BAB II
KERANGKA TEORITIS

A. Penelitian Rujukan

Peneletian ini dilakukan berdasarkan adanya penelitian rujukan yaitu penelitian sebelumnya yang menitik beratkan terhapat keamanan dengan memamfaatkan algoritma RSA pada kehidupan sehari hari baik individu maupun organisasi guna memberikan keamanan pada pengguna di zaman modern. Banyak penelitian sebelumya telah dilakukan mengenai keamanan dengan menggunakan algoritma RSA.

1. Implementasi Algoritma Kriptografi RSA untuk Enkripsi dan Dekripsi Email(Albert Ginting, R. Rizal Isnanto, Ike Pertiwi Windasari, 02 April 2015

Pada proses pengiriman data(pesan) terdapat beberapa hal yang harus diperhatikan yaitu: kerahasian, integritas data, autentikasi. Oleh karena itu dibutuhkan suatu proses penyandian atau pengkodean pesan sebelum dilakukan proses pengiriman. Sehingga pengiriman pesan yang dikirim terjaga kerahasiannya dan tidak dapat dengan mudah diubah untuk menjaga integritas pesan tersebut. Ilmu yang mempelajari tentang cara pengamanan data dikenal dengan istilah kriptografi,sedangkan langkah langkah dalam kriftograpi disebut algoritma kriftografi. Contoh algoritma kriptografi yang dapat diandalkan adalah RSA.

Tujuan dari penelitian ini adalah Merancang dan membangun purwarupa email client yang mampu melakukan enkripsi dan dekripsi dengan menerapkan ilmu kriptografi RSA sehingga dirasakan aman.

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. Kenyataannya, memfaktorkan bilangan bulat menjadi faktor primanya bukanlah pekerjaan yang mudah. Karena belum ditemukan algoritma yang efisien untuk melakukan pemfaktoran. Cara yang bisaa digunakan dalam pemfaktoran adalah dengan menggunakan pohon faktor. Jika semakin besar bilangan yang akan difaktorkan, maka semakin lama

waktu yang dibutuhkan. Jadi semakin besar bilangan yang difaktorkan, semakin sulit pemfaktorannya, semakin kuat pula algoritma RSA.

a. Berdasarkan hasil penelitian dan pembahasan yang telah dilakukan, dapat diambil beberapa kesimpulan sebagai berikut :
b. Aplikasi yang menerapkan algoritma kriptografi RSA ini berjalan dengan baik mampu mengirim dan menerima email, dan dapat mengenkripsi dan dekripsi kotak masuk yang diterima.
c. Dengan perangkat lunak ini, tujuan penelitian tercapai yaitu keamanan dalam menerima email terjamin. Ada pengamanan ganda untuk membuka pesan tersandi. Saat mendekripsi pesan yang telah dienkripsi harus memasukkan password terlebih dahulu, apabila masukan password salah pesan tidak akan didekripsi.
d. Perangkat lunak ini hanya mengamankan isi pesan masuk email bukan mengamankan jalur transfer email.
e. Pada aplikasi yang dikembangkan ini, satu pesan asli dapat menghasilkan ciphertext yang berbeda-beda, karena proses pembangkitan kunci RSA didasarkan oleh nilai P dan Q yang acak.

Pesan kesalahan akan ditampilkan apabila terjadi kesalahan saat memasukkan suatu nilai yang salah saat enkripsi atau dekripsi pesan. Saat enkripsi masukan bit bernai kosong dan saat dekripsi masukan password salah.

2. Rancang Bangun Sistem Pengamanan Dokumen Pada Sistem Informasi Akademikdengan Menggunakan Digital Signature(Ahmaddul Hadi, September 2013)

