta, Indonesia. Hal 9.
- Sugiyono. 2013, *Metode Penelitian Pendidikan (Pendekatan Kuantitatif, Kualitatif, dan R&D)*. Bandung : Alfabeta.
- Bramer, Max. (2007). *Principles of Data Mining*.
London: Springer. ISBN-10: 1-84628-765-0, ISBN-13: 978-1-84628-765-7.