**RANCANG BANGUN SISTEM PENGAMANAN DATA REKAM MEDIS MENGGUNAKAN ALGORITMA RSA BERBASIS *WEB* (STUDI KASUS: RSUD ANUTAPURA KOTA PALU)**

****

**PROPOSAL SKRIPSI**

Diajukan untuk memenuhi sebagian persyaratan memperoleh gelar

Sarjana Komputer pada Program Studi Teknik Informatika

Jurusan Teknologi Informasi Fakultas Teknik Universitas Tadulako

Disusun oleh:

**RINI WULANSARI**

**F 551 13 077**

**PROGRAM STUDI TEKNIK INFORMATIKA**

**JURUSAN TEKNOLOGI INFORMASI**

**FAKULTAS TEKNIK**

**UNIVERSITAS TADULAKO**

**PALU**

**2019**

# **LEMBAR PERSETUJUAN PEMBIMBING**

Nama Mahasiswa : Rini Wulansari

No. Stambuk : F 551 13 077

Konsentrasi : Sistem Cerdas

Judul : **RANCANG BANGUN SISTEM PENGAMANAN DATA REKAM MEDIS MENGGUNAKAN ALGORITMA RSA BERBASIS *WEB* (STUDI KASUS: RSUD ANUTAPURA KOTA PALU)**

Jumlah SKS : 139 IPK : 3,21

Mata Kuliah Pendukung Skripsi (minimal 4 mata kuliah) :

|  |  |  |  |
| --- | --- | --- | --- |
| No. | Kode Mata Kuliah | Nama Mata Kuliah | Nilai |
| 1  2  3  4  5 | F09171015  F09171018  F09171017  F09171020  F09171031 | Sistem Informasi  Kriptografi  Perancangan dan Analisis Algoritma II  Pemrograman Web II  Metode Penelitian | B  B  A  B  B |

Pembimbing 1 : Dr. Anita Ahmad Kasim, S.Kom., M.Cs.

Pembimbing 2 : Yusuf Anshori, S.T., M.T.

Menyetujui untuk : Seminar Proposal/Seminar Hasil/Ujian Skripsi \*)

Palu, ............................... 2019

Pembimbing 1 Pembimbing 2

**Dr. Anita Ahmad Kasim, S.Kom., M.Cs. Yusuf Anshori, S.T., M.T.**

**NIP. 19790112 200501 2 002 NIP. 19801027 2006004 1 001**

Mengetahui,

Ketua Program Studi S1 Teknik Informatika,

**Yusuf Anshori, S.T., M.T.**

**NIP. 19801027 2006004 1 001**

# **halaman peRSETUJUAN**

**PROPOSAL SKRIPSI**

**RANCANG BANGUN SISTEM PENGAMANAN DATA REKAM MEDIS MENGGUNAKAN ALGORITMA RSA BERBASIS *WEB*  (STUDI KASUS: RSUD ANUTAPURA KOTA PALU)**

Yang diajukan oleh:

**Rini Wulansari**

**F 551 13 077**

Palu, 2019

Telah disetujui oleh:

Pembimbing I Pembimbing II

**Dr. Anita Ahmad Kasim, S.Kom., M.Cs. Yusuf Anshori, S.T., M.T.**

**NIP. 19790112 200501 2 002 NIP. 19801027 200604 1 001**

Mengetahui :

Ketua Program Studi Teknik Informatika,

**Yusuf Anshori, S.T., M.T.**

**NIP. 19801027 200604 1 001**

# **KATA PENGANTAR**

Puji dan syukur, serta hormat kemuliaan dipanjatkan kehadirat Tuhan Yang Maha Kuasa, karena atas ridho-Nya serta anugerah-Nya penulis dapat menyelesaikan Skripsi yang berjudul **“Klasifikasi Penyakit Tumor Payudara Menggunakan Algoritma Naive Bayes (Studi Kasus: Rumah Sakit Di Kota Palu)”** sebagai syaratutama untuk mendapatkan gelar S1 dari Program Studi Teknik Informatika, Jurusan Teknologi Informasi, Fakultas Teknik, Universitas Tadulako.

Skripsi ini dapat diselesaikan karena bantuan dan dorongan dari berbagai pihak. Untuk itu pada kesempatan ini penulis mengucapkan terima kasih kepada:

1. Bapak Dr. Eng. Ir. Andi Rusdin, S.T., M.T., Msc. selaku Dekan Fakultas Teknik, Universitas Tadulako.
2. Bapak Dr. Eng. Ir. Andi Rusdin, S.T., M.T., Msc. selaku Wakil Dekan I Fakultas Teknik.
3. Bapak Yusuf Anshori, S.T.,M.T., selaku Koordinator Program Studi Teknik Informatika dan Ketua Jurusan Teknologi Informasi, Fakultas Teknik, Universitas Tadulako.
4. Ibu Dessy Santi, S.Kom., M.Kom. sebagai Ketua KDK Sistem Cerdas pada Program Studi Teknik Informatika, Jurusan Teknologi Informasi, Fakultas Teknik, Universitas Tadulako
5. Ibu Dr. Anita Ahmad Kasim, S.Kom., M.Cs., selaku pembimbing I dan Bapak Yusuf Anshori, S.T., M.T. selaku pembimbing II penulis atas arahan serta nasehat-nasehat yang sangat membantu penulis dari awal hingga akhir penyusunan skripsi ini.
6. Seluruh staf pengajar (Dosen) dalam lingkungan Fakultas Teknik Universitas Tadulako, khususnya dalam lingkup Program Studi Teknik Informatika.
7. Kedua Orang Tuaku tercinta Bapak Azis dan Ibu Zamriah, S.Pd. Serta Saudaraku Dedi Supriadi, S.Si., Hari Gunawan S.Hut., Syaiful, Annisa, Moh. Rizki, dan Nur Zahira Putri serta semua Keluarga yang senantiasa mendukung, mendoakan serta memberikan motivasi untuk tetap berjuang.
8. Teman seperjuangan, “SC Only” Astuti, Rahmatanti, S.Kom, Raziyan Dwi Pathan, S.Kom, Munifa, Norma, Anjani, Nur Aisyah, Jahria dan semua 2013 yang telah bersama berjuang dan saling memberi semangat dalam perkuliahan.
9. Seseorang terkasih, Egi Priyatman yang telah menemani dan membantu penulis menyelesaikan skripsi.
10. Seluruh pihak baik secara langsung maupun tidak, Tuhan akan memberkati.

Penelitian berharap kritik dan saran yang membangun dari semua pihak agar skripsi ini dapat dimanfaatkan bagi masyarakat luas.

|  |  |
| --- | --- |
|  | Palu, Desember 2019  Penulis  **Rini Wulansari** |

# **DAFTAR ISI**

Halaman

HALAMAN JUDUL i

LEMBAR PERSETUJUAN PEMBIMBING ii

HALAMAN PERSETUJUAN iii

KATA PENGANTAR iv

DAFTAR ISI vi

DAFTAR GAMBAR viii

DAFTAR TABEL ix

DAFTAR ARTI SIMBOL DAN SINGKATAN x

BAB I PENDAHULUAN

1.1. Latar Belakang 1

1.2. Rumusan Masalah 3

1.3. Batasan Masalah 4

1.4. Tujuan Penelitian 4

1.5. Manfaat Penelitian 4

1.6. Sistematika Penulisan 5

BAB II TINJAUAN PUSTAKA DAN LANDASAN TEORI

2.1. Tinjauan Pustaka 6

2.2. Landasan Teori 9

2.2.1. Pengertian Sistem 9

2.2.2. Keamanan Data 14

2.2.3. Pengertian Rekam Medis 21

2.2.4. Pengertian Kriptografi 23

2.2.1.1. Kriptografi Simetrik 12

2.2.1.2 Kriptografi Asimetrik 13

2.2.5. Algoritma RSA 23

2.2.2.1. Besaran-besaran pada algoritma RSA 14

2.2.2.2. Proses Pembangkitan Kunci 15

2.2.2.3. Proses Enkripsi 19

2.2.2.4. Proses Dekripsi 20

2.2.10. Kode ASCII 27

2.2.10. Pengertian *Web* 27

BAB III METODE PENELITIAN

3.1. Bahan dan Alat Penelitian 30

3.1.1 Bahan Penelitian 30

3.1.2 Alat Penelitian 30

3.2. Desain Penelitian 31

3.2.1 Jenis Penelitian 31

3.2.2 Tipe Penelitian 31

3.3. Objek, Waktu dan Lokasi Penelitian 31

3.4. Jenis dan Sumber Data 32

3.4.1. Data Primer 32

3.4.2. Data Sekunder 32

3.5. Teknik Pengumpulan data 32

3.5.1 Observasi 33

3.5.1 Wawancara 33

3.5.1 Studi Literatur 33

3.6 Metode Analisis Data 33

3.7 Metode Pengembangan Sistem 34

3.8 Tahapan Diagram Alir Penelitian 36

DAFTAR PUSTAKA 48

**DAFTAR GAMBAR**

No. Gambar Halaman

2.1. Skema Enkripsi dan Dekripsi 11

2.2. Kriptografi Simetris 12

2.3. Kriptografi Asimetris 13

3.1. Model *Waterfall* 34

3.2. *Flowchart* Tahapan Penelitian 36

3.3.Form Input Login 39

3.4. Form Input Data Dokter 40

3.5. Form Input Data Pasien 40

3.6. Form Input Data Rawat Inap Pasien 41

3.7. Tabel Data Dokter 41

3.8. Tabel Data Pasien 42

3.9. Tabel Akun 42

3.10. Tabel Rekam Medis 42

3.11. Tabel RSA 43

3.12. Proses Pembangkit Kunci Algoritma RSA 44

3.13. Proses Enkripsi Algoritma RSA 45

3.14. Proses Dekripsi Algoritma RSA 46

# **DAFTAR TABEL**

No. Tabel Halaman

2.1. Kode ASCII………. 28

# **DAFTAR ARTI SIMBOL DAN SINGKATAN**

**Daftar Arti Simbol**

|  |  |  |
| --- | --- | --- |
| **No.** | **Simbol** | **Arti Simbol** |
| 1. |  | Terminal *point* simbol merupakan simbol *flowchart* berfungsi sebagai permulaan (*start*) atau akhir (*stop*) dari suatu kegiatan. |
| 2. |  | *Processing* Simbol merupakan simbol *flowchart* berfungsi untuk menunjukkan pengolahan yang dilakukan oleh komputer/pc. |
| 3. |  | Keterangan Simbol *Decision* adalah simbol berfungsi untuk memilih proses berdasarkan kondisi yang ada. |
| 4. |  | Simbol input/output menunjukkan proses input-output yang terjadi tanpa bergantung dari jenis peralatannya. |
| 5. |  | Merupakan simbol *flowchart* berfungsi untuk menghubungkan antara simbol satu dengan simbol yang lain atau menyatakan jalannya arus dalam suatu proses. Simbol arus ini sering disebut juga dengan *connecting* *line*. |

**Daftar Singkatan**

|  |  |  |
| --- | --- | --- |
| **No.** | **Singkatan** | **Kepanjangan Singkatan** |
| 1. | TI | Teknologi Informasi |
| 2. | RSA | *Rivest Shamir Adleman* |
| 3. | RM | Rekam Medis |
| 4. | *Dkk* | Dan kawan-kawan |
| 5. | *DES* | *Data Encryption Standart* |
| 6. | MIT | *Massachussets Institute of Technology* |
| 7. | *RSA* | *Rivest Shamir Adleman* |
| 8. | *ASCII* | *American Standard Code for Information Interchange* |
| 9. | *PHP* | *Perl Hypertext Preprocessor* |
| 10. | *MySQL* | *My Structured Query Language* |
| 11. | *OS* | *Operating System* |
| 12. | *UML* | *Unified Modelling Language* |
| 13. | *DFD* | *Data Flow Diagram* |
| 14. | *ERD* | *Entity Relationship Diagram* |

