

KOMPARASI ALGORITMA RSA DAN ELGAMAL PADA PENGAMAN REKAM MEDIS BERBASIS WEB

SKRIPSI

Sebagai Salah Satu Syarat Untuk Memperoleh Gelar Sarjana Strata 1
Program Studi Teknik Informatika

Disusun Oleh:

ANANDA AMALIA YUNUS 192014

BASO SAMRIADI 192061

Disetujui untuk dipertahankan oleh:

Pembimbing I

**(Nurdin, S.Kom., MT.,)
NIDN: 0907117303**

Pembimbing II

**(Usman, SE., M.Kom)
NIDN: 0927037502**

PENGESAHAN NASKAH SKRIPSI

Judul : Komparasi Algoritma RSA dan ElGamal Pada Pengaman
Rekam Medis Berbasis Web

Mahasiswa 1 : Ananda Amalia Yunus

NIM 1 : 192014

Mahasiswa 2 : Baso Samriadi

NIM 2 : 192061

Tanggal Ujian :

Disetujui oleh:

Pembimbing I

Pembimbing II

Nurdin, SKom., MT.,
NIDN : 0907117303

Usman, SE.M.Kom
NIDN : 0927037502

Penguji I,

Penguji II,

....
NIDN :

....
NIDN :

Mengetahui
Ketua Program Studi Teknik Informatika
Universitas Dipa Makassar

Ir. Irsal., M.T.
NIDK : 9990216745

ABSTRAK

Data rekam medis adalah dokumen yang sangat rahasia, yang bisa memiliki dan mengakses informasi di dalamnya hanyalah sarana pelayanan kesehatan dan pasien terkait. Seluruh informasi yang berkaitan dengan identitas pasien, diagnosis, riwayat penyakit, riwayat pemeriksaan, dan pengobatan pasien bersifat rahasia. Fasilitas pelayanan kesehatan rawan terhadap tuntutan hukum terkait kebocoran informasi medis, dan profesi kesehatan termasuk Perekam Medis dan Informasi Kesehatan (PMIK) berpotensi "terlibat" dalam kebocoran informasi medis. Sehingga, teknologi informasi berperan penting dalam menjaga kerahasiaan informasi medis. Untuk mengatasi dan menghindari masalah tersebut diperlukan sebuah sistem yang dapat mengamankan data rekam medis.

Kata Kunci : Komparasi, Pengamanan, Klinik, Website.

Abstarct

Medical record data is a highly confidential document, only health service facilities and related patients can possess and access the information in it. All information relating to the patient's identity, diagnosis, medical history, examination history, and patient treatment is confidential. Healthcare facilities are prone to lawsuits related to leakage of medical information, and health professionals including Medical Records and Health Information (PMIK) have the potential to be "involved" in medical information leaks. Thus, information technology plays an important role in maintaining the confidentiality of medical information. To overcome and avoid these problems, we need a system that can secure medical record data.

Keywords : Comparison, Security, Clinic, Website.

KATA PENGANTAR

Segala puji dan syukur kehadiran Allah SWT yang senantiasa memberikan rahmat, petunjuk, serta ridho-Nya kepada penulis sehingga proposal yang berjudul “*Komparasi Algoritma RSA dan ElGamal Pada Pengaman Rekam Medis Berbasis Web*” dapat kami selesaikan. Proposal ini dibuat untuk memenuhi syarat-syarat untuk memperoleh gelar sarjana Teknik Informatika di Universitas Dipa Makassar.

Penulis menyadari sepenuhnya bahwa proposal penelitian ini tidak mungkin terwujud tanpa bantuan dan dorongan dari berbagai pihak, baik bantuan moril maupun materil. Untuk itu, dengan segala keikhlasan dan kerendahan hati, penulis mengucapkan banyak terima kasih dan penghargaan yang setinggi-tingginya kepada:

1. Dr. Y. Johny W. Soetikno, SE., M.M., selaku Rektor Universitas Dipa Makassar.
2. Ir.H. Irsal, M.T., selaku ketua jurusan Teknik Informatika Universitas Dipa Makassar.
3. Nurdin S.Kom., MT. dan Usman SE.,M.Kom selaku dosen Pembimbing I dan II yang telah meluangkan waktunya untuk memberi bimbingan dan arahan kepada penulis.
4. Dosen Universitas Dipa Makassar yang telah mendidik dan mengajarkan berbagai disiplin ilmu kepada penulis

5. Kedua Orang Tua kami yang tercinta, atas segala kasih sayang, jerih payah dan doa restunya dalam membesarkan dan mendidik kami.
6. Kepada semua pihak yang ikut membantu dalam memberikan solusi dan arahan penyelesaian proposal ini yang tak sempat penulis sebutkan satu-persatu.

Penulis menyadari bahwa penulisan proposal ini masih jauh dari kesempurnaan. Oleh karena itu, kritik dan saran diharapkan penulis dalam penyempurnaan penulisan skripsi ini.

DAFTAR ISI

	Halaman
ABSTRAK	iii
KATA PENGANTAR.....	iv
DAFTAR TABEL	viii
DAFTAR GAMBAR.....	ix
BAB I.....	1
1.1 Latar Belakang	1
1.2 Rumusan Masalah	5
1.3 Batasan Masalah.....	5
1.4 Tujuan dan Manfaat Penelitian	5
1.4.1 Tujuan Perancangan	5
1.4.2 Manfaat Perancangan	5
1.5 Sistematika Penulisan.....	6
BAB II	7
2.1 Kerangka berpikir.....	7
2.2 Kerangka Teori.....	8
2.2.1 Sistem Informasi.....	8
2.2.2 <i>Web</i>	8
2.2.3 <i>HTML</i>	8
2.2.4 <i>Cascading Style Sheet (CSS)</i>	9
2.2.5 <i>Javascript</i>	9
2.2.6 <i>PHP</i>	10
2.2.7 <i>Database</i>	10
2.2.8 <i>XAMPP</i>	11
2.2.9 <i>MySQL</i>	11
2.2.10 <i>Apache</i>	12
2.2.11 Kriptografi	13

2.2.12 Kriptografi Asimetris.....	13
2.2.13 Kriptanalisis.....	14
2.2.14 Pseudocode	14
2.2.15 <i>ElGamal</i>	20
2.3 Penelitian Terkait	24
BAB III.....	27
3.1 Waktu dan Tempat Penelitian	27
3.2 Alat dan Bahan Penelitian	27
3.3 Jenis dan Variabel Penelitian	28
3.4 Metode Pengujian Sistem.....	29
3.5 Tahap dan Rancangan Penelitian	29
3.5.1 Tahap Penelitian	29
3.5.2 Rancangan Jadwal Penelitian	31
BAB IV	32
4.1 Analisis Data	32
4.2 Kriptanalisis Algoritma RSA dan ElGamal	38
4.3 Komparasi RSA dan Elgamal	41
4.4 Perancangan dan Implementasi Sistem	44
4.4.1 Sistem yang berjalan.....	44
4.4.2 Sistem yang diusulkan.....	45
4.4 Pengujian Sistem	60
BAB V.....	64
5.1 Kesimpulan.....	64
5.2 Saran.....	64
DAFTAR PUSTAKA	65

DAFTAR TABEL

Tabel	Halaman
Tabel 3.1 Perangkat lunak yang digunakan.....	27
Tabel 3.2 Perangkat keras yang digunakan	28
Tabel 3.3 Bahan penelitian	28
Tabel 3.4 Rancangan Jadwal Penelitian	31
Tabel 4. 1 Kunci publik RSA	32
Tabel 4. 2 Pemilihan kunci ElGamal.....	35
Tabel 4. 3 Hasil enkripsi ElGamal	41
Tabel 4. 4 Percobaan enkripsi RSA.....	41
Tabel 4. 5 Percobaan Enkripsi ElGamal.....	42
Tabel 4. 6 Tabel admin.....	51
Tabel 4. 7 Tabel user	51
Tabel 4. 8 Tabel dokter.....	51
Tabel 4. 9 Tabel perawat	52
Tabel 4. 10 Tabel pasien.....	52
Tabel 4. 11 Tabel riwayat.....	53

DAFTAR GAMBAR

Gambar	Halaman
Gambar 2. 1 Bagan Kerangka Pikir	7
Gambar 2. 2 Flowchart Algoritma RSA	17
Gambar 2. 3 Daftar Kode ASCII	18
Gambar 2. 4 Pseudocode Algoritma RSA	20
Gambar 2. 5 Bagan alir pembentukan kunci	22
Gambar 2. 6 Pseudocode Algoritma ElGamal	24
Gambar 4. 1 Sistem yang berjalan	44
Gambar 4. 2 Use Case admin dan user	45
Gambar 4. 3 Sequence Diagram Administrasi	46
Gambar 4. 4 Sequence Diagram Kasir	46
Gambar 4. 5 Activity Diagram Login	47
Gambar 4. 6 Activity Diagram Data dokter	48
Gambar 4. 7 Activity Diagram Admin Data Perawat	49
Gambar 4. 8 Activity Diagram Admin Pasien	49
Gambar 4. 9 Activity Diagram Admin Data Riwayat pasien	50
Gambar 4. 10 Activity Diagram Admin Data User	50
Gambar 4. 11 Halaman login	53
Gambar 4. 12 Halaman data dokter	54
Gambar 4. 13 Halaman data perawat	54
Gambar 4. 14 Halaman data pasien	54
Gambar 4. 15 Halaman user	55

Gambar 4. 16 Halaman riwayat pasien.....	55
Gambar 4. 17 Implementasi sistem (login)	56
Gambar 4. 18 Implementasi sistem (Tambah data pasien).....	57
Gambar 4. 19 Implementasi sistem (table data pasien)	58
Gambar 4. 20 Implementasi sistem (data pasien).....	58
Gambar 4. 21 Implementasi sistem (data hasil dekripsi).....	59
Gambar 4. 22 Pengujian halaman login.....	60
Gambar 4. 23 Pengujian halaman data pasien	61
Gambar 4. 24 Pengujian halaman tambah data pasien	62
Gambar 4. 25 Pengujian halaman deksripsi data pasien	63

BAB I

PENDAHULUAN

1.1 Latar Belakang

Perkembangan teknologi sangatlah pesat, sehingga keberadaan komputer pada saat ini penting dalam pengolahan data. Karena teknologi komputer dapat membantu dalam mempercepat, mempermudah, dan menciptakan keakuratan pengolahan data. Pada bidang kesehatan seperti klinik seharusnya telah menggunakan sistem informasi yang didesain khusus untuk menangani berbagai lingkup, misalnya seperti pengamanan data rekam medis.

Institusi pelayanan kesehatan seperti rumah sakit, klinik, dan dinas kesehatan merupakan salah satu lembaga yang juga secara langsung mengikut arus digitalisasi dalam perkembangan organisasinya, sebab efesiensi dan kecepatan informasi akan sangat dibutuhkan pada institusi yang disebutkan di atas. Dalam konteks dokumen medis, dalam istilah kesehatan dapat diterapkan pada beberapa hal, salah satunya adalah data pasien pada insitusi pelayanan kesehatan, atau yang lazim sering digunakan adalah data rekam medis. Banyak manfaat yang diperoleh dengan memafaatkan teknologi digital pada rekam medic, salah satunya dapat meningkatkan perlindungan data terhadap kerahasiaan informasi karena memerlukan kunci dan kendali akses. Digitalisasi data ini dapat meningkatkan kesinambungan pelayanan serta berperan penting menjadi sebagai sumber daya bagi pihak manajemen dari sistem pelayanan kesehatan dalam pengembangan pengetahuan.

Data rekam medis merupakan data dokumen yang berisi riwayat penyakit yang diderita pasien. Data tersebut digunakan sebagai isi rekam yang akan dipakai untuk pengobatan dan pemeliharaan kesehatan pasien. Selain itu, rekam medis berfungsi juga untuk bukti penegakan hukum dan disiplin kedokteran serta penegakan etika kedokteran.

Data rekam medis adalah dokumen yang sangat rahasia, yang bisa memiliki dan mengakses informasi di dalamnya hanyalah sarana pelayanan kesehatan dan pasien terkait. Seluruh informasi yang berkaitan dengan identitas pasien, diagnosis, riwayat penyakit, riwayat pemeriksaan, dan pengobatan pasien bersifat rahasia.

Dalam Peraturan Menteri Kesehatan no. 269 Tahun 2008 tentang Rekam Medis, disebutkan bahwa meskipun informasi tentang identitas, diagnosis, riwayat penyakit, riwayat pemeriksaan, dan riwayat pengobatan pasien harus dijaga kerahasiaannya oleh petugas pengelola dan pimpinan sarana kesehatan, namun informasi ini dapat dibuka untuk memenuhi permintaan aparat penegak hukum atas perintah pengadilan dan memenuhi permintaan lembaga atau institusi sesuai dengan ketentuan perundang-undangan. Rekam medis pasien mulai beralih menjadi berbasis elektronik dengan diterbitkannya Peraturan Menteri Kesehatan (PMK) nomor 24 tahun 2022 tentang Rekam Medis. Melalui kebijakan ini, fasilitas pelayanan kesehatan (Fasyankes) diwajibkan menjalankan sistem pencatatan riwayat medis pasien secara elektronik dan pada tempat penelitian yang akan diambil penulis yaitu Klinik Botolempang belum menerapkan pencatatan rekam medis yang berbasis elektronik.

Pada awal tahun 2022 yang lalu, Indonesia sempat digemparkan oleh berita tentang data rekam medis pasien bocor dan sekitar enam juta data rekam medis tersebut dijual di situs RaidForums. Fasilitas pelayanan kesehatan rawan terhadap tuntutan hukum terkait kebocoran informasi medis, dan profesi kesehatan termasuk Perkam Medis dan Informasi Kesehatan (PMIK) berpotensi "terlibat" dalam kebocoran informasi medis. Sehingga, teknologi informasi berperan penting dalam menjaga kerahasiaan informasi medis.

Untuk mengatasi dan menghindari masalah tersebut diperlukan sebuah sistem yang dapat mengamankan data rekam medis. Dalam penelitian ini adalah bagaimana mengamankan sebuah file data rekam medis menggunakan dua metode. Metode yang digunakan adalah Metode RSA (Rivest Shamir Adleman) dan Metode ElGamal. Alasan penggunaan metode RSA (Rivest Shamir Adleman) yaitu terletak pada sulitnya memfaktorkan bilangan besar menjadi faktor-faktor prima, Selama pemfaktoran bilangan besar menjadi faktor-faktor prima belum ditemukan algoritma yang mangkus, maka selama itu pula keamanan algoritma RSA tetap terjamin. Sedangkan alasan pemilihan algoritma ElGamal dikarenakan algoritma ElGamal merupakan bagian dari kriptografi asimetris yang pembentukan salah satu kuncinya menggunakan bilangan prima dan menitik beratkan kekuatan kuncinya pada pemecahan masalah logaritma diskrit. Dengan memanfaatkan bilangan prima yang besar serta masalah logaritma diskrit yang cukup menyulitkan, maka keamanan kuncinya lebih terjamin

Dalam RSA, pesan yang ingin dikirim diubah menjadi bilangan bulat, kemudian dienkrpsi dengan menggunakan kunci publik. Setelah pesan terenkrpsi,

hanya kunci privat yang dapat digunakan untuk mendekripsinya. Kunci publik dan kunci privat dipilih secara khusus untuk memastikan bahwa hanya kunci privat yang dapat digunakan untuk mendekripsi pesan, sementara kunci publik dapat dibagikan kepada siapa saja tanpa mengkhawatirkan keamanan pesan yang telah dienkripsi.

