IMPLEMENTASI *DIGITAL SIGNATURE* MENGGUNAKAN ALGORITMA KRIPTOGRAFI RSA UNTUK PENGAMANAN DATA DI SMK WIRAKARYA 1 CIPARAY

Hani Widia[#1], Yaya Suharya, S.Kom, M.T [*2], Nurul Imamah, S.T., M.T [#3]

[#]*Fakultas Teknologi Informasi, Universitas Bale Bandung*
Jl. Raden AA Wiranatakusumah No.7, Baleendah, Kec. Baleendah, Bandung, Jawa Barat 40375

[1]hani.widia23@gmail.com

[2]Yaya@cdi.co.id

[3]nurulimamah@unibba.ac.id

Abstract - ***Data or information is one of the elements that play a very large role in various fields of life. With the development of computer technology, more and more people are able to tamper with the data even though it has been stored neatly. Digital signing or digital signature is considered to provide document security and can avoid document forgery and hoaxing. Wirakarya 1 Ciparay is one of the large educational institutions in Bandung regency, so that the threat of pirating data or documents does not occur in Wirakarya 1 Ciparay, the compiler will build a data security system using digital signature cryptography. Cryptography is one of the techniques used to improve the security aspects of data or information. Cryptography is the science and art of maintaining the confidentiality of a message or data*.**

Keywords - ***Data, Cryptography, RSA, Digital Signature, Security.***

Abstrak – **Data atau informasi merupakan salah satu elemen yang memegang peranan yang sangat besar dalam berbagai bidang kehidupan. Dengan semakin berkembangnya teknologi komputer, semakin banyak orang yang sanggup mengutak-atik data meskipun telah disimpan dengan rapi. Penandatanganan secara digital atau *digital signature* dinilai dapat memberi keamanan dokumen serta dapat menghindari pemalsuan dokumen dan *hoaks*. SMK Wirakarya 1 Ciparay adalah salah satu instansi pendidikan yang cukup besar di kabupaten Bandung, agar ancaman pembajakan data atau dokumen tidak terjadi di SMK Wirakarya 1 Ciparay, maka penyusun akan membangun sebuah sistem pengamanan data dengan menggunakan kriptografi *digital signature*. Kriptografi adalah salah satu teknik yang digunakan untuk meningkatkan aspek keamanan suatu data atau informasi. Kriptografi merupakan ilmu dan seni untuk menjaga kerahasiaan suatu pesan atau data.**

***Kata kunci* – Data, Kriptografi, RSA, *Digital Signature*, Pengamanan.**

I. PENDAHULUAN

Data atau informasi merupakan salah satu elemen yang memegang peranan yang sangat besar dalam berbagai bidang kehidupan. Dengan semakin berkembangnya teknologi komputer, semakin banyak orang yang sanggup mengutak-atik data meskipun telah disimpan dengan rapi. Untuk mencegah terjadinya pencurian data oleh pihak-pihak yang tidak berhak atas data tersebut, maka dikembangkan berbagai teknik pengamanan data.

Kriptografi adalah salah satu teknik yang digunakan untuk meningkatkan aspek keamanan suatu data atau informasi. Kriptografi merupakan ilmu dan seni untuk menjaga kerahasiaan suatu pesan atau data. Dalam hal ini data akan diberi *digital signature* sehingga data terjaga keamanan dan keasliannya. Penandatanganan secara digital atau *digital signature* dinilai dapat memberi keamanan dokumen serta dapat menghindari pemalsuan dokumen dan *hoaks*.

SMK Wirakarya 1 Ciparay adalah salah satu instansi pendidikan yang cukup besar di kabupaten Bandung, agar ancaman pembajakan data atau dokumen tidak terjadi di SMK Wirakarya 1 Ciparay, maka penyusun akan membangun sebuah sistem pengamanan data dengan menggunakan kriptografi *digital signature* untuk mengamankan data atau dokumen di SMK Wirakarya 1 Ciparay.

Secara umum proses pemberian tanda tangan digital dapat dibagi ke dalam dua langkah, yaitu:

1. Pemberiantandatangan digital.
2. Otentifikasi/verifikasi.

RSA (*Rivest Shamir Adleman*) merupakan algoritma tandatangan digital yang terkenal dan banyak digunakan. Algoritma ini menjadi unggul karena mudah untuk diimplementasikan dan sangat kuat. Pada RSA, algoritma

enkripsi dan dekripsi identik, sehingga proses pemberian tanda tangan digital dan verifikasinya juga identik.