# **BAB I**

**PENDAHULUAN**

* 1. **Latar Belakang**

Masalah keamanan data merupakan salah satu aspek penting dari sebuah sistem informasi yang akan di bangun. Sehingga perlu di perhatikan oleh para pemilik dan pengelola sistem informasi tersebut. Keamanan data merupakan salah satu masalah yang dianggap penting dan harus dicari pemecahan masalahnya. Keamanan yang sangat penting dijaga yaitu keamanan *database* dari sistem informasi tersebut. *Database* adalah sekumpulan data atau informasi yang disimpan di dalam komputer secara sistematik yang dapat digunakan melalui sebuah aplikasi komputer tertentu untuk menjalankannya. Keamanan database dapat dilakukan dengan berbagai cara, dimulai dari pembatasan hak akses user terhadap data yang ada pada database itu sendiri, penggunaan nama field yang hanya dimengerti oleh administrator sehingga tidak semua user yang diberi izin mengakses database mengerti alur database yang ada guna menghindari pencurian data, manipulasi data, perusakan data dan lainnya, maka dari itu digunakanlah metode *kriftografi* sebagai metode pengamanan pada aplikasi terhadap *field* data di dalam *database*nya dengan tujuan *field* data yang disimpan menjadi lebih terjamin privasinya dan tidak dapat dimengerti oleh pihak luar maupun pihak dalam. Salah satu masalah keamanan data yang kurang mendapat perhatian adalah keamanan data pada aplikasi rekam medis pasien.

Rekam medis merupakan sebuah rekaman kesehatan yang memuat kumpulan data-data penting berkaitan dengan identitas, hasil anamnesis, hasil pemeriksaan fisik dan catatan segala kegiatan para tenaga kesehatan terhadap pasien yang telah diperiksa dan mendapat pelayanan kesehatan di rumah sakit tersebut.

RSUD Anutapura Kota Palu merupakan instansi kesehatan yang telah menyelenggarakan layanan kesehatan kepada setiap pasien. Setiap pasien yang datang dan melakukan pemeriksaan kepada tenaga medis akan memiliki data rekam medis. Yang dimana dalam data rekam medis tersebut terdapat data pasien maupun hasil diagnosa pasien. Data tersebut disimpan dalam sebuah sistem informasi rekam medis. Data rekam medis pasien merupakan data yang bersifat sangat rahasia, hanya pasien, tenaga medis dan staff rekam medis yang dapat mengetahui isi dari rekam medis pasien tersebut. Namun system informasi tersebut masih memiliki kekurangan, yaitu dalam system keamanan. Keamanan dalam sistem informasi rekam medis masih kurang mendapat perhatian dari pengelola sistem informasi tersebut. Sehingga sewaktu-waktu data tersebut bisa saja mengalami pencurian data, manipulasi data dan kebocoran data sehingga merugikan banyak pihak yaitu pasien dan pihak rumah sakit.

Berdasarkan uraian latar belakang di atas, maka penulis berencana membangun suatu penelitian dengan judul **“Rancang Bangun Sistem Pengamanan Data Rekam Medis Menggunakan Algoritma RSA Berbasis *Web* (Studi Kasus: RSUD Anutapura Kota Palu)”**.

* 1. **Rumusan Masalah**

Rumusan masalah dalam penelitian ini adalah bagaimana membangun sebuah sistem pengamanan data rekam medis menggunakan algoritma RSA pada Rumah Sakit umum daerah (RSUD) Anutapura Kota Palu?

* 1. **Batasan Masalah**

Penelitian ini diharapkan terfokus pada pokok permasahannya, sehingga penulis membatasi topik permasalahan yang akan dilakukan, adapun batasan permasalahan pada penelitian ini adalah:

1. Algoritma yang digunakan adalah algoritma RSA (*Rivest-Shamir-Adleman*).
2. Untuk tujuan kode etik, maka identitas/nama pasien dari data disamarkan.
3. Data yang dienkripsi dan didekripsi yaitu nama pasien dan diagnosa pasien*.*
4. Data rekam medis yang akan digunakan diperoleh dari Rumah Sakit Umum daerah (RSUD) Anutapura Kota Palu.
   1. **Tujuan Penelitian**

Tujuan penelitian ini adalah membangun sebuah sistem pengamanan data rekam medis menggunakan algoritma RSA berbasis *Web* dengan Studi Kasus RSUD Anutapura Kota Palu.

* 1. **Manfaat Penelitian**

Manfaat yang diharapkan dengan adanya penelitian ini yaitu:

* 1. Manfaat Akademik

1. Bagi penulis dapat menambah pengetahuan dan wawasan tentang kriptografi khususnya teknik enkripsi dan deskripsi dalam pengamanan data rekam medismenggunakan algoritma RSA (*Rivest Shamir Adleman*)*.*
2. Bagi peneliti lain dapat dijadikan sebagai bahan referensi dan acuan terhadap pengembangan ataupun pembuatan penelitian yang memiliki topik yang sama dengan penelitian ini.
   1. Manfaat Praktis

Hasil penelitian ini dapat dimanfaatkan oleh pihak Rumah Sakit Anutapura Kota Palu untuk mengamankan data rekam medis, agar data yang diamankan tidak bisa diakses oleh pihak-pihak yang tidak berwenang.

* 1. **Sistematika Penulisan**

Adapun sistematika penulisan pada penelitian ini adalah sebagai berikut:

BAB I: PENDAHULUAN

Bab ini terdiri dari latar belakang, rumusan masalah, batasan masalah, tujuan penelitian, manfaat penelitian, dan sistematika penulisan.

BAB II: TINJAUAN PUSTAKA DAN LANDASAN TEORI

Bab ini menjelaskan tentang perbandingan antara penelitian ini dengan penelitian lain yang pernah ada sebelumnya serta teori-teori yang digunakan dalam menyusun proposal ini.

BAB III: METODE PENELITIAN

Bab ini menjelaskan tentang bahan dan alat yang akan digunakan dalam penelitian, tahapan penelitian, dan hipotesis yang dibuat berdasarkan teori dasar serta rumusan masalah yang ada.

BAB IV: HASIL DAN PEMBAHASAN

Bab ini menjelaskan tentang hasil dari penelitian dan perancangan yang telah dilakukan selama beberapa bulan.

BAB V: KESIMPULAN DAN SARAN

Bab ini berisi kesimpulan yang diambil berdasarkan analisa yang telah dilakukan serta saran-saran yang bermanfaat bagi penelitian-penelitian yang akan dilakukan di kemudian hari.

DAFTAR PUSTAKA

Pada bagian ini berisi tentang referensi yang dijadikan rujukan dalam melakukan penelitian.

# **BAB II**

**TINJAUAN PUSTAKA DAN LANDASAN TEORI**

* 1. **Tinjauan Pustaka**

Penulis meninjau penelitian ini berdasarkan dari hasil-hasil penelitian yang dilakukan sebelumnya yang pernah dilakukan. Adapun penelitian-penelitian yang terkait adalah sebagai berikut.

1. Pahrizal dan Pratama (2016), dalam penelitiannya Implementasi Algoritma RSA Untuk Pengamanan Data Berbentuk Teks. Tujuan penelitian ini adalah untuk menerapkan keamanan *file* menggunakan algoritma RSA. Kesimpulan dari penelitian Pahrizal dan Pratama yaitu aplikasi pengamanan mempunyai kalimat sandi yang harus diingat dan bersifat sensitif, maksudnya huruf besar dan kecil dibedakan, agar sandi sulit ditebak oleh siapapun. Setelah melakukan uji coba, *file* yang telah diterapkan aplikasi pengamanan akan memiliki empat aspek keamanan, yaitu kerahasiaan, integritas data, otentikasi, dan nirpenyangkalan. Persamaan penelitian Pahrizal dan Pratama dengan penelitian yang dilakukan oleh penulis yaitu menerapkan algoritma RSA, namun perbedaan dari penelitian ini penulis menggunakan algoritma RSA untuk mengamankan pengaksessan pemakaian sistem, dan juga menjaga kerahasiaan rekam medis pasien.
2. Diarse dan Bendi (2016), dalam penelitiannya Penerapan Algoritma RSA Pada Sistem Kriptografi File Audio Mp3. Tujuan penelitian Diarse dan Bendi adalah untuk menerapkan algoritma RSA pada audio mp3. Sehingga *audio* tersebut dapat di enkripsi/dekripsi dan orang yang dapat mendengarkan *audio* tersebut adalah orang yang mengirimkan *audio* dan orang yang mengetahui kunci tersebut. Kesimpulan dari penelitian Diarse dan Bendi yaitu dari hasil pembangunan aplikasi sistem kriptografi untuk mengamankan *file audio* Mp3 dengan penerapan algoritma RSA, maka dapat disimpulkan bahwa algoritma RSA dapat diterapkan untuk proses enkripsi dan dekripsi *file audio* Mp3 pada aplikasi sistem kriptografi. Persamaan penelitian Diarse dan Bendi dengan penelitian yang dilakukan oleh penulis yaitu menerapkan algoritma RSA, namun perbedaan dari penelitian ini penulis menggunakan algoritma RSA untuk mengamankan pengaksesan pemakaian sistem, dan juga menjaga kerahasiaan rekam medis pasien. Sedangkan pada penelitian sebelumnya algoritma RSA digunakan untuk meng-enkripsi dan dekripsi *file audio*.
3. Martono (2017), dalam penelitiannya Model Modifikasi Kriptografi Algoritma RSA Untuk Keamanan Data Pada Database E-Voting. Tujuan penelitian Martono adalah untuk menjaga dan meningkatkan keamanan serta kerahasiaan data pada database e-voting menggunakan algoritma RSA. Agar data tersebut tidak lagi mudah dibobol oleh orang yang tidak bertanggung jawab sehingga tidak merugikan pihak pemilik data. Kesimpulan dari penelitian Martono yaitu pengamanan data dalam database sangatlah dibutuhkan agar data tersebut tidak jatuh ke tangan orang yang tidak berhak atas data terebut, sehingga menggunakan algoritma RSA sebagai Teknik enkripsi dekripsi suatu record yang ada dalam database. Dimana algoritma RSA menggunakan kunci yang berbeda saat melakukan enkripsi dan dekripsi. Kunci untuk proses enkripsi menggunakan kunci publik (*public* key), sedangkan kunci untuk proses dekripsi menggunakan kunci pribadi (*private* key). Kunci public bersifat tidak rahasia sehingga dan boleh diketahui oleh orang lain, sedangkan kunci pribadi bersifat rahasia dan tidak boleh diketahui oleh orang lain. Kekuatan algoritma RSA terletak pada sulitnya memfaktorkan bilangan besar menjadi faktor-faktor bilangan primanya. Persamaan penelitian Martono dengan penelitian yang dilakukan oleh penulis yaitu menerapkan algoritma RSA sebagai Teknik enkripsi dan dekripsinya dan juga mengamankan database, namun perbedaan dari penelitian ini penulis menggunakan algoritma RSA untuk mengamankan database rekam medis pasien sedangkan Penelitian Martono mengamankan database E-Voting.
   1. **Landasan Teori**
      1. **Definisi Sistem**