Metode ElGamal merupakan bagian dari kriptografi asimetris. Algoritma ElGamal terdiri dari tiga proses, yaitu proses pembentukan kunci, proses enkripsi dan proses dekripsi. Algoritma ini merupakan cipher blok, yaitu melakukan proses enkripsi pada blok-blok plainteks dan menghasilkan blok-blok cipherteks yang kemudian dilakukan proses dekripsi dan hasilnya digabungkan.

Hasil dari penelitian ini akan diimplementasikan dalam sebuah program berbasis website menggunakan bahasa pemrograman PHP yang dapat memberikan kemudahan bagi setiap orang yang akan mengamankan file-file penting sehingga tidak terjadi lagi kebocoran data yang mengakibatkan kerugian bagi pasien dan pihak Institusi pelayanan kesehatan.

Berdasarkan masalah yang telah diuraikan, maka dibuatlah penelitian dengan judul : “KOMPARASI ALGORITMA RSA DAN ELGAMAL PADA PENGAMAN REKAM MEDIS BERBASIS *WEB*”.

1.2 Rumusan Masalah

Berdasarkan latar belakang masalah yang telah diuraikan di atas, maka yang Menjadi rumusan masalah adalah bagaimana tingkat kekuatan algoritma RSA dan ElGamal terhadap pengamanan data rekam medis dengan menggunakan kriptanalisis?.

1.3 Batasan Masalah

Batasan masalah dan ruang lingkup kajian dalam merancang aplikasi warung pintar ini antara lain :

1. Masalah yang diteliti hanya menyangkut masalah bagaimana pengamanan data rekam medis.
2. Metode yang dilakukan untuk pengamanan data rekam medis menggunakan dua metode yaitu metode RSA dan ElGamal.
3. Melakukan komparasi dari dua metode tersebut untuk menentukan metode mana yang lebih unggul dalam melakukan pengaman data.

1.4 Tujuan dan Manfaat Penelitian

1.4.1 Tujuan Perancangan

Adapun tujuan perancangan adalah untuk mengetahui tingkat kekuatan Algoritma RSA dan ElGamal dengan cara melakukan perbandingan pada kedua algoritma tersebut.

1.4.2 Manfaat Perancangan

1. Manfaat terhadap penulis
Menambah pengetahuan dan wawasan tentang bagaimana menganalisis dan merancang sebuah *website*.

2. Manfaat terhadap dunia akademik

Hasil perancangan ini diharapkan dapat menjadi referensi untuk mahasiswa Universitas Dipa Makassar dalam melakukan penelitian lanjutan.

1.5 Sistematika Penulisan

Sistematika penulisan skripsi ini di bagi dalam beberapa bab sebagai berikut:

BAB I PENDAHULUAN

Bab ini membahas tentang latar belakang masalah, rumusan masalah, batasan masalah, tujuan dan manfaat penelitian, dan sistematika penulisan.

BAB II TINJAUAN PUSTAKA

Bab ini merupakan kerangka pikir dan landasan teori.

BAB III METODE PENELITIAN

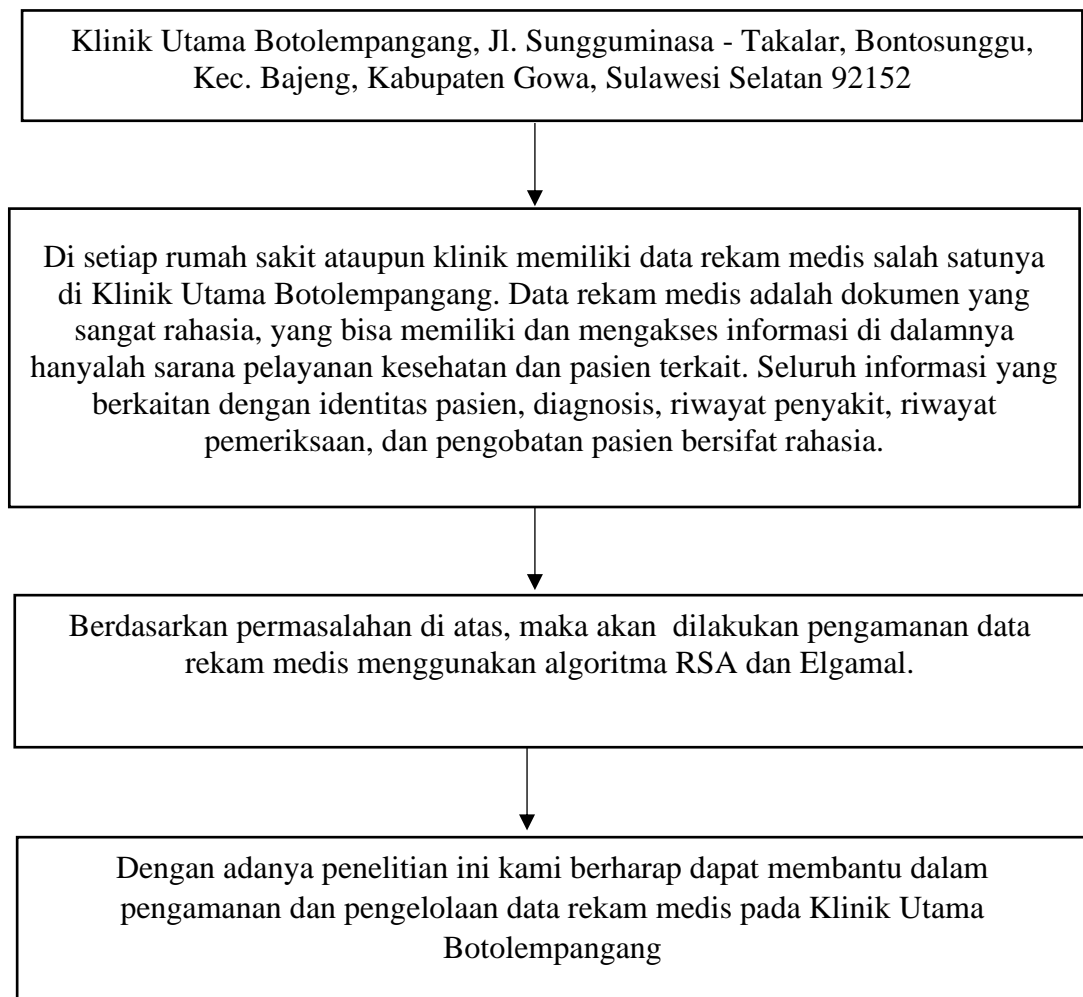
Bab ini membahas waktu, jenis, sumber data, metode penelitian, alat dan bahan yang digunakan dalam penelitian dan perancangan sistem, metode pengujian perangkat lunak dan jadwal penelitian.

BAB II

TINJAUAN PUSTAKA

2.1 Kerangka berpikir

Untuk memperjelas kerangka berpikir penulis dalam merancang sistem ini, maka dapat digambarkan pada gambar 2.1



Gambar 2. 1 Bagan Kerangka Pikir

2.2 Kerangka Teori

2.2.1 Sistem Informasi

Menurut Abdillah, (2020), Sistem informasi merupakan sekumpulan komponen yang saling terkait mengumpulkan, memproses, menyimpan dan menyebarluaskan data dan informasi.

2.2.2 Web

Menurut Reikha Rahmadhayanti, (2017:11), *Website* adalah sekumpulan halaman informasi yang disediakan melalui jalur internet sehingga bisa diakses di seluruh dunia selama terkoneksi dengan jaringan internet. Intinya bahwa pengguna internet bisa memanfaatkan berbagai macam fasilitas informasi dengan biaya murah tanpa harus datang secara langsung ketempatnya. Informasi atau dokumen dapat diakses berupa data teks, gambar atau image, animasi, video, suara atau kombinasi diantaranya bahkan komunikasi bisa dilakukan secara langsung dengan suara dan video sekaligus.

2.2.3 HTML

Menurut Reikha Rahmadhayanti (2017:38), HTML (Hypertext Markup Language) adalah sebuah protokol yang digunakan untuk membuat format suatu dokumen web yang mampu dibaca dalam browser dari berbagai platform computer.

Dalam penamaan sebuah dokumen yang akan ditampilkan pada web browser maka nama yang digunakan harus diakhiri dengan ekstensi (.html.) atau (.htm.). Ekstensi dokumen HTML awalnya 3 karakter, yaitu untuk mengakomodasi sistem penamaan dalam DOS.

Hypertext Mark Up Language atau yang disingkat dengan HTML yaitu bahasa standar pemrograman untuk membuat suatu website yang bisa diakses dengan internet halaman website biasanya disusun dengan menggunakan bahasa ini dan kemudian diterjemahkan oleh komputer agar dapat dipahami oleh penggunanya. Html merupakan standar pembuatan website secara luas agar laman website dapat ditampilkan pada layar komputer.

2.2.4 *Cascading Style Sheet (CSS)*

Menurut Reikha Rahmadhayanti (2017:40) CSS adalah singkatan dari cascading style sheet yang merupakan kumpulan perintah yang dibentuk dari berbagai sumber yang disusun menurut urutan tertentu sehingga mampu mengatasi konflik style.

CSS kependekan dari Cascading Style Sheet. CSS yaitu kumpulan kode-kode yang membuat menghias dan mengatur *style* tampilan/*layout* pada halaman web agar lebih menarik. CSS yaitu sebuah teknologi internet yang direkomendasikan oleh World Wide Web Consortium atau W3C pada tahun 1996. Awalnya, CSS dikembangkan di SGML pada tahun 1970, dan terus dikembangkan hingga saat ini. CSS telah mendukung banyak bahasa markup seperti HTML, XHTML, XML, SVG (Scalable Vector Graphics) dan Mozilla XUL (XML User Interface Language).

2.2.5 *Javascript*

Menurut Vivian Siahaan (2018), “JavaScript merupakan bahasa skript populer yang dipakai untuk menciptakan halaman Web yang dapat berinteraksi

dengan pengguna dan dapat merespon event yang terjadi pada halaman. JavaScript merupakan perekat yang menyatukan halaman-halaman Web”.

Berdasarkan pendapat yang dikemukakan di atas dapat disimpulkan bahwa, Java Script yaitu Bahasa pemrograman atau Bahasa script yang membuat halaman web lebih dinamis dan interaktif

2.2.6 PHP

Menurut Reikha Rahmadhayanti, (2017:34), PHP (Hypertext Preprocessor) adalah suatu bahasa pemrograman yang digunakan untuk menerjemahkan baris kode program menjadi kode mesin yang dapat dimengerti oleh komputer yang bersifat server-side yang dapat ditambahkan kedalam HTML.

Pada awalnya PHP merupakan singkatan dari Personal Home Page. Sesuai dengan namanya, PHP digunakan untuk membuat website pribadi. Dalam beberapa tahun perkembangannya, PHP sekarang menjadi bahasa pemrograman web yang *powerfull* dan tidak hanya digunakan untuk membuat halaman web sederhana.

2.2.7 Database

Menurut Reikha Rahmadhayanti, (2017:30), Database adalah struktur penyimpanan data. Untuk menambah, mengakses dan memproses data yang disimpan dalam sebuah database komputer, diperlukan sistem manajemen database seperti MySQL Server.

Database yaitu sekelompok data yang mempunyai ciri-ciri khusus dan dapat dikelola sedemikian rupa sehingga dapat menghasilkan sebuah format data yang

baru dan juga sebagai aspek yang sangat penting dalam sistem informasi karena berfungsi sebagai gudang penyimpanan data yang akan diolah lebih lanjut.

Basis data menjadi penting karena dapat mengorganisasi data, menghindari duplikasi data, menghindari hubungan antar data yang tidak jelas dan juga update yang rumit.

2.2.8 XAMPP

Menurut Reikha Rahmadhayanti (2017:47), Xampp adalah paket webprogramming, akan tetapi kita bisa memanfaatkan database MySQL server-nya untuk belajar Programming Visual, juga disana telah tersedia tools php Myadmin yang hanya berjalan disisi server web seperti Apache Server.

2.2.9 MySQL

Menurut Buana & Setia, (2014): “MySQL Merupakan database server yang paling sering digunakan dalam pemograman PHP. MySQL digunakan untuk menyimpan data dalam database dan memanipulasi data-data yang diperlukan. Manipulasi data tersebut berupa menambah, mengubah, dan menghapus data yang berada dalam database.

MySQL yaitu singkatan “*My Structured Query Language*”.Program ini berjalan sebagai server menyediakan multi-user mengakses ke sejumlah *database*. MySQL umumnya digunakan oleh perangkat lunak bebas yang memerlukan fitur penuh sistem manajemen *database*, seperti WordPress, phpBB dan perangkat lunak lain yang dibangun pada perangkat lunak LAMP. Ia juga digunakan dalam skala sangat tinggi *World Wide Web*.

MySQL dapat di kelompokkan menjadi 3 macam yaitu:

1. *Data Definition Language (DDL)*

DDL bertugas untuk membuat objek *SQL* dan menyimpan definisi ini dalam *table*. Contoh dari objek yang di maksud di atas ialah *table*, *view*, dan *index*.

Pembuat *table*, perubahan struktur *table*, perubahan nama *table* serta perintah-perintah untuk menghapus *table* dilakukan dengan sub bahasa yang tergolong dalam DDL, yaitu *create*, *alter*, dan *drop*.

2. *Data Manipulation Language (DML)*

DML digunakan untuk memproses data dalam objek skema. Dengan menggunakan perintah-perintah ini dapat menampilkan data (*select*), mengubah data (*update*), menghapus data (*delete*), dan menambahkan atau menyisipkan data baru (*insert*).

3. *Data Control language (DCL)*

Sebagai alat kontrol keamanan terhadap database dan tabelnya, terdapat dua perintah utama diantaranya adalah *grant* dan *revoke*. *Grant* digunakan untuk mengijinkan user mengakses *table* dalam *database* tertentu, sedangkan *revoke* adalah sebaliknya

2.2.10 *Apache*

Menurut (Putratama, 2016) “Apache adalah perangkat lunak server yang berfungsi untuk menerima permintaan dalam bentuk situs web melalui HTTP atau HTTPS dari klien itu, yang dikenal sebagai browser web dan mengirimkan kembali (reaksi) hasil dalam bentuk situs yang biasanya merupakan dokumen HTML”.

Apache memiliki fitur-fitur canggih seperti pesan kesalahan yang dapat dikonfigurasi, autentikasi berbasis basis data dan lain-lain. Apache juga didukung oleh sejumlah antar muka pengguna berbasis grafik (GUI) yang memungkinkan penanganan server menjadi mudah.

2.2.11 Kriptografi

Kriptografi merupakan ilmu yang berperan penting di dalam bidang keamanan informasi. Kriptografi digunakan untuk menjaga keamanan pesan atau informasi, baik informasi yang ditransmisikan melalui saluran komunikasi maupun informasi disimpan di dalam media penyimpanan. Bahkan, kehidupan kita saat ini dilingkupi oleh kriptografi; mulai dari transaksi di mesin ATM, transaksi di dalam perdagangan elektronik (e-commerce), transaksi dengan kartu kredit, percakapan melalui telepon genggam, mengakses internet, sampai mengaktifkan peluru kendali pun menggunakan kriptografi. Begitu pentingnya kriptografi untuk keamanan informasi, sehingga jika berbicara mengenai masalah keamanan yang berkaitan dengan penggunaan komputer, maka orang tidak bisa memisahkannya dengan kriptografi, (Munir, Rinaldi. 2019).