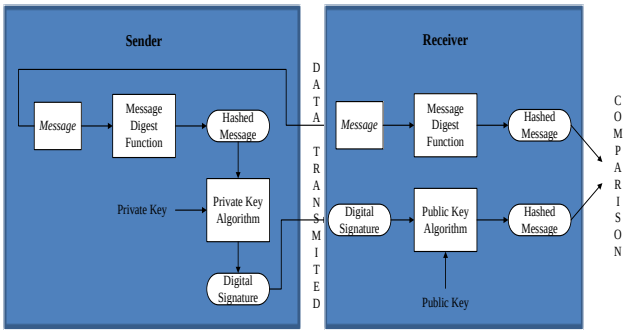
Berdasarkan uraian diatas, maka penyusun tertarik untuk melakukan penelitian dengan mengimplementasi algoritma kriptografi *digital signature* dengan metode RSA untuk pengamanan data di sekolah. Sehingga penelitian ini berjudul "Implementasi *Digital Signature* Menggunakan Algoritma Kriptografi RSA untuk Pengamanan Data Di SMK Wirakarya 1 Ciparay".

II. LANDASAN TEORI

A. Tanda Tangan Digital (*Digital Signature*)

Tanda tangan digital adalah mekanisme otentikasi yang mengijinkan pemilik pesan membubuhkan sebuah sandi pada pesannya yang bertindak sebagai tanda tangan. Tanda tangan dibentuk dengan mengambil nilai *hash* dari pesan dan mengenkripsi nilai *hash* pesan tersebut dengan kunci privat pemilik pesan (Stallings, 2005).

Fungsi utama dari tanda tangan digital pada pada aspek keamanan kriptografi adalah *non-repudiation* atau anti penyangkalan dimana apabila dokumen valid maka pengirim tidak bisa menyangkal bahwa keberadaan dokumen benar dikirim oleh pengirim yang bersangkutan. Suatu tanda tangan digital dapat digunakan di segala macam pesan, apakah itu terenkripsi maupun tidak, sehingga penerima dapat memastikan identitas pengirim itu dan pesan tiba secara utuh.



Gambar 1 Skema Tanda Tangan Digital

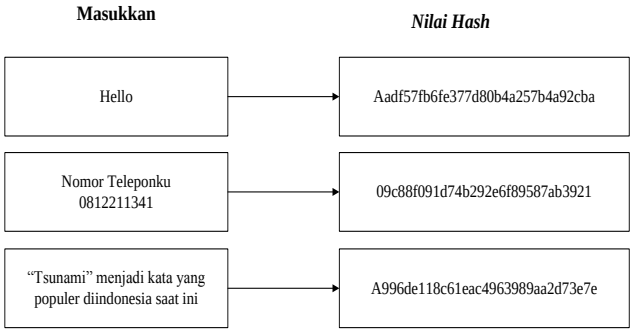
B. Fungsi *Hash*

Fungsi *Hash* merupakan algoritma yang mengubah teks atau pesan (*text or message*) menjadi sederetan karakter acak yang memiliki karakter yang sama. Hash juga termasuk salah satu bentuk teknik kriptografi tanpa menggunakan kunci (*unkeyed cryptosystem*). Selain itu *hash* memiliki nama lain yang juga dikenal yaitu "*one-way function*".

Fungsi *Hash* adalah fungsi yang menerima masukan string yang panjangnya sembarang selanjutnya mentransformasikannya menjadi string keluaran yang panjangnya tetap *(fixed)* yang biasanya berukuran jauh lebih kecil daripada ukuran string semula.

Menurut Kaufman et. al. (2002), Fungsi *hash* dapat digunakan sebagai:

1). Menyimpan *Password*
2). Sebagai *Message Integrity*
3). Sebagai *Message Fingerprint*



Gambar 2 Contoh Penggunaan Fungsi *Hash*

Fungsi *hash* sering juga disebut fungsi satu arah (*one way function*), *message digest*, f*ingerprint*, fungsi kompresi, dan *Message Authentication Code* (MAC). Fungsi ini biasanya diperlukan bila kita menginginkan pengambilan sidik jari suatu pesan. Dinamakan fungsi kompresi karena biasanya masukan fungsi satu arah ini selalu lebih besar dari keluarannya, sehingga seolah-olah mengalami kompresi. Namun kompresi hasil fungsi ini tidak dapat dikembalikan ke asalnya sehingga disebut sebagai fungsi satu arah.

C. Algoritma

Menurut Kamus Besar Bahasa Indonesia (KBBI), Algoritma adalah sebagai berikut :

1. prosedur sistematis untuk memecahkan masalah matematis dalam langkah-langkah terbatas.
2. urutan logis pengambilan keputusan untuk pemecahan masalah

Menurut Goodman Hedet Niemi, Algoritma adalah : **"***Algoritma adalah urutan terbatas dari operasi-operasi terdefinisi dengan baik, yang masing-masing membutuhkan memori dan waktu yang terbatas untuk menyelesaikan suatu masalah.*"

D. Kriptografi

Kriptografi (*cryptography*) berasal dari Bahasa Yunani, yaitu "*cryptós*" dan "*gráphein*". *Cryptós* berarti rahasia, sedangkan *gráphein* memiliki arti tulisan. Jadi, ditinjau dari segi asal kata, kriptografi berarti tulisan rahasia.