Hutahaean (2014), Pengertian sistem menurut para ahli:

1. Pengertian sistem menurut Fat adalah suatu himpunan suatu “benda” nyata atau abstrak (*a set of thing*) yang terdiri dari bagian-bagian atau kompononen-komponen yang saling berkaitan, berhubungan, berketergantungan, saling mendukung, yang secara keseluruhan bersatu dalam satu kesatuan (*unity*) untuk mencapai tujuan tertentu secara efisien dan efektif.
2. Pengertian sistem menurut Indrajit adalah kumpulan-kumpulan dari komponen-komponen yang dimiliki unsur keterkaitan antara satu dengan lainnya.
3. Pengertian sistem menurut Jogianto adalah kumpulan dari elemen-elemen yang berinteraksi untuk mencapai suatu tujuan tertentu. Sistem ini menggambarkan suatu kejadian-kejadian dan kesatuan yang nyata adalah suatu objek nyata, seperti tempat, benda, dan orang-orang yang betul-betul ada dan terjadi.
4. Pengertian sistem menurut Murdick, R.G. adalah seperangkat elemen yang membentuk kumpulan atau bagan-bagan pengolahan yang mencari suatu tujuan tertentu.
5. Pengertian sistem menurut Jerry Futz Gerald adalah suatu jaringan kerja dari prosedur-prosedur yang saling berhubungan, berkumpul bersama-sama untuk melakukan suatu kegiatan atau untuk menyelesaikan suatu sasaran yang tertentu.
6. Pengertian sistem menurut Davis, G.B. adalah kumpulan dari elemen-elemen yang beroperasi bersama-sama untuk menyelesaikan suatu sasaran.
7. Pengertian sistem menurut Dr. Ir. Harijono Djojodiharjo adalah sekumpulan objek yang mencakup hubungan fungsional antara tiap-tiap objek dan hubungan antara ciri tiap objek dan yang secara keseluruhan merupakan suatu kesatuan secara fungsional.
8. Pengertian sistem menurut Lani Sidharta adalah himpunan dari bagian-bagian yang saling berhubungan yang secara bersama mencapai tujuan-tujuan yang sama.

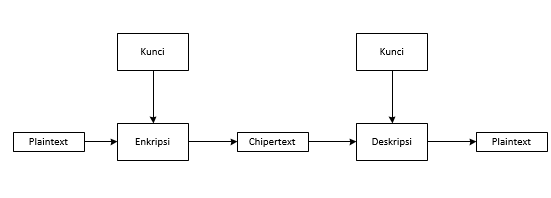
Dengan demikian sistem adalah suatu jaringan kerja dari prosedur-prosedur yang saling berhubungan, berkumpul Bersama-sama untuk melakukan kegiatan atau melakukan sasaran yang tertentu. Pendekatan sistem yang merupakan jaringan kerja dari prosedur lebih menekankan urutan-urutan operasi di dalam sistem.

* 1. Keamanan Data
     1. **Rekam medis**

Rizki (2018), Rekam medis adalah berkas yang berisi catatan dan dokumen tentang identitas pasien, pemeriksaan, pengobatan, tindakan dan pelayanan kesehatan. Secara sederhana rekam medis merupakan berkas yang berisikan catatan dan dokumen tentang pasien yang berisikan tentang identitas seorang pasien, pemeriksaan, pengobatan, tindakan medis pada sarana pelayanan kesehatan rawat jalan, rawat inap baik dikelola pemerintah maupun swasta.

* + 1. **Pengertian Kriptografi**

Kriptografi adalah ilmu dan seni untuk menjaga kerahasiaan pesan dengan cara menyandikannya ke dalam bentuk yang tidak dapat dimengerti lagi maknanya. Dalam ilmu kriptografi, terdapat dua buah proses yaitu melakukan enkripsi dan dekripsi. Pesan yang akan dienkripsi disebut sebagai *plaintext* (teks biasa). Disebut demikian karena informasi ini dengan mudah dapat dibaca dan dipahami oleh siapa saja. Algoritma yang dipakai untuk mengenkripsi dan mendekripsi sebuah *plaintext* melibatkan penggunaan suatu bentuk kunci. Pesan *plaintext* yang telah dienkripsi (atau dikodekan) dikenal sebagai *ciphertext* (teks sandi). Di dalam kriptografi kita akan sering menemukan berbagai istilah atau terminology. Beberapa istilah yang harus diketahui yaitu: 1. Pesan, *Plaintext*, dan *Ciphertext* Pesan (*message*) adalah data atau informasi yang dapat dibaca dan dimengerti maknanya. Nama lain untuk pesan adalah (*plaintext*) atau teks jelas (*cleartext*). 2. Pengirim dan Penerima Komunikasi data melibatkan pertukaran pesan antara dua entitas. Pengirim (*sende*r) adalah entitas yang mengirim pesan kepada entitas lainnya. Penerima (*receiver*) adalah entitas yang menerima pesan. 3. Enkripsi dan dekripsi Proses menyandikan *plaintext* menjadi *ciphertext* disebut enkripsi (*encryption*) atau *enciphering* (standard nama menurut ISO 7498-2). Sedangkan proses mengembalikan *ciphertext* menjadi *plaintext* semula disebut dekripsi (*decryption*) atau *deciphering* (standard nama menurut ISO 7498-2). 4. *Cipher* dan kunci Algoritma kriptogarfi disebut juga *cipher*, yaitu aturan untuk enkripsi dan dekripsi, atau fungsi matematika yang digunakan untuk enkripsi dan dekripsi. Beberapa *cipher* memerlukan algoritma yang berbeda untuk enkripsi dan dekripsi. Konsep matematis yang mendasari algoritma kriptografi adalah relasi antara dua buah himpunan yang berisi elemen-elemen *plaintext* dan himpunan yang berisi *ciphertext*. Enkripsi dan dekripsi merupakan fungsi yang memetakan elemen-elemen antara dua himpunan tersebut. Misalkan P menyatakan *plaintext* dan C menyatakan *ciphertext*, maka: E(P) = C merupakan fungsi enkripsi, E memetakan P ke C D(C) = P merupakan fungsi dekripsi, D memetakan C ke P Karena proses enkripsi kemudian dekripsi mengembalikan pesan ke pesan asal, maka persamaan D(E(P)) = P harus benar. Kriptografi mengatasi masalah keamanan data dengan menggunakan kunci, yang dalam hal ini algoritma tidak dirahasiakan lagi, tetapi kunci harus tetap dijaga kerahasiaannya. Kunci (*key*) adalah parameter yang digunakan untuk transformasi enkripsi dan dekripsi. Kunci biasanya berupa string atau deretan bilangan. Dengan menggunakan kunci K, maka fungsi enkripsi dan dekripsi dapat ditulis sebagai skema diperlihatkan pada Gambar 2.1.



Gambar 2.1. Skema Enkripsi dan Dekripsi

(Sumber: Munir *dalam* Pabokory dkk, 2015)

Kriptografi bertujuan memberikan layanan pada aspek-aspek keamanan antara lain:

1. Kerahasiaan (*confidentiality*)*,* yaitu menjaga supaya pesan tidak dapat dibaca oleh pihak-pihak yang tidak berhak.

2. Integritas data (*data integrity*)*,* yaitu memberikan jaminan bahwa untuk tiap bagian pesan tidak akan mengalami perubahan dari saat data dibuat/dikirim oleh pengirim sampai dengan saat data tersebut dibuka oleh penerima data.

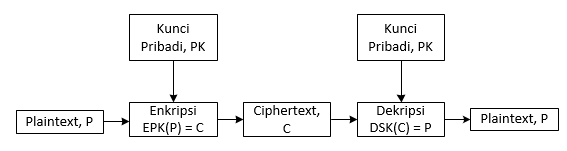
3. Otentikasi (*authentication*)*,* yaitu berhubungan dengan identifikasi, baik mengidentifikasi kebenaran pihak-pihak yang berkomunikasi maupun mengidentifikasi kebenaran sumber pesan.

4. Nirpenyangkalan (*nonrepudiation*)*,* yaitu memberikan cara untuk membuktikan bahwa suatu dokumen datang dari seseorang tertentu sehingga apabila ada seseorang yang mencoba mengakui memiliki dokumen tersebut, dapat dibuktikan kebenarannya dari pengakuan orang tersebut (Munir *dalam* Pabokory dkk, 2015).

Berdasarkan kunci yang digunakan untuk enkripsi dan dekripsi, kriptografi dapat dibedakan atas dua golongan, yaitu:

* + - 1. **Kriptografi Simetrik (*Symetric Cryptography*)**

*Symmetric cryptosystem* atau kriptografi simteris atau disebut juga algoritma kriptografi konvensional adalah algoritma yang menggunakan kunci untuk proses enkripsi sama dengan kunci untuk proses dekripsi. Algoritma kriptografi simetris dibagi menjadi 2 kategori yaitu algoritma aliran (*Stream Ciphers*) dan algoritma blok (*Block Ciphers*). Pada algoritma aliran, proses penyandiannya berorientasi pada satu bit atau satu byte data. Sedang pada algoritma blok, proses penyandiannya berorientasi pada sekumpulan bit atau *byte* data (per blok). Ini adalah jenis kriptografi yang paling umum dipergunakan. Kunci untuk membuat pesan yang disandikan sama dengan kunci untuk membuka pesan yang disandikan itu. Jadi pembuat pesan dan penerimanya harus memiliki kunci yang sama persis. Contoh algoritma kunci simetris yang terkenal adalah DES (Data *Encryption Standard*) dan RC-4. Skema algoritma ditunjukkan pada gambar 2.2.

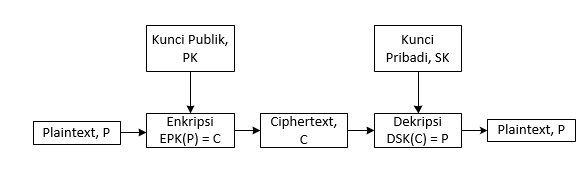


Gambar 2.2 Kriptografi Simetrik

(Sumber : Kurniawan *dalam* Basri, 2014)

* + - 1. **Kriptografi Asimetrik (*Asymetric Cryptography*)**

Pada pertengahan tahun 70-an Whitfield Diffie dan Martin Hellman menemukan teknik enkripsi asimetris yang merevolusi dunia kriptografi. Kunci asimetris adalah pasangan kunci-kunci kriptografi yang salah satunya dipergunakan untuk proses enkripsi dan yang satu lagi untuk dekripsi. Semua orang yang mendapatkan kunci publik dapat menggunakannya untuk mengenkripsikan suatu pesan, sedangkan hanya satu orang saja yang memiliki rahasia tertentu dalam hal ini kunci *private* untuk melakukan pembongkaran terhadap sandi yang dikirim untuknya. Sebagai contoh jika Anto mengirim pesan untuk Badu, Anto dapat merasa yakin bahwa pesan tersebut hanya dapat dibaca oleh Badu, karena hanya Badu yang bisa melakukan dekripsi dengan kunci privatnya. Tentunya Anto harus memiliki kunci publik Badu untuk melakukan enkripsi. Anto bisa mendapatkannya dari Badu, ataupun dari pihak ketiga seperti Tari. Skema algoritma kriptografi asimetris terlihat pada gambar 2.3.



Gambar 2.3 Kriptografi Asimetrik

(Sumber: Kurniawan *dalam* Basri, 2014)

Contoh algoritma terkenal yang menggunakan kunci Asimetris adalah RSA (merupakan singkatan penemunya yakni *Rivest, Shamir dan Adleman*).