2.2.12 Kriptografi Asimetris

Algoritma Asimetris (Asymmetric atau Public Key) adalah algoritma yang menggunakan kunci yang berbeda untuk proses enkripsi dan dekripsi. Algoritma enkripsi asimetris termasuk Rivest–Shamir–Adleman (RSA), Diffie-Hellman, Digital Secure Algorithm (DSA), XTR, Elliptic Curve Cryptography (ECC), dan Elgamal Encryption System (ESS) (Abood & Guirguis, 2018).

2.2.13 Kriptanalisis

Kriptanalisis (cryptanalysis) adalah suatu ilmu dan seni membuka (breaking) ciphertext menjadi plaintext tanpa mengetahui kunci yang digunakan. Pelaku kriptanalisis disebut kriptanalisis (cryptanalyst). Kriptanalisis merupakan lawan kriptografer. Persamaan kriptanalisis dan kriptografer adalah bahwa kedua sama-sama menerjemahkan ciphertext menjadi plaintext, (Chandra Frenki Sianturi, 2020).

2.2.14 Pseudocode

Pseudocode atau kode semu merupakan deskripsi tingkat tinggi informal dan ringkas atas algoritme pemrograman komputer yang menggunakan konvensi struktural atas suatu bahasa pemrograman. Pembuatan kode semu ditujukan untuk dibaca oleh manusia dan bukan oleh mesin. Tujuan dari penggunaan kode-semu adalah untuk mempermudah manusia dalam pemahaman dibandingkan menggunakan bahasa pemrograman yang umum digunakan, terlebih aspeknya yang ringkas serta tidak bergantung pada suatu sistem tertentu merupakan prinsip utama dalam suatu algoritme (Wikipedia).

RSA adalah sebuah metode kriptografi yang digunakan untuk mengamankan data dengan cara mengenkripsi dan mendekripsi pesan dengan menggunakan pasangan kunci publik dan kunci privat. Metode ini dinamai berdasarkan tiga orang yang mengembangkan algoritma ini, yaitu Ron Rivest, Adi Shamir, dan Leonard Adleman pada tahun 1977.

Keamanan algoritma RSA terletak pada sulitnya memfaktorkan bilangan yang besar menjadi faktor-faktor prima. Pemfaktoran dilakukan untuk memperoleh kunci privat. Selama pemfaktoran bilangan besar menjadi faktor-faktor prima belum ditemukan algoritma yang mampu, maka selama itu pula keamanan algoritma RSA tetap terjamin (Syahputra, 2012).

RSA dapat digunakan untuk mengamankan komunikasi internet, seperti transaksi perbankan, email, dan pesan instan. Dalam RSA, pesan yang ingin dikirim diubah menjadi bilangan bulat, kemudian dienkripsi dengan menggunakan kunci publik. Setelah pesan terenkripsi, hanya kunci privat yang dapat digunakan untuk mendekripsinya. Kunci publik dan kunci privat dipilih secara khusus untuk memastikan bahwa hanya kunci privat yang dapat digunakan untuk mendekripsi pesan, sementara kunci publik dapat dibagikan kepada siapa saja tanpa mengkhawatirkan keamanan pesan yang telah dienkripsi.

Besaran-besaran yang digunakan pada algoritma RSA:

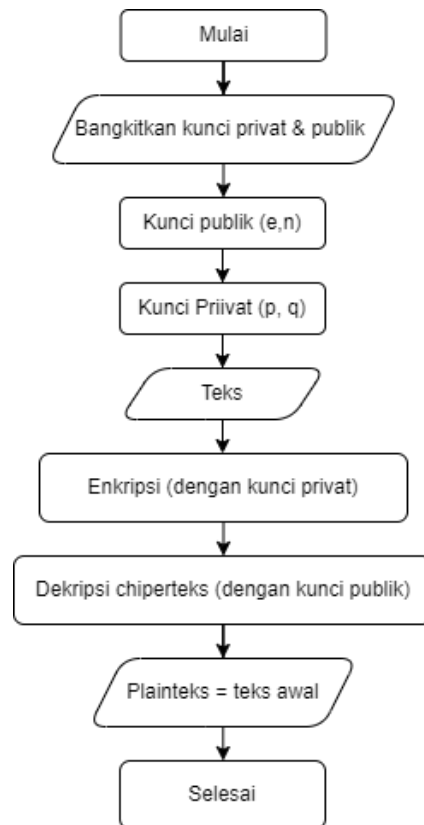
1. p dan q bilangan prima (rahasia)
2. $r = p \cdot q$ (tidak rahasia)
3. $\phi(r) = (p - 1)(q - 1)$ (rahasia)
4. PK (kunci enkripsi) (tidak rahasia)
5. SK (kunci dekripsi) (rahasia)
6. X (plaintexts) (rahasia)
7. Y (ciphertexts) (tidak rahasia)

Adapun langkah-langkah untuk proses mendapatkan kunci publik dan kunci privat adalah sebagai berikut:

- a. Pilih 2 buah bilangan prima secara acak, p & q .
- b. Kemudian untuk mendapatkan nilai r maka, $r = p \times q$
- c. Untuk mendapatkan nilai ϕr maka, $(p-1)(q-1)$
- d. Bangkitkan kunci public (public key) PK dengan cara mencari nilai yang relative prima terhadap ϕr
- e. Bangkitkan kunci rahasia (security key) SK dengan menggunakan $SK \cdot PK = 1 \pmod{\phi r}$.
- f. $SK \cdot PK = 1 \pmod{\phi r}$ ekuivalen dengan $SK \cdot PK = 1 + \text{mod}(\phi r)$ sehingga dapat dihitung dengan $SK = \frac{1 + \text{mod}(\phi r)}{PK}$.

Pada proses enkripsi, plainteks diubah ke dalam bentuk bilangan dengan menggunakan kode ASCII dalam bilangan decimal, sehingga plaintks m dinyatakan menjadi blok-blok x_1, x_2, x_3 , dalam $[0, n-1]$. Kemudian dienkripsi menggunakan rumus: $y_1 = x_i^{PK} \pmod r$. Dalam proses dekripsinya, cipherteks didekripsi kembali blok C_i menggunakan rumus : $x_1 = y_i^{PK} \pmod r$, lalu diubah kembali ke bentuk huruf dengan kode ASCII.

Di bawah ini merupakan flowchart algoritma RSA:



Gambar 2. 2 Flowchart Algoritma RSA

Dari gambar di atas dapat disimpulkan bahwa pada algoritma RSA awalnya diamankan dengan proses enkripsi yang akan berubah menjadi susunan huruf/angka acak sehingga tidak dapat diakses oleh siapapun kemudian agar teks tersebut dapat dibaca oleh orang yang dituju, maka dilakukan proses dekripsi kembali. Berikut Langkah-langkah dalam proses enkripsi RSA :

1. Hitung kunci publik dengan cara menghitung modulus r yaitu:

$$\begin{aligned}
 n &= p \times q \\
 &= 13 \times 31 \\
 &= 403
 \end{aligned}$$

kemudian,

$$\begin{aligned}\emptyset(r) &= (p-1)(q-1) \\ &= (13-1)(31-1) \\ &= 360\end{aligned}$$

Setelah mendapatkan kunci publik, kemudian menentukan nilai PK yang merupakan faktorial dari $\emptyset(r)$, faktorial dari $\emptyset(r)$ adalah 7.

- Setelah nilai PK sudah ditentukan, setelah itu menentukan nilai SK dengan

$$\text{rumus SK} = \frac{1+m\emptyset(r)}{PK} = \frac{1+m360}{7} = 103$$

- Setelah semua parameter telah berhasil dihitung dilakukan proses enkripsi, seperti dengan plainteks = “BELAJAR” dengan kode ASCII.

Binary	Oct	Dec	Hex	Glyph	Binary	Oct	Dec	Hex	Glyph	Binary	Oct	Dec	Hex	Glyph
010 0000	040	32	20	sp	100 0000	100	64	40	@	110 0000	140	96	60	`
010 0001	041	33	21	!	100 0001	101	65	41	A	110 0001	141	97	61	a
010 0010	042	34	22	"	100 0010	102	66	42	B	110 0010	142	98	62	b
010 0011	043	35	23	#	100 0011	103	67	43	C	110 0011	143	99	63	c
010 0100	044	36	24	\$	100 0100	104	68	44	D	110 0100	144	100	64	d
010 0101	045	37	25	%	100 0101	105	69	45	E	110 0101	145	101	65	e
010 0110	046	38	26	&	100 0110	106	70	46	F	110 0110	146	102	66	f
010 0111	047	39	27	'	100 0111	107	71	47	G	110 0111	147	103	67	g
010 1000	050	40	28	(100 1000	110	72	48	H	110 1000	150	104	68	h
010 1001	051	41	29)	100 1001	111	73	49	I	110 1001	151	105	69	i
010 1010	052	42	2A	*	100 1010	112	74	4A	J	110 1010	152	106	6A	j
010 1011	053	43	2B	+	100 1011	113	75	4B	K	110 1011	153	107	6B	k
010 1100	054	44	2C	,	100 1100	114	76	4C	L	110 1100	154	108	6C	l
010 1101	055	45	2D	-	100 1101	115	77	4D	M	110 1101	155	109	6D	m
010 1110	056	46	2E	.	100 1110	116	78	4E	N	110 1110	156	110	6E	n
010 1111	057	47	2F	/	100 1111	117	79	4F	O	110 1111	157	111	6F	o
011 0000	060	48	30	0	101 0000	120	80	50	P	111 0000	160	112	70	p
011 0001	061	49	31	1	101 0001	121	81	51	Q	111 0001	161	113	71	q
011 0010	062	50	32	2	101 0010	122	82	52	R	111 0010	162	114	72	r
011 0011	063	51	33	3	101 0011	123	83	53	S	111 0011	163	115	73	s
011 0100	064	52	34	4	101 0100	124	84	54	T	111 0100	164	116	74	t
011 0101	065	53	35	5	101 0101	125	85	55	U	111 0101	165	117	75	u
011 0110	066	54	36	6	101 0110	126	86	56	V	111 0110	166	118	76	v
011 0111	067	55	37	7	101 0111	127	87	57	W	111 0111	167	119	77	w
011 1000	070	56	38	8	101 1000	130	88	58	X	111 1000	170	120	78	x
011 1001	071	57	39	9	101 1001	131	89	59	Y	111 1001	171	121	79	y
011 1010	072	58	3A	:	101 1010	132	90	5A	Z	111 1010	172	122	7A	z
011 1011	073	59	3B	;	101 1011	133	91	5B	[111 1011	173	123	7B	{
011 1100	074	60	3C	<	101 1100	134	92	5C	\	111 1100	174	124	7C	
011 1101	075	61	3D	=	101 1101	135	93	5D]	111 1101	175	125	7D	}
011 1110	076	62	3E	>	101 1110	136	94	5E	^	111 1110	176	126	7E	~
011 1111	077	63	3F	?	101 1111	137	95	5F	_					

Gambar 2. 3 Daftar Kode ASCII

B	E	L	A	J	A	R
66	69	76	65	74	65	82

Sehingga didapat enkripsinya dengan cara kode ASCII dipangkatkan dengan PK kemudian dikalikan dengan modulo n, seperti di bawah ini:

$$B = 66^7 \bmod 403 = 326$$

$$E = 69^7 \bmod 403 = 121$$

$$L = 76^7 \bmod 403 = 236$$

$$A = 65^7 \bmod 403 = 234$$

$$J = 74^7 \bmod 403 = 334$$

$$A = 65^7 \bmod 403 = 234$$

$$R = 82^7 \bmod 403 = 173$$

Dalam proses dekripsi juga memiliki cara yang sama dengan enkripsi, namun ada sedikit perbedaan dari rumusnya, yaitu $Chiperteks^{KS} \bmod n$.

$$B = 326^{103} \bmod 403 = 66$$

$$E = 121^{103} \bmod 403 = 69$$

$$L = 236^{103} \bmod 403 = 76$$

$$A = 234^{103} \bmod 403 = 65$$

$$J = 334^{103} \bmod 403 = 74$$

$$A = 234^{103} \bmod 403 = 65$$

$$R = 173^{103} \bmod 403 = 82$$

Dari hasil proses dekripsi membuktikan bahwa nilai-nilai pada karakter kembali ke kode ASCII nya masing-masing tiap huruf.

Berikut merupakan pseudocode dari algoritma RSA :

```

Begin
    bin(1,1):= Binary Equivalent of d (or e)
    Initialise i= 1; rslt = 1; base = C (or M); modu = n
    Repeat until i>0
        If bin(1,i):=1
            rslt:= (rslt*base) modulus modu
        end
        base:= (base*base) modulus modu
        i:= i-1
    end
End

```

Gambar 2. 4 Pseudocode Algoritma RSA

2.2.15 ElGamal

Algoritma kriptografi ElGamal merupakan salah satu algoritma kunci asimetris yang didasarkan pada logaritma diskrit. Masalah logaritma diskrit adalah dengan memperhatikan hal berikut. Jika diberikan suatu bilangan a , maka menghitung $b \equiv \alpha a \pmod{p}$ adalah mudah, tetapi jika diberikan suatu bilangan b , maka untuk menemukan a sehingga $b \equiv \alpha a \pmod{p}$ adalah permasalahan yang sulit. Algoritma ini dikembangkan pertama kali oleh ilmuwan Mesir Taher ElGamal pada tahun 1985 (Nur Rochmat, 2012).

Seperti halnya RSA, ElGamal menggunakan pasangan kunci publik dan kunci privat untuk mengamankan komunikasi. Namun, ElGamal menggunakan algoritma yang berbeda untuk melakukan enkripsi dan dekripsi pesan.

Dalam ElGamal, pesan dienkripsi dengan mengalikan pesan dengan bilangan acak (yang disebut sebagai "bilangan enkripsi"), dan kemudian diubah

menjadi bilangan bulat. Pesan yang telah diubah menjadi bilangan bulat ini kemudian dikirim kepada penerima. Penerima kemudian menggunakan kunci privatnya untuk mendekripsi pesan.

Selain itu, ElGamal juga dapat digunakan untuk pertukaran kunci Diffie-Hellman, yaitu metode pertukaran kunci rahasia yang aman dan dapat dipercaya antara dua pihak yang ingin berkomunikasi secara rahasia di jaringan komputer. Kunci rahasia yang dihasilkan dari pertukaran kunci Diffie-Hellman kemudian digunakan untuk mengamankan komunikasi selanjutnya. ElGamal saat ini kurang populer dibandingkan RSA dan AES, meskipun tetap menjadi pilihan yang valid untuk keamanan komunikasi dan pertukaran kunci rahasia antara dua pihak yang ingin berkomunikasi secara aman.

Proses pembentukan kunci merupakan proses penentuan suatu bilangan yang kemudian akan digunakan sebagai kunci pada proses enkripsi dan dekripsi pesan. Kunci untuk enkripsi terdiri dari nilai p , g , y sedangkan kunci untuk dekripsi terdiri dari nilai x , p . Masing-masing nilai mempunyai persyaratan yang harus dipenuhi.