Menurut Rinaldi Munir dalam bukunya yang berjudul "Kriptografi", kriptografi adalah "ilmu dan seni untuk menjaga keamanan pesan." Kriptografi juga dapat diartikan sebagai "ilmu yang mempelajari teknik-teknik matematika yang berhubungan dengan aspek keamanan informasi seperti kerahasiaan, integritas data, serta otentikasi.".

Awal tahun 400 SM, bangsa Spartan di yunani memanfaatkan kriptografi di bidang militer dengan menggunakan alat yang disebut *scytale*, yakni pita

panjang berbahan daun *papyrus* yang dibaca dengan cara digulungkan ke sebatang silinder.

Gambar 3 *Scytale*

E. RSA

Algoritma RSA dibuat oleh tiga orang peneliti dari MIT (*Massachussets Institute of Technology*) pada tahun 1976, yaitu Ron Rivest, Adi Shamir dan Leonard Adleman. RSA adalah salah satu teknik kriptografi dimana kunci untuk melakukan enkripsi berbeda dengan kunci untuk melakukan dekripsi. Kunci untuk melakukan enkripsi disebut sebagai kunci publik, sedangkan kunci untuk melakukan dekripsi disebut sebagai kunci privat. Orang yang mempunyai kunci publik dapat melakukan enkripsi tetapi yang dalam melakukan dekripsi hanyalah orang yang memiliki kunci privat. Kunci publik dapat dimiliki oleh sembarang orang, tetapi kunci privat hanya dimiliki oleh orang tertentu saja.

F. Teori Bilangan

Teori bilangan (*number theory*) merupakan teori dasar dalam memahami kriptografi. Bilangan yang dimaksud hanya bilangan bulat (*integer*), yang tidak mempunyai pecahan desimal. Teori bilangan yang akan dibahas dalam skripsi ini adalah teori-teori yang merupakan dasar dari algoritma RSA, seperti algortima *Euclidean*, relatif prima, aritmetika modulo, bilangan prima, dan fungsi *Totient Euler*.

Sifat pembagian dalam bilangan bulat melahirkan konsep-konsep bilangan, seperti bilangan prima, *Euclidean*, aritmatika modulo, dll.

G. ALGORITMA RSA UNTUK TANDA TANGAN DIGITAL

RSA (*Rivest Shamir Adleman*) merupakan algoritma pertama yang diketahui cocok untuk digunakan dalam proses tanda tangan digital dan juga enkripsi. RSA digunakan secara luas dalam protokol *e-commerce* dan dipercaya masih aman sampai saat ini jika diberikan kunci dengan panjang bit yang cukup besar.

RSA merupakan sebuah algoritma yang mengimplementasikan kriptosistem kunci publik dengan ide utama berupa:

1. *Public key encryption*
2. *Signature*

H. JAVA

Java adalah bahasa pemrograman dan platform komputasi pertama kali dirilis oleh *Sun Microsystems* pada tahun 1995. Java merupakan teknologi yang mendasari kekuatan program untuk utilitas, permainan, dan aplikasi bisnis. Java berjalan pada lebih dari 850 juta komputer pribadi di seluruh dunia, dan pada miliaran perangkat di seluruh dunia, termasuk ponsel dan perangkat TV. Salah satu karakteristik Java adalah portabilitas, yang berarti bahwa program komputer yang ditulis dalam bahasa Java harus dijalankan secara sama, pada setiap *hardware / platform* sistem operasi.

I. *NETBEANS*

NetBeans IDE adalah sebuah *Integrated Development Environment* untuk para pengembang software. Pengguna *NetBeans* IDE bisa mendapatkan segala *tools* yang diperlukan untuk membuat aplikasi-aplikasi desktop profesional, perusahaan, *web*, dan *mobile* dengan bahasa Java, C/C++, dan bahkan bahasa-bahasa dinamis seperti PHP, *JavaScript*, *Groovy*, dan *Ruby*. *Netbeans* IDE mudah diinstal dan digunakan langsung di luar kotaknya dan berjalan di banyak *platforms* termasuk Windows, Linux, Mac OS X dan Solaris

J. *Flowchart*

Flowchart adalah adalah suatu bagan dengan simbol-simbol tertentu yang menggambarkan urutan proses secara mendetail dan hubungan antara suatu proses (instruksi) dengan proses lainnya dalam suatu program.

