PENERAPAN TANDA TANGAN DIGITAL UNTUK VERIFIKASI LEMBAR PENGESAHAN SKRIPSI MENGGUNAKAN METODE *KECCAK* DAN *RSA*

PROPOSAL PENELITIAN

MUHAMMAD AKBAR

13020160073

PROGRAM STUDI TEKNIK INFORMATIKA

FAKULTAS ILMU KOMPUTER

UNIVERSITAS MUSLIM INDONESIA

MAKASSAR

2021

YAYASAN WAKAF UMI
UNIVERSITAS MUSLIM INDONESIA
FAKULTAS ILMU KOMPUTER
PROGRAM STUDI TEKNIK INFORMATIKA
Kampus II UMI, Jl. Urip Sumoharjo KM. 05 Telp. (0411)447562, Makassar 90231

Bismillahirrohmanirrohiim

LEMBAR PENGESAHAN SEMINAR PROPOSAL

Nama	:	MUHAMMAD AKBAR
Stambuk	:	13020160073
Program Studi	:	Teknik Informatika (S-1)
Judul Penelitian	:	PENERAPAN TANDA TANGAN DIGITAL UNTUK VERIFIKASI LEMBAR PENGESAHAN SKRIPSI MENGGUNAKAN *KECCAK* DAN *RSA*

Berdasarkan Surat Penunjukan Dekan Fakultas Ilmu Komputer Universitas Muslim Indonesia Nomor : 0127/H.22/FIK-UMI/I/2020 tentang penetapan Dosen Pembimbing.

Makassar, Maret 2021

Dosen Pembimbing

Pembimbing Utama	Pembimbing Pendamping
(Poetri Lestari L.B, S.Kom.,M.T)	**(Farniwati Fattah,S.T., M.T)**

Mengetahui
Ketua Program Studi Teknik Informatika

(Tasrif Hasanuddin, S.T., M.Cs)

YAYASAN WAKAF UMI
UNIVERSITAS MUSLIM INDONESIA
FAKULTAS ILMU KOMPUTER
PROGRAM STUDI TEKNIK INFORMATIKA
Kampus II UMI, Jl. Urip Sumoharjo KM. 05 Telp. (0411)447562, Makassar 90231

Bismillahirrohmaanirrohiim

LEMBAR PERBAIKAN SEMINAR PROPOSAL

Berdasarkan berita acara Ujian Seminar Proposal Mahasiswa Program Studi Teknik Informatika (S1) pada tanggal, 17 Maret 2021, maka selaku panitia dan atas nama dosen pembimbing menyatakan bahwa:

Nama	:	MUHAMMAD AKBAR
Stambuk	:	13020160073
Program Studi	:	Teknik Informatika (S-1)
Judul Penelitian	:	PENERAPAN TANDA TANGAN DIGITAL UNTUK VERIFIKASI LEMBAR PENGESAHAN SKRIPSI MENGGUNAKAN METODE *KECCAK* DAN *RSA*

Telah menyelesaikan perbaikan, diperiksa, dan disetujui oleh tim penguji yang terdiri dari:

Makassar, Maret 2021

Pembimbing Utama	Pembimbing Pendamping
(Poetri Lestari L.B, S.Kom., M.T)	**(Farniwati Fattah,S.T., M.T)**

Dosen Penguji

1. Penguji 1 (.....)
2. Penguji 2 (.....)
3. Penguji 3 (.....)

Mengetahui

Ketua Program Studi Teknik I

(Tasrif Hasanuddin, S.T., M.Cs)

KATA PENGANTAR

Bismillahir rohmaani rohiim

Assalamu Alaikum Warahmatullahi Wabarakatuh.

Alhamdulillahi Robbil 'alamin, segala puji bagi *Allah Subhanallahu Wa Ta'ala*, yang Maha Menciptakan, Menghidupkan dan Mematikan, yang Rahmat-Nya meliputi langit dan bumi, dunia dan akhirat dan kepada-Nyalah semua akan kembali. Shalawat serta salam semoga senantiasa terlimpahkan kepada Rasul yakni Nabi Muhammad *Shallallahu 'Alaihi Wasallam*, beserta seluruh keluarga dan para sahabat beliau yang telah mengorbankan harta, diri dan keluarga demi untuk perjuangan agama Islam.

Tak lupa penulis mensyukuri segala Rahmat dan Karunia yang telah dilimpahkan sehingga penulis dapat menyelesaikan proposal ini dengan judul "Penerapan Tanda Tangan Digital Untuk Verifikasi Lembar Pengesahan Skripsi Menggunakan Metode Keccak Dan RSA". Proposal ini diajukan sebagai salah satu syarat dalam mencapai jenjang Sarjana Komputer (S1) yang nantinya dapat memberikan kontribusi kepada para pembacanya untuk dijadikan acuan dalam melakukan penelitian dibidang ilmu komputer kedepannya.