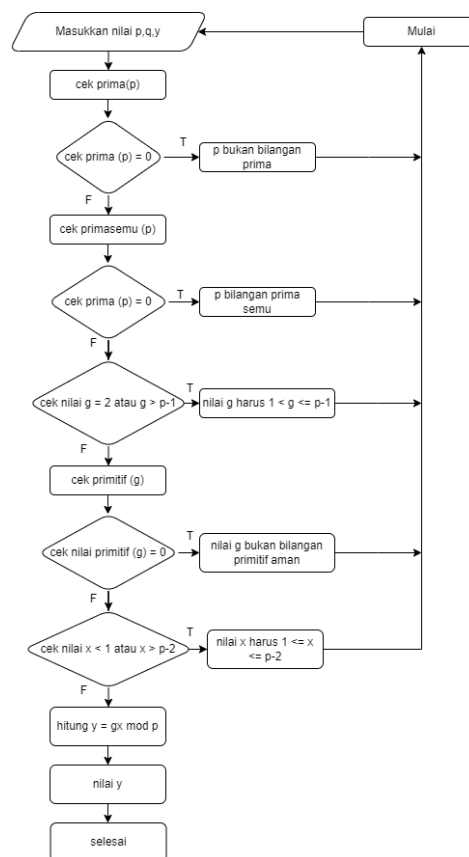
Langkah-langkah dalam pembuatan kunci adalah sebagai berikut.

1. Pilih bilangan prima acak p , dengan syarat $p > 255$.
 - a. Cek bilangan prima.
 - b. Cek prima semu (cek bilangan komposit) $\frac{p-1}{2} = x$.
2. Pilih bilangan elemen primitif g dengan syarat $1 < g \leq p-1$.

$$g^2 \bmod p \neq 1 \text{ dan } g^{\frac{p-1}{2}} \bmod p \neq 1.$$

3. Pilih bilangan acak x , dengan syarat $1 \leq x \leq p-2$.
4. Hitung $y = gx \bmod p$.

Dari langkah-langkah di atas akan diperoleh kunci publik yang digunakan untuk enkripsi adalah nilai p , g , y dan kunci pribadi yang digunakan untuk dekripsi adalah nilai x , p . Nilai p , g , y bersifat tidak rahasia sedangkan nilai x bersifat rahasia.



Gambar 2. 5 Bagan alir pembentukan kunci

Proses enkripsi merupakan proses mengubah pesan asli (plaintext) menjadi pesan rahasia (ciphertext). Pada proses ini digunakan kunci publik (p , g , y). Langkah-langkah dalam mengenkripsi pesan adalah sebagai berikut.

1. Potong plaintext menjadi blok-blok m_1, m_2, \dots , nilai setiap blok di dalam selang $[0, p-1]$.
2. Ubah nilai blok pesan ke dalam nilai ASCII.
3. Pilih bilangan acak k , dengan syarat $1 \leq k \leq p-2$.
4. Setiap blok m dienkripsi dengan rumus sebagai berikut.

$$\gamma(\gamma) = g^k \bmod p.$$

$$\delta(\delta) = y^k m \bmod p.$$
5. Susun ciphertext dengan urutan $\gamma_1, \delta_1, \gamma_2, \delta_2, \dots, \gamma_n, \delta_n$.

Pasangan γ dan δ adalah ciphertexts untuk blok pesan m . Hasil yang didapat dari proses enkripsi berupa pesan rahasia (ciphertext).

Proses dekripsi merupakan proses mengubah pesan rahasia (ciphertext) menjadi pesan asli (plaintext). Pada proses ini digunakan kunci pribadi (x, p) .

Langkah-langkah dalam mendekripsi pesan adalah sebagai berikut.

1. Penentuan nilai gamma dan delta. Nilai $\gamma(\gamma)$ diperoleh dari ciphertext dengan urutan ganjil sedangkan $\delta(\delta)$ dengan urutan genap.
2. Hitung plaintext m dengan persamaan rumus berikut.

$$m = \delta \cdot \gamma^{(p-1-x)} \bmod p.$$
3. Ubah nilai m yang didapat kedalam nilai ASCII.
4. Susun plaintext dengan urutan m_1, m_2, \dots, m_n .

Hasil yang didapat dari proses enkripsi berupa pesan asli (plaintext). Gambar di bawah merupakan proses alur dekripsi pesan.

Berikut merupakan pseudocode dari proses enkripsi ElGamal :

```

Procedure ElGamalEnkripsi(
  input g,p,m[n],x : integer,
  output a,b :integer)

{ Prosedur Enkripsi pada Algoritma ElGamal
  Masukan : g,p,x, plainteks m[1]..m[n]
  Keluaran: cipherteks a[1]b[1]..a[n]b[n]
}

Deklarasi
  k:integer
Algoritma
  temp_y ← 1
  For i ← 1 to x do
    temp_y ← temp_y * g
  Endfor
  y ← (temp_y) mod p
  for i ← 1 to n do
    k ← random(p-2)
    temp_a ← 1
    temp_b ← 1
    for j ← 1 to k do
      temp_a ← temp_a * g
      temp_b ← temp_b * y
    endfor
    a[i] ← (temp_a) mod p
    b[i] ← (temp_b * m[i]) mod p
  endfor

```

Diagram illustrating the ElGamal encryption procedure with annotations:

- C1**: $\{ \text{temp_y} \leftarrow 1 \}$
- x**: $\{ \text{For } i \leftarrow 1 \text{ to } x \text{ do} \dots \text{Endfor} \}$
- C2**: $\{ y \leftarrow (\text{temp_y}) \bmod p \}$
- C3**: $\{ \text{temp_a} \leftarrow 1, \text{temp_b} \leftarrow 1 \}$
- k**: $\{ \text{for } j \leftarrow 1 \text{ to } k \text{ do} \dots \text{endfor} \}$
- C4**: $\{ a[i] \leftarrow (\text{temp_a}) \bmod p, b[i] \leftarrow (\text{temp_b} * m[i]) \bmod p \}$
- n**: $\{ \text{for } i \leftarrow 1 \text{ to } n \text{ do} \dots \text{endfor} \}$

Gambar 2. 6 Pseudocode Algoritma ElGamal

2.3 Penelitian Terkait

adapun penelitian sebelum yang kami gunakan sebagai rujukan terhadap penelitian ini adalah sebagai berikut :

1. Penelitian ini dilakukan Tampubolon A dengan mengambil judul :
 “IMPLEMENTASI KOMBINASI ALGORITMA RSA DAN ALGORITMA DES PADA APLIKASI PENGAMAN PESAN TEKS”.

Dalam penelitian ini perbedaannya yaitu penelitian tersebut lebih umum membahas tentang pengamanan data pesan teks sedangkan penelitian yang akan dibuat membahas pengamanan data rekam medis.

Persamaan penelitian tersebut dengan penelitian yang akan dibuat yaitu pada algoritma yang digunakan, yaitu sama – sama menggunakan algoritma RSA.

2. Penelitian ini dilakukan oleh Edi Rahmansyah pada tahun 2019 dengan mengambil judul : “IMPLEMENTASI ALGORITMA ELGAMAL DENGAN PEMBANGKIT BILANGAN PRIMA LEHMANN DAN ALGORITMA LEAST SIGNIFICANT BIT (LSB) DENGAN COVER IMAGE BITMAP UNTUK KEAMANAN DATA TEXT”.

Perbedaan penelitian di atas dengan penelitian yang penulis akan buat yaitu penelitian di atas melakukan pengaman dengan menggunakan lebih dari satu algoritma sedangkan yang penulis akan buat hanya menggunakan satu algoritma saja, tetapi juga melakukan pengamanan dengan algoritma lain, kemudia melakukan komparasi atau perbandingan algoritma mana yang lebih aman.

Persamaan penelitian tersebut dengan penelitian yang akan dibuat yaitu pada salah satu algoritma yang digunakan yaitu sama-sama menggunakan algoritma elgamal.

3. Penelitian ini dilakukan Sutejo pada tahun 2021 dengan mengambil judul : “IMPLEMENTASI ALGORITMA KRIPTOGRAFI RSA (RIVEST SHAMIR ADLEMAN) UNTUK KEAMANAN DATA REKAM MEDIS PASIEN”.

Perbedaan penelitian di atas dengan penelitian yang penulis akan buat yaitu penelitian tersebut hanya menggunakan satu metode algoritma yaitu algoritma RSA sedangkan yang penulis akan buat menggunakan dua algoritma yaitu RSA dan ElGamal.

Persamaan penelitian di atas dengan penelitian yang penulis akan buat yaitu penelitian tersebut sama-sama menggunakan algoritma RSA.

4. Penelitian ini dilakukan Susilawati pada tahun 2018 dengan judul :
“PERANCANGAN KUNCI PUBLIC RSA DAN ELGAMAL PADA KRIPTOGRAFI UNTUK KEMANANAN INFORMASI”.

Perbedaan penelitian di atas dengan penelitian yang penulis akan buat yaitu penelitian tersebut tidak memiliki objek penelitian sedangkan yang penulis akan buat mengambil objek data rekam medis pada klinik.

Persamaan penelitian di atas dengan penelitian yang penulis akan buat yaitu penelitian tersebut sama-sama menggunakan algoritma RSA dan ElGamal.

BAB III

METODE PENELITIAN

3.1 Waktu dan Tempat Penelitian

Proses penelitian ini dilaksanakan di Klinik Utama Botolempang, Jl. Sungguminasa - Takalar, Bontosunggu, Kec. Bajeng, Kabupaten Gowa, 92152 Sulawesi Selatan. Adapun waktu penelitian adalah selama dua bulan, yakni dari bulan mei 2023 sampai juni 2023.

3.2 Alat dan Bahan Penelitian

Adapun Alat dan Bahan Penelitian yang penulis gunakan dalam penelitian ini antara lain sebagai berikut:

1. Alat Penelitian

Alat Penelitian yang digunakan terdiri dari 2 bagian yaitu Perangkat Lunak dan Perangkat Lunak yang dapat dilihat di tabel 3.1 dan tabel 3.2.

Tabel 3.1 Perangkat lunak yang digunakan

No	Perangkat Lunak	Unit	Spesifikasi
1	Sistem Operasi	1	Microsoft Windows 11
2	Database	1	<i>Mysql</i>
3	<i>Editor Text</i>	1	<i>Visual Studio Code</i>
4	<i>Browser</i>	1	<i>Chrome</i>
5	Bahasa Pemrograman	1	<i>Php</i>

Tabel 3.2 Perangkat keras yang digunakan

No	Perangkat Keras	Unit	Spesifikasi
1	<i>Processor</i>	1	<i>Intel Core i5</i>
2	<i>Harddisk</i>	1	1048 Gb
3	RAM	1	DD3 4B

2. Bahan Penelitian

Tabel 3.3 Bahan penelitian

No	Bahan Penelitian	Keterangan
1	Data Rekam Medis	Catatan

3.3 Jenis dan Variabel Penelitian

Dalam menyelesaikan penulisan ini, jenis penelitian yang dilakukan ialah sebagai berikut:

1. Penelitian lapangan (*Library Research*)

Penelitian lapangan adalah penelitian yang dilakukan dengan melakukan pengambilan data secara langsung.

2. Penelitian pustaka (*Field Research*)

Penelitian pustaka adalah penelitian yang dilakukan dengan mengambil beberapa buku rujukan dan jurnal mengenai definisi dan konsep perancangan aplikasi pemesanan.

3.4 Metode Pengujian Sistem

Pengujian sistem dilakukan untuk mengetahui sistem yang dibangun, apakah dapat berfungsi sesuai dengan yang diharapkan. Metode pengujian sistem yang digunakan pada pengujian ini adalah Black Box testing. Pengujian Black Box berfokus pada persyaratan fungsional perangkat lunak. Pengujian Black Box merupakan pendekatan komplementer yang kemungkinan besar mampu mengungkap kelas kesalahan. Metode pengujian ini sangat tepat digunakan untuk mengetahui apakah sistem bekerja dengan baik, apabila sistem memberikan output yang tidak sesuai, maka telah terjadi kesalahan dalam sistem dan berusaha menemukan kesalahan dalam kategori sebagai berikut:

1. Fungsi yang tidak benar atau hilang.
2. Kesalahan dalam struktur data atau akses database eksternal.
3. Kesalahan kinerja.

Dalam pengujian ini target yang hendak dicapai ialah apakah sistem dapat memberikan informasi yang efektif.

3.5 Tahap dan Rancangan Penelitian

3.5.1 Tahap Penelitian

1. Survei lokasi : melihat tempat penelitian.
2. Pengumpulan data : mengumpulkan informasi yang dilakukan secara langsung ke tempat penelitian atau melalui studi literatur.
3. Analisis Sistem : penguraian dari suatu aplikasi yang utuh ke dalam bagian-bagian komponennya dengan maksud untuk mengidentifikasi dan mengevaluasi permasalahan, kesempatan, hambatan, yang terjadi

dan kebutuhan yang diharapkan sehingga dapat diusulkan perbaikan-perbaikannya.

4. Perancangan sistem : merupakan strategi untuk memecahkan masalah dan mengembangkan solusi terbaik bagi permasalahan.
5. Coding adalah menerjemahkan persyaratan logika dari *pseudocode* atau diagram alur ke dalam suatu bahasa pemrograman baik huruf, angka, dan simbol yang membentuk program.
6. Pengujian Program : mengetahui cara kerja dari aplikasi yang dirancang secara terperinci sesuai spesifikasi dan menilai apakah setiap fungsi atau prosedur yang dirancang sudah bebas dari kesalahan logika.
7. Implementasi merupakan penerapan aplikasi dari hasil perancangan sistem yang ada untuk mencapai suatu tujuan yang diinginkan. Implementasi melaksanakan perintah-perintah yang secara terstruktur dari awal sampai akhir.

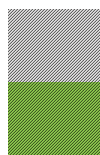
3.5.2 Rancangan Jadwal Penelitian

Tahapan dalam perancangan sistem informasi yang disertai dengan perkiraan waktu pengerjaan, ditunjukkan pada tabel 3.4 Rancangan Jadwal Penelitian sebagai berikut :

Tabel 3.4 Rancangan Jadwal Penelitian

No	Tahapan Penelitian	Mei 2023				Juni 2023				Juli 2023			
		1	2	3	4	1	2	3	4	1	2	3	4
1.	Survei Lokasi Penelitian												
2.	Pengumpulan data												
3.	Analisis												
4.	Perancangan Sistem												
5.	<i>Coding</i> / Pembuatan Aplikasi												
6.	Pengujian												

Keterangan :



Sudah dilaksanakan

Belum dilaksanakan

BAB IV

HASIL PENELITIAN DAN PEMBAHASAN

4.1 Analisis Data

4.1.1 Analisis Kriptografi RSA

Pada bagian ini akan dilakukan pengujian terhadap enkripsi dan dekripsi dari algoritma RSA. Pengujian secara manual dilakukan dengan tujuan membandingkan hasil akhir dari proses enkripsi berupa cipherteks dan hasil akhir proses dekripsi berupa plainteks.

Tabel 4. 1 Kunci publik RSA

keterangan	nilai
pesan(m) / plainteks	Ananda
kunci publik (e,n)	(3,319)

Pada tabel 4.1 terdapat pesan atau plaintext dengan nilai “Ananda” yang akan dienkripsi dengan menggunakan kunci publik (e, n) “3, 310”.

1. Pengujian Enkripsi

Langkah-langkah penyelesaian proses enkripsi secara manual adalah sebagai berikut.

Diketahui :

Plainteks (m) : “Ananda”

Kunci publik (e, n) : (3, 319)

Jawab :

1) Ambil kunci publik penerima pesan (e, n) = (3, 319).