K. MDD (*MODEL DRIVEN DEVELOPMENT)*

Teknik pengembangan berbasis model (MDD) menekankan gambar model untuk membantu memvisualisasikan dan menganalisis masalah, mendefinisikan kebutuhan bisnis, dan merancang sistem informasi. Analisis dan desain sistem terstruktur - berpusat pada proses Teknik informasi (IE) - berpusat pada data Analisis dan desain berorientasi obyek (OOAD) - terpusat pada objek (integrasi data dan masalah proses) Rute *model driven development*.

Tahapan yang dipakai pada penelitian adalah sebagai berikut:

1) *Preliminary investigation* (investigasi awal)
2) *Problem analysis* (Analsis masalah)
3) *Requirements analysis* (Analisis Kebutuhan)
4) *Design* (Desain)
5) *Construction* (Kontruksi)
6) *Implementation* (implementasi).

III. PEKERJAAN DAN DISKUSI HASIL

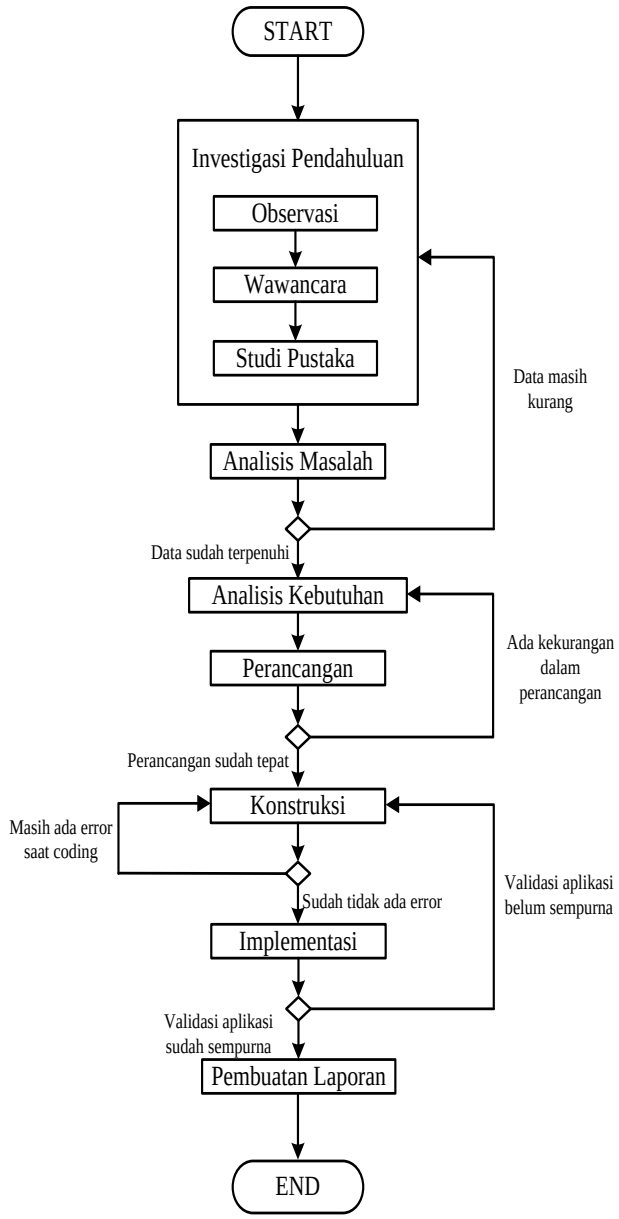
A. Proses Pekerjaan

Proses pekerjaan atau metodologi penelitian dalam penelitian ini melalui berbagai tahapan yaitu metode pengumpulan data dan metode pengembangan sistem. Metode pengumpulan data yaitu meliputi observasi, wawancara, dan studi pustaka. Sedangkan dalam metode

pengembangan sistem menggunakan *Model Driven Development*. Berikut adalah kerangka berfikir dan perancangan aplikasi.

1. Kerangka Berfikir

Berikut adalah langkah-langkah yang di lakukan untuk mencapai tujuan dari penelitian ini adalah sebagai berikut



Gambar 4 Kerangka Pikir

2. Analisis Sistem

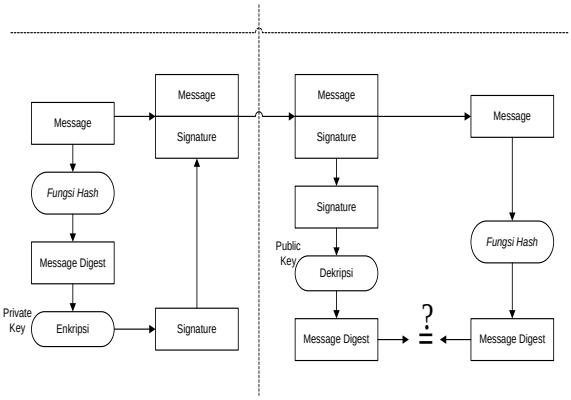
Analisis merupakan tahapan untuk pemahaman terhadap aplikasi yang akan dibuat. Pada tahap ini berisi Analisis Masalah, Instrument Penelitian, Analisis Pengguna, Analisis Kebutuhan User, Analisis Program Aplikasi, Hasil Analisis dan Perancangan

Analisis sistem ini dilakukan untuk memberikan solusi terhadap permasalahan yang ada di SMK Wirakarya 1 Ciparay.