Berkat bimbingan dan bantuan dari berbagai pihak proposal ini dapat diselesaikan tepat pada waktunya. Oleh karena itu dengan hati yang tulus, penulis mengucapkan banyak terima kasih yang sebesar-besarnya. Terutama kepada orang tua penulis yaitu ayahanda penulis dan ibunda penulis yang selalu memberikan doa, kasih sayang dan dukungan baik moral maupun materil merupakan kekuatan besar bagi penulis untuk menyelesaikan proposal ini.

Proposal ini dapat penulis selesaikan dengan bantuan berbagai pihak, sehingga sudah sepantasnya penulis mengucapkan terima kasih yang sebesar-besarnya kepada:

1. Ibu Poetri Lestari L.B, S.Kom., M.T selaku pembimbing utama yang telah banyak membantu dan membimbing dalam penyelesaian proposal ini.
2. Ibu Farniwati Fattah,S.T., M.T selaku pembimbing pemdamping yang telah banyak membantu dan membimbing dalam penyelesaian proposal ini.

3. Kepada seluruh pihak yang tidak dapat disebutkan satu per satu, yang telah dengan tulus ikhlas memberikan doa dan motivasi kepada penulis sehingga dapat terselesaikan proposal ini.

Dengan begitu penulis menyadari bahwa dalam proposal ini masih jauh dari kesempurnaan. Oleh karena itu, penulis mengharapkan kritik dan saran yang mampu membangun penulis baik dari pembimbing, teman-teman dan pembaca untuk menyempurnakan proposal ini. Akhir kata semoga proposal ini dapat bermanfaat bagi masyarakat dan Mahasiswa Universitas Muslim Indonesia Makassar.

Wassalamu Alaikum Warahmatullahi Wabarakatuh.

Makassar, Maret 2021

Penulis

DAFTAR ISI

DAFTAR TABEL

DAFTAR GAMBAR

PENERAPAN TANDA TANGAN DIGITAL UNTUK VERIFIKASI LEMBAR PENGESAHAN SKRIPSI MENGGUNAKAN METODE *KECCAK* DAN *RSA*

A. Latar Belakang

Pengesahan dokumen tugas akhir mahasiswa Fakultas Ilmu Komputer Universitas Muslim Indonesia telah dapat dilakukan secara daring, mahasiswa yang skripsinya telah di ACC oleh kedua pembimbingnya, cukup mengirimkan lembar pengesahan skripsi kepada dosen pembimbing dan ketua program studi melalui melalui media sosial maupun *cloud storage.*

Dokumen digital lembar pengesahan skripsi yang telah diterima oleh dosen pembimbing mahasiswa dan ketua program studi ditanda tangani secara digital dengan cara menandatangani langsung dokumen digital, atau menambahkan salinan tanda tangan elektronik yang telah dibuat sebelumnya. Lembar pengesahan skripsi yang telah ditanda tangani selanjutnya dikirimkan kembali kepada mahasiswa yang bersangkutan

Lembar pengesahan skripsi yang telah diberi tanda tangan elektronik, telah dapat digunakan sebagai salah satu dokumen persyaratan mengikuti ujian tugas akhir, hal ini memberikan kemudahan karena lembar pengesahan skripsi mahasiswa dapat ditanda tangani kapan pun dimanapun dan dengan mudah dikirimkan kembali kepada mahasiswa selama memiliki akses ke internet

Dengan adanya kemudahan menandatangani lembar pengesahan skripsi secara elektronik juga memiliki kekurangan yaitu tanda tangan dapat diduplikasi sehingga dapat digunakan oleh pihak yang tidak bertanggung jawab untuk menandatangi lembar pengesahan skripsi tanpa sepengetahuan pemilik tanda tangan, sehingga lembar pengesahan skripsi yang telah ditanda tangani tidak dapat diverifikasi untuk menjamin keabsahannya

Atas dasar kekurangan dari tanda tangan elektronik, penulis berencana menggunakan tanda tangan digital untuk mengatasi kekurangan tanda tangan elektronik yang ditambahkan ke lembar pengesahan skripsi. Tanda tangan digital

berbeda dengan tanda tangan elektronik, tanda tangan digital adalah sebuah kombinasi unik dari fungsi *hash* dan enkripsi dengan metode asimetris (Schneier, 1995).