2) Ubah plainteks (m) menjadi pesan dengan nilai ASCII.

$$A = 65, n = 110, a = 97, n = 110, d = 100, a = 97.$$

3) Potong pesan menjadi blok-blok pesan m_1, m_2, m_3, \dots

4) Setiap blok m dihitung dengan rumus $e_i = m_i^e \bmod n$.

$$c^1 = 65^3 \bmod 319 = 285$$

$$c^2 = 110^3 \bmod 319 = 132$$

$$c^3 = 97^3 \bmod 319 = 14$$

$$c^4 = 110^3 \bmod 319 = 132$$

$$c^5 = 100^3 \bmod 319 = 254$$

$$c^6 = 97^3 \bmod 319 = 14$$

5) Susun nilai c hasil enkripsi dengan susunan $c^1, c^2, c^3, \dots, c^n$ sehingga diperoleh cipherteks dari pesan m.

Cipherteks : 285,132, 14, 132, 254, 14.

2. Pengujian Dekripsi

Langkah-langkah penyelesaian proses enkripsi secara manual adalah sebagai berikut.

Diketahui : Cipherteks (m) : “285,132, 14, 132, 254, 14.”.

Kunci rahasia (d, n) : (187, 319)

Jawab :

1) Ambil pesan (cipherteks) yang telah diterima. Cipherteks (m) : “285,132, 14, 132, 254, 14.”.

2) Kemudian ambil kunci rahasia (d,n) = (187, 319).

3) Potong pesan menjadi blok-blok pesan c_1, c_2, c_3, \dots

4) Hitung $m_i = c_i^d \bmod n$.

$$m_1 = 285^{187} \bmod 319 = 65$$

$$m_2 = 132^{187} \bmod 319 = 110$$

$$m_3 = 14^{187} \bmod 319 = 97$$

$$m_4 = 132^{187} \bmod 319 = 110$$

$$m_5 = 254^{187} \bmod 319 = 100$$

$$m_6 = 14^{187} \bmod 319 = 97$$

5) Ubah nilai $m_1, m_2, m_3, \dots, m_n$ sesuai dengan tabel ASCII sehingga diperoleh plainteks (pesan asli) dari cipherteks yang diterima.

$$65 = A, 110 = n, 97 = a, 110 = n, 100 = d, 97 = a.$$

6) Susun nilai ASCII yang dihasilkan.

Hasil penyusunan inilah yang merupakan pesan asli (plainteks) setelah melalui proses dekripsi. Pesan asli (plainteks) : “Ananda”.

4.1.2 Analisis Kriptografi ElGamal

Pengujian dilakukan dengan cara membandingkan hasil proses enkripsi dan dekripsi dari program aplikasi yang telah dibuat dengan hasil penghitungan enkripsi dan dekripsi secara manual. Data yang digunakan untuk pengujian ini adalah seperti dibawah ini.

Tabel 4. 2 Pemilihan kunci ElGamal

keterangan	nilai
pesan(m) / plainteks	Ananda
Nilai (p,g,y,x)	(257, 2, 129, 255)
Nilai k	$k_1 = 2, k_2 = 5, k_3 = 1, k_4 = 1, k_5 = 7, k_6 = 2$

Pada tabel 4. 2 pemilihan kunci elgamal, pesan atau plaintext yang akan dienkripsi adalah “Ananda”, dengan menggunakan kunci $p = 257$, $g = 2$, $y = 129$, dan $x = 255$.

Untuk nilai acak ‘k’ yang digunakan berdasarkan jumlah karakter pesan yaitu 6 adalah $k_1 = 2, k_2 = 5, k_3 = 1, k_4 = 1, k_5 = 7, k_6 = 2$.

1. Pengujian Enkripsi

Langkah-langkah penyelesaian proses enkripsi secara manual adalah sebagai berikut:

Diketahui :

Plaintext : “Ananda”

Nilai $p = 257$, $g = 2$ dan $y = 129$.

Nilai $k_1 = 4, k_2 = 5, k_3 = 1, k_4 = 1, k_5 = 7, k_6 = 2$.

Jawab :

a. Ubah pesan asli (plaintext) ke dalam ASCII

$$A = 65, n = 110, a = 97, n = 110, d = 100, a = 97.$$

sehingga nilai pesan ASCII adalah sebagai berikut :

$$m_1 = 65, m_2 = 110, m_3 = 97, m_4 = 110, m_5 = 100, m_6 = 97.$$

b. Hitung gamma (γ) dengan rumus $\gamma = g^k \bmod p$.

$$\gamma_1 = 2^2 \bmod 257 = 4$$

$$\gamma_2 = 2^5 \bmod 257 = 32$$

$$\gamma_3 = 2^1 \bmod 257 = 2$$

$$\gamma_4 = 2^1 \bmod 257 = 2$$

$$\gamma_5 = 2^7 \bmod 257 = 128$$

$$\gamma_6 = 2^2 \bmod 257 = 4$$

c. Hitung delta dengan rumus $\delta = y^k \cdot m \bmod p$

$$\delta_1 = 129^2 \cdot 65 \bmod 257 = 209$$

$$\delta_2 = 129^5 \cdot 110 \bmod 257 = 148$$

$$\delta_3 = 129^1 \cdot 97 \bmod 257 = 177$$

$$\delta_4 = 129^1 \cdot 110 \bmod 257 = 55$$

$$\delta_5 = 129^7 \cdot 110 \bmod 257 = 57$$

$$\delta_6 = 129^2 \cdot 97 \bmod 257 = 217$$

d. Susun hasil perhitungan gamma (γ) dan delta (δ)

Ciphertext : 4, 209, 32, 148, 2, 177, 2, 55, 128, 57, 4, 217.

2. Pengujian Deskripsi

Langkah-langkah penyelesaian proses dekripsi secara manual adalah sebagai berikut :

Diketahui :

Ciphertext : 4, 209, 32, 148, 2, 177, 2, 55, 128, 57, 4, 217.

Nilai $p = 257$, $x = 255$.

Jawab :

a. Pisahkan nilai gamma dan delta pada pesan rahasia (ciphertext).

γ = Ciphertext urutan ganjil.

δ = Ciphertext urutan genap.

Nilai gama $\gamma_1 = 4$, $\gamma_2 = 32$, $\gamma_3 = 2$, $\gamma_4 = 2$, $\gamma_5 = 128$, $\gamma_6 = 4$,

Nilai delta $\delta_1 = 209$, $\delta_2 = 148$, $\delta_3 = 177$, $\delta_4 = 55$, $\delta_5 = 128$, $\delta_6 = 217$.

b. Hitung m (pesan asli) dengan rumus :

$$m = \delta \cdot \gamma^{(p-1-x)} \bmod p$$

$$m_1 = 209 \cdot 4^{(257-1-255)} \bmod 255$$

$$= 836 \bmod 257$$

$$= 65$$

Dst..

Sehingga Hasil nya :

$$m_1 = 65, m_2 = 110, m_3 = 97, m_4 = 110, m_5 = 100, m_6 = 97.$$

c. Ubah m kedalam ASCII.

$$65 = A, 110 = n, 97 = a, 110 = n, 100 = d, 97 = a.$$

d. Hasil dari penyusunan inilah yang merupakan pesan asli (plaintext) yang dihasilkan pada proses dekripsi. plaintext: "Ananda".

Hasil proses perhitungan enkripsi dekripsi dengan program aplikasi dan secara manual adalah sama. Selain itu plaintext setelah dekripsi sama dengan nilai plaintext sebelum di enkripsi.

4.2 Kriptanalisis Algoritma RSA dan ElGamal

4.2.1 Kriptanalisis RSA

1. Serangan Faktorisasi

Serangan yang sering dilakukan terhadap algoritma kriptografi RSA adalah faktorisasi. Penyerangan ini bertujuan untuk memfaktorkan nilai n menjadi dua buah faktor primanya yaitu p dan q . Jika p dan q berhasil difaktorkan, fungsi euler $\phi(n) = (p - 1)(q - 1)$ akan dapat dikomputasi dengan mudah dan kemudian kunci rahasia (d , n) dapat diketahui. Fungsi totien euler ϕ mendefinisikan $\phi(n)$ untuk $n \geq 1$ yang menyatakan bilangan bulat positif $< n$ yang relatif prima dengan n .

Dari pengujian diatas diketahui bahwa kunci publik $(e, n) = (3, 319)$. Setelah diketahui nilai n adalah 319, maka kriptanalisis akan mencari nilai $\phi(319)$. Untuk menemukan nilai p dan q , kriptanalisis harus mencoba seluruh bilangan bulat positif yang benilai lebih kecil dari n yang relatif prima dengan n .

2. Serangan Brute-force

Brute-Force merupakan sebuah teknik serangan terhadap sebuah sistem keamanan komputer dengan melakukan percobaan terhadap kombinasi pasangan kunci rahasia (d , n) yang mungkin. Nilai n dapat

diketahui karena bersifat tidak rahasia dan digunakan pada saat proses enkripsi.

Percobaan dilakukan dengan asumsi kriptanalisis mengetahui cipherteks dan kunci publik (e, n). Percobaan dilakukan sebanyak tiga kali dengan mengkombinasikan nilai d dan n yang mungkin.

Percobaan dilakukan dengan dekripsi terhadap cipherteks yang telah didapatkan dengan menggunakan kemungkinan kunci pribadi yang ada. Kemudian akan dibandingkan plainteks hasil dari percobaan serangan Brute-Force dengan plainteks asli. Berikut ini adalah proses dekripsi dari salah satu percobaan serangan Brute-Force menggunakan kunci rahasia (89, 319).

$$m_1 = 285^{89} \bmod 319 = 65$$

$$m_2 = 132^{89} \bmod 319 = 110$$

$$m_3 = 14^{89} \bmod 319 = 48$$

$$m_4 = 142^{89} \bmod 319 = 110$$

$$m_5 = 254^{89} \bmod 319 = 100$$

$$m_6 = 14^{89} \bmod 319 = 48$$

Dari percobaan diatas, plainteks masih bernilai desimal sehingga perlu diubah melalui tabel ASCII untuk mengetahui isi dari plainteks aslinya.

Jadi plainteks dari hasil serangan Brute-Force tidak ada yang sesuai dengan plainteks pesan asli, yaitu “Ananda”. Pengujian Brute-Force didasarkan pada jumlah karakter kunci d . Jumlah karakter kunci

ini akan menentukan banyaknya jumlah percobaan yang harus dilakukan untuk mendapatkan plainteks.

Dapat diketahui bahwa jumlah bit kunci adalah 2 karakter kunci atau (16 bit). Maka dengan menggunakan rumus jumlah kemungkinan kunci yang mungkin adalah sebagai berikut: Jumlah kemungkinan kunci = 2, bit kunci = $2^{16} = 65.536$. Jadi jumlah kemungkinan kunci yang dapat dicoba pada serangan Brute-Force adalah sebanyak 65.536 buah kunci.

4.2.2 Kriptanalisis ElGamal

1. *Known-plain attack*

Untuk mengetahui keamanan ElGamal dari jenis serangan ini akan dilakukan tiga kali percobaan proses enkripsi pesan dengan plaintext dan kunci yang sama. Nilai plaintext: “Ananda”, dengan kunci publik $(p, g, y) = (257, 2, 129)$.

Pada tiga kali percobaan dihasilkan data seperti terlihat pada data di bawah ini. Dari tersebut dapat dilihat bahwa dengan plaintext dan kunci yang sama menghasilkan ciphertext yang berbeda. Hal ini dikarenakan adanya nilai k yang acak. Nilai k yang acak membuat nilai γ dan δ selalu berubah sehingga ciphertext yang dihasilkan untuk setiap percobaan selalu berubah. Hal tersebut akan menyulitkan kriptanalisis dalam mengkorelasikan (menemukan hubungan) antara plaintext dengan ciphertext, sehingga akan menyulitkan penemuan algoritma alternatif

Tabel 4. 3 Hasil enkripsi ElGamal

Plaintext	Kunci (p, g, y)	Chipertext
Ananda	257, 2, 129	16, 245, 2, 55, 2, 177, 32, 148, 32, 228 128, 63.
Ananda	257 ,2, 129	64, 254, 4, 156, 16, 247, 64, 74, 16, 199, 2, 177.
Ananda	257, 2, 129	64, 254, 16, 39, 8, 237, 64, 74, 8, 141, 8, 237.

Pada tabel 4.3 merupakan hasil percobaan proses enkripsi pesan dengan plaintext dan kunci yang sama sebanyak tiga kali. Pesan atau plaintext yang digunakan adalah “Ananda”, yang menghasilkan chipertext yang berbeda tiap proses enkripsi.

4.3 Komparasi RSA dan Elgamal

4.3.1 Proses Enkripsi

Proses enkripsi pada algoritma RSA menghasilkan karakter chipertext yang lebih sedikit serta chipertext yang sama tiap melakukan enkripsi, berbeda dengan algoritma ElGamal yang menghasilkan chipertext yang lebih banyak serta chipertext yang berbeda tiap enkripsinya. Seperti yang terlihat pada tabel di bawah ini.

Tabel 4. 4 Percobaan enkripsi RSA

NO	Plaintext	Jumlah Karakter plaintext	Chipertext	Jumlah karakter chipertext
1	Ananda	6	285 132 14 132 254 14	21
2	Ananda	6	285 132 14 132 254 14	21
3	Ananda	6	285 132 14 132 254 14	21
4	Ananda	6	285 132 14 132 254 14	21
5	Ananda	6	285 132 14 132 254 14	21

Tabel 4. 5 Percobaan Enkripsi ElGamal

NO	Plaintext	Jumlah Karakter Plaintext	Chipertext	Jumlah Karakter chipertext
1	Ananda	6	4 209 32 148 2 177 2 55 128 57 4 217	36
2	Ananda	6	8 233 16 39 8 237 128 37 8 141 64 126	37
3	Ananda	6	128 127 2 55 16 247 2 55 2 50 4 217	35
4	Ananda	6	8 233 16 39 8 237 4 156 2 50 4 217	35
5	Ananda	6	16 245 128 37 8 237 16 39 4 25 2 177	37

Tabel 4.4 dan tabel 4.5 merupakan hasil percobaan enkripsi menggunakan RSA dan ElGamal yang dilakukan sebanyak lima kali. Pada percobaan menggunakan RSA chipertext yang dihasilkan akan selalu sama berbeda dengan percobaan menggunakan ElGamal, chipertext yang dihasilkan akan selalu berbeda.

4.3.2 Proses Deskripsi

Proses deskripsi pada algoritma RSA menggunakan rumus yang sama tiap karakter chipertext untuk mendapatkan plaintext, sedangkan pada algoritma ElGamal proses deksripsi lebih rumit karena terlebih dahulu memisahkan urutan karakter chipertext berdasarkan urutan ganjil dan urutan genap.