* + 1. **Algoritma RSA (*Rivest-Shamir-Adleman*)**

Munir (dalam Diarse dan Bendi, 2016) Dari sekian banyak algoritma kriptografi kunci publik yang pernah dibuat, algoritma yang paling populer adalah algoritma RSA. Algoritma RSA dibuat oleh 3 orang peneliti MIT (*Massachussets Institute of Technology*) pada tahun 1976, yaitu: Ron (R)ivest, Adi (S)hamir, dan Leonard (A)dleman. Keamanan algoritma RSA terletak pada sulitnya memfaktorkan bilangan yang besar menjadi faktor-faktor prima, sehingga semakin besar bilangan prima Pemfaktoran dilakukan untuk memperoleh kunci pribadi.

Pada Algoritma RSA terdapat tiga proses yaitu, pembangkitan kunci, proses enkripsi dan proses dekripsi. Letak kesulitan algoritma ini adalah bagaimana menemukan dua faktor bilangan prima yang besar yang akan digunakan sebagai kunci publik dan kunci privat. Dua bilangan prima besar tersebut *p* dan *q* dimana *p ≠ q.*

* + - 1. **Besaran-besaran pada algoritma RSA**

Besaran-besaran yang digunakan pada algoritma RSA adalah sebagai berikut:

1. p dan q bilangan prima (Rahasia)
2. n = p \* q (*public key*) (Tidak Rahasia)
3. φ (n) = (p - 1) (q - 1) (Rahasia)
4. e (kunci enkripsi) (Tidak Rahasia)
5. d (kunci deskripsi) (Rahasia)
6. m (*plainteks/message*) (Rahasia)
7. c (*chiperteks*) (Tidak Rahasia)
   * + 1. **Proses Pembangkitan Kunci**

Langkah-langkah pada proses pembangkitan kunci publik dan kunci privat pada algoritma RSA adalah sebagai berikut:

1. Langkah Pertama: Pilih 2 bilangan prima yang berbeda secara acak untuk nilai p dan q. Dengan syarat nilai p ≠ q. Semakin besar nilainya semakin baik. Keduanya bilangan prima ini, p dan q bersifat rahasia.
2. Langkah Kedua: Hitung nilai n menggunakan persamaan 1.

n = p \* q (1)

dimana n digunakan untuk modulos pada kunci public dan kunci privat. Nilai n tidak rahasia.

1. Langkah Ketiga: Hitung nilai Φ(n) menggunakan persamaan 2.

Φ(n) = (p - 1) \* (q – 1) (2)

Digunakan untuk pencarian kunci privat. Nilai Φ(n) bersifat rahasia.

1. Langkah Keempat: Hitung nilai e dengan cara memilih bilangan bulat dengan syarat e > 1, dan GCD(e, φ(n)) = 1. Nilai e bersifat tidak rahasia.
2. Langkah Kelima: Pilh nilai d yang merupakan bilangan bulat dengan syarat nilai d memenuhi (d \* e) mod φ(n) = 1 atau d = (1 + k \* φ(n)) / e, nilai k dapat ditentukan secara acak. Nilai d bersifat rahasia.

Sehingga dari langkah-langkah pada proses pembangkitan kunci di atas didapatkan kunci public (e, n) dan kunci privat (d, n). Contoh proses pembangkitan kunci public dan kunci privat pada algoritma RSA:

1. Nilai bilangan prima p = 53 dan q = 79.
2. Hitung nilai n = p \* q

n = 53 \* 79 = 4187

1. Hitung Φ(n) = (p - 1) \* (q – 1)

Φ(n) = (53 – 1) \* (79 – 1)

= 52 \* 78 = 4056

1. Hitung nilai e

sebagai contoh, nilai e = 73 dan φ = 4056. Sesuai persyaratan, tes terlebih dahulu apakah GCD(73,4056) = 1 ?

4056 mod 73 = 41

73 mod 41 = 32

41 mod 32 = 9

32 mod 9 = 5

9 mod 5 = 4

5 mod 4 = **1**

Ternyata benar GCD(73,4056) = 1 (1 didapat dari angka yang di *bold*).

Untuk membangkitkan kunci *public* dan kunci privat maka menentukan nilai p dan q yaitu:

Nilai p: 53

Nilai q: 79

1. Langkah Kedua: Hitung nilai n.

Untuk menghitung nilai n digunakan persamaan:

*n* = *p \* q*

Dimana, n = kunci *public*

p = nilai p

q = nilai q

menentukan nilai pembangkit kunci *public*

Untuk n = p \* q

= 53 \* 79 = 4187

1. Langkah Ketiga: Hitung φ (di baca phi). Φ(n) = (p - 1) \* (q - 1).

Menentukan totient dari kunci public (n) digunakan persamaan:

Φ(n) = (p - 1) \* (q – 1)

Dimana, Φ = totient dari kunci public

p = nilai p

q = nilai q

untuk Φ (n)= (p - 1) \* (q - 1)

= (53-1) \* (79-1)

= 52 \* 78 = 4056

1. Langkah Keempat: Pilih nilai kunci enkripai (e) dengan syarat e > 1, dan GCD(e, φ(n)) = 1

sebagai contoh, nilai e = 73 dan φ = 4056. Sesuai persyaratan, tes terlebih dahulu apakah GCD(73,4056) = 1 ?

4056 mod 73 = 41

73 mod 41 = 32

41 mod 32 = 9

32 mod 9 = 5

9 mod 5 = 4

5 mod 4 = **1**

Ternyata benar GCD(73,4056) = 1 (1 didapat dari angka yang di *bold*).

1. Langkah Kelima: tentukan nilai d, dimana k ditentukan secara acak/sembarang dan perhitungan nilai d menggunakan persamaan sebagai berikut:

Dimana, d = kunci privat

k = bilangan bulat

Φ = nilai *totient*

e = kunci *public*

menentukan nilai dari kunci privat

untuk

Dengan mencoba nilai k = 16 diperoleh nilai *d* yang bulat adalah 889. Ini adalah kunci private untuk mendeskripsi pesan.

Kunci *Public* :

Kunci *Private* :

* + - 1. **Proses Enkripsi**

Proses enkripsi menggunakan algoritma RSA terhadap *plainteks* m = TEKNIK, pertama-tama *plaintext* diubah menjadi format ASCII (*Decimal*) sebagai berikut:

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| TEXT (Karakter) | B | A | T | U | K |
| ASCII (Decimal) | 84 | 69 | 75 | 78 | 73 |

m = TEKNIK = 846975787375, kemudian pecahkan m dengan membuat blok yang masing-masing blok tersebut terdapat 3 digit.

|  |  |  |  |
| --- | --- | --- | --- |
| 846 | 975 | 787 | 375 |

m1 = 846 m3 = 787

m2 = 975 m4 = 375

misalkan e = 73 dan n = 4187, lalu enkripsikan setiap blok *plaintext* menggunakan persamaan sebagai berikut:

C = Me mod n

keterangan:

C = *Ciphertext*

M = *Plaintext*

e = Kunci *public*

n = pembangkit kunci *public*

menghitung nilai *ciphertext* dari m1, m2, m3, dan m4 yang telah didapatkan sebelumnya.

c1 = 846^73 mod 4187 = 3927

c2 = 975^73 mod 4187 = 2701

c3 = 787^73 mod 4187 = 3252

c4 = 375^73 mod 4187 = 714

Jadi *ciphertext* (c) adalah = 3927 2701 3252 714

* + - 1. **Proses Dekripsi**

Proses dekripsi algoritma RSA menggunakan persamaan sebagai berikut:

Keterangan:

P = Cd mod n

P = *Plaintext*

C = *Ciphertext*

d = Kunci Privat

n = Pembangkit Kunci *public*

Sebelumnya telah didapatkan nila d = 889 dan n = 4187, setiap blok *ciphertext* di dekripsikan sebagai berikut:

m1 = 3927^889 mod 4187 = 846

m2 = 2701^889 mod 4187 = 975

m3 = 3252^889 mod 4187 = 787

m4 = 714^889 mod 4187 = 375

Jadi dapat diperoleh plainteks (m) = 846975787375, dimana ketika dikonversi kedalam ASCII m = TEKNIK. Diatas adalah contoh sederhana pengamanan data dengan algoritma RSA.

* + 1. **ASCII (*American Standard Code for Information Interchange*)**

Ariyus (dalam Kharisma dan Rachman, 2017) ASCII atau kode Standar Amerika untuk Pertukaran Informasi. Merupakan suatu standar internasional dalam kode huruf dan lumeri seperti *Hex* dan *Unicode* tetapi ASCII lebih bersifat universal, contohnya 124 adalah untuk karakter “|”. Biasanya digunakan oleh komputer dan alat komunikasi lain untuk menunjukkan teks. Dalam kriptografi, kode ASCII ini merupakan urutan bit yang akan mewakili teks asli yang kemudian dienkripsi untuk mendapatkan teks kode dalam bentuk urutan bit. ASCII memerlukan 8 bit untuk mendapatkan satu karakter dan blok kode mempunyai 64 bit untuk satu blok.

Kharisma dan Rachman (2017), Karakter control pada ASCII dibedakan menjadi 5 kelompok sesuai dengan penggunaan yaitu berturut-turut meliputi *logical communication, Device control, Information separator, Code extention*, dan *physical communication*. Kode ASCII ini banyak dijumpai pada keyboard komputer atau instrumen-instrumen digital. Berikut adalah tabel ASCII.

Tabel 2.1 Kode ASCII

(Sumber: Kharisma dan Rachman, 2017)

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Karakter | Decimal | Karakter | Decimal | Karakter | Decimal |
| Spasi | 32 | @ | 64 | ` | 96 |
| ! | 33 | A | 65 | A | 97 |
| “ | 34 | B | 66 | B | 98 |
| # | 35 | C | 67 | C | 99 |
| $ | 36 | D | 68 | D | 100 |
| % | 37 | E | 69 | E | 101 |
| & | 38 | F | 70 | F | 102 |
| ‘ | 39 | G | 71 | G | 103 |
| ( | 40 | H | 72 | H | 104 |
| ) | 41 | I | 73 | I | 105 |
| \* | 42 | J | 74 | J | 106 |
| + | 43 | K | 75 | K | 107 |
| , | 44 | L | 76 | l | 108 |
| - | 45 | M | 77 | m | 109 |
| . | 46 | N | 78 | n | 110 |
| / | 47 | O | 79 | o | 111 |
| 0 | 48 | P | 80 | p | 112 |
| 1 | 49 | Q | 81 | q | 113 |
| 2 | 50 | R | 82 | r | 114 |
| 3 | 51 | S | 83 | s | 115 |
| 4 | 52 | T | 84 | t | 116 |
| 5 | 53 | U | 85 | u | 117 |
| 6 | 54 | V | 86 | v | 118 |
| 7 | 55 | W | 87 | w | 119 |
| 8 | 56 | X | 88 | x | 120 |
| 9 | 57 | Y | 89 | y | 121 |
| : | 58 | Z | 90 | z | 122 |
| ; | 59 | [ | 91 | { | 123 |
| < | 60 | \ | 92 | | | 124 |
| = | 61 | ] | 93 | } | 125 |
| > | 62 | ^ | 94 | ~ | 126 |
| ? | 63 | \_ | 95 |  |  |

* + 1. **Pengertian Web**

# **BAB III**

**METODE PENELITIAN**

1. **Bahan dan Alat Penelitian**
2. Bahan Penelitian

Dalam penelitian ini, bahan penelitian yang akan digunakan adalah hasil studi literatur yang telah dilakukan yang menyangkut tentang algoritma RSA dan beberapa data yang diperoleh pada RSUD Anutapura Kota Palu yaitu:

1. Data Pasien

2. Data Dokter

3. Data Penyakit

4. Data Rekam Medis

1. Alat Penelitian

Pada penelitian ini akan menggunakan beberapa perangkat lunak (*software*) dan perangkat keras (*hardware*). Berikuti adalah perangkat lunak yang digunakan:

1. *Sublime* 3sebagai editor
2. *Xampp* Versi 3.2.2

Sedangkan perangkat keras yang digunakan minimum spesifikasinya yaitu:

1. Model prosesor: *Intel Core i3.*

2. Memori: 4GB, DDR3.

3. Tempat penyimpanan: HDD, 500GB.

4. Model GPU: AMD *Radeon* HD 7670M.

1. **Desain Penelitian**

### 3.2.1. Jenis Penelitian

Penelitian ini menggunakan jenis penelitian kualitatif.