Pengamanan dokumentasi baik yang tercetak (paper) maupun yang tidak tercetak (paperless) sangat diperlukan terlebih dokumen tersebut digunakan sebagai bukti transaksi dari sebuah proses aplikasi. Penggunaan tandatangan digital (Digital Signature) yang ditambahkan pada setiap lembaran tercetak merupakan salah satu alternatif pengamanan dokumen terlebih dengan menggunakan algoritma tandatangan digital DSA (Digital Signature Algorythm) yang dapat memberikan keamanan lebih karena telah di enkripsi dengan metode SHA Model dengan panjang 32bit. Output sistem informasi akademik (SIA) UNP berupa KRS, LHS, dan dokumen lainnya ditambahkan tandatangan digital pada saat melakukan perintah cetak. Informasi (plaintext) yang di-enkripsi pada proses signing yaitu NIM, indek prestasi, jenis dokumen dan waktu cetak. Pada proses signing ke empat variabel ini di-enkripsik dengan algoritma DSA menghasilkan kunci public r

yang tersimpan pada sebuah tabel database, kunci private s serta chipertext (ds code). Pada proses pengujian keabsahan tandatangan dibuat sebuah aplikasi yang berfungsi menguji tandatangan (verifying) yang telah dihasilkan pada proses signing dengan menggunakan kunci public yang telah ada dan mencari kunci private dari proses dekripsi nilai chipertext, jika nilai kunci cocok maka ditampilkan informasi valid dari dokumen.

Kesimpulan dari tulisan ini tulisan ini adalah sebagai berikut :

a. Pengamanan dokumen elektronik sistem informasi akademik (SIA) menggunakan digital signatur dengan algoritma kurva eliptik dapat diimplementasikan dengan baik dan dibantu dengan barcode reader yang berfungsi membantu untuk meng-inputkan karakter ke form input, dan kecendrung akan salah jika menggunakan keyboard yang diketikkan dengan tangan.
b. Algoritma DSA yang digunakan relative lebih baik jika dibandingkan dengan algoritma jenis lainnya karena sama-sama terbaca chipper text dengan aplikasi sniffing tetapi tidak dapat didekripsikan.

3. Tanda tangan Digital Menggunakan Algoritme Keccak dan RSA (Rezania Agramanisti Azdy, 3, Agustus 2016)

Dengan semakin berkembangnya internet, sebuah dokumen kini tidak hanya diterbitkan dalam bentuk cetak saja, tetapi juga dalam bentuk digital. Akan tetapi, sebuah dokumen yang ditransmisikan melalui internet sangat rentan terhadap kemungkinan modifikasi serta sulitnya pembuktian keaslian dokumen tersebut. Selain itu, seorang pengirim dapat dengan mudahnya menyangkal bahwa dialah yang telah menulis atau mengirimkan dokumen tersebut. Tanda tangan digital merupakan sebuah teknik dalam kriptografi yang dapat digunakan untuk menandatangani dokumen digital. Berbeda dengan persepsi masyarakat pada umumnya mengenai tanda tangan digital yang merupakan hasil digitalisasi dari tanda tangan seseorang, tanda tangan digital sebenarnya merupakan hasil dari diberlakukannya teknik kriptografi terhadap pesan atau dokumen asli.

Pada dunia nyata, tanda tangan digunakan untuk mengidentifikasi keabsahan seseorang pada dokumen yang ditandatanganinya. Selain itu, tanda tangan juga dapat digunakan untuk membuktikan bahwa penandatangan telah mengetahui dan menyetujui isi dari dokumen yang ditandatanganinya tersebut. Atribut yang harus dimiliki oleh sebuah tandatangan adalah:

a. Autentikasi penandatangan, yaitu tanda tangan dapat secara unik mengidentifikasi pembuat dokumen tanpa dapat ditiru oleh orang lain.
b. Autentikasi dokumen, yaitu tanda tangan dapat digunakan untuk membuktikan keaslian dokumen, sehingga dapat diketahui jika dokumen asli telah dimodifikasi.

Pada makalah ini telah diimplementasikan algoritme Keccak dan RSA pada tanda tangan digital dengan menggunakan program sederhana yang ditulis dengan bahasa Java.

Penggunaan algoritme Keccak berhasil menjaga aspek keamanan dalam hal integritas data. Hal ini dikarenakan sampai saat ini Keccak masih bersifat collision resistance, sehingga belum ditemukan adanya dua data yang berbeda menghasilkan message digest yang sama. Penggunaan algoritme RSA dapat menjamin aspek keamanan dalam hal autentikasi dan non-repudiation. Pembangkitan kunci pada RSA memastikan hanya pasangan kunci yang digunakan untuk proses enkripsilah yang dapat digunakan untuk proses dekripsinya. Sehingga dengan pasangan kunci yang tepat proses enkripsi dan dekripsi dapat menghasilkan hasil yang tepat, dan tidak dapat dielakkan lagi bahwa pembuat dokumen adalah orang yang sama dengan pemilik kunci yang digunakan untuk proses enkripsinya. 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.