Pembuatan fungsi *hash* lembar pengesahan skripsi, penulis menggunakan metode Keccak, Keccak merupakan salah satu algoritme fungsi hash yang dirancang oleh Guido Bertoni, Joan Daemen, Michaël Peeteres, dan Gilles Van Assche (Bentivenga dkk, 2010). Keccak merupakan pemenang kompetisi SHA-3 *Cryptographic Hash Algorithm Competition* yang diselenggarakan oleh NIST dan telah dijadikan standar untuk algoritme fungsi *hash Secure Hash Algorithm* (SHA-3) yang baru (Romine, 2015)

Untuk enkripsi nilai *hash* penulis menggunakan metode RSA, RSA merupakan algoritma kriptografi kunci public (asimetris). Ditemukan pertama kali pada tahun 1977 oleh Ron Rivest, Adi Shamir, dan Len Adleman. Nama RSA sendiri diambil dari ketiga penemunya tersebut. Sebagai algoritma kunci publik, RSA mempunyai dua kunci, yaitu kunci publik dan kunci rahasia. RSA mendasarkan proses enkripsi dan dekripsinya pada konsep bilangan prima dan aritmetika modulo. Baik kunci enkripsi maupun dekripsi keduanya merupakan bilangan bulat. Kunci enkripsi tidak dirahasiakan dan diberikan kepada umum (sehingga disebut dengan kunci publik), namun kunci untuk dekripsi bersifat rahasia (kunci privat). Untuk menemukan kunci dekripsi, dilakukan dengan memfaktorkan suatu bilangan bulat menjadi faktor-faktor primanya (Ginting dkk, 2015)

B. Rumusan Masalah

Pada penelitian ini, rumusan masalah sebagai berikut:

1. Bagaimana merancangan aplikasi tanda tangan digital lembar pengesahan skripsi mahasiswa fakultas ilmu komputer menggukan metode Keccak dan RSA?
2. Bagaimana menverifikasi keabsahan lembar pengesahan skripsi mahasiswa fakultas Ilmu Komputer Universitas Muslim Indonesia?

C. Batasan Masalah

Batasan masalah pada penelitian ini adalah sebagai berikut:

1. Dokumen yang digunakan adalah lembar pengesahan skripsi berekstensi pdf.
2. Perancangan aplikasi tanda tangan digital berbasis website.

D. Tujuan Penelitian

Tujuan penelitian yang ingin dicapai adalah sebagai berikut:

1. Merancangan aplikasi tanda tangan digital lembar pengesahan skripsi mahasiswa fakultas ilmu komputer menggukan metode Keccak dan RSA Manfaat Penelitian
2. Verifikasi keabsahan lembar pengesahan skripsi mahasiswa Fakultas Ilmu Komputer Universitas Muslim Indonesia

E. Manfaat penelitian

Manfaat dengan adanya aplikasi tanda tangan digital lembar pengesahan skripsi mahasiswa Ilmu Komputer Universitas Muslim Indonesia mampu menjadi salah satu solusi untuk menverifikasi keabsahan lembar pengesahan skripsi.

F. Jadwal Penelitian

Adapun jadwal penelitian yang dilakukan ditunjukkan pada Tabel 1.

Tabel 1. Jadwal Penelitian

No	Tahap Penelitian	Maret 2021			April 2021				Mei 2021				Juni 2021				Juli 2021				Agustus 2021			
		2	3	4	1	2	3	4	1	2	3	4	1	2	3	4	1	2	3	4	1	2	3	4
1.	Identifikasi Masalah																							
2.	Analisis Kebutuhan Sistem																							
3.	Rancangan Sistem																							

No	Tahap Penelitian	Maret 2021			April 2021				Mei 2021				Juni 2021				Juli 2021				Agustus 2021			
		2	3	4	1	2	3	4	1	2	3	4	1	2	3	4	1	2	3	4	1	2	3	4
4.	Rancangan Bangun Program																							
5.	Uji Coba Program (*Testing*)																							
6.	Revisi Konsep dan Desain Rancangan																							
7.	Implementasi Program																							
8.	Pembimbingan Naskah Skripsi																							
9.	Penulisan Akhir Laporan																							
10.	Pendadaran																							

Adapun penjelasan secara detail mengenai jadwal penelitian yang dilakukan selama meneliti, sebagai berikut:

1. Identifikasi masalah

   Pada bulan Maret 2021 tepatnya pada minggu ke-2 sampai 4 peneliti melakukan identifikasi masalah terkait dengan permasalahan yang ada.

2. Analisis kebutuhan sistem

   Pada analisis kebutuhan sistem peneliti melakukannya pada minggu ke-4 di bulan Maret 2021 peneliti akan menganalisis apa saja yang dibutuhkan sistem dalam proses pengembangannya menjadi sebuah aplikasi tanda tangan digital lembar pengesahan skripsi.