4.3.3 Proses Kriptanalisis

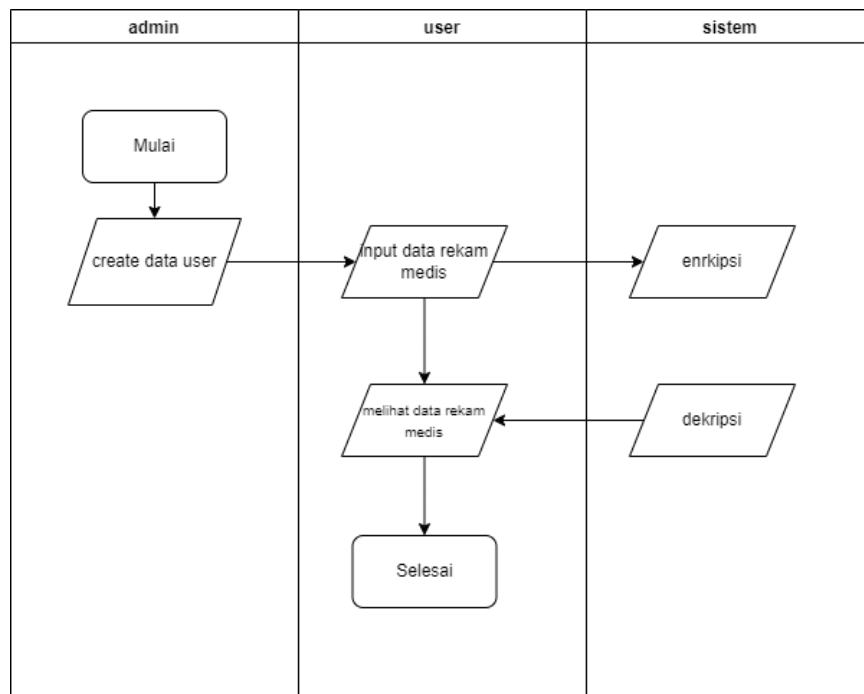
Berdasarkan percobaan serangan yang dilakukan pada hasil enkripsi algoritma RSA dan ElGamal, kemungkinan jumlah kunci yang didapat untuk memecahkan ciphertext dari RSA memerlukan 65.536 percobaan, seperti pada hasil serangan *brute-force*. Tidak menutup kemungkinan terdapat sistem yang berhasil dibuat untuk memecahkan kunci tersebut.

Sedangkan pada percobaan serangan enkripsi ElGamal, masih belum ada algoritma atau sistem yang dapat memecahkan kemungkinan - kemungkinan kunci akan didapat karena tiap enkripsi ElGamal menghasilkan ciphertext yang selalu berbeda meskipun menggunakan kunci enkripsi yang sama.

4.4 Perancangan dan Implementasi Sistem

4.4.1 Sistem yang berjalan

Penulis menggambarkan komparasi algoritma RSA (risvet shamir adleman) dan Elgamal pada pengamanan data rekam medis berbasis web yang berjalan dapat dilihat pada Gambar 4.1. Berdasarkan gambar tersebut dapat kita amati .

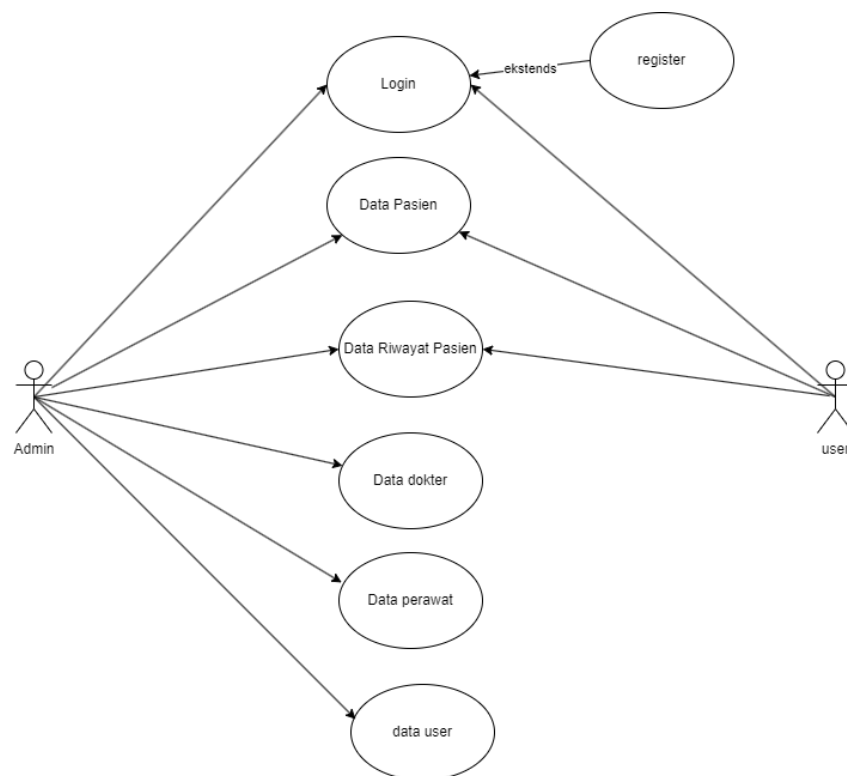


Gambar 4. 1 Sistem yang berjalan

4.4.2 Sistem yang diusulkan

a. Use Case Diagram

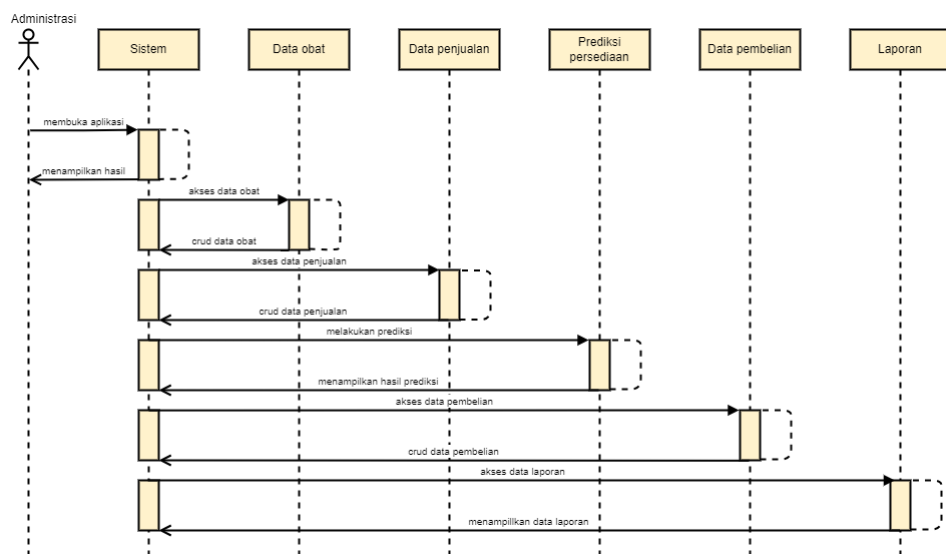
Use case diagram menggambarkan fungsionalitas yang diharapkan dari sebuah sistem. Yang ditekankan adalah “apa” yang diperbuat sistem, dan bukan “bagaimana”. Sebuah *use case* merepresentasikan atau menggambarkan sebuah interaksi antar aktor dengan sistem. *Use case* merupakan sebuah pekerjaan tertentu, misalnya *login* ke sistem, *mengcreate* sebuah data, dan sebagainya.



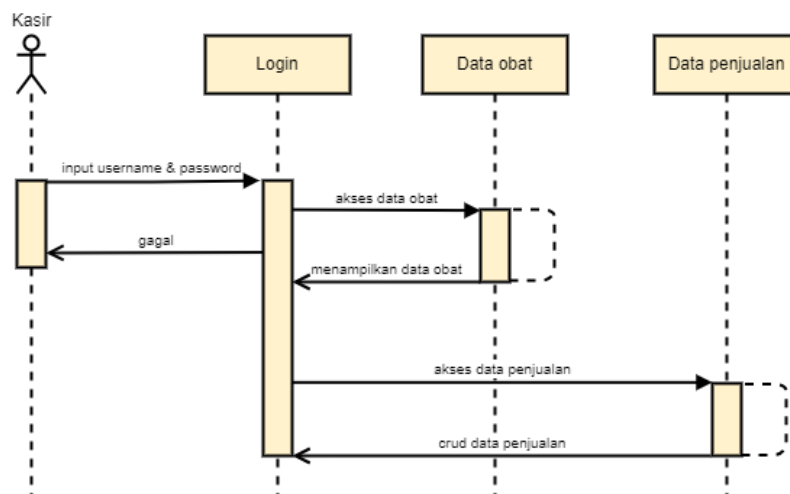
Gambar 4. 2 Use Case admin dan user

b. Sequence Diagram

Sequence diagram (diagram urutan) adalah suatu diagram yang memperlihatkan atau menampilkan interaksi-interaksi antar objek di dalam sistem yang disusun pada sebuah urutan atau rangkaian waktu. Interaksi antar objek tersebut termasuk pengguna, *display* dan sebagainya berupa meng-*create* data dan sebagainya.



Gambar 4. 3 *Sequence Diagram* Administrasi

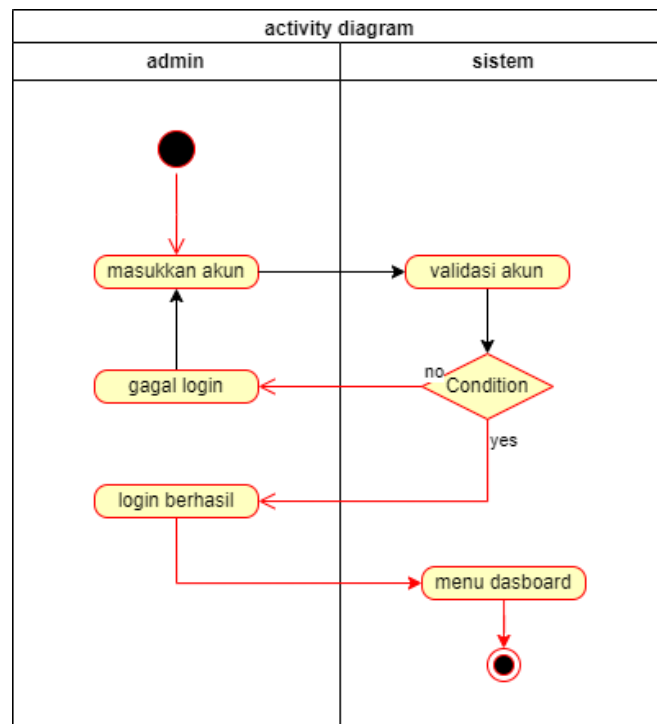


Gambar 4. 4 *Sequence Diagram* Kasir

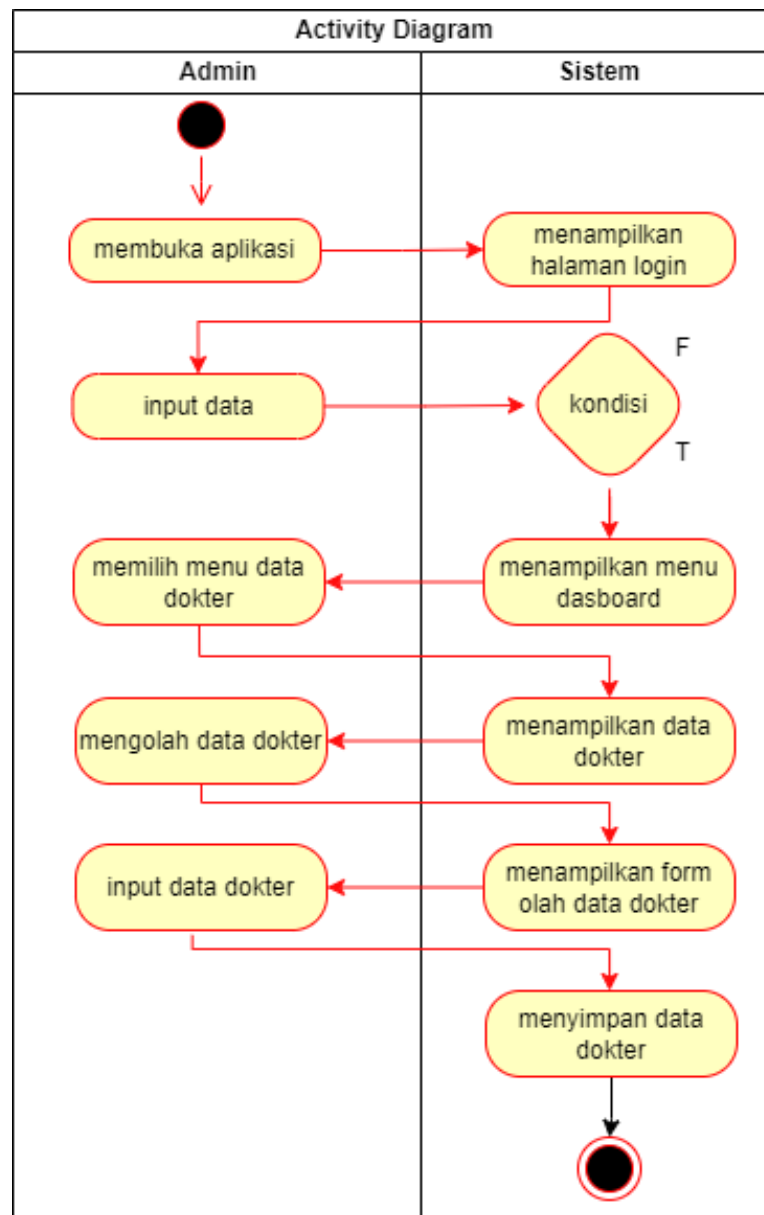
c. Activity Diagram

1) Activity Diagram

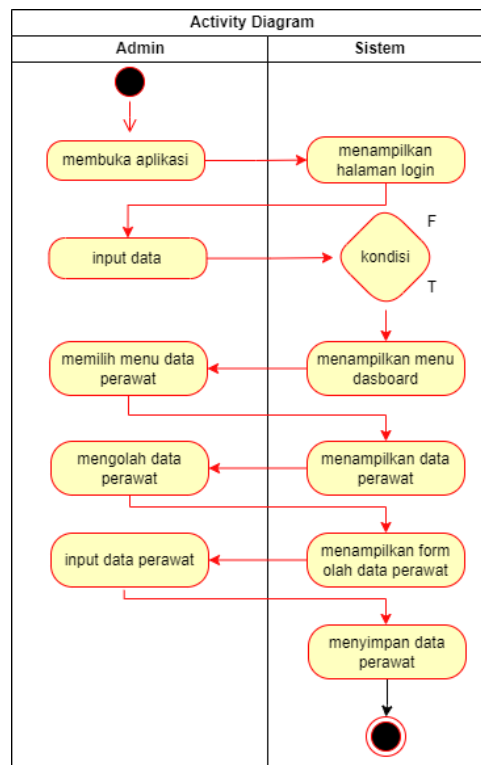
Activity Diagram menggambarkan alur aktivitas dalam sistem dalam proses penginputan login dan input dan sebagainya, yang berawal dari start state dimana terdapat state data admin kemudian dilanjutkan *activity* untuk menginput data dokter dan sebagainya, *Activity diagram* juga dapat menggambarkan proses paralel yang mungkin terjadi pada beberapa eksekusi.



