

Penerapan Algoritma Rivest Shamir Adleman (RSA) Pada Aplikasi Keamanan Data Pembuatan SIM Baru Di Satlantas Polres Belawan

Implementation of the Rivest Shamir Adleman (RSA) Algorithm in the Data Security Application for Making New Driving Licenses at the Belawan Police Traffic Unit

Juli Ramadhani^{a,1}, Rita Novita Sari^{b,2}

^{a,b}Universitas Potensi Utama, K.L. Yos Sudarso KM 6.5 No. 3A Tj. Mulia, Kota Medan, 20241, Indonesia
juliramadhani27@gmail.com¹, rita.ns89@gmail.com²

ABSTRAK

Satlantas Polres Belawan yang bergerak dibidang layanan kemasyarakatan salah satunya dalam pembuatan SIM mengemudi. Setiap harinya Satlantas Polres Belawan menerima jasa pembuatan SIM baik untuk SIM A, SIM B dan jenis SIM Dengan banyaknya data pembayaran dari masyarakat yang diberikan kepada pihak Satlantas Polres Belawan sering terjadi kebocoran data pribadi yang amat disayangkan bila data pribadi tersebut jatuh kepada orang yang salah dan disalah gunakan. Data - data pembuatan dan pengurusan SIM berupa nama pengemudi, alamat, nomor SIM, dan data lainnya yang disimpan belum memiliki keamanan untuk menjaga data - data tersebut dari kebocoran data, yang sering terjadi kebocoran data dan disalah gunakan oleh pihak yang tidak bertanggung jawab. Keamanan merupakan salah satu aspek terpenting dari sebuah sistem informasi. Masalah keamanan sering kurang mendapat perhatian dari para perancang dan pengelola sistem informasi. Masalah keamanan sering berada diurutan setelah tampilan, atau bahkan diurutan terakhir dalam daftar hal-hal yang dianggap penting. Untuk mengatasi permasalahan yang dihadapi maka peneliti menggunakan teknik kriptografi dengan digunakannya metode RSA. Data yang di input banyak terdapat data pribadi yang sangat penting, maka dari itu di tambahkan kriptografi dalam keamanan pembuatan SIM agar data yang disimpan dapat diamankan.

Kata Kunci : Keamanan data, Pengurusan SIM, RSA

ABSTRACT

Belawan Police Traffic Unit which operates in the field of community services, one of which is in making driving licenses. Every day the Belawan Police Traffic Unit receives SIM making services for both SIM A, B SIM and other types of SIM. With the large amount of payment data from the public provided to the Belawan Police Traffic Unit, there is often a leak of personal data which is very threatening if the personal data falls to the wrong person and misuse. The data for creating and managing a driver's license in the form of the driver's name, address, driver's license number and other data that is stored does not have the security to protect the data from data leaks, which often occur and are misused by irresponsible parties. Security is one of the most important aspects of an information system. Security issues often receive little attention from designers and managers of information systems. Security issues are often ranked after appearance, or even last on the list of things that are considered important. To overcome the problems faced, researchers used cryptographic techniques using the RSA method. The data that is input contains a lot of very important personal data, therefore cryptography is added to the security of making a SIM so that the stored data can be secured.

Keywords: Data security, SIM management, RSA

1. PENDAHULUAN

Pengertian aplikasi adalah suatu bagian dari perangkat lunak yang dapat digunakan untuk menyelesaikan masalah-masalah yang khusus yang dihadapi user dengan menggunakan kemampuan komputer. Sedangkan pengertian penjualan adalah suatu proses seseorang atau organisasi untuk meyakinkan customer membeli produk yang ditawarkan. Aplikasi mobile dapat diartikan sebagai sebuah produk dari sistem komputasi mobile, yaitu sistem komputasi yang dapat dengan mudah dipindahkan

secara fisik dan yang komputasi kemampuan dapat digunakan saat mereka sedang dipindahkan. Contohnya adalah personal digital assistant (PDA), smartphone dan ponsel[1].

RSA merupakan algoritma kriptografi kunci publik (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. Kenyataannya, memfaktorkan bilangan bulat menjadi faktor primanya bukanlah pekerjaan yang mudah. Karena belum ditemukan algoritma yang efisien untuk melakukan pemfaktoran. Cara yang bisa digunakan dalam pemfaktoran adalah dengan menggunakan pohon faktor. Jika semakin besar bilangan yang akan difaktorkan, maka semakin lama waktu yang dibutuhkan. Jadi semakin besar bilanganyang difaktorkan, semakin sulit pemfaktornya, semakin kuat pula algoritma RSA[2].

Kriptografi berasal dari Bahasa Yunani, yaitu kriptos dan graphia. Menurut bahasa kriptos berarti rahasia (secret) dan graphia berarti tulisan (writing). Menurut terminology, Kriptografi adalah ilmu seni untuk menjaga keamanan pesan ketika pesan dikirim dari suatu tempat ke tempat yang lain. Secara keseluruhan kriptografi dapat disimpulkan sebagai ilmu yang mempelajari tentang pengacakan pesan dengan fungsi perhitungan matematika agar tidak bisa dibaca oleh pihak yang tidak berwenang. Kriptografi merupakan studi matematika yang mempunyai hubungan dengan aspek keamanan informasi seperti integritas data dan keaslian data. Selain itu kriptografi juga dapat dibagi berdasarkan jenis kunci yaitu algoritma simetris dan asimetris. Algoritma simetris adalah algoritma yang menggunakan kunci yang sama untuk melakukan enkripsi dan dekripsi, sedangkan algoritma asimetris adalah algoritma yang menggunakan kunci berbeda untuk melakukan enkripsi dan dekripsi, untuk enkripsi menggunakan kunci public dan dekripsi menggunakan kunci private[3]. AES Merupakan standar algoritma kriptografi terbaru yang dipublikasikan oleh NIST (National Institute of Standard and Technology) sebagai pengganti algoritma DES (Data Encryption Standard) yang sudah berakhir masa penggunaannya. Algoritma AES adalah algoritma kriptografi yang dapat mengenkripsi dan mendeskripsi data dengan panjang kunci 128 bit, 192 bit, dan 256 bit. Pada Algoritma AES[4]. Pada algoritma AES, jumlah blok input, blok output, dan state adalah 128 bit. Dengan besar data 128 bit, berarti $N_b = 4$ yang menunjukkan panjang data 22 tiap baris adalah 4 byte. Dengan blok input atau blok data sebesar 128 bit, key yang digunakan pada algoritma AES tidak harus mempunyai besar yang sama dengan blok input. Cipher key pada algoritma AES bisa menggunakan kunci dengan panjang 128 bit, 192 bit atau 256 bit. Perbedaan panjang kunci akan mempengaruhi jumlah round yang akan di implementasikan pada algoritma AES ini[5].