3. Rancangan sistem

Pada analisis kebutuhan sistem peneliti melakukannya pada minggu ke-4 di bulan Maret sampai minggu ke-2 pada bulan April 2021 peneliti akan melakukan perancangan sistem pada aplikasi tanda tangan digital lembar pengesahan skripsi.

4. Rancangan Bangun Program

   Pada tahap ini peneliti telah masuk ketahap pembuatan aplikasi tanda tangan digital lembar pengesahan skripsi. Pada tahap ini akan dimulai pada minggu ke-3 dibulan April 2021 dan akan berakhir pada minggu ke-2 dibulan Juni 2020. Dalam membangun program ini peneliti menggunakan Visual Studio Code sebagai salah satu *tools* dalam melakukan proses pengkodean.

5. Uji Coba Program (*Testing*)

   Pada tahap ini peneliti akan melakukan pengujian program yaitu pada minggu ke-1 dan 2 pada bulan Agustus 2021, Tujuan dilakukannya *testing* ini agar aplikasi yang dibangun sesuai dengan desain yang diinginkan.

6. Revisi Konsep dan Desain Rancangan

   Tahap ini dilakukan setelah melakukan tahap uji coba program. Peneliti harus memperbaiki apa saja yang harus ditambahkan dan apa saja yang harus dihilangkan serta apa saja yang harus diperbaiki, agar menghasilkan aplikasi yang mampu memberikan kemudahan kepada penggunanya. Pada tahap ini akan dilakukan pada minggu ke-2 dibulan Juni 2021.

7. Implementasi Program

   Peneliti pada tahap implementasi program dilakukan pada minggu ke-3 dibulan Juni 2021 hinnga minggu ke-2 dibulan Agustus. Tahap ini dimana program telah dapat digunakan oleh pengguna.

8. Pembimbingan Naskah Skripsi

   Setelah melalui tahap demi tahap peneliti sekarang telah memasuki tahap pembimbingan naskah skripsi yang dilakukan pada minggu ke-1 dibulan Juli 2021 dan akan berakhir pada minggu ke-3 dibulan Agustus 2021.

9. Penulisan akhir laporan

Pada tahap ini peneliti di peruntukkan untuk menulis hasil dari penelitian yang dilakukan yang dimulai pada bulan Maret 2021. Tahap ini dilakukan pada minggu ke-2 dan 3 pada bulan Agustus 2021.

10. Pedadaran

Setelah melalui begitu banyak tahap, maka peneliti akan memasuki tahap akhir dimana peneliti akan mempresentasekan hasil penelitian yang selama ini dilakukan mulai dari bulan Maret 2021 sampai dengan Juni 2021. Pendadaran ini akan dilakukan pada minggu ke-4 dibulan Agustus 2021.

G. Tinjauan Pustaka

Tinjauan pustaka ini terdiri dari beberapa jurnal sebagai referensi pelengkap guna terselesaikannya penelitian ini. Adapun beberapa penelitian yang terkait dengan penelitian ini ditunjukkan pada Tabel 2.

Tabel 2. Penelitian Terkait

No	Peneliti	Judul Penelitian	Hasil
1	Azdy (2016)	Tanda tangan Digital Menggunakan Algoritma Keccak dan RSA	Pengujian penelitian ini memberikan hasil bahwa implementasi algoritme Keccak dan RSA pada tanda tangan digital dapat menjamin keaslian dokumen yang diterima, keabsahan pembuatan dokumen, dan anti penyangkalan oleh pembuat dokumen.
2	Isnaini (2017)	Penerapan Skema Tanda Tangan Schnorr pada Pembuatan Tanda Tangan Digital	Tanda tangan digital yang dihasilkan berupa string ini dapat memastikan keaslian pesan yang dikirim jika memenuhi syarat, sehingga menjamin keamanan bertukar informasi dua pihak.
3	Abraham (2018)	Tandatangan Digital Sebagai Solusi Teknologi Informasi Dan Komunikasi (TIK) Hijau: Sebuah Kajian Literatur	Dari literatur yang sudah dikemukanan menunjukan bahwa penggunaan TTD terbukti dapat mengurangi penggunaan kertas dimana dengan mengurangi kertas dan beralih ke dokumen elektronik sepenuhnya akan mewujudkan