4. Implementasi Kriptografi Kunci Publik dengan Algoritma RSA-CRT pada Aplikasi Instant Messaging(Ashari Arief dan Ragil Saputra, Vol. 3, No. 1, Mei 2016)

Salah satu kemajuan teknologi komunikasi yaitu menghasilkan aplikasi instant messaging atau pesan instan. Instant messaging merupakan fasilitas komunikasi chatting untuk para pengguna internet sehingga user dapat berkomunikasi dengan cara mengirimkan pesan berupa teks dengan user lain. Namun seiring dengan kemajuan teknologi, dengan semakin banyaknya pengguna yang menggunakan aplikasi instant messaging terdapat dampak negatif berupa penyadapan data khususnya saat terjadi komunikasi yang bersifat rahasia dan penting sehingga aspek keamanan dalam pertukaran informasi dianggap penting.

Aplikasi instant messaging menggunakan algoritma kriptografi RSA-CRT dengan pemrograman soket berbasis TCP, sehingga dibuatnya class

TcpListener dengan port 8888 dan class TcpClient (untuk server), class TcpClient (untuk client), serta dibuatnya inisialisasi port 8888 untuk melakukan hubungan (pada sisi client).

Pengujian algoritma kriptografi RSA-CRT pada aplikasi instant messaging yang utama adalah membandingkan kecepatan dekripsi antara algoritma kriptografi RSA dengan algoritma kriptografi RSA-CRT. Waktu yang digunakan untuk melakukan proses dekripsi sebagai perbandingan antar kedua algoritma kriptografi.

Pengujian dilakukan dengan menggunakan 1800 karakter dummy, jumlah bit n yang digunakan mulai dari 56 bit sampai 88 bit, dikarenakan pesan yang digunakan untuk melakukan pengujian yaitu 1.800 karakter sehingga mempunyai syarat nilai n harus lebih besar atau sama dengan 1.000.000.,maka dapat di tarik kesimpulan dengan hasil yaitu:

Implementasi algoritma kriptografi kunci publik dengan algoritma RSA-CRT pada aplikasi instant messaging, proses dekripsi menggunakan algoritma RSA-CRT untuk 1.800 karakter dengan bit n dari 56 bit sampai 88 bit memiliki kecapatan rata-rata dua kali lebih cepat dibandingkan menggunakan algoritma RSA. Semakin besar panjang string, nilai n kemungkinan besar semakin cepat waktu dekripsi menggunakan RSA-CRT.

5. **Implementasi Kriptografi Algoritma Rivest Shamir Adleman dengan Playfair Cipher pada Pesan Teks Berbasis Android (Satriya Tri Cahya Kurniawan, Dedih , Supriyadi, Desember 2017 : 102-109)**

Algoritma RSA termasuk ke dalam jenis algoritma kriptografi asimetri. Algoritma RSA melakukan pemfaktoran bilangan yang sangat besar sehingga algoritma RSA dianggap aman. Keamanan algoritma RSA terletak pada tingkat kesulitan dalam memfaktorkan bilangan non-prima menjadi faktor prima lainnya. Kriptografi sering menimbulkan kecurigaan pihak ketiga, sebab file dokumen yang sulit dimengerti dapat menunjukkan bahwa file dokumen itu berisi informasi penting Untuk menghindari permasalahan tersebut maka lahir ilmu yang dikenal dengan nama steganografi.

Salah satu metode steganografi yang banyak digunakan yaitu metode Least Significant Bit (LSB). Metode LSB memiliki kelebihan pada proses embedding (encoding) dan extracting(decoding) yang lebih cepat dari metode steganografi lainnya. Metode LSB hanya mengubah nilai byte satu lebih tinggi atau satu lebih rendah dari nilai sebelumnya sehingga tidak berpengaruh terhadap persepsi visual.