Secara umum kriptografi adalah teknik mengamankan data dengan cara mengubah atau mengolah informasi asli (plaintext) menggunakan kunci dan dengan sebuah metode enkripsi tertentu sehingga menghasilkan informasi yang baru (ciphertext) yang sulit dibaca secara langsung. Agar dapat terbaca kembali, ciphertext tersebut harus di dekripsi dengan kunci tertentu agar kembali menjadi plaintext. Maka dari itu dibangun suatu aplikasi yang mampu mengamankan data dengan bahasa pemrograman Java. Dari hasil pengujian yang dilakukan, aplikasi dapat merubah isi file asli (plaintext) menjadi karakter yang sulit dipahami (ciphertext) sehingga file terjaga keamanannya dan kecepatan penggunaan aplikasi sangat bergantung dengan ukuran file yang akan dienkripsi maupun didekripsi[6]. Metode algoritma kriptografi RSA untuk mengamankan data rekam medis pasien yang berisikan catatan dan dokumen tentang identitas pasien, diagnosa penyakit, pengobatan, tindakan dan pelayanan lain. RSA merupakan algoritma kriptografi asimetris yang menggunakan sepasang kunci, yaitu kunci publik dan kunci pribadi. Keamanan algoritma RSA terletak pada sulitnya memfaktorkan bilangan prima. Pada pengujian sistem menggunakan metode blackbox yang berfokus pada spesifikasi fungsional dari perangkat lunak[7].

Algoritma ini memiliki keamanan yang terletak pada kesulitan dalam menghitung algoritma diskrit. Baik kunci enkripsi maupun dekripsi keduanya merupakan bilangan prima. Bilangan algoritma freivalds tipen algoritma kriptografi asimetris terdiri atas dua buah kunci yaitu kunci public untuk melakukan enkripsi sedangkan kunci pribadi untuk melakukan deskripsi. Algoritma RSA merupakan salah satu metode dalam cabang ilmu kriptografi, dimana RSA adalah jenis kriptografi asimetris yang menggunakan dua kunci yaitu kunci pablik dan private. Algoritma kriptografi RSA didesain sesuai fungsinya sehingga kunci yang digunakan untuk enkripsi berbeda dari kunci yang digunakan untuk dekripsi. Kunci untuk enkripsi pesan disebut publik, sedangkan kunci untuk medekripsi pesan yang diterima disebut *private*[8]. Pada penelitian lain, RSA berperan sebagai enkripsi dan dekripsi untuk kunci AES yang berperan sebagai enkriptor dan dekriptor dokumen/data. Dengan kombinasi ini, kelebihan keduanya dapat dimanfaatkan untuk mencapai keamanan dan kerahasiaan data yang kuat. Untuk itu penulis berupaya mewujudkan implementasi keamanan data pada PT.XYZ. Pada penelitian ini, penulis melakukan pengamanan dokumen prosedur dan metode kalibrasi[9].

Keamanan komputer merupakan tindakan pencegahan dari serangan pengguna komputer atau pengakses jaringan yang tidak bertanggung jawab. Banyak yang belum mengetahui bahwa keamanan (security) merupakan sebuah komponen yang sangat penting. Bagi perancang dan pengelola sistem informasi, masalah kewanaman sering menjadi masalah. Kriptografi juga sangat berperan dalam berkomunikasi, untuk melakukan enkripsi (pengacakan) data, lalu ditransaksikan dari awal ke akhir bahkan bisa melakukan dekripsi data yang diacak tersebut [10]. Penelitian lain mensyaratkan sistem memiliki mekanisme perlindungan data yang memanfaatkan teknik kriptografi basis data, Dimungkinkan untuk menghindari penyalahgunaan oleh pihak yang tidak bertanggung jawab untuk mengubah atau mencuri informasi pasien. Catatan dan dokumen yang berkaitan dengan identitas pasien, aktivitas, dan layanan lainnya dilindungi oleh penelitian ini menggunakan algoritma Kriptografi RSA. Data didekripsi menggunakan sepasang kunci-kunci publik dan kunci pribadi dalam algoritme enkripsi asimetris yang dikenal sebagai RSA[11].