Berikut adalah beberapa analisis yang dilakukan untuk membangun Aplikasi pembuatan tanda tangan digital

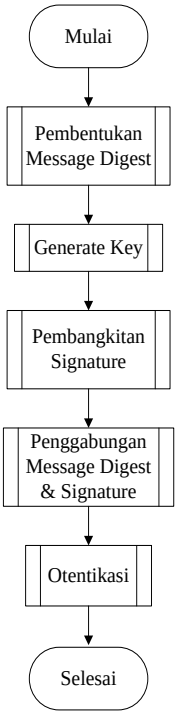
a. Deskripsi Umum Sistem

Proses system dimana pada perancangan system digambarkan, rancangan sistem yang akan dibangun sebelum dilakukan pengkodean kedalam suatu bahasa pemrograman. Desain umum yang akan diaplikasikan bertujuan untuk memberikan gambaran secara umum kepada pengguna tentang sistem yang akan dibangun.



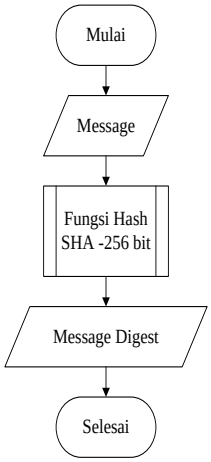
Gambar 5 Gambar Umum Sistem RSA *Digital Signature*

b. Analisis Metode RSA



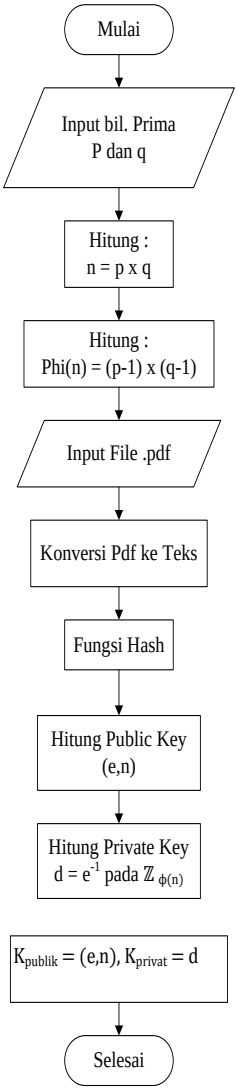
Gambar 6 *Flowchart* Proses TandaTangan Digital

c. Analisis Pembentukkan *Message Digest*



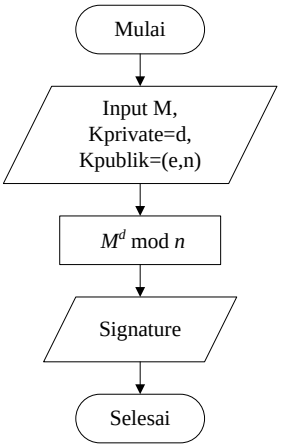
Gambar 7 *Folwchart* Pembentukkan *Message Digest*

d. Analisis Pembangkitan Pasangan Kunci RSA



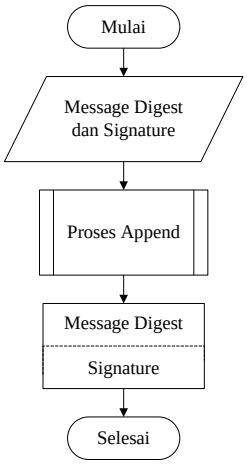
Gambar 8 *Flowchart* Pembentukkan Kunci

e. Analisis Pembentukan *Digital Signature*



Gambar 9 *Flowchart* Pembentukan *Digital Signature*

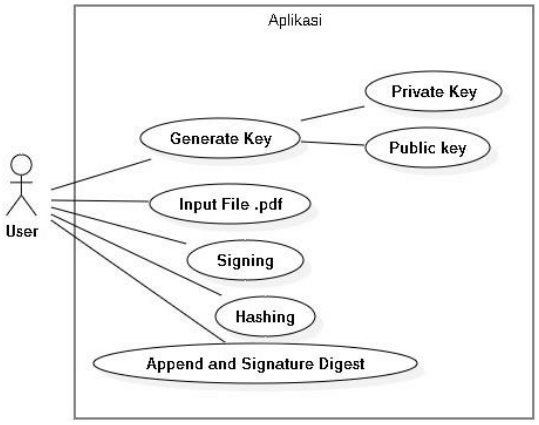
f. Analisis Penggabungan Pesan dan *Digital Signature*