Fase perancangan, pada fase ini dibuat rancangan aplikasi yang terdiri dari beberapa tahapan, seperti perancangan struktur navigasi, perancangan diagram UML (Unified Modeling Language) dan perancangan tampilan atau user interface aplikasi. Fase implementasi dilakukan implementasi dengan membangun aplikasi dengan menuliskan kode program menggunakan bahasa pemrograman C#.NET.

Fase uji coba yaitu melakukan pengujian terhadap aplikasi yang telah dibangun dengan mencoba melakukan enkripsi pada file dokumen penting yang didapat melalui internet dan kemudian hasil enkripsi disembunyikan dengan cara disisipkan (encoding) pada sebuah citra gambar. Kemudian citra gambar hasil encoding dilakukan decoding untuk mendapatkan informasi yang telah dienkripsi sebelumnya dan pada informasi tersebut dilakukan dekripsi untuk mendapatkan informasi yang dapat dibaca.

Dari hasil uji coba aplikasi yang telah dilakukan dapat dilihat bahwa proses enkrispi dan penyisipan (encoding) dapat berjalan dengan baik pada file teks maupun dokumen. Pada proses ekstraksi(decoding) dan dekripsi, aplikasi juga dapat berjalan dengan baik. Dari skenario uji coba enkripsi dan dekripsi dapat dilihat bahwa jumlah karakter hasil enkripsi lebih banyak dari karakter yang dienkripsi. Ukuran file setelah dienkripsi lebih besar dari sebelum dilakukan.

Enkripsi dan ukuran file setelah dekripsi lebih kecil dari sebelum dilakukan dekripsi. Semakin besar bilangan prima yang digunakan untuk enkripsi maka semakin banyak karakter hasil enkripsi yang dihasilkan. Pada skenario uji coba encoding dan decoding tidak terjadi perubahan ukuran pada gambar dengan format *.bmp yang disisipi baik setelah dilakukan encoding maupun decoding Sehingga penggunaan gambar dengan format *.bmp dapat dikatakan lebih baik.

6. **Implementasi Algoritma rivest-shamir-adleman (rsa) dan metode least significant bit(lsb) untuk keamanan file teks dan dokumen menggunakan visual c# (Kemal Ade Sekarwati, Ariep Budiman, April 2017)**

Algoritma RSA termasuk ke dalam jenis algoritma kriptografi asimetri. Algoritma RSA melakukan pemfaktoran bilangan yang sangat besar sehingga algoritma RSA dianggap aman. Keamanan algoritma RSA terletak pada tingkat kesulitan dalam memfaktorkan bilangan non-prima menjadi faktor prima lainnya. Kriptografi sering menimbulkan kecurigaan pihak ketiga, sebab file dokumen yang sulit dimengerti dapat menunjukkan bahwa file dokumen itu berisi informasi penting. Untuk menghindari permasalahan tersebut maka lahir

ilmu yang dikenal dengan nama steganografi. Salah satu metode steganografi yang banyak digunakan yaitu metode Least Significant Bit (LSB). Metode LSB memiliki kelebihan pada proses embedding (encoding) dan extracting(decoding) yang lebih cepat dari metode steganografi lainnya. Metode LSB hanya mengubah nilai byte satu lebih tinggi atau satu lebih rendah dari nilai sebelumnya sehingga tidak berpengaruh terhadap persepsi visual.

Penelitian ini akan membuat sebuah aplikasi yang mengimplementasikan teknik kriptografi dengan algoritma RSA dan teknik steganografi dengan metode Least Significant Bit (LSB) untuk keamanan file dokumen menggunakan bahasa pemrograman C#.NET.