No	Peneliti	Judul Penelitian	Hasil
			Green ICT, terutama di lingkungan pemerintah. Dengan Tanda Tangan Digital Akan mewujudkan kembali semangat awal pengembangan TIK, yaitu menjadikan teknologi yang ramah lingkungan. TTD di Indonesia juga sebaiknya memiliki peraturan sendiri dan memiliki peraturan yang mendukungnya yaitu Sistem Legal Digital dan Identitas Digital. Identitas Digital di Indonesia mungkin sudah diwakili oleh e-KTP, tetapi penggunaan e-KTP masih belum masif, dan harus dukung dengan kebijakan yang ada. Selain itu, dengan adanya peraturan yang kuat, akan sedikit memaksa para pengguna sistem elektronik untuk menggunakan TTD secara luas.
4	Arifin dkk (2017)	Verifikasi Tanda Tangan Asli Atau Palsu Berdasarkan Sifat Keacakan (Entropi)	Sebaran nilai entropi tanda tangan asli menunjukkan bahwa 29 responden nilai entropinya mengumpul menjadi satu (dalam satu kelas) dan 1 responen nilai entropinya terpisah. Sebaran nilai entropi pada tanda tangan asli mempunyai error 3,31% dari total responden (30 responden). Nilai error 3,31% ini merupakan nilai entropi yang keluar kelompoknya atau kelasnya. Waktu perhitungan nilai entropi pada tanda tangan palsu jika coretan atau piksel pada citra lebih besar dari citra tanda tangan asli maka waktu perhitungan nilai entropinya relatif lebih lama dibandingkan dengan citra tanda tangan asli

No	Peneliti	Judul Penelitian	Hasil
5	Anshori dkk (2019)	Implementasi Algoritma Kriptografi Rivest Shamir Adleman (RSA) pada Tanda Tangan Digital	1. Aplikasi tanda tangan digital berhasil melakukan enkripsi pada dokumen sehingga menghasilkan tanda tangan digital 2. Pembangkitan kunci pada algoritma kriptografi RSA memastikan bahwa hanya pasangan kunci yang digunakan untuk proses enkripsi, yang dapat digunakan pada proses dekripsinya 3. Pengujian penelitian ini memberikan hasil bahwa aplikasi tanda tangan digital menggunakan algoritma kriptografi RSA dapat menjamin keamanan dokumen yang ditandatanganinya dalam aspek integrity, authentication, dan non-repudiation

H. Landasan Teori

Dalam penelitian ini juga terdapat beberapa landasan teori yang digunakan serta dijadikan sebagai acuan dalam penelitian ini antara lain:

1. Tanda tangan digital

   Tanda tangan digital merupakan mekanisme otentikasi yang memungkinkan pembuat pesan menambahkan sebuah kode yang bertindak sebagai tanda tangannya. Tanda tangan digital dapat digunakan untuk melakukan pembuktian secara matematis bahwa data tidak mengalamai modifikasi secara illegal, sehingga bisa digunakan sebagai salah satu solusi untuk melakukan verifikasi data

2. Meode Keccak

   Keccak adalah algoritma fungsi hash satu arah berdasarkan konstruksi spons menggunakan *f-keccak* fungsi permutasi dengan panjang permutasi berbagai b ukuran masing-masing jalur. Kondisi dari b ditunjukkan dengan persamaan (1) dan persamaan (2) (Nazal dkk, 2019).

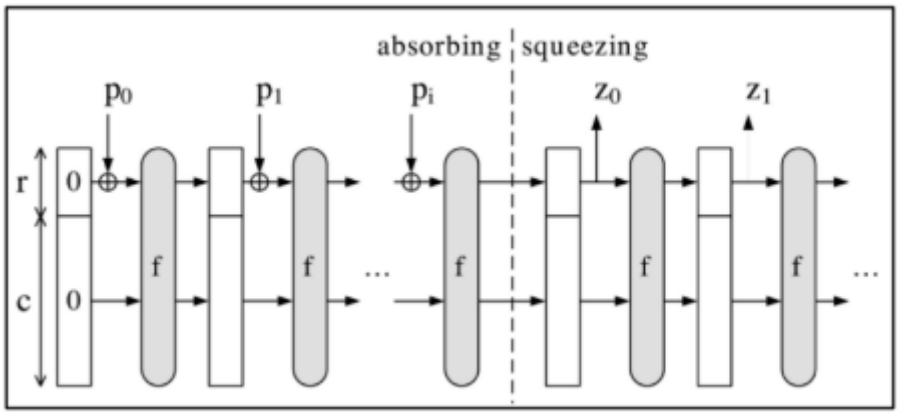
$$b = 25 \times 2^{l} \quad (1)$$

$$0 \leq l \leq 6 \quad (2)$$

Algoritma Keccak memiliki prinsip yang sama dengan algoritma *cipher block*, dimana proses dilakukan pada blok, setiap hasil proses tergantung pada masukan dan hasil dari proses sebelumnya, dan setiap proses dikenakan pada fungsi utama yang terdiri dari beberapa putaran fungsi yang diiterasi beberapa kali. Namun ada perbedaan antara algoritma keccak, dengan algoritma *cipher block*, sebagai berikut:

a. Keccak tidak memiliki jadwal utama
b. Menggunakan konstanta bulat yang tetap

Fungsi Sponge pada Keccak didasarkan pada skema kerja spons. Pekerjaan sponsskema proses adalah skema proses berulang sederhana untuk membangun fungsi spons denganpanjang variabel masukan dan panjang keluaran variabel tergantung pada panjang tetaptransformasi (atau permutasi) f yang beroperasi dalam bilangan tetap b dalam bit