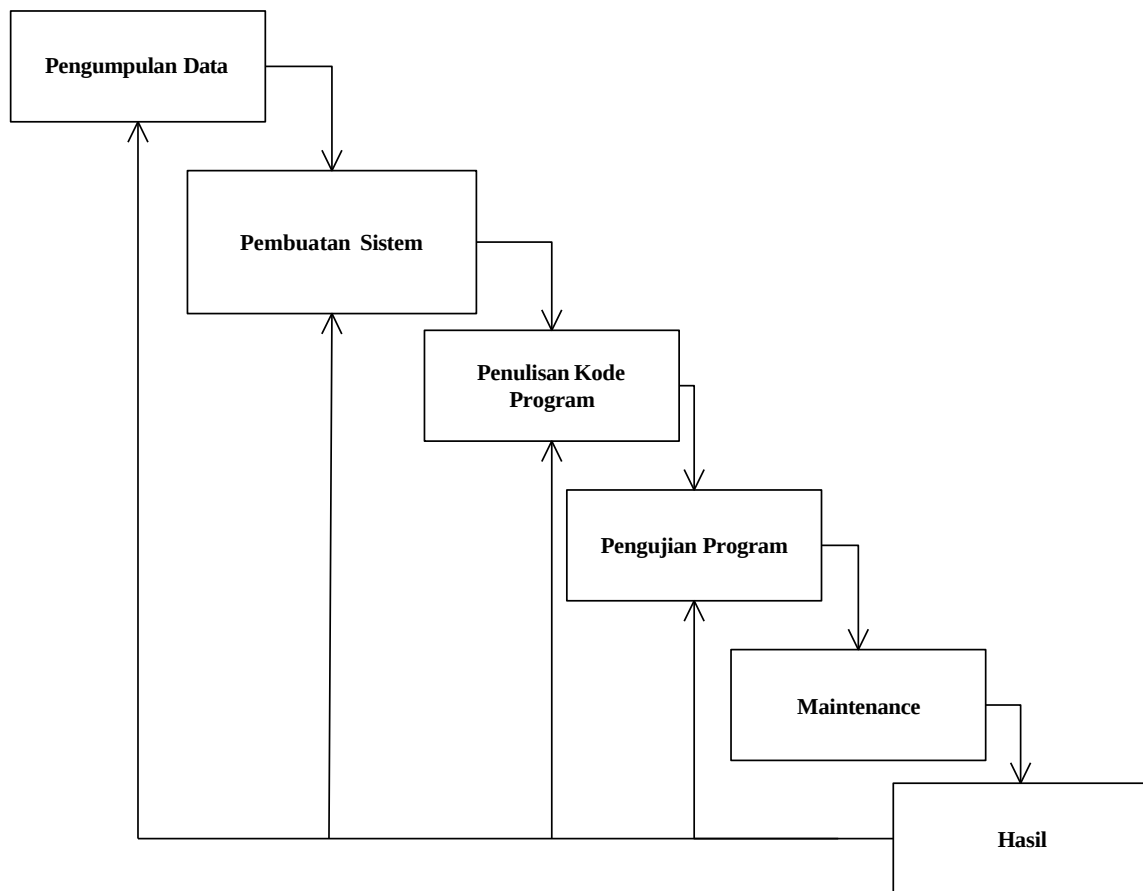
Basis data atau database merupakan koleksi dari data-data yang terorganisir dengan rapi sehingga data dapat dengan mudah disimpan dan dimanipulasi. Kita dapat menjumpai pemanfaatan database dalam kehidupan sehari-hari, seperti penggunaan mesin ATM, sistem akademi kuniversitas/sekolah, sistem informasi penjualan. Salah satu tujuan dari database adalah memberikan pengguna suatu pandangan abstrak dari data, yaitu sistem menyembunyikan rincian bagaimana data disimpan dan dipelihara. Sisem database harus dibuat semudah mungkin untuk dimengerti karena kebanyakan pengguna sistem *database* adalah orang-orang yang kurang terlatih di bidang teknologi [12].

Pada penelitian ini *database* yang digunakan untuk menyimpan data hasil dari inputan yaitu menggunakan *Firebase*. *Firebase* memiliki produk utama, yaitu menyediakan database realtime dan backend sebagai layanan (*Backend as a Service*). Layanan ini menyediakan pengembang aplikasi API yang memungkinkan aplikasi data yang akan disinkronisasi di klien dan disimpan di *cloud Firebase*. *Firebase* menyediakan library untuk berbagai client platform yang memungkinkan integrasi dengan Android, iOS, JavaScript, Java, Objective-C dan Node aplikasi Js dan dapat juga disebut sebagai layanan DbaaS (*Database as a Service*) dengan konsep *realtime*. *Firebase* digunakan untuk mempermudah dalam penambahan fitur-fitur yang akan dibangun oleh *developer*. *Database Realtime* merupakan basis data dalam *firebase* yang berbasis cloud dan tidak memerlukan *query* berbasis SQL untuk menyimpan dan mengambil data. Basis data ini terkenal sangat handal dan supercepat dalam peroses update data dan sinkronisasi sehingga data tetap dipertahankan bahkan ketika user tidak terhubung dengan internet sekalipun data tetap di pertahankan. *Firebase* dianggap sebagai platform aplikasi web. Itu membantu pengembang membuat aplikasi berkualitas tinggi. Ini menyimpan data di Format *JavaScript Object Notation* (JSON) yang tidak digunakan permintaan untuk memasukkan, memperbarui, menghapus atau menambahkan data ke dalamnya. Ini backend dari sistem yang digunakan sebagai database untuk menyimpan data[13].

Sedangkan, pada perancangan yang digunakan dalam penelitian ini adalah UML (*Unified Modelling Language*). *Unified Modelling Language* (UML) merupakan satu kumpulan konvensi pemodelan yang digunakan untuk menentukan atau menggambarkan sebuah sistem software yang terkait dengan objek. UML merupakan salah satu alat bantu yang sangat handal dalam bidang pengembangan sistem berorientasi objek karena UML menyediakan Bahasa pemodelan visual yang memungkinkan pengembang sistem membuat blue print atas visinya dalam bentuk yang baku. UML berfungsi sebagai jembatan dalam mengkomunikasikan beberapa aspek dalam sistem melalui jumlah elemen grafis yang bisa dikombinasikan[14]. Bahasa pemrograman yang digunakan pada penelitian ini adalah Bahasa pemrograman PHP. PHP atau kependekan dari *Hypertext Preprocessor* adalah salah satu bahasa pemrograman *opensource* yang sangat cocok atau dikhususkan untuk pengembangan web dan dapat ditanamkan pada sebuah skripsi HTML. Bahasa PHP dapat dikatakan menggambarkan beberapa bahasa pemrograman seperti C, Java, dan Perl serta mudah untuk dipelajari. PHP merupakan bahasa scripting server – side, dimana pemrosesan datanya dilakukan pada sisi server. Sederhananya, server yang akan menterjemahkan skrip program, baru kemudian hasilnya akan dikirim kepada client yang melakukan permintaan. Adapun pengertian lain PHP adalah akronim dari *Hypertext Preprocessor*, yaitu suatu bahasa pemrograman berbasis kode – kode (script) yang digunakan untuk mengolah suatu data dan mengirimkannya kembali ke web browser menjadi kode HTML[15].