Rahardjo (2017), penelitian kualitatif adalah penelitian yang bermaksud untuk memahami fenomena tentang apa yang dialami oleh subjek penelitian misalnya perilaku, persepsi, motivasi, tindakan, dan lain-lain. Penelitian kualitatif sendiri adalah prosedur penelitian yang menghasilkan data deskriptif berupa kata-kata tertulis atau lisan dari orang-orang dan perilaku yang diamati.

### 3.2.2. Tipe Penelitian

Tipe penelitian ini adalah penelitian deskriptif.

Linarwati, dkk(2016), Penelitian deskriptif merupakan penelitian yang berusaha mendeskripsikan dan menginterpretasikan sesuatu, misalnya kondisi atau hubungan yang ada, pendapat yang berkembang, proses yang sedang berlangsung, akibat atau efek yang terjadi, atau tentang kecenderungan yang tengah berlangsung.

1. **Objek, Waktu, dan Lokasi Penelitian**

Objek dalam penelitian ini adalah data rekam medis pasien. Penelitian ini dilakukan pada rumah sakit daerah anutapura yang berada di Kota Palu. Adapun waktu yang ditargetkan oleh peneliti adalah 6 (enam) bulan dari pengajuan proposal penelitian ini dimulai pada bulan Agustus 2019 sampai Februari 2020.

1. **Jenis dan Sumber Data**

### 3.4.1. Data Primer

Data primer dalam penetian ini diperoleh langsung dari beberapa pihak rumah sakit pada bagian data rekam medis. Sehingga informasi yang diperoleh relevan dengan masalah dan tujuan penelitian.

### 3.4.2. Data Sekunder

Data sekunder yang digunakan dalam penelitian diperoleh dari sumber-sumber yang relevan dengan penelitian. Data sekunder ini merupakan data yang sifatnya mendukung keperluan data primer seperti buku-buku, literatur dan bacaan yang berkaitan dengan pengamanan *database* menggunakan algoritma RSA*.*

1. **Teknik Pengumpulan Data**

Adapun teknik pengumpulan data yang digunakan dalam penelitian ini adalah observasi, wawancara, dan studi literatur.

* + - 1. Observasi

Metode observasi dilakukan dilakukan untuk mendapatkan gambaran yang jelas mengenai pelaksanaan sistem yang berjalan serta mencari dan mengumpulkan data yang dibutuhkan langsung dari sumbernya.

Dalam pengumpulan informasi mengenai kebutuhan sistem *(system requirements),* penulis melakukan pengumpulan data dengan cara observasi di tempat penelitian, yang dalam hal ini adalah RSUD (Rumah Sakit Umum Daerah) Anutapura Kota Palu.

* + - 1. Wawancara

Wawancara adalah proses memperoleh keterangan dengan cara tanya jawab seraya bertatap muka antara pewawancara dengan informan atau orang yang diwawancarai. Dalam hal ini informan yang diwawancarai adalah pihak Rumah Sakit Umum Anutapura bagian rekam medis terkait dengan keamanan data rekam medis yang ada di rumah sakit tersebut.

* + - 1. Studi Literatur

Pada tahapan ini, dilakukan pengumpulan data dengan cara studi pustaka, dimana penulis mencari referensi-referensi yang relevan dengan objek yang akan diteliti. Pencarian referensi dilakukan dengan mencari sumber melalui buku-buku secara manual, maupun secara *online* melalui internet sebagai sumber data yang relevan guna memperoleh informasi-informasi yang dibutuhkan dalam penelitian ini.

Informasi yang didapatkan digunakan dalam penyusunan landasan teori, metodologi penelitian serta pengembangan aplikasinya secara langsung. Pustaka-pustaka yang dijadikan acuan dapat dilihat di Daftar Pustaka.

1. **Metode Analisis Data**

Dalam penggalian data dan informasi, penulis menggunakan pendekatan dengan menggunakan metode UML (*Unified Modelling Language*) yaitu suatu metode pemodelan secara visual atau bahasa yang sudah menjadi standar pendokumentasian sistem *software*. Adapun jenis UML yang digunakan yaitu *Use case diagram*. Selain jenis UML tersebut, penulis juga menggunakan *Data Flow Diagram* (DFD). Untuk pemodelan basis data penulis menggunakan *Entity Relationship Diagram* (ERD).

1. **Metode Pengembangan Sistem**

Metode pengembangan sistem yang digunakan adalah model *waterfall*. Model *Waterfall* dapat dilihat pada Gambar 3.1.

Adapun penjelasannya sebagai berikut:

* + - 1. Analisa Kebutuhan

Pada tahap ini merupakan analisa terhadap kebutuhan sistem. Pengumpulan data dalam tahap ini bisa melakukan sebuah penelitian, wawancara atau studi literatur. Penulis akan menggali informasi sebanyak-banyaknya dari *user* sehingga tercipta sebuah sistem komputer yang bisa melakukan tugas-tugas yang diinginkan oleh *user*. Tahapan ini akan menghasilkan data *user requirment* atau bisa dikatakan sebagai data yang berhubungan dengan keinginan *user* dalam pembuatan sistem. Data inilah yang akan menjadi acuan penulis untuk menerjemahkan ke dalam Bahasa pemrograman.

* + - 1. Desain Sistem

Proses desain akan menerjemahkan syarat kebutuhan ke sebuah perancangan perangkat lunak yang dapat diperkirakan sebelum dibuat *coding*. Proses ini berfokus pada: struktur data, arsitektur perangkat lunak, representasi *interface*, dan detail algoritma *procedural*. Tahapan ini akan menghasilkan data yang disebut *software requirement*. Data inilah yang akan digunakan penulis untuk melakukan aktivitas pembuatan sistemnya.

* + - 1. Penulisan Kode Program

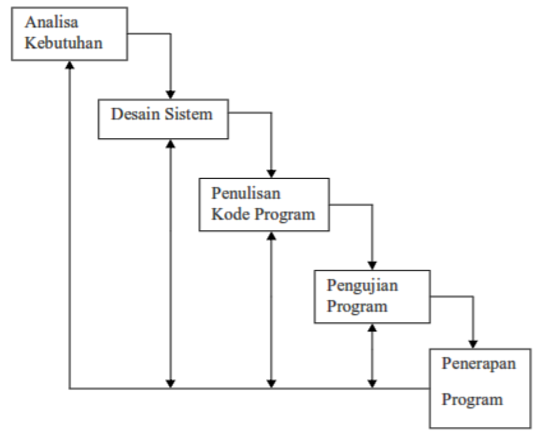
*Coding* atau kode program merupakan penerjemahan desain dalam Bahasa yang bisa dikenali oleh komputer. Dilakukan oleh penulis yang akan menerjemahkan transaksi yang diminta oleh *user*. Tahapan inilah yang merupakan tahapan secara nyata dalam mengerjakan suatu sistem. Dalam tahap ini penggunaan komputer akan dimaksimalkan.

* + - 1. Pengujian Program

Pada tahap ini akan dilakukan pengujian terhadap program yang telah dibuat. Tujuan pengujian program adalah untuk menemukan kesalahan-kesalahan terhadap program tersebut dan kemudian bisa diperbaiki.

* + - 1. Penerapan Program

Tahapan ini bisa dikatakan final dalam pembuatan sebuah sistem. Setelah melakukan Analisa, desain dan pengkodean maka sistem yang sudah jadi akan digunakan oleh *user*.



Gambar 3.1. *Model Waterfall*

(Sumber: Pressman dalam Natsir, 2017)

1. **Tahapan dan Diagram Alir Penelitian**

Terdapat beberapa tahapan yang perlu dilakukan agar penelitian ini dapat berjalan dengan baik. Tahapan Penelitian dapat dilihat pada Gambar 3.2.

Adapun tahapan penelitian ini adalah:

* + 1. Survei Literatur

Melakukan pengumpulan bahan, informasi, dan referensi yang relevan berkaitan dengan topik penelitian.

* + 1. Identifikasi Masalah

Melakukan identifikasi masalah untuk menentukan solusi dan pembahasan apa yang diperlukan, berkaitan dengan topik penelitian.

* 1. Pengumpulan Data

Melakukan wawancara secara langsung kepada pihak yang terkait untuk mendapatkan informasi dan keperluan sistem, seperti staff bagian rekam medis dan kepala bagian rekam medik pada rumah sakit umum anutapura.

* 1. Analisis Data

Setelah pengumpulan data telah selesai maka data-data tersebut dianalisis terlebih dahulu seperti:

1. Data Dokter

Data dokter yang digunakan untuk mendata semua dokter yang melakukan praktek di Rumah Sakit Umum Anutapura Kota Palu.

1. Data Pasien

Digunakan untuk mendata pasien yang masuk di Rumah Sakit Umum Anutapura Kota Palu.

1. Data Penyakit

Data Penyakit digunakan untuk menginput jenis penyakit apa saja yang diderita pasien.

1. Data Rekam Medis

Digunakan untuk melihat hasil diagnosis dari pasien.

* 1. Perancangan Perangkat Lunak

Pada perancangan perangkat lunak, tahapan yang dilakukan dengan merancang Sistem Pengamanan Data Rekam Medis menggunakan Algoritma RSA. Rancangan desain tampilan dan basis data sistem dijelaskan sebagai berikut:

1. Input data dokter

Input data dokter dilakukan oleh admin, data yang diinputkan antara lain, id dokter, nama dokter, spesialis, jenis kelamin, tempat lahir, tanggal lahir, no. telpon, dan alamat.

1. Input data pasien

Input data pasien dilakukan oleh admin, data yang diinputkan antara lain, no. rekam medis, nama pasien, tanggal lahir, umur, jenis kelamin, agama, pekerjaan, alamat, no.telpon.

1. Input data penyakit

Input data penyakit dilakukan oleh admin, data yang diinputkan antara lain, kode penyakit dan jenis penyakit.

1. Input data rekam medis

Input data rekam medis dilakukan oleh admin, data yang diinputkan antara lain, no. register, no. rekam medis, nama pasien, tanggal masuk, jam masuk, unit rawat, rujukan dari, ruangan, penanggung jawab, dokter pemeriksa, diagnosa, dan tindakan.