Gambar 1. Konsturksi spons algoritma keccak

3. Metode RSA

RSA di bidang kriptografi adalah sebuah algoritme pada enkripsi public key. RSA merupakan algoritme pertama yang cocok untuk digital signature seperti halnya enkripsi, dan salah satu yang paling maju dalam bidang kriptografi public key. RSA masih digunakan secara luas dalam protokol electronic commerce, dan dipercaya dalam mengamankan dengan menggunakan kunci yang cukup panjang.

Proses pembentukan kunci public dan kunci private RSA adalah sebagai berikut (Agustina, 2015)

a. Menentukan 2 bilangan prima, dengan nama p dan q. Misal nilai p = 51 dan q = 5. (1)

b. Menghitung nilai modulus (n) :

$n = p \times q$ (2)

$n = 51 \times 5$

$n = 255$

Keterangan:

n : Nilai modulus

c. Menghitung nilai totient n :

$(n) = (p-1) \times (q-1)$ (3)

$(n) = (51-1) \times (5-1)$

$(n) = (50 \times 4)$

$(n) = 200$

d. Menentukan nilai e dengan syarat gcd (e, (n)) = 1 (4)

Keterangan:

e : bilangan prima, dan $1 < e < (n)$.

Pilih kunci publik e adalah 7 (relatif prima terhadap 200)

e. Mencari nilai *deciphering exponent* (d), maka :

$d = (1 + (k \times (n)) / e)$ (5)

$d = (1 + (k \times 200)) / 7$

Keterangan:

d : *deciphering exponent*

k : sembarang angka untuk pencarian hingga dihasilkan suatu nilai integer atau bulat

f. Dari langkah-langkah yang sudah diuraikan sebelumnya, maka nilai n, e, dan d telah didapatkan sehingga pasangan kunci telah terbentuk.

a) Pasangan kunci publik (n, e) = (255, 7)

b) Pasangan kunci rahasia (n, d) = (255, 343)

Proses Enkripsi metode RSA sebagai berikut (Agustina, 2015):

Plaintext : polsri

Nilai ASCII: p=112, o=111, l=108, s=115, r=114, i=105

Hasil enkripsi

Enkripsi RSA

112^7 mod 255 = 73, pada tabel ascii adalah karakter I

111^7 mod 255 = 36, pada tabel ascii adalah karakter #

108^7 mod 255 = 252, pada tabel ascii adalah karakter w

115^7 mod 255 = 55, pada tabel ascii adalah karakter ***n***

114^7 mod 255 = 24, pada tabel ascii adalah karakter (cancel)

115^7 mod 255 = 45, pada tabel ascii adalah karakter –

Proses dekripsinya adalah sebagai berikut (Agustina, 2015):

75^{343} mod 255 = 112, pada tabel ascii adalah karakter p

36^{343}mod 255 = 36, pada tabel ascii adalah karakter o

252^{343} mod 255 = 252, pada tabel ascii adalah karakter l

55^{343} mod 255 = 55, pada tabel ascii adalah karakter s

24^{343} mod 255 = 24, pada tabel ascii adalah karakter r

45^{343} mod 255 =45, pada tabel ascii adalah karakter i

I. Metodologi Penelitian

Dalam penelitian ini, metode penelitian yang digunakan adalah penelitian tindakan (*action research*), menurut Hasibuan(2007, h. 79) penelitian tindakan merupakan "penelitian yang berfokus langsung pada tindakan sosial. Penelitian tindakan ini merupakan metode yang didasarkan pada tindakan masyarakat yang seringkali diselenggarakan pada suatu latar yang luas, seperti di rumah sakit, pabrik, sekolah, dan lain sebagainya". Metode penelitian tindakan diduga kuat sesuai dengan permasalahan yang diteliti penulis karena didasarkan pada permasalah penggunaan tanda tangan elektronik yang tidak dapat diverifikasi. Penelitian tindakan dapat terdiri dari satu, dua, tiga ataupun empat siklus dan masing-masing siklus terdiri dari permasalahan, pengumpulan data, perencanaan tindakan (Pratika, 2015). Berikut adalah tahap dan insrumen penelitian:

1. Tahap Penelitian

Dalam penelitian yang penulis lakukan terbagi menjadi beberapa tahap penelitian yaitu :

a. Menentukan topik penelitian

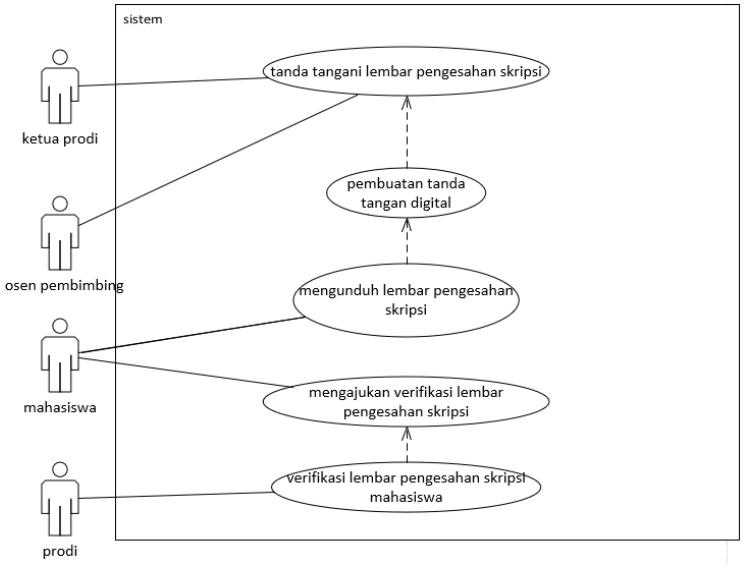
Pada tahap ini penulis menetukan topik penelitian yaitu penerapan tanda tangan digital untuk verifikasi lembar pengesahan skripsi menggunakan metode Keccak dan RSA. Untuk mendukung penelitian, penulis melakukan studi literatur untuk menjadi landasan penelitian yang dilakukan yang sesuai dengan topik penelitian yaitu perancangan tanda tangan digital

b. Pengumpulan data

Pada proses ini penulis mengumpulkan dokumen berekstensi pdf lembar pengesahan skripsi mahasiswa yang telah memiliki tanda tangan elektornik, dokumen yang telah terkumpul digunakan sebagai data penelitian.

c. Analisis Perancangan Alur Sistem

Analisis perancangan alur sistem merupakan tahapan-tahapan analisis untuk menggambarkan alur sistem yang akan dibangun. Berikut adalah tahapan-tahapan analisis alur sistem:



Gambar 2. *Use case*

1) Tanda tangani lembar pengesahan skripsi

   dosen pembimbing menandatangi lembar pengesahan skripsi mahasiswa, selanjutnya dokumen yang telah ditanda tangani oleh dosen pembimbing, kemudian ditanda tangani oleh ketua program studi

2) pembuatan tanda tangan digital

   jika lembar pengesahan telah ditanda tangani oleh dosen pembimbing, dan ketua progra studi, sistem akan membuat tanda tangan digital

3) Mengunduh lembar pengesahan skripsi

   Jika lembar pengesahan skripsi telah memiliki tanda tangan digital mahasiswa telah dapat mengunduhnya

4) Mengajukan verifikasi lembar pengesahan skripsi

   Mahasiswa mengajukan berkas lembar pengesahasan skripsi untuk diverifikasi

5) Verifikasi lembar pengesahan skripsi

   Prodi melakukan verifikasi terhadap berkas lembar pengesahan skripsi mahasiswa

d. Pengujian

   Untuk melakukan pengujian penulis menggunakan pengujian *blackbox* untuk fitur-fitur aplikasi yang dibangun, dan melakukan pengujian verifikasi berkas lembar pengesahan skripsi.

2. Instrumen Penelitian

Instrumen penelitian adalah alat bantu yang dipilih dalam kegiatannya agar sistematis dan mempermudah peneliti selama melakukan penelitian. Instrumen ini terbagi menjadi dua yaitu:

a. Perangkat Keras (*Hardware*)

   Perangkat keras atau *Hardware* yang digunakan dalam pengembangan aplikasi adalah:

   1. *Processor* minimal *core i3.*
   2. Memory (RAM) minimal 4,00 GB.

b. Perangkat Lunak (*Software*)

Perangkat lunak atau *software* yang digunakan adalah:

i. Sistem operasi Microsoft Windows 10 Professional 64-bit,
ii. Code editor Visual Studio Code versi 1.39.1 64-bit
iii. Database Mysql, menggunakan Xampp versi 7.1.9.0.,
iv. Browser versi 72.0.3626.119,
v. Environtment bahasa pemrograman javascript yaitu Node js