2. METODE

Penelitian ini akan melalui beberapa tahapan. Tahapan dalam penelitian ini dapat di modelkan pada diagram Waterfall. Adapun beberapa tahapan yang digunakan dalam penelitian ini adalah sebagai berikut:



Gambar I. Diagram *Waterfall*

Keterangan :

1. Pengumpulan Data
Pada tahapan ini merupakan analisa terhadap kebutuhan yang diperlukan untuk mencapai tujuan penelitian yang akan dilakukan yaitu data pengurusan SIM pada Satlantas Polres Belawan.
2. Pembuatan Sistem
Desain sistem yang digunakan dalam teori adalah pemodelan UML yaitu use case diagram, class diagram, activity diagram dan sequence diagram.
3. Penulisa Kode Program
Pada tahapan ini peneliti menggunakan web browser dengan menggunakan DART. Peneliti menggunakan hardware komputer/laptop. Database yang digunakan adalah Firebase.
4. Pengujian
Pada tahapan ini peneliti menguji sistem yang telah dibuat menggunakan pengujian teori dan praktek. Pengujian teori peneliti menggunakan blackbox testing.
5. Maintenace
Perangkat lunak yang susah disampaikan kepada pengguna sistem pasti akan mengalami perubahan. Perubahan tersebut bisa karena mengalami kesalahan karena perangkat lunak harus menyesuaikan dengan lingkungan baru.
6. Hasil
Hasil dari penelitian ini adalah aplikasi keamanan data pembuatan sim baru di Satlantas Polres Belawan.

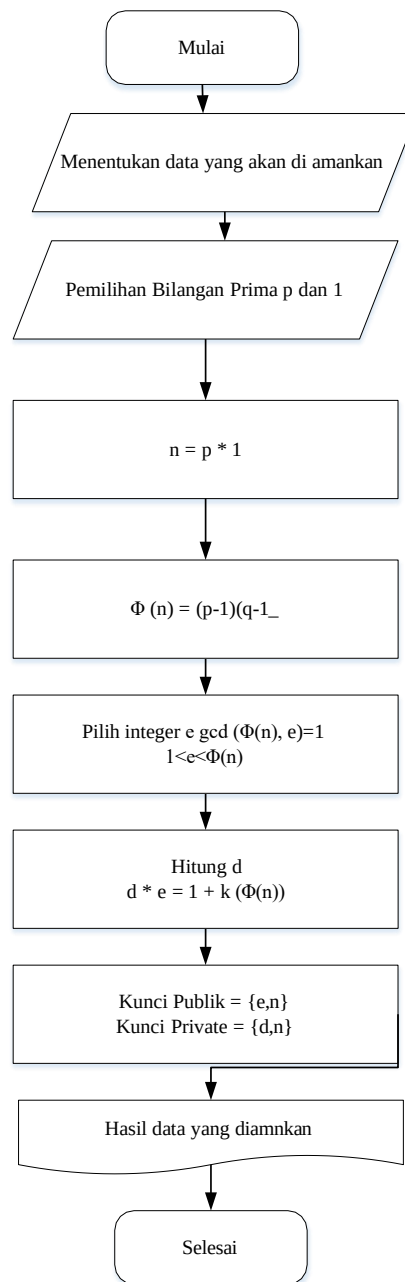
3. HASIL DAN PEMBAHASAN

Satlantas Polres Belawan yang bergerak dibidang layanan kemasyarakatan salah satunya dalam pembuatan SIM mengemudi. Setiap harinya Satlantas Polres Belawan menerima jasa pembuatan SIM baik untuk SIM A, SIM B dan jenis SIM Lainnya. Dengan banyaknya data pembayaran dari masyarakat yang diberikan kepada pihak Satlantas Polres Belawan sering terjadi kebocoran data pribadi yang amat disayangkan bila data pribadi tersebut jatuh kepada orang yang salah dan disalah gunakan.

Data - data pengurusan SIM berupa nama pengendara, alamat, nomor SIM, dan data lainnya yang disimpan belum memiliki keamanan untuk menjaga data - data terbut dari kebocoran data, yang sering terjadi kebocoran data dan disalah gunakan oleh pihak yang tidak bertanggung jawab. Keamanan merupakan salah satu aspek terpenting dari sebuah sistem informasi. Untuk mengatasi permasalahan yang dihadapi maka peneliti menggunakan teknik kriptografi dengan digunakannya metode RSA.