Ada bebrapa fase dalam melakukan penelitian ini diantaranya:

a) Fase analisa. Dengan mengumpulkan berbagai informasi dan bahan-bahan yang digunakan untuk menyelesaikan masalah dan menunjang penulisan serta pembuatan aplikasi, yaitu mempelajari berbagai sumber pustaka yang berhubungan dengan Kriptografi, Algoritma RSA, Steganografi, metode Least Significant Bit (LSB) dan bahasa pemrograman C#.NET.
b) Fase perancangan. Pada fase ini dibuat rancangan aplikasi yang terdiri dari beberapa tahapan, seperti perancangan struktur navigasi, perancangan diagram UML (Unified Modeling Language) dan perancangan tampilan atau user interface aplikasi. Fase implementasi dilakukan implementasi dengan membangun aplikasi dengan menuliskan kode program menggunakan bahasa pemrograman C#.NET.
c) Fase uji coba. Pada fase ini melakukan pengujian terhadap aplikasi yang telah dibangun dengan mencoba melakukan enkripsi pada file dokumen penting yang didapat melalui internet dan kemudian hasil enkripsi disembunyikan dengan cara disisipkan (encoding) pada sebuah citra gambar. Kemudian citra gambar hasil encoding dilakukan decoding untuk mendapatkan informasi yang telah dienkripsi sebelumnya dan pada informasi tersebut dilakukan dekripsi untuk mendapatkan informasi yang dapat dibaca.

Dari hasil uji coba aplikasi yang telah dilakukan dapat dilihat bahwa proses enkrispi dan penyisipan (encoding) dapat berjalan dengan baik pada file teks maupun dokumen. Pada proses ekstraksi (decoding) dan dekripsi, aplikasi juga dapat berjalan dengan baik.

B. Landasan Teori

1. Kriptografi

Dalam kriptografi klasik (simetris), jika seseorang mengetahui cara mengen kripsi naskah asli menjadi naskah acak, maka orang tersebut juga mengetahui cara mendekripsi naskah acak yang dihasilkan. Demikian juga jika seseorang mengetahui cara mendekripsi naskah acak, maka orang tersebut juga menge tahui cara mengenkripsi naskah asli untuk menghasilkan naskah acak.

Sekitar pertengahan tahun 1970an, muncul konsep baru dalam kriptografi yaitu kriptografi public key (asimetris). Seseorang yang mengetahui cara meng enkripsi naskah asli belum tentu mengetahui juga cara mendekripsi naskah acak yang dihasilkan. Demikian juga seseorang yang mengetahui cara mendekripsi naskah acak belum tentu mengetahui juga cara mengenkripsi naskah asli untuk menghasilkan naskah acak tersebut. Enkripsi dan dekripsi dalam kriptografi public key menggunakan sepasang kunci yaitu kunci publik (*public key*) dan kunci privat (*private key*). Naskah yang telah dienkripsi menggunakan kunci privat hanya dapat didekripsi menggunakan kunci publik dan naskah yang dapat didekripsi menggunakan kunci publik dapat dipastikan telah dienkripsi menggunakan kunci privat. Sebaliknya, naskah yang telah dienkripsi menggunakan kunci publik hanya dapat didekripsi menggunakan kunci privat. Mekanisme ini memungkinkan berbagai aplikasi, dua yang terpenting di antaranya adalah distribusi kunci sesi dan tanda tangan digital (*digital signature*).

Jika A ingin mengirim kunci sesi atau rahasia lainnya ke B dan hanya ingin B yang dapat membacanya, maka A mengenkripsi rahasia tersebut menggu nakan kunci publik milik B. Dengan asumsi hanya B yang memiliki kunci privat B, maka hanya B yang dapat mendekripsi rahasia yang telah dienkripsi tersebut. Cara inilah yang kerap digunakan untuk mendistribusikan kunci sesi menggunakan kriptografi public.

Jika A ingin menanda tangan suatu naskah secara digital, maka A mengenkripsi naskah tersebut menggunakan kunci privat miliknya dan hasil enkripsi merupakan \tanda tangan," Jika seseorang (sebut saja B) ingin memeriksa apakah naskah tersebut telah ditanda-tangan oleh A, maka B mendekripsi \tanda tangan" tersebut dengan kunci publik milik A dan membandingkan hasil dekripsi dengan naskah yang ditanda-tangan. Jika sama maka B dapat meyakinkan dirinya sendiri bahwa A telah menanda-tangan naskah tersebut karena hanya A yang memiliki kunci privat yang

digunakan untuk mengenkripsi naskah untuk menghasilkan \tanda-tangan." Dalam prakteknya yang dienkripsi bukan naskah penuh melainkan digest dari naskah tersebut.