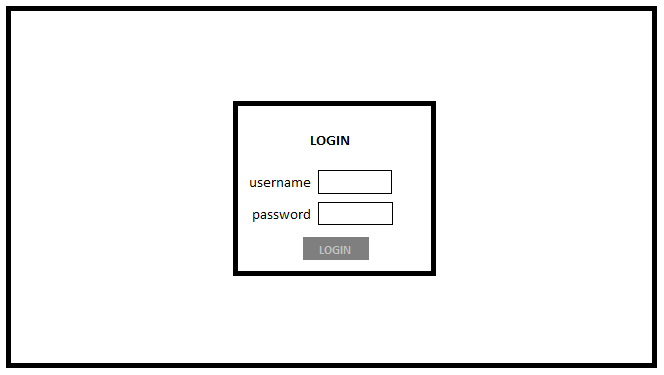
1. RSA

RSA sebagai tempat penyimpanan kunci-kunci yang dibutuhkan untuk membuat suatu enkripsi atau dekripsi algoritma RSA.

Berikut adalah perancangan *form* tampilan dari system pengamanan data rekam medis menggunakan algoritma RSA (Studi Kasus: RSUD Anutapura Kota Palu) yang dapat dilihat pada gambar 3.4 sampai dengan gambar 3.9.

1. *Form Login*

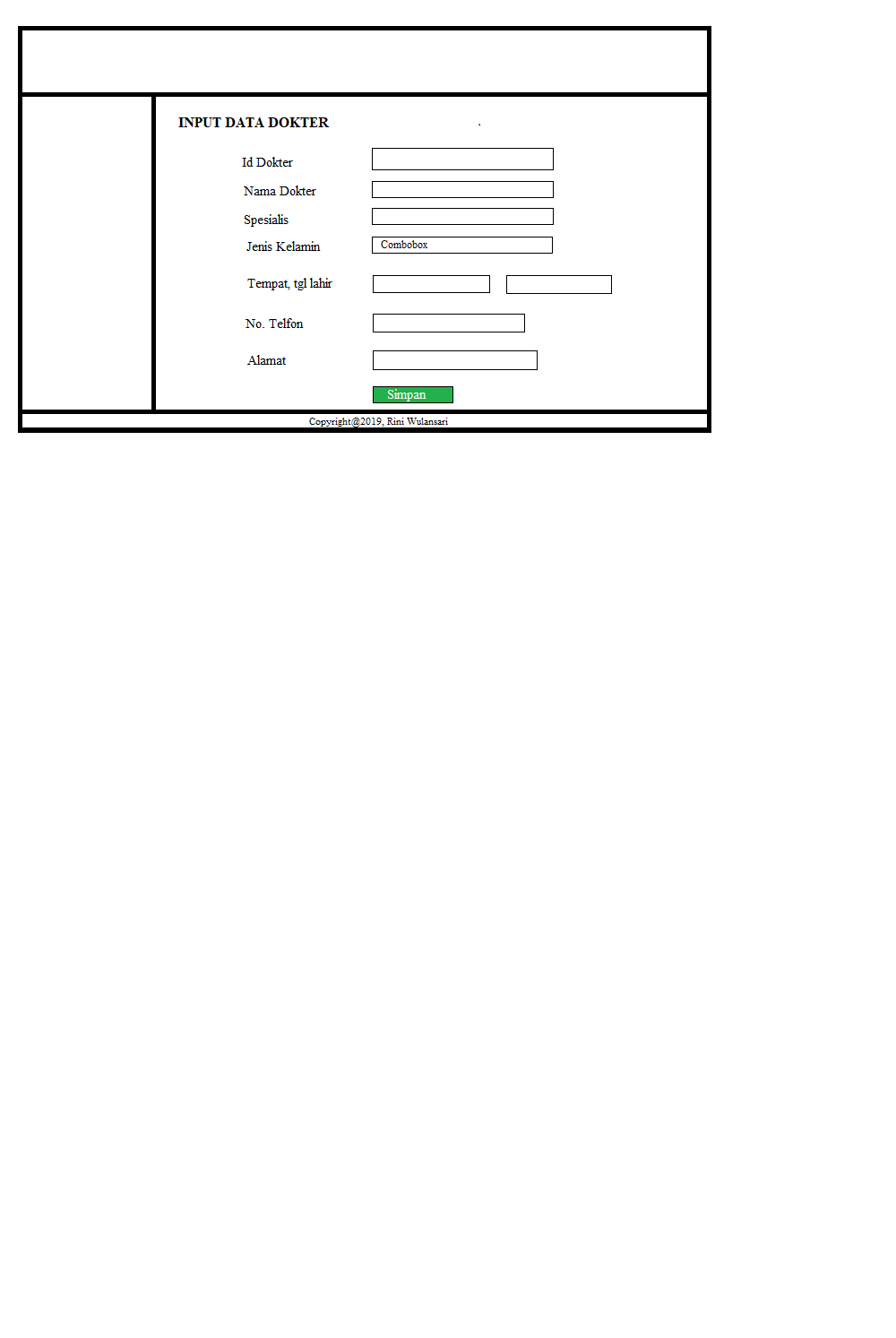
*Form* ini digunakan Admin/Operator untuk *login.* Berikut adalah rancangan tampilannya.



Gambar 3.3. *Form input login*

1. *Form* *Input* Data Dokter

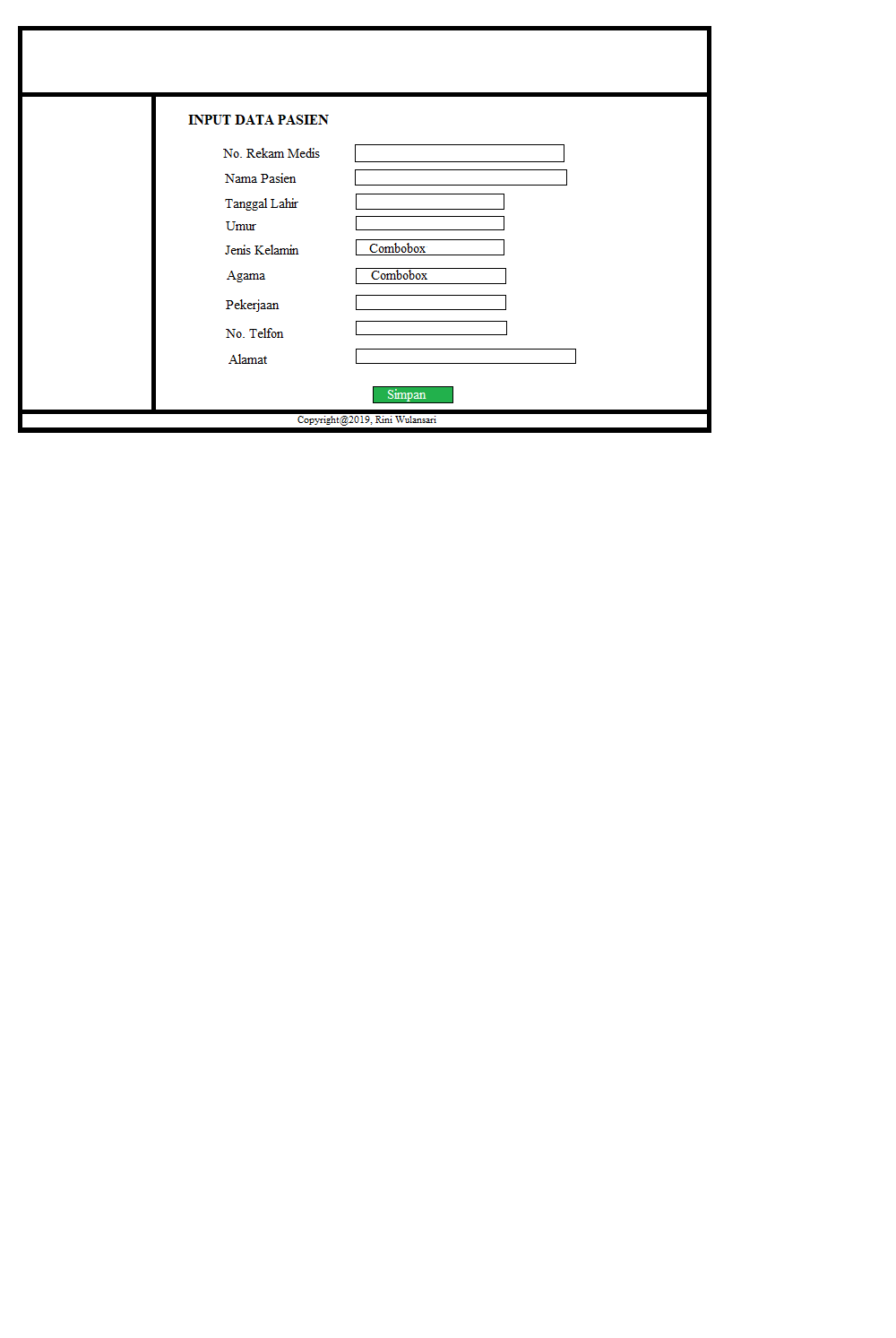
*Form* ini digunakan untuk menginput data Dokter yang bertugas memeriksa pasien pada rumah sakit umum daerah anutapura. Berikut adalah rancangan tampilannya.



Gambar 3. 4. *Form* *input* data dokter

1. Form Input Data Pasien

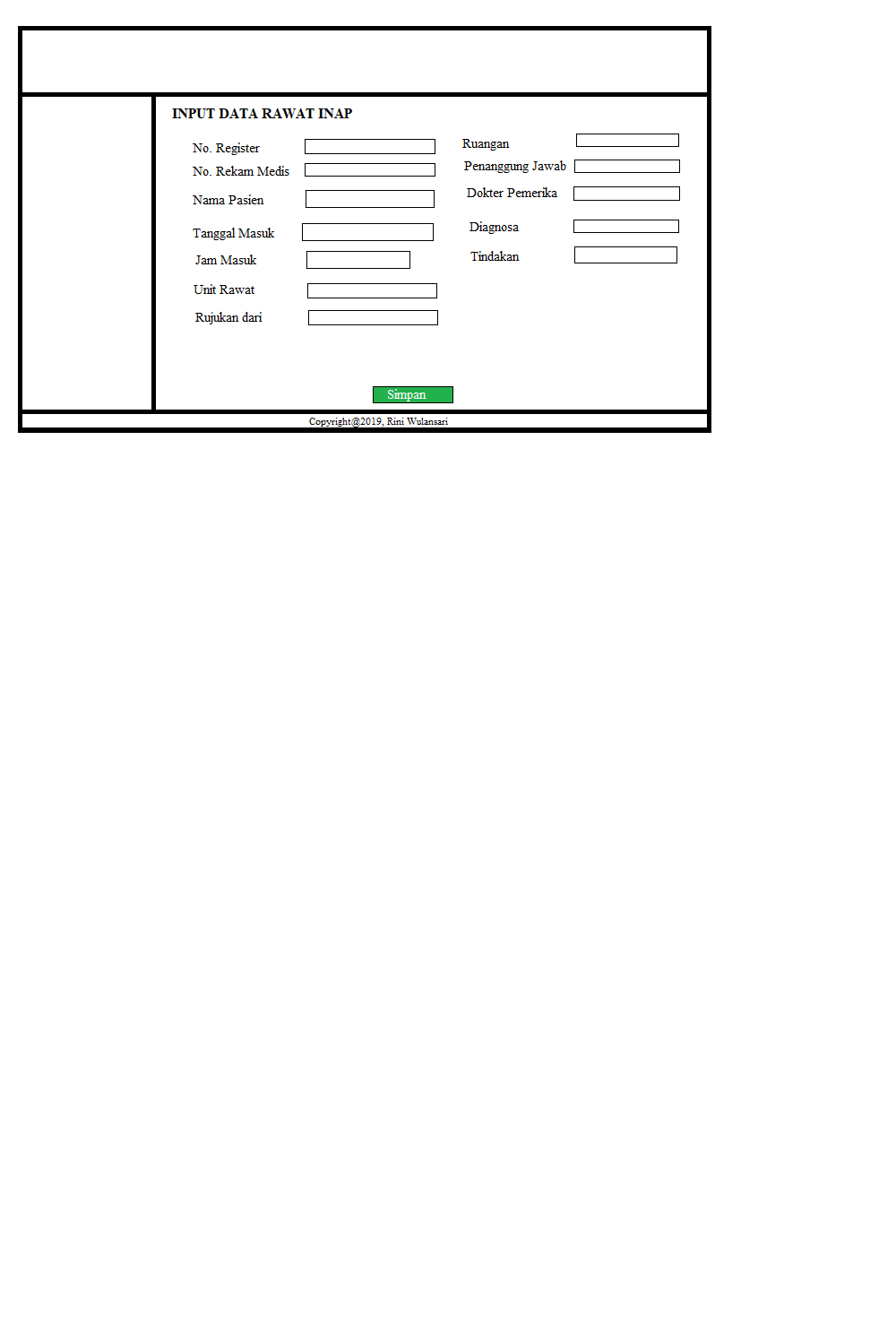
*Form* ini digunakan untuk menginput data pasien baru yang masuk di rumah sakit umum daerah anutapura. Berikut adalah rancangan tampilannya.