3.1. Penerapan Metode RSA

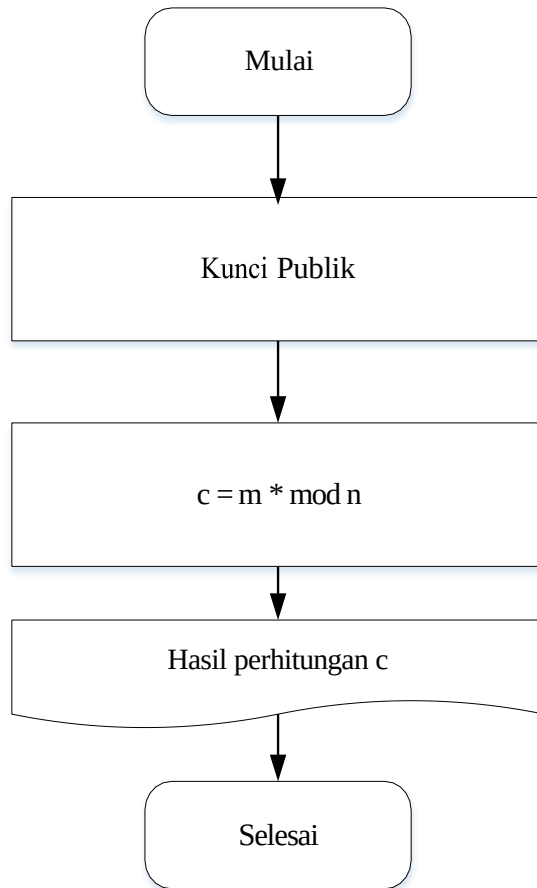
RSA merupakan algoritma kriptografi kunci publik (asimetris). Ditemukan pertama kali pada tahun 1977 oleh Ron Rivest, Adi Shamir, dan Len Adleman. Nama RSA sendiri diambil dari ketiga penemunya tersebut. Sebagai algoritma kunci publik, RSA mempunyai dua kunci, yaitu kunci publik dan kunci rahasia. RSA 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. Kenyataannya, memfaktorkan bilangan bulat menjadi faktor primanya bukanlah pekerjaan yang mudah. Jika semakin besar bilangan yang akan difaktorkan, maka semakin lama waktu yang dibutuhkan. Jadi semakin besar bilanganyang difaktorkan, semakin sulit pemfaktorannya, semakin kuat pula algoritma RSA. Adapun flowchart metode RSA adalah sebagai berikut:



Gambar 2. Flowchart Pembangkitan Kunci Metode RSA

Adapun keterangan dari Flowchart Pembangkitan Kunci Metode RSA adalah sebagai berikut :

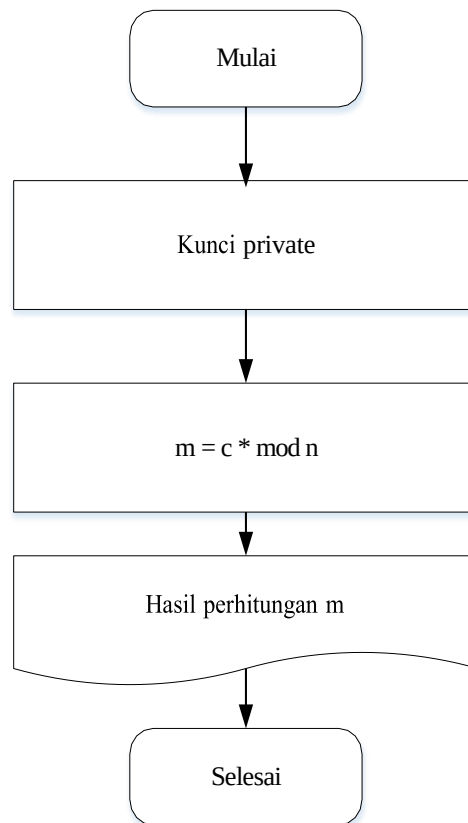
1. Mulai
2. Menentukan data yang diamankan
3. Menentukan pemilihan bilangan prima p dan q
4. Menentukan nilai n dengan $p * q$
5. Menentukan nilai bilangan
6. Menentukan nilai integer
7. Menentukan nilai d
8. Menentukan nilai Kunci publik dan kunci private
9. Selesai.



Gambar 3. *Flowchart Enkripsi Metode RSA*

Adapun keterangan dari Flowchart Enkripsi Metode RSA adalah sebagai berikut :

1. Mulai
2. Menentukan Kunci Publik
3. Menentukan nilai C
4. Selesai.



Gambar 4. Flowchart Dekripsi Metode RSA

Adapun keterangan dari Flowchart Dekripsi Metode RSA adalah sebagai berikut :

1. Mulai
2. Menentukan Kunci Private
3. Menentukan nilai M
4. Selesai.

Akan dilakukan enkripsi menggunakan algoritma RSA terhadap plaintext M = KEUANGAN. Pertama-tama plaintext tersebut diubah menjadi format ASCII sebagai berikut :

Tabel 1. Tabel ASCII Karakter "KEUANGAN":

Huruf	ASCII
K	75
E	69
U	85
A	65
N	78
G	71
A	65
N	78

Data yang Sudah Ditetapkan:

□ $p=61$, $q=53$

- $n=p \times q=61 \times 53=3233$
- $\phi(n)=(p-1) \times (q-1)=3120$
- Eksponen publik $e=17$
- Eksponen privat $d=2753$

Enkripsi dengan Kunci Publik

Enkripsi dilakukan dengan menggunakan rumus:

$$C = M^e \bmod n$$

di mana:

- M adalah nilai ASCII dari huruf
- $e=17$ adalah eksponen publik
- $n=3233$

1. Huruf "K" (ASCII = 75):

$$C = 75^{17} \bmod 3233$$

Langkah perhitungan:

$$75^{17} = 169518829100544703125$$

$$C = 169518829100544703125 \bmod 3233 = 2201$$

Jadi, ciphertext untuk "K" adalah 2201.

2. Huruf "E" (ASCII = 69):

$$C = 69^{17} \bmod 3233$$

Langkah perhitungan:

$$69^{17} = 1041273502979112415329$$

$$C = 1041273502979112415329 \bmod 3233 = 1313$$

Ciphertext untuk "E" adalah 1313.

3. Huruf "U" (ASCII = 85):

$$C = 85^{17} \bmod 3233$$

Langkah perhitungan:

$$85^{17} = 418211942557747392265625$$

$$C = 418211942557747392265625 \bmod 3233 = 2535$$

Ciphertext untuk "U" adalah 2535.

4. Huruf "A" (ASCII = 65):

$$C = 65^{17} \bmod 3233$$

Langkah perhitungan:

$$65^{17} = 8650415919381337933$$

$$C = 8650415919381337933 \bmod 3233 = 2790$$

Ciphertext untuk "A" adalah 2790.