Jadi dalam kriptografi *public key*, kunci publik dapat disebar luaskan ke pada umum dan sebaiknya disebar luaskan. Sebaliknya, kunci privat harus dirahasiakan oleh pemiliknya(Sentot Kromodimoeljo,2009,297-298)

2. Sertifikat Digital (Digital Certificates)

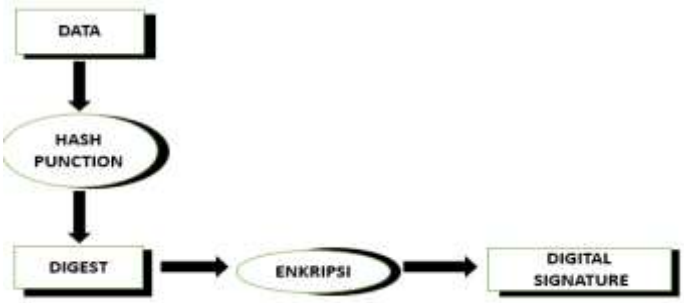
Sejak ditemukan pada tahun 1970-an, tanda tangan digital diharapkan dapat berperan sebagai tanda tangan pada dokumen kertas.perkembangan teknologi yang pesat menjadikan tanda tangan digital sebagai komponen penting dalam bisnis di *cyberscape* saat ini. Bahkan di beberapa negara maju tanda tangan digital telah memiliki kekuatan hukum.

Disaat tanda tangan digital mulai lazim digunakan dan bahkan berkakuatan hukum, sebagai ahli di bidang informatika justru mulai mempertanyakan ke absahan tanda tangan digital. Bukan karena lemahnya kekuatan matematis dari algoritma yang di gunakan tetapi lebih kepada banyaknya celah kelemahan pada implementasi tanda tangan digital tersebut.

Tanda tangan digital merupakan tanda tangan yang dilakukan dengan memakai alat elektronik yang berfungsi sama dengan tanda tangan manual. Tanda tangan digital merupakan kumpulan bit yang bisa melakukann fungsi elektronik yang memakai fungi Hash satu arah. Pada dasarnya tanda tangan digital dari setiap dokumen berbeda dengan dokumen lain karena diambil dari dokumen itu sendiri. Bilamana terjadi perubahan pada dokumen maka hal itu tentu akan menciptakan tanda tangan digital yang berbeda. Tanda tangan digital juga mempunyai fungsi yang sama dengan tanda tangan manual yang mengabsahkan suatu dokumen yang bisa dijadikan persetujuan, tanda terima dan lain sebagainya(Dony Arius,2008,295-296)

Sifat dari tanda tangan digital di antaranya:

1) Authentication,jaminan dari suatu pesan yang belum dimodifikasi di dalam pengiriman (keaslian pesan atau integritas pesan).
2) Cuma berlaku untuk sekali pengiriman dokumen.
3) Keabsahan tanda tangan digital itu dapat diperiksa oleh pihak yang menerima pesan walaupunbelum pernah saling bertemu sekalipun.



Gambar 2. 1 Proses Tanda Tangan Digital

3. OpenSSL

OpenSSL adalah suatu protokol tambahan yang digunakan untuk Secure Socket Layer. Yang maksudnya adalah mengamankan jaringan kita antara client dan server. Dengan OpenSSL ini, maka jaringan akan sulit di sniffing. Jika dalam keadan HTTP biasa (Plain TEXT), kemungkinan besar bisa terkenad MITM Attack (Man In The Middle Attack).