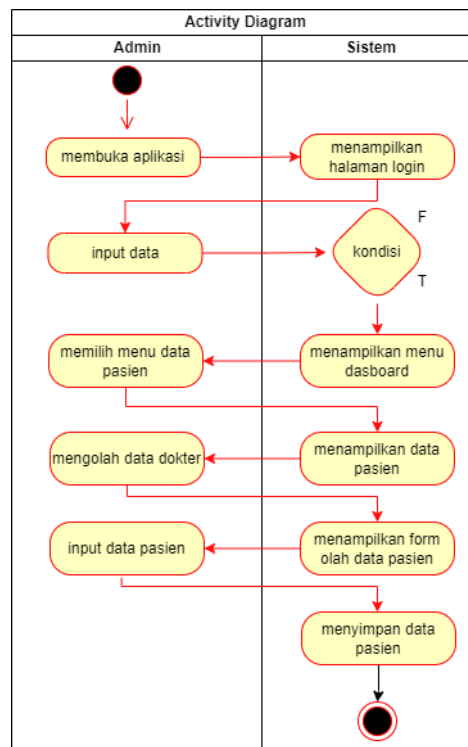
Gambar 4. 5 Activity Diagram Login



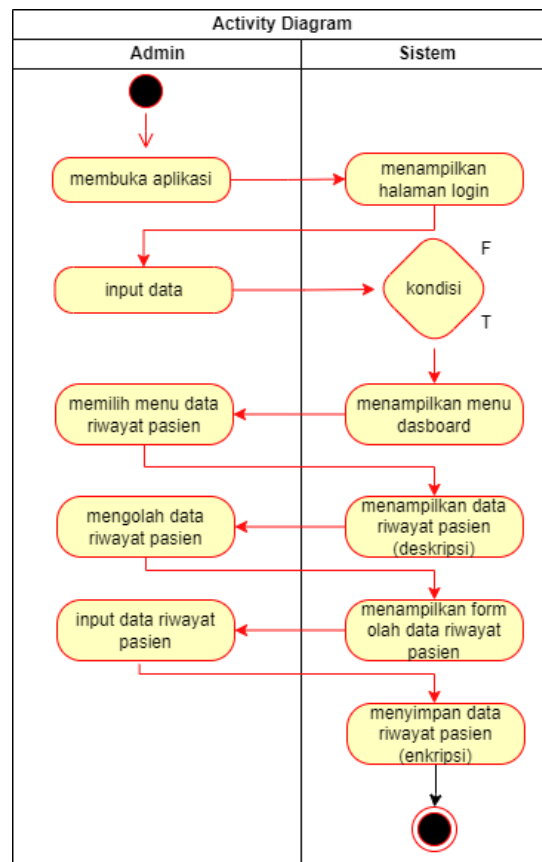
Gambar 4. 6 *Acitivity Diagram* Data dokter



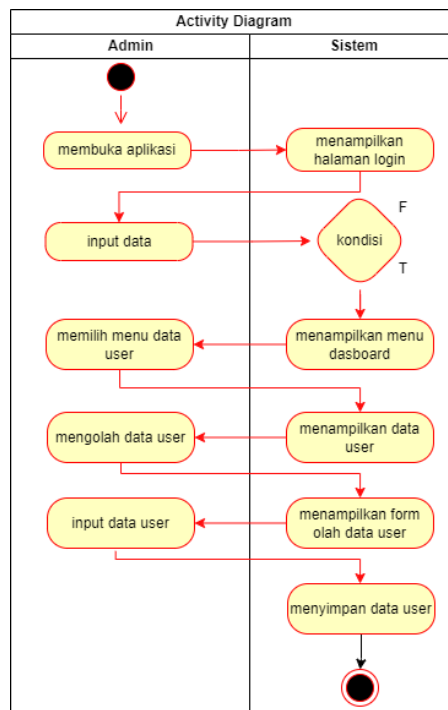
Gambar 4. 7 *Activity Diagram Admin Data Perawat*



Gambar 4. 8 *Activity Diagram Admin Pasien*



Gambar 4. 9 Activity Diagram Admin Data Riwayat pasien



Gambar 4. 10 Activity Diagram Admin Data User

d. Struktur Tabel

1. Tabel admin

Tabel 4. 6 Tabel admin

No	Nama Field	Tipe	Ukuran	Keterangan
1.	id_admin	int	11	Id admin
2.	username	Varchar	100	Username
3.	password	Varchar	100	Password
4.	nama_lengkap	Varchar	100	Nama admin

2. Tabel user

Tabel 4. 7 Tabel user

No	Nama Field	Tipe	Ukuran	Keterangan
1.	id_user	int	11	Id user
2.	username	Varchar	100	Username
3.	Password	Varchar	100	Password
4.	nama_lengkap	Varchar	100	Nama admin

3. Tabel dokter

Tabel 4. 8 Tabel dokter

No	Nama Field	Tipe	Ukuran	Keterangan
1.	id_dokter	int	11	Id dokter
2.	Nama_dokter	Varchar	100	Nama dokter
3.	Nip	Varchar	100	Nip
3.	Nomor_handphone	Varchar	100	Nomor handphone
4.	Foto	Varchar	100	foto

4. Tabel perawat

Tabel 4. 9 Tabel perawat

No	Nama Field	Tipe	Ukuran	Keterangan
1.	id_perawat	Int	11	Id perawat
2.	Nama_perawat	Varchar	100	Nama perawat
3.	Nip	Varchar	100	Nip
4.	Nomor_handphone	Varchar	100	Nomor handphone
5.	Foto	Varchar	100	foto

5. Tabel pasien

Tabel 4. 10 Tabel pasien

No	Nama Field	Tipe	Ukuran	Keterangan
1.	id_pasien	Int	11	Id pasien
2.	Nama_pasien	Varchar	100	Nama pasien
3.	Kode_pasien	Varchar	100	Kode pasien
4.	Kategori	Varchar	100	Kategori
5.	Umur	Int	50	Umur
6.	Jenis_kelamin	Enum		Jenis kelamin
5.	Nomor_hp	Int	50	Nomor hp

6. Tabel riwayat

Tabel 4. 11 Tabel riwayat

No	Nama Field	Tipe	Ukuran	Keterangan
1.	id_riwayat	Int	11	Id riwayat
2.	Tanggal_berobat	Date		Tanggal berobat
3.	Gejala	Varchar	100	gejala
4.	Obat	Varchar	100	Obat
5.	perawat	varchar	100	Perawat
6.	dokter	Varchar	100	Dokter

e. Rancangan Antarmuka Aplikasi

A Web Page

https://

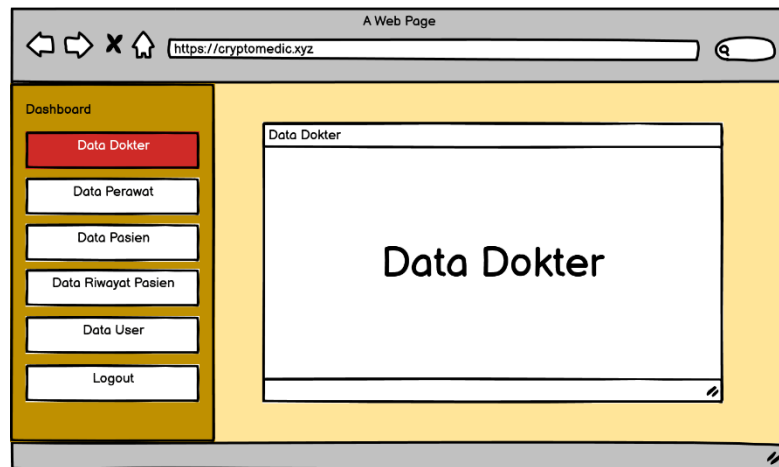
LOGIN

username

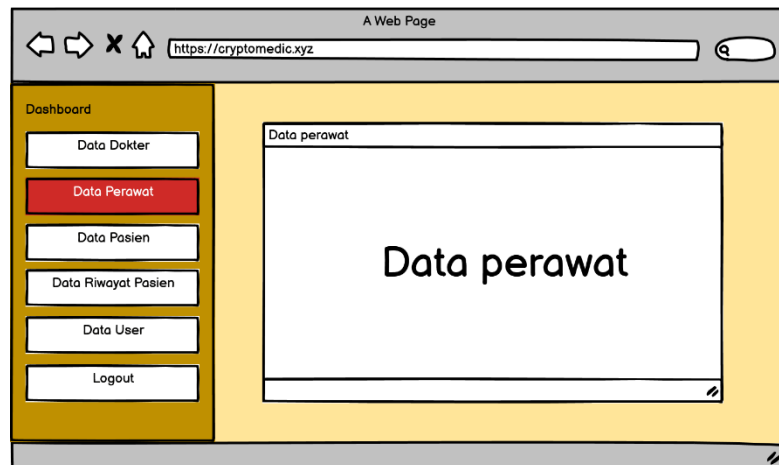
password

MASUK

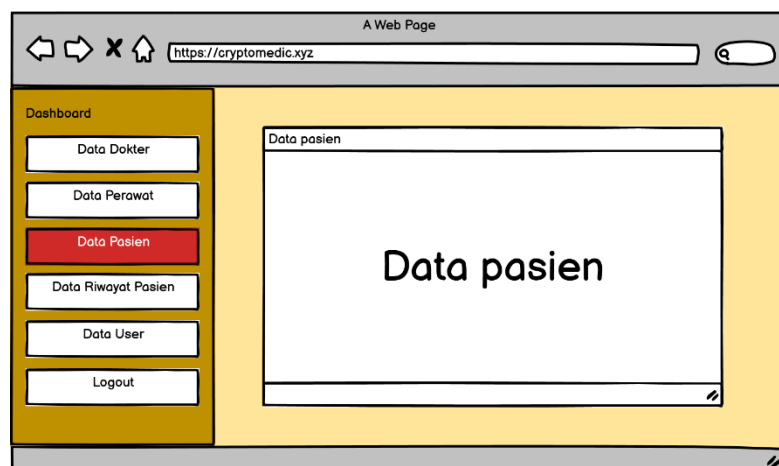
Gambar 4. 11 Halaman login



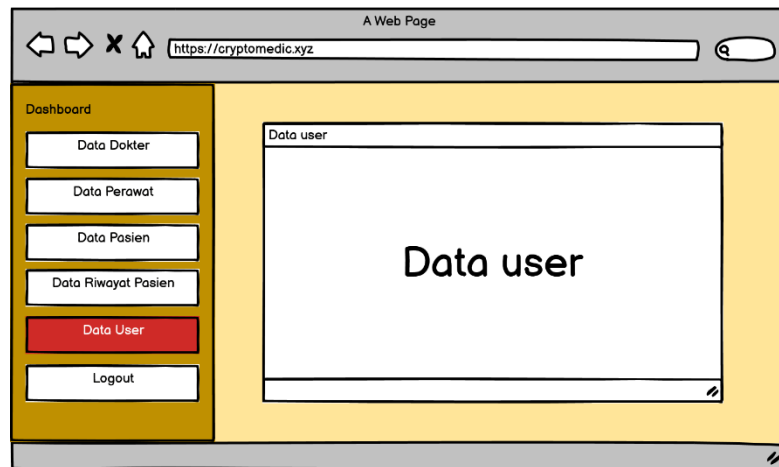
Gambar 4. 12 Halaman data dokter



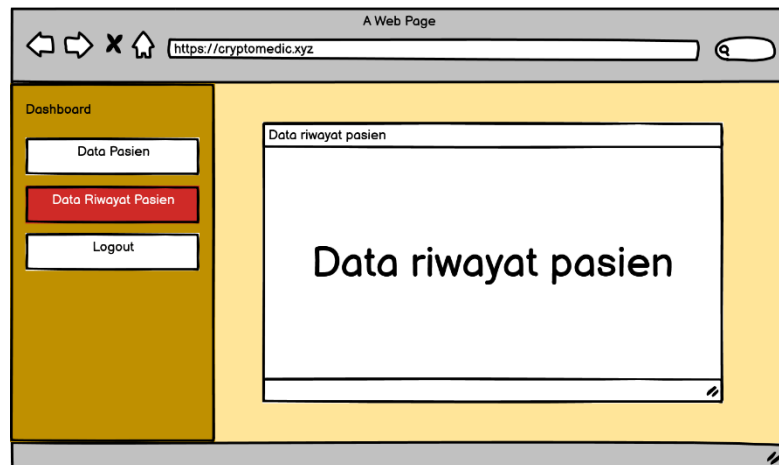
Gambar 4. 13 Halaman data perawat



Gambar 4. 14 Halaman data pasien

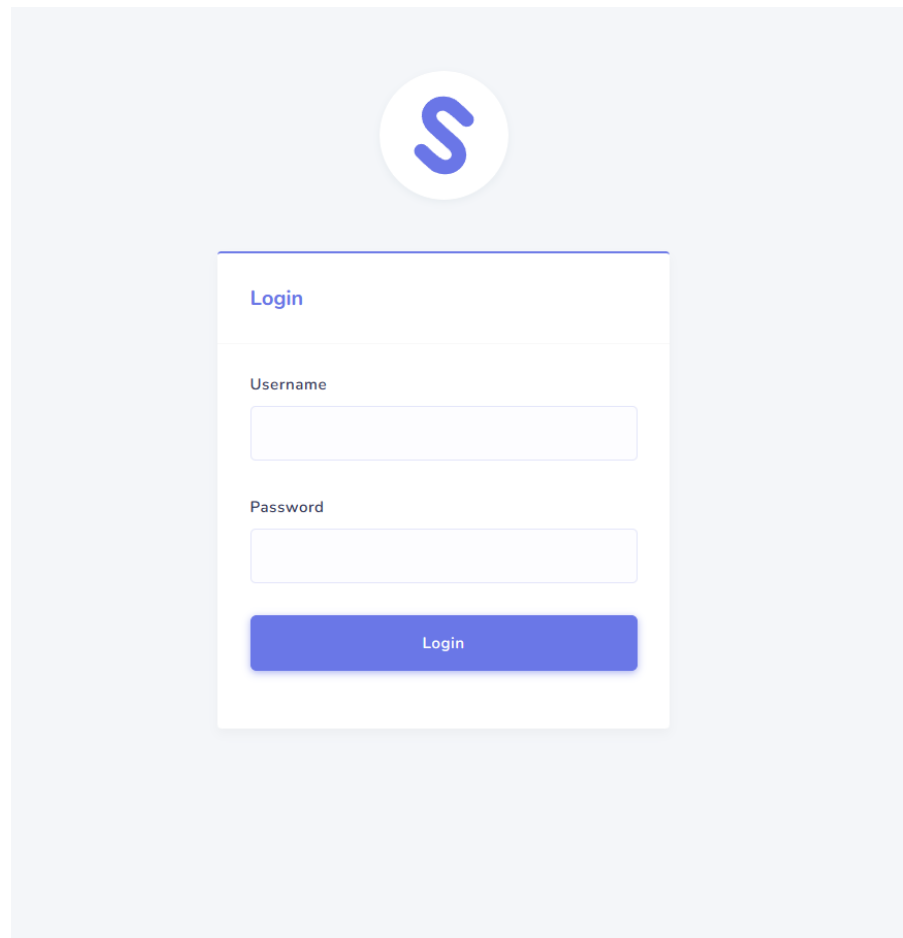


Gambar 4. 15 Halaman user



Gambar 4. 16 Halaman riwayat pasien

f. Implementasi Sistem



The image shows a login interface on a light gray background. At the top center is a circular logo with a blue 'S' on a white background. Below the logo is a white rectangular form with a thin blue border. The form has a title 'Login' in blue text at the top left. Below the title are two input fields: 'Username' and 'Password', each with a light gray border. At the bottom of the form is a blue button with the text 'Login' in white.

Gambar 4. 17 Implementasi sistem (login)

Pada gambar 4.17, untuk melakukan login atau masuk ke sistem diperlukan sebuah username dan password yang dimasukkan terlebih dahulu di form halaman login

KLINIK BOTOLEMPANGANG

Tambah Pasien

Nama Pasien

Ananda

Kode Pasien

P-01

Kategori Pasien

Dewasa

Umur Pasien

22

Jenis Kelamin Pasien

Perempuan

Nomor HP Pasien

082188819900

Simpan Data

DASHBOARD

Dashboard

PAGES

Data Dokter

Data Perawat

Data Pasien

Data Riwayat Pasien

Gambar 4. 18 Implementasi sistem (Tambah data pasien)

Seperti pada gambar 4.18 untuk proses enkripsi dilakukan oleh sistem saat penginputan data seperti pada contoh yaitu penginputan data pasien. Jika button simpat data ditekan maka data yang telah dimasukkan di form akan dienkripsi dengan algoritma RSA atau Elgamal sesuai pilihan, akan di simpan ke dalam database.