5. Huruf "N" (ASCII = 78):

$$C = 78^{17} \bmod 3233$$

Langkah perhitungan:

$$78^{17} = 82724026188633676417793$$

$$C = 82724026188633676417793 \bmod 3233 = 2591$$

Ciphertext untuk "N" adalah 2591.

6. Huruf "G" (ASCII = 71):

$$C = 71^{17} \bmod 3233$$

Langkah perhitungan:

$$71^{17} = 16448102661888121144271$$

$$C = 16448102661888121144271 \bmod 3233 = 1730$$

Ciphertext untuk "G" adalah 1730.

7. Huruf "A" (ASCII = 65):

Karena "A" sudah dienkripsi sebelumnya, ciphertext-nya adalah:

$$C = 2790$$

8. Huruf "N" (ASCII = 78):

Ciphertext untuk "N" sudah dihitung:

C=2591

Hasil Enkripsi:

Setelah dienkripsi, teks "KEUANGAN" berubah menjadi deretan ciphertext:

- **2201 1313 2535 2790 2591 1730 2790 2591**

Dekripsi dengan Kunci Privat

Dekripsi dilakukan dengan menggunakan rumus:

$$M=C^d \bmod n$$

di mana:

- C adalah nilai ciphertext
- d=2753 adalah eksponen privat
- n=3233

Dekripsi setiap ciphertext untuk mendapatkan kembali teks asli.

1. Ciphertext 2201 (untuk "K"):

$$M=2201^{2753} \bmod 3233$$

Dengan menggunakan metode eksponensiasi modular:

$$M=75$$

Ini mengembalikan huruf "K".

2. Ciphertext 1313 (untuk "E"):

$$M=1313^{2753} \bmod 3233$$

Hasilnya adalah:

$$M=69$$

Ini mengembalikan huruf "E".

3. Ciphertext 2535 (untuk "U"):

$$M=2535^{2753} \bmod 3233$$

Hasilnya adalah:

$$M=85$$

Ini mengembalikan huruf "U".

4. Ciphertext 2790 (untuk "A"):

$$M=2790^{2753} \bmod 3233$$

Hasilnya adalah:

$$M=65$$

Ini mengembalikan huruf "A".

5. Ciphertext 2591 (untuk "N"):

$$M=2591^{2753} \bmod 3233$$

Hasilnya adalah:

$$M=78$$

Ini mengembalikan huruf "N".

6. Ciphertext 1730 (untuk "G"):

$$M=1730^{2753} \bmod 3233$$

Hasilnya adalah:

$$M=71$$

Ini mengembalikan huruf "G".

7. Ciphertext 2790 (untuk "A"):

$$M=2790^{2753} \bmod 3233$$

Hasilnya adalah:

$$M=65$$

Ini mengembalikan huruf "A".

8. Ciphertext 2591 (untuk "N"):

$$M=2591^{2753} \bmod 3233$$

Hasilnya adalah:

M=78

Ini mengembalikan huruf "N".

Hasil Dekripsi:

Setelah dekripsi, maka mendapatkan kembali teks asli:

- **KEUANGAN**

Kesimpulan:

- **Enkripsi** mengubah teks "KEUANGAN" menjadi deretan ciphertext 2201 1313 2535 2790 2591 1730 2790 2591 menggunakan kunci publik.
- **Dekripsi** menggunakan kunci privat mengembalikan ciphertext tersebut menjadi teks asli "KEUANGAN".

4. KESIMPULAN

Berdasarkan hasil pembahasan dan uji coba yang telah dilakukan yaitu Sistem Informasi Keamanan Data Pembuat SIM Baru Menggunakan Algoritma RSA Di Satlantas Polres Belawan Berbasis Web, dapat disimpulkan :

1. Dengan menggunakan aplikasi ini user dapat melakukan proses enkrip dan dekrip data Pembuat SIM Baru dan melakukan generate kunci RSA dalam proses enkripsi data.
2. Penerapan metode RSA dalam proses kerahasiaan data Pembuat SIM Baru dengan aplikasi berbasis web.
3. Dengan menggunakan aplikasi yang dibangun dapat memudahkan Satlantas Polres Belawan dalam menjaga kerahasiaan data Pembuat SIM Baru dari pihak yang tidak berwenang.

UCAPAN TERIMA KASIH

Penulis mengucapkan terima kasih kepada Dosen Pembimbing telah membimbing dan membantu dalam proses pembuatan Karya Tulis Ilmiah ini dan penulis juga mengucapkan terimakasih banyak kepada Universitas Potensi Utama yang telah memberikan kesempatan kepada penulis agar menyelesaikan Karya Tulis Ilmiah ini. Penulis berharap karya ilmiah ini dapat diambil ilmu dan manfaatnya.

REFERENSI

- [1] P. Hendriyati and A. Yusta, "Implementasi Aplikasi E-Commerce Berbasis Web," *JURSIMA (Jurnal Sist. Inf. dan Manajemen)*, vol. 9, no. 1, pp. 40–48, 2021, [Online]. Available: <https://ejournal.stmikgici.ac.id/index.php/jursima/article/view/232>.
- [2] C. Repi, J. Titaley, and E. Ketaren, "Implementasi Kriptografi Dalam Pengamanan Data Gambar Menggunakan Algoritma Rsa," *J. TIMES*, vol. 13, no. 1, pp. 93–99, 2024, doi: 10.51351/jtm.13.1.2024750.
- [3] D. K. Maulana, S. M. Tanjung, R. S. Ritonga, and A. Ikhwani, "Penerapan Kriptografi Vigenere Cipher Pada Kekuatan Kata Sandi," *J. Sains dan Teknol.*, vol. 3, no. 1, pp. 47–52, 2023, doi: 10.47233/jsit.v3i1.483.
- [4] F. A. Sitorus, N. B. Nugroho, and U. F. S. S. Pane, "Implementasi Algoritma Advanced Encryption Standard (AES) 128 Bit untuk Keamanan Data Transaksi Penjualan Pada PT. Mitsubishi Electric Indonesia," *J. CyberTech*, no. x, pp. 1–15, 2020.
- [5] F. S. Y. Arifah, M. Tahir, M. K. Fadli, F. N. Nafasa, S. A. Zahrah, and A. Rohmah, "Implementasi Algoritma Kriptografi RC4 Untuk Keamanan Database Aplikasi Voting Pemilihan Ketua Umum Berbasis