Gambar 10 *Flowchart* Penggabungan Pesan dan *Digital Signature*

3. Perancangan

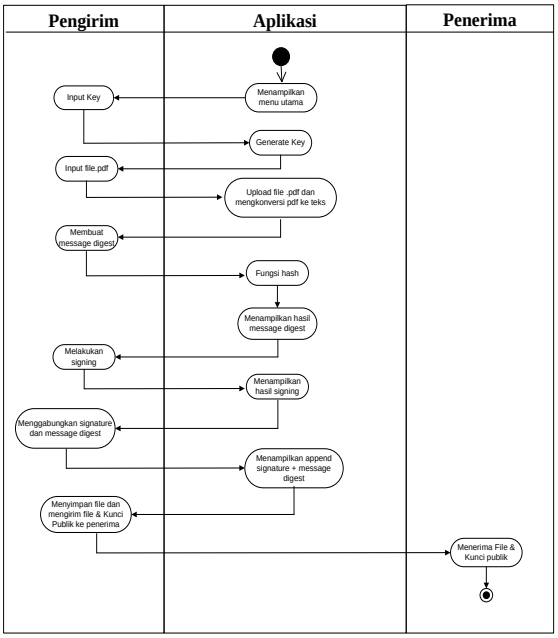
a. *Use Case Diagram* Aplikasi *Digital Signature*



Gambar 11 *Use Case Diagram Digital Signature*

b. Activity Diagram Digital Signature

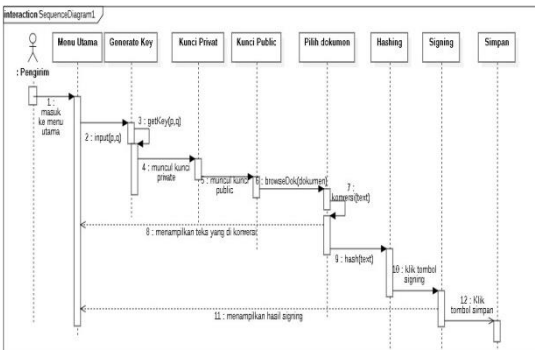
Activity Diagram merupakan cara memodelkan aktifitas yang ada dalam suatu *Use Case*.



Gambar 12 *Activity Diagram DigitalSignature*

c. Sequence Diagram

Sequence Diagram merupakan diagram yang menggambarkan interaksi antar objek disekitar aplikasi.



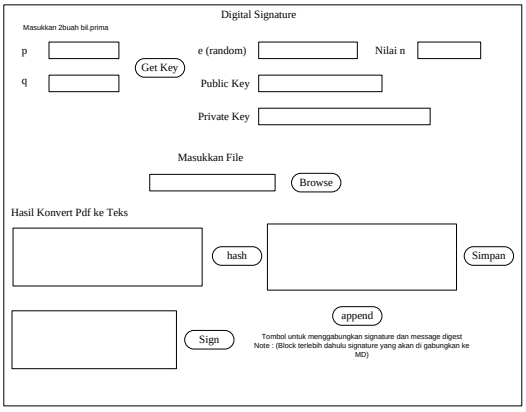
Gambar 13 *Sequence Diagram Digital Signature*

B. Hasil Pekerjaan

1. Implementasi *User Interface*

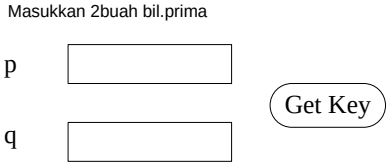
   a. Tampilan Struktur Menu

   Berdasarkan perancangan yang dilakukan telah diketahui bahwa struktur menu bertujuan untuk memudahkan pengoperasian dalam aplikasi. Berikut ini merupakan tampilan struktur menu berdasarkan hasil perancangan.



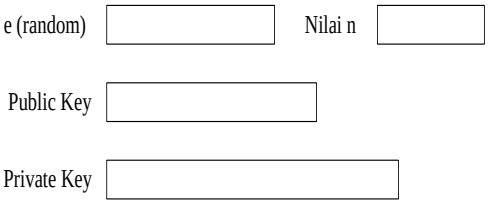
Gambar 14 Tampilan Struktur Menu *Digital Signatur*

b. Tombol *Get Key*



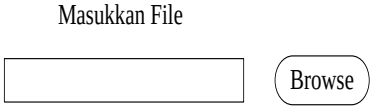
Gambar 15 Tombol *Get Key*

c. *Generate Key*



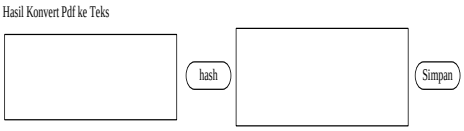
Gambar 16 *Generate Key*

d. Tombol *Input File*



Gambar 17 Tombol *Input File*

e. Tombol *Hash*



Gambar 18 Tombol *Hash*

f. Perancangan Tombol *Sign*

Gambar 19 Tombol *Sign*

2. Pengujian

a. Pengujian Pembangkitan Kunci Publik dan Kunci Privat

Dalam proses pembangkitan kunci, baik kunci public maupun kunci privat pada algoritma kriptografi RSA, hal yang pertama dilakukan adalah pemilihan bilangan prima sembarang p dan q. nilai $p \neq q$ karena apabila $p = q$, maka p^2 sehingga p dapat diperoleh dengan menarik akar pangkat dua dari n. tabel 5.1 pengujian pembangkitan kunci public dan privat dimana nilai $p \neq q$.