Gambar 3. 5. *Form* *input* data pasien

1. *Form Input* data rawat inap

*Form* ini digunakan untuk menginput data-data pasien rawat inap. Berikut adalah rancangan tampilannya.



Gambar 3.6. *Form input* data rawat inap pasien

Perancangan database yang akan dibuat pada penelitian ini dapat dilihat pada tabel 3.2 sampai dengan tabel 3.3.

1. Tabel Akun

Tabel akun yang dapat dilihat pada tabel 4.1 digunakan untuk menyimpan data pengguna.

Tabel 4.1 Akun

|  |  |  |  |
| --- | --- | --- | --- |
| ***Field*** | ***Type*** | ***Length/Values*** | ***Index*** |
| Id\_akun | Int | 11 | Primary |
| *Username* | Varchar | 15 | - |
| *Password* | Varchar | 15 | - |
| Nama | Varchar | 50 | - |
| Email | Varchar | 50 | - |
| Status | Varchar | 25 | - |
| Level | Varchar | 25 | - |

1. Tabel data tenaga medis

Tabel data tenaga medis yang dapat dilihat pada tabel 4.1 digunakan untuk menyimpan data tenaga medis.

Tabel 4.1 Data tenaga medis

|  |  |  |  |
| --- | --- | --- | --- |
| ***Field*** | ***Type*** | ***Length/Values*** | ***Index*** |
| Id | Int | 11 | Primary |
| Nama | Varchar | 15 | - |
| Spesialis | Varchar | 20 | - |
| Jk | Varchar | 50 | - |
| Alamat | Varchar | 50 | - |
| No\_telp | Varchar | 25 | - |

1. Tabel data pasien

Tabel data pasien yang dapat dilihat pada tabel 4.1 digunakan untuk menyimpan data tenaga medis.

Tabel 4.1 Data pasien

|  |  |  |  |
| --- | --- | --- | --- |
| ***Field*** | ***Type*** | ***Length/Values*** | ***Index*** |
| No\_rm | Int | 11 | Primary |
| Nama | Varchar | 15 | - |
| Tgl\_lahir | Varchar | 30 | - |
| Umur | Varchar | 50 | - |
| Jk | Varchar | 50 | - |
| Agama | Varchar | 25 | - |
| Pekerjaan | Varchar | 25 | - |
| Alamat | Varchar | 25 | - |
| No\_telp | Varchar | 12 | - |

1. Tabel rekam medis

Tabel data rekam medis yang dapat dilihat pada tabel 4.1 digunakan untuk menyimpan data rekam medis.

Tabel 4.1 Rekam medis

|  |  |  |  |
| --- | --- | --- | --- |
| ***Field*** | ***Type*** | ***Length/Values*** | ***Index*** |
| No\_rm | Int | 11 | Primary |
| Nama | Varchar | 15 | - |
| Tgl\_lahir | Varchar | 30 | - |
| Umur | Varchar | 50 | - |
| Jk | Varchar | 50 | - |
| Alamat | Varchar | 30 | - |
| Tgl\_masuk | Varchar | 25 | - |
| Diagnosa | Varchar | 25 | - |
| Tindakan | Varchar | 25 | - |
| Pemeriksa | Varchar | 12 | - |

1. Pembuatan Perangkat Lunak

Pembuatan perangkat lunak antara lain melakukan persiapan *software* yang akan digunakan, membuat desain, *database* dan *coding.* Terdapat beberapa tahapan yang dilakukan dalam implementasi algoritma RSA pada sistem pengamanan rekam medis yaitu perancangan desain tampilan dan basis data sistem.

Pada Algoritma RSA terdapat tiga proses yaitu, pembangkitan kunci, proses enkripsi dan proses dekripsi.

1. Proses pembengkit kunci

Proses pembangkit kunci dimulai dengan menginput bilangan prima p, kemudian menginputkan bilangan prima q, kemudian hitung bilangan kunci *public* menggunakan rumus n = p \* q, setelah itu hitung bilangan totient, kemudian hitung kunci enkripsi (e). Setelah itu input bilangan bulat k, kemudian menghitung kunci dekripsi menggunakan bilsngan k yang telah diinputkan sebelumnya. Maka didapatlah output bilangan prima e, output bilangan prima d dan output bilangan prima n. Proses tersebut dapat dilihat pada Gambar 3.12.



Gambar 3.12. Proses Pembangkit Kunci Algoritma RSA

1. Proses Enkripsi

Proses enkripsi pada Algoritma RSA pertama-tama input *plaintext* kemudian ubah plaintext ke dalam kode ASCII (*decimal*) setelah itu pecah plaintext yang sudah di konversi ke dalam ASCII menjadi blok 0 > m > n – 1, kemudian input kunci public, setelah itu mencari nilai enkripsi menggunakan rumus c = m^e mod n, setelah mendapatkan nilai enkripsi di dapatlah output *ciphertext*. Proses tersebut dapat dilihat pada Gambar 3.13.



Gambar 3.13 Prose Enkripsi Algoritma RSA

1. Proses Deskripsi

Proses deskripsi pada algoritma RSA pertama-tama input ciphertext, kemudian input kunci private, lalu mencari nilai dekripsi menggunakan rumus m = c^d mod n, setelah didapatkan nilai dekripsi maka didapatlah output *plaintext*. Proses tersebut dapat dilihat pada Gambar 3.14.



Gambar 3.14. Proses Dekripsi Algoritma RSA

1. Penginputan Data

Setelah mengumpulkan data pasien, dokter, rawat inap pasien, rekam medis dan rawat jalan pasien selanjutnya penginputan data-data yang telah dikumpulkan kedalam program rekam medis.

1. Menjalankan Perangkat Lunak

Setelah pembuatan program penerapan algoritma RSA pada sistem pengamanan data rekam medis dan pengumpulan data selesai, selanjutnya menjalankan program untuk mengetahui program yang dibuat dapat berjalan dengan baik atau tidak.

1. PengujianPerangkat Lunak

Pada tahap ini semua fungsi-fungsi program rekam medis yang telah dibuat harus diuji coba secara menyeluruh, untuk memastikan tidak adanya *bug* atau *error* pada program, sehingga program sesuai dengan yang diharapkan. Penulis menggunakan *Blackbox Testing* untuk digunakan sebagai metode pengujian pada penelitian ini. *Blackbox testing* adalah pengujian yang dilakukan dengan cara mengamati hasil eksekusi melalui data uji dan memeriksa fungsional dari perangkat lunak

1. Kesimpulan

Pada tahapan ini kesimpulan merupakan hasil akhir yang diharapkan mampu menjawab tujuan penelitian yaitu Sistem pengamanan data rekam medis menggunakan algoritma RSA.



Gambar 3.2. *Flowchart* Tahapan Penelitian

**3.9. Hipotesis Penelitian**

Hipotesis yang penulis buat pada penelitian ini adalah bahwa pengamanan *database* rekam medismenggunakan algoritma RSAdapat mencapai hasil yang optimal dan algoritma RSAberhasil mengamankan *database* rekam medis yang bersifat rahasia pada Rumah Sakit Umum Daerah (RSUD) Anutapura Kota Palu.

**3.10. Rencana Jadwal Penelitian**

Rencana jadwal penelitian akan dilaksanakan pada bulan Agustus 2019 dan berakhir pada bulan Januari 2020 dengan jadwal seperti terlihat pada tabel 3.1.

Tabel 3.1. Rencana Jadwal Penelitian

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| No. | Jenis kegiatan | Bulan | | | | | | | | | | | | | | | | | | | | | | | | |
| Agustus  2019 | | | | September  2019 | | | | Oktober  2019 | | | | November  2018 | | | | Desember  2018 | | | | Januari  2018 | | | | |
| 1 | 2 | 3 | 4 | 1 | 2 | 3 | 4 | 1 | 2 | 3 | 4 | 1 | 2 | 3 | 4 | 1 | 2 | 3 | 4 | 1 | 2 | 3 | 4 |
| 1 | Studi Literatur, Identifikasi masalah, Konsultasi dosen pembimbing |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| 2 | Seminar Proposal |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| 3 | Pengumpulan & Analisis Data Variabel dan Perancangan Sistem |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| 4 | Pembuatan Perangkat lunak |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| 5 | Penginputan data |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| 6 | Menjalankan perangkat lunak |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| 7 | Analisa hasil penelitian dan Pengujian perangkat lunak |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| 8 | Seminar Hasil |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| 9 | Skripsi |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |

**BAB IV**

**HASIL DAN PEMBAHASAN**

* 1. **Hasil Penelitian**
     1. **Analisa Sistem**

1. *Diagram* Konteks (DK)

*Diagram* Konteks merupakan data *flow* diagram dengan menggambarkan garis besar operasional sistem. Konteks diagram menggambarkan hubungan sistem dengan entitas-entitas diluar sistem. Skema *Diagram* Konteks Penerapan algoritma RSA (*Rivest-Shamir-Adleman*) pada sistem pengamanan data nilai akademik dapat dilihat pada gambar 4.1.



Gambar 4.1 *Diagram* konteks Penerapan Algoritma RSA (*Rivest-Shamir-Adleman*) Pada Sistem Pengamanan Data Nilai Akademik.

Keterangan gambar 4.1 dapat dilihat pada poin-poin sebagai berikut:

Mahasiswa

Mahasiswa hanya bisa melihat/mencetak transkip nilai/kartu hasil studi.

1. Dosen

Dosen memasukkan nilai akhir mahasiswa menggunakan sistem, serta dapat melihat seluruh nilai mahasiswa yang ada di Program Studi Teknik Informatika, Jurusan Teknologi Informasi, Fakultas Teknik Universitas Tadulako.

1. Admin

Admin bertugas untuk memasukkan data-data mahasiswa, dosen, matakuliah, tahun ajaran dan rekap nilai jika dosen berhalangan untuk mengisi rekap nilai.