- WEB,” *J. Inf. Syst.*, vol. 3, no. 1, pp. 1–9, 2023, doi: 10.61488/jis.v3i1.208.
- [6] I. D. Sari, H. L. Sari, and J. Jumadi, “Expert System to Diagnose Angina Pectoris Disease (Sitting Wind) Using the Naïve Bayes Method Sistem Pakar Untuk Mendiagnosa Penyakit Angina Pectoris (Angin Duduk) Dengan Menggunakan Metode Naïve Bayes,” *J. Media Comput. Sci.*, vol. 2, no. 2, pp. 169–184, 2023.
- [7] S. Sutejo, “Implementasi Algoritma Kriptografi Rsa (Rivest Shamir Adleman) Untuk Keamanan Data Rekam Medis Pasien,” *INTECOMS J. Inf. Technol. Comput. Sci.*, vol. 4, no. 1, pp. 104–114, 2021, doi: 10.31539/intecom.v4i1.2437.
- [8] S. Andika, “Implementasi Algoritma Freivlds Untuk Pembangkitan Kunci AlgoritmaRSA Pada Pengamanan Data Video,” *Pelita Inform. Inf. dan Inform.*, vol. 10, no. 2, pp. 70–77, 2021.
- [9] D. Alfiani Fauzan and A. Fathurrozi, “Perancangan Aplikasi Pengamanan Data Menggunakan Algoritma RSA (Rivest Shamir Adleman) dan AES (Advanced Encryption Standard) Berbasis Web,” *J. Inf. Inf. Secur.*, vol. 4, no. 1, pp. 2722–4058, 2023, [Online]. Available: <http://ejurnal.ubharajaya.ac.id/index.php/jiforty>.
- [10] A. A. Cherniaeva, “Частота Асимптоматической Гиперурикемии Среди Взрослых Больных Сахарным Диабетом 1-Го И 2-Го Типа,” *Int. J. Endocrinol.*, vol. 16, no. 4, pp. 327–332, 2021, doi: 10.22141/2224-0721.16.4.2020.208486.
- [11] Irma Listiani, Maimanah Salsabila Nasution, Wini Istya Sari, and Adnan Buyung Nasution, “Perancangan Keamanan Data Pasien Di Klinik Kecantikan Ratu Beauty Studio Menggunakan Metode Kriptografi Rsa,” *J. Inform. Teknol. dan Sains*, vol. 4, no. 4, pp. 437–443, 2022, doi: 10.51401/jinteks.v4i4.2173.
- [12] F. Fernando and C. J. Sianturi, “Perancangan Aplikasi Pembelian Bahan Baku Produk Kalengan pada PT. Toba Surimi Industries berbasis Android,” *J. Innov. Res. Knowl.*, vol. 1, no. 9, pp. 1157–1164, 2022.
- [13] N. Metafani, Djameludin, and A. Hardiyanto, “Pengenalan Cagar Budaya Tangerang Berbasis Android di Dinas Kebudayaan dan Pariwisata Kota Tangerang,” *J. Ilm. Fak. Tek.*, vol. 1, no. 1, pp. 66–73, 2020, [Online]. Available: ojs.ejournal.unis.ac.id/article/515.
- [14] H. Wulandari, S. Rosida, S. Teknologi, S. Komputer, U. Pembangunan, and P. Budi, “Perancangan Sistem Informasi Berbasis Web Penjualan Cake dan Bakery Napoleon,” pp. 573–579.
- [15] M. Ronaldo and D. Pasha, “Sistem Informasi Pengelolaan Data Santri Pondok Pesantren an-Ahl Berbasis Website,” *Telefortech*, vol. 2, no. 1, pp. 17–20, 2021.
- [16] Surbakti, A. S. B., & Pohan, Y. A. (2024). Pengaruh lingkungan kerja, stres kerja dan budaya organisasi terhadap kinerja karyawan. *Jurnal Manajemen dan Bisnis Jayakarta*, 5(2), 180–189. <https://www.journal.stiejayakarta.ac.id/index.php/JMBJayakarta/article/view/197>
- [17] Purba, S. E., & Pohan, Y. A. (2024). Pengaruh keterampilan dan pengalaman kerja terhadap kemampuan kerja perawat pada Rumah Sakit Umum Wulan Windy. *Jurnal Dunia Pendidikan*, 4(3), 1213–1226. <https://doi.org/10.55081/juridip.v4i3.2039>
- [18] Zagoto, E., & Pohan, Y. A. (2024). Pengaruh pelatihan kerja, motivasi kerja dan disiplin kerja, terhadap kinerja karyawan Rumah Sakit Umum Mitra Medika Medan. *Jurnal Dunia Pendidikan*, 4(3), 1159–1179. <https://doi.org/10.55081/juridip.v4i3.1981>
- [19] Gulo, A. F., & Pohan, Y. A. (2024). Pengaruh disiplin kerja, kompensasi dan motivasi kerja terhadap kinerja karyawan pada PT. Yumeida Utama Industry. *Jurnal Dunia Pendidikan*, 4(3), 1125–1137. <https://doi.org/10.55081/juridip.v4i3.1978>
- [20] Mauliza, P., Prabowo, A., & Aspan, H. (2023). Analisis social media promotion, perceived value, dan customer satisfaction terhadap revisit intention wisatawan pada Sawah Lukis Binjai. *Jurnal Menara Ekonomi: Penelitian dan Kajian Ilmiah Bidang Ekonomi*, 9(1). <https://doi.org/10.31869/me.v9i1.4788>
- [21] Prabowo, A., & Risal, T. (2023). Peran entrepreneurial orientation dan social media marketing terhadap
DOI: <https://www.doi.org/10.22303>