Tabel 1 pengujian kunci privat dan publik

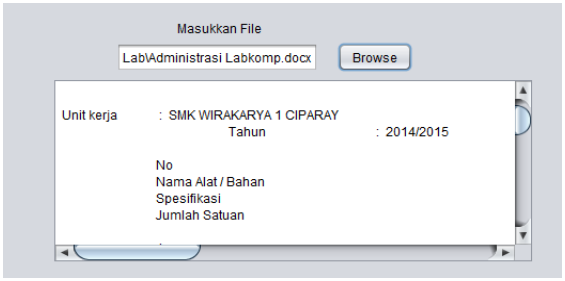
Percobaan ke -	p	q	n	e (Kunci Publik)	e (Kunci Privat)
1	13	11	143	107.143	83
2	17	15	255	65.255	193
3	23	21	483	287.483	23

b. Pengujian *Browse File* dan konversi file

1) *Browse File Excel*

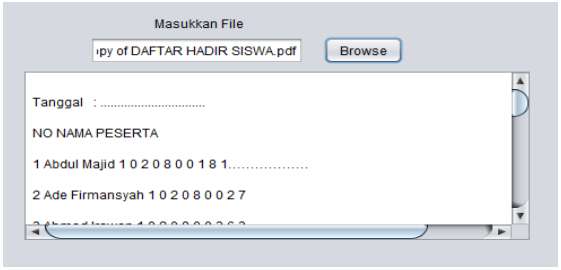
Gambar 20 *Browse File Excel*

2) *Browse File Document*



Gambar 21 *Browse File Document*

3) *Browse File* Pdf



Gambar 22 *Browse File* Pdf

c. Pengujian Aplikasi

Pengujian aplikasi ini dilakukan dengan cara *blackbox* dengan hanya memperhatikan masukkan ke dalam sistem dan keluaran dari masukkan tersebut.

Tabel 2 Pengujian Aplikasi

Pengujian Aplikasi				
No	**Item Uji**	**Skenario Uji**	**Hasil Yang Di Harapkan**	**Hasil Pengujian**
1	Tombol *Get Key*	Memasukkan Bilangan prima p dan q Dan menekan tombol *get key*	Ketika memasukkan bilangan prima p dan q system akan secaraotomatis menghitung nilai p dan q sehingga menampilkan kunci public dan kunci pivat	+Berhasil
2	Tombol *Browse*	Menekan tombol *Browse* dan Memasukkan dokumen transkip .pdf	Dokumen file pdf yang dibrowse ditampilkan di form digital signature yang kemudian dikonversi keteks secaraotomatis.	+Berhasil
3	Tombol *Hash*	Menekan Tombol *Hash*	Dokumen yang telah di konversi ke teks kemudian di hitung nilai hashnya untuk didapatkan *Message Digest*	+Berhasil
4	Tombol *Signing*	Menekan tombol *Sign*	Memberi *Digital Signature*	+Berhasil
5	Tombol *Append*	Menekan Tombol *Append*	Setelah *Digital Signature* di dapatkan, satukan dengan *Message Digest* dengan menekan tombol *Append*	+Berhasil
6	Tombol Simpan	Menekan Tombol Simpan	*Digital Signature* yang telah di gabungkan dengan *Message Digest* kemudian disimpan dikomputer laludikirim kepenerima	+Berhasil

IV. KESIMPULAN

Bab ini menjelaskan tentang kesimpulan dari aplikasi yang telah dibuat dan beberapa kekurangan dari aplikasi yang dapat menjadi saran untuk pihak lain jika akan mengembangkan aplikasi ini:

A. Kesimpulan

Berdasarkan hasil analisis penelitian dan perancangan, maka hasil yang tercapai penyusun menyelesaikan laporan dan aplikasi *Digital Signature*

menggunakan algoritma kriptografi RSA, penyusun dapat menyimpul kan bawa:

1. Aplikasi ini dapat digunakan untuk pengamanan data berekstensi .doc, .xlsx, dan .pdf.
2. Aplikasi ini dapat digunakan untuk pemberian *digital signature* terhadap dokumen transkip akademik yang berupa file .doc, .xlsx .pdf sehingga dapat mencegah terjadinya pemalsuan terhadap data atau dokumen sekolah