J. Kerangka Pikir

1. Judul Penelitian

Judul dari penelitian ini adalah Penerapan Tanda Tangan Digital Untuk Verifikasi Lembar Pengesahan Skripsi Menggunakan Metode Keccak Dan RSA

2. Latar Belakang

Dengan adanya kemudahan menandatangani lembar pengesahan skripsi secara elektronik juga memiliki kekurangan yaitu tanda tangan dapat diduplikasi sehingga dapat digunakan oleh pihak yang tidak bertanggung jawab untuk menandatangi lembar pengesahan skripsi tanpa sepengetahuan pemilik tanda tangan, sehingga lembar pengesahan skripsi yang telah ditanda tangani tidak dapat diverifikasi untuk menjamin keabsahannya.

Atas dasar kekurangan dari tanda tangan elektronik, penulis berencana menggunakan tanda tangan digital untuk mengatasi kekurangan tanda tangan elektronik yang ditambahkan ke lembar pengesahan skripsi. Tanda tangan digital berbeda dengan tanda tangan elektronik, tanda tangan digital adalah sebuah kombinasi unik dari fungsi hash dan enkripsi dengan metode asimetris.

3. Metode Penelitian

Metode yang digunakan dalam penelitian ini adalah metode *Action Research* dan tanda tangan digital menggunakan metode Keccak dan RSA

4. Tujuan Penelitian

Tujuan penelitian yang ingin dicapai adalah sebagai berikut:

a. Merancangan aplikasi tanda tangan digital lembar pengesahan skripsi mahasiswa fakultas ilmu komputer menggukan metode Keccak dan RSA Manfaat Penelitian
b. Verifikasi keabsahan lembar pengesahan skripsi mahasiswa Fakultas Ilmu Komputer Universitas Muslim Indonesia

5. Hasil Penelitian

Hasil dari penelitian ini adalah sebagai berikut:

1. Telah mampu merancang aplikasi tanda tangan digital menggunakan metode Keccak dan RSA
2. Aplikasi yang telah dibangun mampu memverifikasi keabsahan dokumen lembar pengesahan skripsi mahasiswa

DAFTAR PUSTAKA

Schneier, B. (1995). Applied Cryptography (2Nd Ed.): Protocols, Algorithms, and Source Code in C. New York, NY, USA: John Wiley & Sons, Inc.

Bentivenga, C., Christie., Kitson, M. (2010) Keccak Final Paper.

Romine, C, H. (Agt. 2015) SHA-3 Standard: Permutation-Based Hash and Extendable-Output Functions

Ginting, Albert., Isnanto R. Rizal., Windasari, Ike Pertiwi. (2015). Implementasi Algoritma Kriptografi RSA untuk Enkripsi dan Dekripsi Email. Jurnal Teknologi dan Sistem Komputer, Vol.3, No.2

Abraham, F. Z., Santosa, P. I. and Winarno, W. W. (2018) 'TANDATANGAN DIGITAL SEBAGAI SOLUSI TEKNOLOGI INFORMASI DAN KOMUNIKASI (TIK) HIJAU : SEBUAH KAJIAN LITERATUR', pp. 111–124.

Agustina, A. N. (2015) 'PENGAMANAN DOKUMEN MENGGUNAKAN METODE RSA (RIVEST SHAMIR ADLEMAN) BERBASIS WEB', pp. 14–19.

Anshori, Y., Erwin Dodu, A. Y. and Wedananta, D. M. P. (2019) 'Implementasi Algoritma Kriptografi Rivest Shamir Adleman (RSA) pada Tanda Tangan Digital', *Techno.Com*, 18(2), pp. 110–121. doi: 10.33633/tc.v18i2.2166.

Arifin, J. and Zidny, M. (2017) 'Verifikasi Tanda Tangan Asli Atau Palsu Berdasarkan Sifat Keacakan (Entropi)'.

Azdy, R. A. (2016) 'Tanda tangan Digital Menggunakan Algoritme Keccak dan RSA', 5(3), pp. 184–191.

Isnaini, H. F., Karyati, K. and Matematika, J. P. (2017) 'Penerapan Skema Tanda Tangan Schnorr pada Pembuatan Tanda Tangan Digital Implementation of Schnorr Signature Scheme in The Form of Digital Signature', 12(1), pp. 57–64.

Nazal, M. A., Pulungan, R. and Riasetiawan, M. (2019) 'Data Integrity and Security using Keccak and Digital Signature Algorithm (DSA)', *IJCCS (Indonesian Journal of Computing and Cybernetics Systems)*, 13(3), p. 273. doi: 10.22146/ijccs.47267.