- peningkatan strategi bersaing (UMKM) coffe shop pada era modern customer di Kota Medan. *Menara Ekonomi*, 9(1). <https://jurnal.umsb.ac.id/index.php/menaraekonomi/article/download/4785/pdf>
- [22] Aspan, H., Rozaini, Prabowo, A., & Zahara, A. N. (2024). Analysis of work discipline and job satisfaction on lecturer performance in Medan City. *International Journal of Economic, Business, Accounting, Agriculture Management and Sharia Administration (IJEBA)*, 4(4), 1193–1205. <https://doi.org/10.54443/ijebas.v4i4.1857>
- [23] Aspan, H., Rozaini, Prabowo, A., & Lestari, D. M. (2024). Implementation of lecturer performance: Through career paths and work environment on private lecturers in Medan City. *International Conference on Health Science, Green Economics, Educational Review and Technology (IHERT)*, 6(1), 114–126. <https://doi.org/10.54443/ihert.v6i1.379>
- [24] Aspan, H., Rozaini, Wahyuni, E. S., & Prabowo, A. (2024). Personal resources and job crafting: Implications work engagement for modern coffee shops employee in Medan City. *Multidisciplinary Output Research for Actual and International Issue (MORFAI)*, 4(2), 556–567. <https://doi.org/10.54443/morfaiv4i2.1859>
- [25] Prabowo, A., Aspan, H., Wahyuni, E. S., & Lestari, I. (2024). Anteseden shopping emotion konsumen dalam berbelanja brand fashion Uniqlo. *Management Studies and Business Journal (PRODUCTIVITY)*, 1(5), 826–834. <https://doi.org/10.62207/ebtme684>
- [26] Azzahri, S., & Prabowo, A. (2024). Pengaruh content creator, price promotion, sosial media marketing terhadap impulsive buying dalam pembelian produk skincare pada aplikasi Tik Tok Shop (Studi kasus mahasiswa/i Fakultas Ekonomi dan Bisnis Universitas Potensi Utama). *Jurnal Widya*, 5(2). <https://doi.org/10.54593/awl.v5i2.366>
- [27] Kadariah, S., & binti Noor Azman, F. K. (2023). Product marketing strategy Muamalat DIN (Digital Islamic Network) at PT. Bank Muamalat Indonesia Tbk. *Journal of Islamic Financial Technology*, 2(2), 40–59. <https://doi.org/10.24952/jiftech.v2i2.10981>
- [28] Kadariah, S., & Utama, U. P. (2023). The impact of online loans on the community. *Journal of Islamic Financial Technology*, 2(1), 132–144. <https://jurnal.uinsyahada.ac.id/index.php/jiftech/article/view/9718>
- [29] Kadariah, S., Nasution, A. W., & Siregar, S. (2023). Penerapan konsep peringkat risiko pada manajemen risiko hukum di perbankan syariah. *Jurnal EMT KITA*, 7(2), 301–307. <https://doi.org/10.35870/emt.v7i2.890>
- [30] Kadariah, S., & Majid, M. S. A. (2023). Krisis ekonomi dalam perspektif Islam. *Jurnal EMT KITA*, 7(1), 18–24. <https://doi.org/10.35870/emt.v7i1.717>
- [31] Nazli, P. (2024). Implementasi perpanjangan masa angsuran pembiayaan murabahah di bank syariah pada masa pandemi Covid-19. *Jurnal Ekonomi, Bisnis dan Manajemen*, 3(1), 174–189. <https://doi.org/10.58192/ebismen.v3i1.1760>
- [32] Aisyah, S., Natasha, S. F., Nazli, P., Anindya, D. A., Anggraini, D. P., & Habibie, M. (2024). Analysis of supporting factors in performance quality of Medan City tourism services for free daily employees. *Economic and Business Horizon*, 3(1), 1–12. <https://doi.org/10.54518/ebh.3.1.2024.239>
- [33] Ridwan, M., Hutagalung, M. A. K., Riski, B., & Rambe, R. (2024). Analisis pengaruh pembiayaan musyarakah, dana pihak ketiga terhadap profitabilitas Bank Sumut Syariah Medan. *J-EBIS (Jurnal Ekonomi dan Bisnis Islam)*, 9(1), 97–116. <https://doi.org/10.32505/j-ebis.v9i1.8786>
- [34] Budimansyah, M., & Ridwan, M. (2023). Analisis penyelesaian akad akad pembiayaan bermasalah di BPRS Al Washliyah Medan. *Innovative: Journal of Social Science Research*, 3(6), 7112–7120. <https://j-innovative.org/index.php/Innovative/article/view/6937>
- [35] Arafah, S., Hutagalung, M. A. K., Mushliha, & Sembiring, E. A. (2024). Determinan keputusan masyarakat dalam berinvestasi di pasar modal syariah. *MUTLAQAH: Jurnal Kajian Ekonomi Syariah*, 5(1), 1–13. <https://doi.org/10.30743/mutlaqah.v5i1.9715>
- [36] Ridwan, M., Hutagalung, M. A. K., Riski, B., & Rambe, R. (2024). Analisis pengaruh pembiayaan musyarakah, dana pihak ketiga terhadap profitabilitas Bank Sumut Syariah Medan. *J-EBIS (Jurnal Ekonomi dan Bisnis Islam)*, 9(1), 97–116. <https://doi.org/10.32505/j-ebis.v9i1.8786>

- [37] Yamin, M., & Murtani, A. (2024). The influence of halal lifestyle, halal knowledge and promotion on Rabbani brand purchasing decisions: (Study on Rabbani consumers in Medan City). *International Journal of Education, Social Studies, and Management (IJESSM)*, 4(3), 1120–1132. <https://doi.org/10.52121/ijessm.v4i3.501>