HTTP itu sendiri memberikan definisi terhadap bagaimana pesan dapat disampaikan dan diformat dari server menuju klien, sedangkan HTTPS atau yang memiliki kepanjangan Hypertext Transfer Protocol Secure ini juga merupakan suatu protokol yang dipakai oleh www dimana https itu sendiri akan memberikan definisi terhadap bagaimana pesan dapat disampaikan dan diformat dari server menuju klien dengan sangat aman. Contoh situs-situs yang menggunakan protokol https,sebagai berikut :

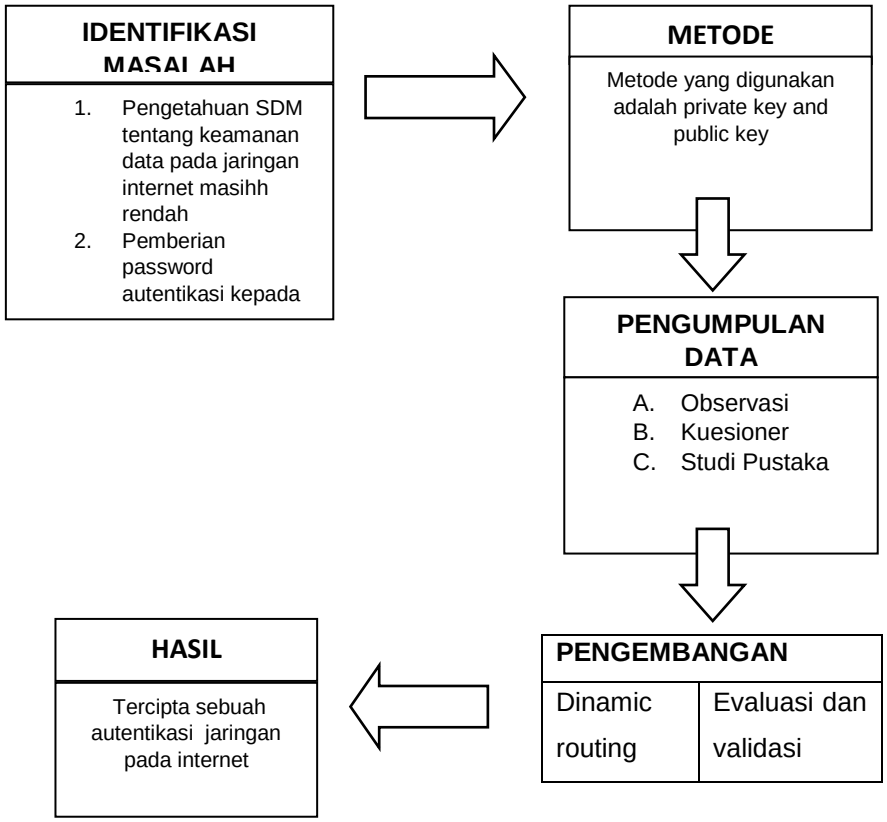
1) https://www.facebook.com
2) https://www.google.com
3) https://www.wordpress.com
4) https://tune-new.telkomuniversity.ac.id
5) https://mail.google.com

SSL merupakan singkatan dari Secure Socket Layer, dikenal juga dengan istilah Transport Secure Layer (TLS). SSL sangat penting dalam menjaga kerahasiaan informasi saat kita menggunakan layanan yang berbasis internet, misalnya internet banking. SSL menggunakan prinsip enkripsi dan dekripsi. Setiap input yang dimasukkan akan di enkripsi sedemikian rupa menggunakan public key sehingga hasil enkripsinya hanya dapat didekripsikan oleh pemegang private key. Penyedia layanan memegang private key, sementara web browser memegang public key. Private key harus

dijaga karena dapat mentranslasikan hasil enkripsi. Dengan adanya SSL, maka kegiatan yang memanfaatkan internet dan membutuhkan privasi yang sangat tinggi sudah dapat dilakukan dengan mudah tanpa khawatir akan bocornya rahasia.

C. Kerangka Pemikiran

Berikut merupakan kerangka pemikiran pemecahan masalah dalam ini yang di gambarkan pada gambar 2. 2.



Gambar 2. 16 kerangka Pemikiran

Penjelasan tentang kerangka pemikiran pada penelitian ini, yaitu :

1. Identifikasi masalah untuk menetapkan tujuan penelitian
2. Dengan menggunakan private and public key dapat dilakukan untuk autentikasi pada jaringan internet.
3. Mengumpulkan data berdasarkan kebutuhan setiap user.
4. Melakukan pengembangan melalui tahap perancangan, tahap implementasi, dan tahap pengujian.
5. Dari hasil yang diharapkan terciptanya sebuah autentikasi jaringan internet yang lebih aman untuk pengguna.