Showing rows 0 - 1 (2 total, Query took 0.0007 seconds.)

SELECT * FROM `pasien`

☐ Profiling [[Edit inline](#)] [[Edit](#)] [[Explain SQL](#)] [[Create PHP code](#)] [[Refresh](#)]

☐ Show all | Number of rows: 25 | Filter rows: Search this table | Sort by key: None

Extra options

	id_pasien	nama_pasien	kode_pasien	kategori_pasien	umur_pasien	jkel_pasien	nohp_pasien
<input type="checkbox"/> Edit Copy Delete	12	285 132 14 132 254 14	P-01	217 250 201 14 202 14	271 271	5 250 108 250 208 52 233 14 132	218 166 271 257 166 166 166 257 173 173 218 218
<input type="checkbox"/> Edit Copy Delete	13	4 209 32 148 2 177 2 55 128 57 4 217	P-02	8 137 2 179 8 47 2 177 32 108 2 177	64 57 8 199	2 40 64 110 32 116 2 179 2 183 16 7 8 111 32 252 1...	16 3 2 28 128 157 128 159 32 66 128 145 4 14 128 1...

↑ ☐ Check all With selected: Edit Copy Delete Export

Gambar 4.19 Implementasi sistem (table data pasien)

Pada gambar 4.19 data pasien yang telah diinput sebelumnya akan tersimpan di dalam database dengan bentuk *chipper text*.

DataPasien Dashboard / Pages / DataPasien

Show 10 entries Search:

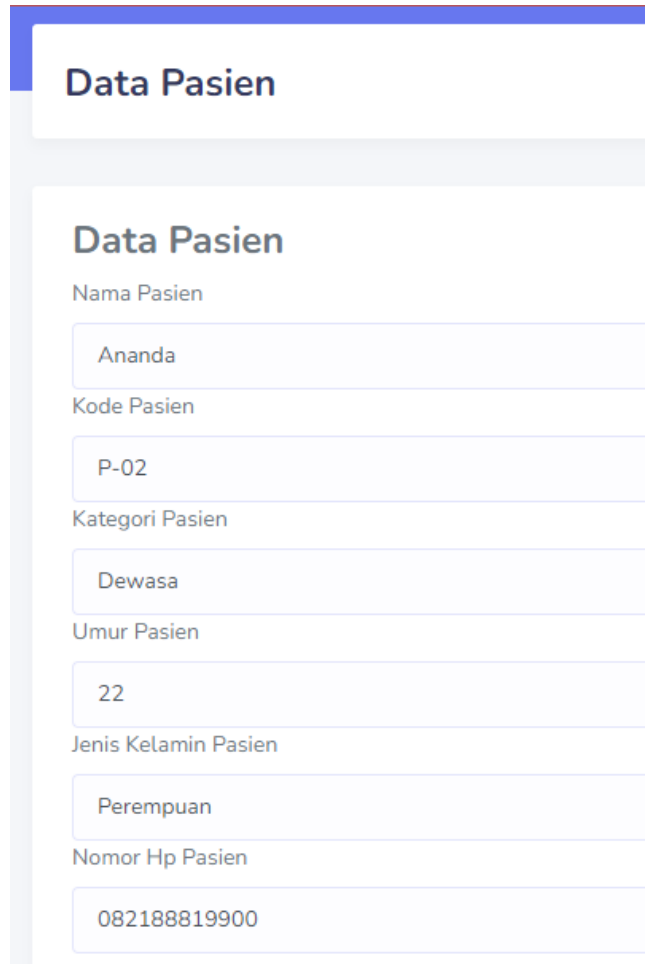
Enkripsi	Kode Pasien	Nama Pasien	Kategori	Umur	Jenis Kelamin	Nomor Hp	Action
RSA	P-01	285 132 14 132 254 14	217 250 201 14 202 14	271 271	5 250 108 250 208 52 233 14 132	218 166 271 257 166 166 166 257 173 173 218 218	<input type="button" value="Edit"/> <input type="button" value="Delete"/> <input type="button" value="Info"/>
ElGamal	P-02	4 209 32 148 2 177 2 55 128 57 4 217	8 137 2 179 8 47 2 177 32 108 2 177	64 57 8 199	2 40 64 110 32 116 2 179 2 183 16 7 8 111 32 252 128 37	16 3 2 28 128 157 128 159 32 66 128 145 4 14 128 159 16 116 32 58 4 12 16 3	<input type="button" value="Edit"/> <input type="button" value="Delete"/> <input type="button" value="Info"/>

Showing 1 to 1 of 1 entries Previous 1 Next

Gambar 4.20 Implementasi sistem (data pasien)

Pada gambar 4.20 pada halaman data pasien. Data yang ditampilkan merupakan hasil enkripsi yang sebelumnya telah tersimpan di database. Di halaman terdapat pilihan untuk melakukan penginputan data menggunakan enkripsi RSA atau Elgamal.

Untuk melakukan dekripsi pada data tersebut dilakukan dengan cara menekan tombol desc.



The image shows a web application interface for patient data. At the top, there is a blue header bar with the text 'Data Pasien' in white. Below this, there is a light gray sidebar with the text 'Data Pasien' in bold. The main content area is white and contains a form with the following fields:

Field Label	Value
Nama Pasien	Ananda
Kode Pasien	P-02
Kategori Pasien	Dewasa
Umur Pasien	22
Jenis Kelamin Pasien	Perempuan
Nomor Hp Pasien	082188819900

Gambar 4. 21 Implementasi sistem (data hasil dekripsi)

Pada gambar 4.21 data yang ditampilkan merupakan hasil dekripsi sebelumnya yang telah dilakukan dengan menekan tombol desc pada halaman tampil data pasien.

4.4 Pengujian Sistem

Pengujian sistem yang dilakukan dengan menggunakan metode pengujian Black Box, dengan menguji fungsionalitas dari aplikasi sistem pengaman rekam medis ini

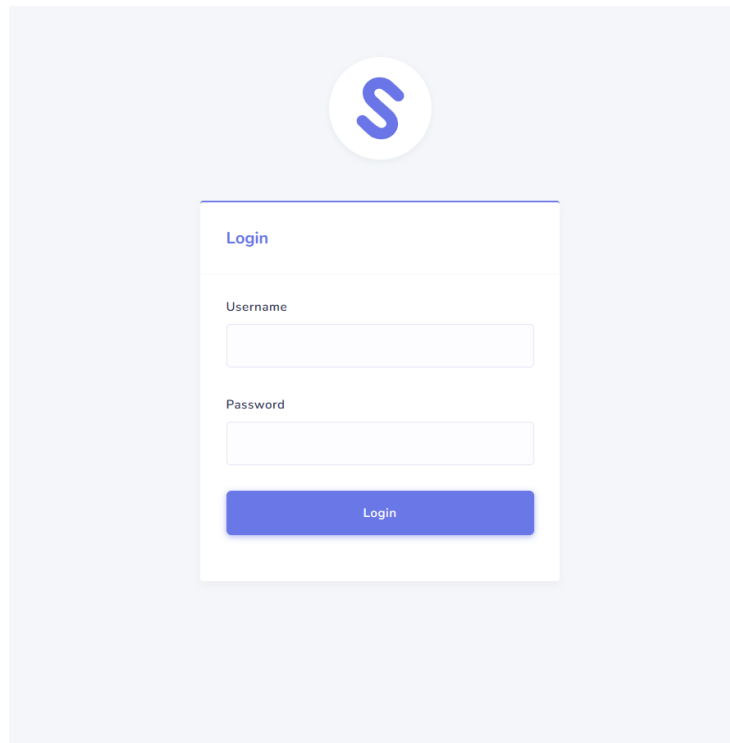
1. Pengujian halaman login admin

Test Factor : Masuk Halaman Login

Hasil : ✓

Keterangan : Admin dapat mengakses halaman *login* dan dapat masuk kehalaman admin dengan cara *login* terlebih dahulu.

Scrennshoot :



Gambar 4. 22 Pengujian halaman login

2. Pengujian Halaman Data Pasien

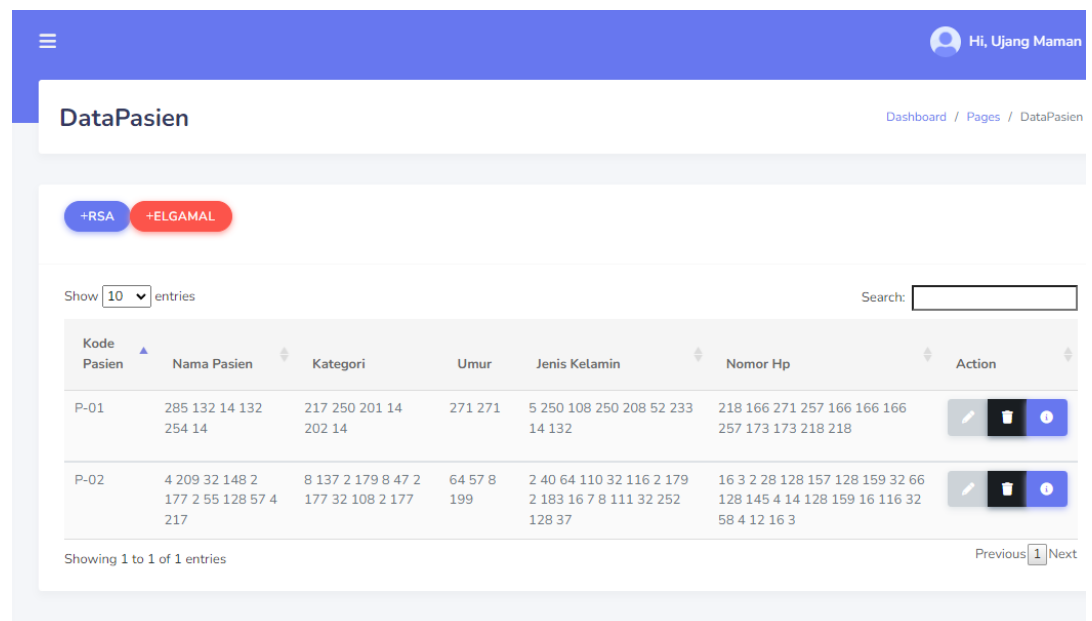
Test Factor : Masuk Halaman Data Pasien

Hasil : ✓

Keterangan : Admin berhasil mengakses halaman data pasien
serta dapat menambah, edit, dan hapus data.

Serta melakukan dekripsi data

Scrennshoot :



Gambar 4. 23 Pengujian halaman data pasien

3. Pengujian halaman tambah data pasien

Test Factor : Masuk Halaman Tambah Pasien

Hasil : ✓

Keterangan : Admin berhasil mengakses halaman tambah data pasien serta dapat menambah data.

Scrennshoot :

The screenshot shows a web application interface for a clinic. On the left is a sidebar menu for 'KLINIK BOTOLEMPANG' with options: Dashboard, Data Dokter, Data Perawat, Data Pasien, and Data Riwayat Pasien. The main area is titled 'Tambah Pasien' and contains the following form fields:

- Nama Pasien:** Ananda
- Kode Pasien:** P-01
- Kategori Pasien:** Dewasa
- Umur Pasien:** 22
- Jenis Kelamin Pasien:** Perempuan
- Nomor HP Pasien:** 082188819900

A blue button labeled 'Simpan Data' is located at the bottom of the form.

Gambar 4. 24 Pengujian halaman tambah data pasien

4. Pengujian halaman dekripsi data pasien

Test Factor : Masuk Halaman deksripsi data pasien

Hasil : ✓

Keterangan : Admin berhasil mengakses halaman data pasien serta dapat mendekripsi data pasien.

Scrennshoot :

The screenshot shows a web application interface for 'KLINIK BOTOLEMPANG'. On the left is a sidebar menu with the following items: 'Dashboard', 'Data Dokter', 'Data Perawat', 'Data Pasien', and 'Data Riwayat Pasien'. The main content area is titled 'Data Pasien' and contains a form with the following fields and values:

Field	Value
Nama Pasien	Ananda
Kode Pasien	P-02
Kategori Pasien	Dewasa
Umur Pasien	22
Jenis Kelamin Pasien	Perempuan
Nomor Hp Pasien	082188819900

Gambar 4. 25 Pengujian halaman dekripsi data pasien

BAB V

KESIMPULAN DAN SARAN

5.1 Kesimpulan

Dari analisis yang telah dilakukan terhadap kekuatan algoritma RSA dan ElGamal dalam pengamanan data rekam medis melalui pendekatan kriptanalisis, dapat disimpulkan bahwa algoritma-algoritma ini mampu melindungi data seperti data rekam medis. Untuk skala data rekam medis yang jumlahnya tidak terlalu banyak seperti pada klinik, algoritma RSA lebih direkomendasikan untuk mengurangi pemborosan penyimpanan data karena hasil pengamanan data dengan algoritma RSA lebih sedikit menggunakan penyimpanan data. Sedangkan untuk data rekam medis yang memiliki skala jumlah yang banyak seperti pada rumah sakit, algoritma ElGamal lebih direkomendasikan karena sudah semestinya sebuah rumah sakit memiliki pengamanan data rekam medis yang layak dan lebih aman.

5.2 Saran

Adapun saran-saran yang diberikan pada penelitian ini adalah :

1. Penambahan fitur pada pengamanan data seperti dapat mengamankan bukan hanya data berupa teks saja tetapi bisa mengamankan data berupa gambar atau bentuk media lainnya.
2. Aplikasi ini dapat dikembangkan lebih lanjut agar dapat memenuhi kebutuhan dimasa yang akan datang seperti pengembangan pada sistem berbasis mobile.

DAFTAR PUSTAKA

- Abdillah, L. A. et al. (2020) Aplikasi Teknologi Informasi: Konsep dan Penerapannya. Medan: Yayasan Kita Menulis
- Edi Rahmansyah (2019). Implementasi algoritma elgamal dengan pembangkit bilangan prima lehmann dan algoritma least significant bit (LSB) dengan cover image bitmap untuk keamanan data text. Jurnal Riset Komputer.
- Munir R (2019). Kriptografi.
- Nur Rochmat, R.Rizal Isnanto, and Maman Somantri (2012). Implementasi Algoritma Kriptografi Elgamal untuk keamanan pesan (*Message Security*). Jurusan Teknik Elektro, Universitas Diponegoro Semarang.
- Putratama, S. V. (2016). *Programmer Web dengan Menggunakan PHP dan Framework*. Yogyakarta: CV. Budi Utama.
- Reikha Rahmadhayanti, (2017). Perancangan Sistem Informasi Sales Report Pada PT Laboratorium Medio Pratama Tangerang.
- Siahaan V, Sianipar R, (2018). JavaScript: Dari A Sampai Z.
- Sianturi C. (2020). Modifikasi Pembangkit Kunci Algoritma RSA Dengan Menerapkan Algoritma Blum Blum Shub (BBS).
- Sutejo S. (2021). Implementasi Algoritma Kriptografi Rsa (Rivest Shamir Adleman) Untuk Keamanan Data Rekam Medis Pasien.
- Susilawati S (2018). Perancangan Kunci Public RSA dan ElGamal pada Kriptografi untuk Keamanan Informasi.
- Tampubolon A. (2021). Implementasi Kombinasi Algoritma RSA dan Algoritma DES Pada Aplikasi Pengaman Pesan Teks. Jurnal SAINTIKOM (Jurnal Sains Manajemen Informatika dan Komputer).