B. . Saran

Dalam proses pembuatan aplikasi *Digital Signature* ini, penyusun masih banyak memiliki kekurangan dan jauh dari kata sempurna. Sehingga penyusun berharap untuk peneliti selanjutnya dapat mengembangkan lagi aplikasi ini, diantaranya :

1. Peneliti selanjutnya diharapkan bisa mengembangkan aplikasi *digital signature* untuk memberi *signature* tidak hanya pada *file* dokumen, tetapi juga untuk foto, video atau audio.
2. Peneliti selanjutnya diarapkan bisa mengembangkan aplikasi *digital signature* agar *file* atau dokumen yang dimasukkan lebi dari 1(satu) halaman.
3. Peneliti selanjutnya diharapkan bisa membuat *fitur* tambahan untuk memilih menu pada aplikasi, sehingga aplikasi tidak hanya terdiri dari 1 (satu) *form* saja.
4. Peneliti selanjutnya diharapkan bisa menambah *fitur* berupa *form Encrypt* kedalam aplikasi *Digital Signature* sehingga keamanannya lebih terjamin.
5. Peneliti selanjutnya diarapkan bisa menambah *fiture* berupa *form Decrypt* yang digunakan oleh *user* penerima dokumen.
6. Peneliti selanjutnya diharapkan bisa membuat *Form* baru untuk proses *Verify* yang digunakan oleh *User* Penerima dokumen.

REFERENSI

[1] Blog.javan.co.id (2017). Apa-itu-tanda-tangan-digital. Retrieved September 2019, from https://blog.javan.co.id/apa-itu-tanda-tangan-digital-92380069398.

[2] Coderanch.com (Juni 2009). *Java-program-add-digital-signature*. Retrieved September 2019, from https://coderanch.com/t/445249/java/java-program-add-digital-signature.

[3] Digitalkrip.blogspot.com (16 Februari 2010). Tanda-tangan-digital-digital-signature. Retrieved September 2019, from https://www.google.com/amp/s/digitalkrip.wordpress.com/2010/02/16/tanda-tangan-digital-*digital-signature*/amp

[4] Docplayer.info (2017). Implementasi-algoritma-kriptografi-kunci-publik. Retrieved September 2019, from https://docplayer.info/343887768-Implementasi-algoritma-kriptografi-kunci-publik.html.

[5] drdobbs. (n.d.). *rsa-digital-signatures*. Retrieved from http://www.drdobbs.com/rsa-digital-signatures/184404605.

[6] Ilmu-kriptografi.blogspot.com (November 2015). Tutorial-pemrograman-kriptografi. Retrieved September 2019, from https://ilmu-kriptografi.blogspot.com/2015/11/tutorial-pemrograman-kriptografi.html.

[7] Ilmukriptografi.wordpress.com (24 Oktober 2012). *Public-key-RSA*. Retrieved September 2019, from https://ilmukriptografi.wordpress.com/2012/10/24/public-key-rsa/.

[8] Ilmuskripsi.com (Juni 2016). Perancangan-Aplikasi-Penyandian. Retrieved Agustus 2019, from https://www.ilmuskripsi.com/2016/06/perancangan-aplikasi-penyandian.html.

[9] Kustiwi, A. (2014). Implementasi Algoritma RSA (Rivest Shamir Adleman). *FMIPA UNIBBA*.

[10] Medium.com (4 Agustus 2018). Tak-pernah-aman-transkip-nilai-pada-siakad. Retrieved September 2019, from https://medium.com/bosnaufalid/client-side-tak-pernah-aman-transkip-nilai-pada-siakad-bbce76ceb25.

[11] Mustikarani, D. A. (2014). *digital-signature-tanda-tangan-digital*. Retrieved 06 2019, from http://dentiastimustikarani.blogspot.com/2014/05/digital-signature-tanda-tangan-digital.html.

[12] Mylopedia.blogspot.com (April 2012). Algoritma-Caesar-Cipher. Retrieved Agustus 2019, from http://mlopedia.blogspot.com/2012/04/algoritma-kriptografi-caesar-cipher.html

[13] Sasmito, R., Rakhmatsyah, A., & Adiwijaya. (2008). Digital Signature Menggunakan Algoritma Kriptografi RSA untuk Perlindungan Data pada MMS.

[14] Sindonews.com (10 Januari 2014). Marak-pemalsuan-transkip-nilai-pts.Retrieved September 2019, From https://daerah.sindonews.com/read/82247/22/marak-pemalsuan-transkip-nilai-pts-1389290969

[15] Suharya, Y. (2017). Analisis Kinerja Implementasi Algoritma Digital Signature Rsa (*Rivest Shamir Adleman*) Dan Elgamal Pada Kriptografi. Universitas Langlang Buana.