1. Data Flow Diagram (DFD)

*Data Flow Diagram* (DFD) sering digunakan untuk menggambarkan suatu sistem yang telah ada atau sistem baru yang akan dikembangkan secara logika tanpa mempertimbangkan lingkungan fisik dimana data disimpan. DFD menggambarkan arus data didalam sistem dengan terstruktur dan jelas. Skema DFD level 1 dan DFD level 2 Penerapan algoritma RSA pada sistem pengamanan data nilai akademik, dapat dilihat masing-masing pada gambar 4.2, gambar 4.3 dan gambar 4.4



Gambar 4.2 DFD level 1 Penerapan Algoritma RSA (*Rivest-Shamir-Adleman*) Pada Sistem Pengamanan Data Nilai Akademik.

Keterangan gambar 4.2 dapat dilihat pada poin-poin berikut:

1. Biodata

Proses ini berfungsi untuk menyimpan data mahasiswa dan dosen yang di masukkan oleh admin. Ketika data-data tersebut tersimpan maka secara otomatis sistem akan membuatkan akun bagi mahasiswa atau dosen yang sudah dimasukkan datanya di *database*. Ketika akun dibuat maka secara otomatis juga password dari akun tersebut akan terenkripsi dengan menggunakan algoritma RSA, dan *key-key* enkripsi dan dekripsinya akan masuk kedalam tabel RSA. Akun tersebut nantinya akan digunakan untuk mengakses Sistem Pengamanan Data Nilai Akademik ini.

1. Kurikulum

Proses ini berfungsi untuk menyimpan data-data matakuliah, tahun ajaran, dan nilai yang di masukkan oleh admin.

1. Rekap Nilai

Pada proses ini data-data dari tabel mahasiswa, nilai, matakuliah, dan tahun ajaran akan di panggil pada proses ini, dimana data-data tersebut akan di tampilkan dalam pilihan *combobox search* sehingga dosen/admin dapat dengan mudah dalam melakukan penginputan nilai akademik.

Setelah nilai akademik dimasukkan oleh admin/dosen maka secara otomatis nilai mahasiswa akan terenkripsi dengan menggunakan algoritma RSA, dan *key-key* enkripsi dan dekripsi akan masuk kedalam tabel RSA.



Gambar 4.3 DFD level 2 Penerapan Algoritma RSA (*Rivest-Shamir-Adleman*) Pada Sistem Pengamanan Data Nilai Akademik.

Keterangan gambar 4.3 dapat dilihat pada poin-poin berikut:

1. Masukkan Data Mahasiswa

Pada proses ini admin wajib memasukkan data-data mahasiswa yang sudah terdaftar menjadi mahasiswa Program Studi Teknik Informaatika, Jurusan Teknologi Informasi, Universitas Tadulako.

1. Enkripsi *Password*

Proses ini dilakukan ketika admin selesai mengisi data mahasiswa/dosen dan meng-klik tombol simpan pada sistem. Ketika admin meng-klik tombol simpan, maka *key-key* yang diperlukan untuk meng-enkripsi *password* akan terbuat dan akan masuk kedalam tabel RSA. Jika yang dimasukkan adalah data mahasiswa maka stambuk dari mahasiswa tersebut akan dijadikan *username* pada *field* tabel akun, dan *password*nya sudah diatur dari sistem dimana *password* tersebut akan dienkripsi dengan menggunakan algoritma RSA sebelum dimasukkan kedalam tabel akun. Kemudian jika data dosen yang dimasukkan oleh admin maka *username* dan *password*nya akan diatur secara otomatis oleh sistem dan *password* dari dosen tersebut akan masuk proses enkripsi terlebih dahulu sebelum masuk ke dalam tabel akun dengan data-data lainnya.

1. Masukkan Data Dosen

Pada proses ini admin wajib memasukkan data-data dosen yang mengajar di Program Studi Teknik Informaatika, Jurusan Teknologi Informasi, Universitas Tadulako.



Gambar 4.4 DFD level 2 Penerapan Algoritma RSA (*Rivest-Shamir-Adleman*) Pada Sistem Pengamanan Data Nilai Akademik.

1. Masukkan Nilai Akhir

Pada proses ini data-data yang diperlukan untuk menginputkan nilai akan ditampilkan pada *form* penginputan nilai seperti nama matakuliah dan kode matakuliah yang diambil dari tabel matakuliah, nama mahasiswa dan stambuk yang diambil dari tabel mahasiswa, tahun ajaran yang diambil dari tabel tahun ajaran, dan nilai yang diambil dari tabel nilai. Sehingga membantu admin/dosen dalam pengimputan nilai.

1. Enkripsi Nilai

Setelah memasukkan nilai akhir selesai, maka proses ini akan berjalan dimana nilai yang dimasukkan oleh admin/dosen akan di enkripsi dengan menggunakan algoritma RSA dan *key* pembangkit nilai akan secara otomatis masuk kedalam tabel rsa, dan data-data nilai akhir seperti kode matakuliah, tahun ajaran, stambuk, nilai yang sudah ter-enkripsi, dan id rsa akan masuk kedalam tabel rekap nilai.

1. Dekripsi Nilai

Proses ini akan dijalankan ketika ingin menampilkan nilai di sistem, dimana nilai yang ter-enkripsi sebelumnya akan masuk kedalam proses dekripsi.

1. Join Tabel

Pada proses ini nama matakuliah dan sks akan dipanggil dari tabel matakuliah yang sesuai dengan kode matakuliah, kemudian nama mahasiswa akan di panggil dari tabel mahasiswa yang sesuai dengan stambuk. Sehingga data-data yang tampil ke mahasiswa yaitu nama mahasiswa, stambuk, nama matakuliah, kode matakuliah, sks matakuliah, nilai, dan tahun ajaran.

1. *Use Case Diagram*

*Use Case Diagram* adalah deskripsi fungsi dari sebuah sistem dari perspektif pengguna. *Use case* bekerja dengan cara mendeskripsikan tipikal interaksi antar pengguna (yang disebut dengan *actor*) sebuah sistem dengan sistemnya sendiri melalui sebuah cerita bagaimana sebuah sistem dipakai. Skema *Use Case Diagram* Penerapan Algoritma RSA (*Rivest-Shamir-Adleman*) Pada Sistem Pengamanan Data Nilai Akademik dapat dilihat pada gambar 4.5.



Gambar 4.5 *Use Case Diagram* Penerapan Algoritma RSA (*Rivest-Shamir-Adleman*) Pada Sistem Pengamanan Data Nilai Akademik.

Keterangan gambar 4.5 dapat dilihat sebagai berikut:

* + - * 1. *Login*

Semua pengguna sistem wajib memasukkan *username, password* dan kunci rsa.

Dimana *username, password* dan kunci rsa akan diverifikasi, jika benar maka dapat *login* ke sistem, jika salah maka akan muncul pesan bahwa *username/password*/kunci tersebut salah.

* + - * 1. Data Mahasiswa

Admin wajib memassukkan data-data mahasiswa yang telah terdaftar menjadi mahasiswa Program Studi Teknik Informaatika, Jurusan Teknologi Informasi, Universitas Tadulako. Admin dapat melihat data mahasiswa, mengubah data mahasiswa dan menghapus data mahasiswa.

Mahasiswa dapat melihat data mahasiswa yang bersangkutan yang sudah di masukkan oleh admin.

* + - * 1. Data Dosen

Admin wajib memasukkan data-data dosen yang mengajar di Program Studi Teknik Informaatika, Jurusan Teknologi Informasi, Universitas Tadulako. Admin dapat melihat data dosen, mengubah data dosen, dan menghapus data dosen.

* + - * 1. Data Matakuliah

Admin wajib memasukkan matakuliah apa saja yang akan diajarkan di Program Studi Teknik Informaatika, Jurusan Teknologi Informasi, Universitas Tadulako. Admin juga dapat melihat data matakuliah, mengubah data matakuliah dan menghapus data matakuliah.

* + - * 1. Data Akun

Admin dapat melihat semua pengguna sistem, serta dapat mengubah data akun, menambahkan akun level admin atau dosen, mengganti *password* pengguna, dan menghapus akun pengguna.

* + - * 1. Data Tahun Ajaran

Admin wajib memasukkan data tahun ajaran kedalam sistem. Admin juga dapat melihat tahun ajaran, mengubah dan menghapus data tahun ajaran.

* + - * 1. Data Nilai

Wajib memasukkan data nilai, untuk ditampilkan nantinya pada form penginputan nilai akhir.

* + - * 1. Nilai Akhir

Pada proses ini admin atau dosen dapat memasukkan nilai-nilai mahasiswa sesuai dengan matakuliah yang diajarkan oleh dosen yang bersangkutan. Dosen atau admin juga dapat melihat nilai-nilai mahasiswa, serta dapat mengubah dan menghapus nilai tersebut.

1. *Entity Relationship Diagram* (ERD)

*Entity Relationship Diagram* (ERD) memiliki dua komponen utama yaitu Entitas (*Entity*) dan Relasi (*Relational*). Kedua komponen ini mesing-masing dilengkapi dengan sejumlah atribut yang mempresentasikan seluruh fakta yang ada di dunia nyata. Skema *Entity Relationship Diagram* sistem pengamanan data nilai akademik dapat dilihat pada gambar 4.6.



Gambar 4.6 *Entity Relationship Diagram* (ERD) Penerapan Algoritma RSA (*Rivest-Shamir-Adleman*) Pada Sistem Pengamanan Data Nilai Akademik.

* + 1. **Implementasi Sistem**
       1. **Implementasi Perangkat Keras dan Perangkat Lunak**

Implementasi perangkat keras yang digunakan untuk membangun sistem pengamanan data nilai akademik yaitu:

*Asus* X450JB *Processor Intel Core i7, RAM 8 GB,* monitor dengan resolusi 1366x768. Untuk implementasi perangkat lunak digunakan bahasa pemrograman *PHP*. Media yang digunakan sebagai editor *PHP* yaitu *Sublime Text 3,* kemudian *Xampp Control Panel* yang fungsinya sebagai server yang berdiri sendiri (localhost).

* + - 1. **Implementasi Basis Data**

*MySQL* digunakan sebagai basis datapada sistem pengamanan data nilai akademik. Tabel-tabel yang ada dalam sistem pengamanan data nilai akademik sebagai berikut:

1. Tabel Akun

Tabel akun yang dapat dilihat pada tabel 4.1 digunakan untuk menyimpan data pengguna

Tabel 4.1 Akun

|  |  |  |  |
| --- | --- | --- | --- |
| ***Field*** | ***Type*** | ***Length/Values*** | ***Index*** |
| Id\_akun | int | 11 | Primary |
| *Username* | varchar | 15 | - |
| *Password* | text | - | - |
| Nama | varchar | 50 | - |
| Email | varchar | 50 | - |
| Status | varchar | 25 | - |
| Level | varchar | 25 | - |

1. Tabel Dosen

Tabel dosen dapat dilihat pada tabel 4.2 digunakan untuk menyimpan data-data dosen.

Tabel 4.2 Dosen

|  |  |  |  |
| --- | --- | --- | --- |
| ***Field*** | ***Type*** | ***Length/Values*** | ***Index*** |
| Id\_dosen | Int | 11 | primary |
| Nip | Varchar | 30 | - |
| Nama | Varchar | 75 | - |
| Jenis\_kelamin | Varchar | 15 | - |
| No\_hp | Varchar | 12 | - |
| Email | Varchar | 50 | - |
| Status | Varchar | 25 | - |
| Alamat | Text | - | - |

1. Tabel Mahasiswa

Tabel mahasiswa dapat dilihat pada tabel 4.3 digunakan untuk menyimpan data-data mahasiswa.

Tabel 4.3 Mahasiswa

|  |  |  |  |
| --- | --- | --- | --- |
| ***Field*** | ***Type*** | ***Length/Values*** | ***Index*** |
| Id | int | 11 | Primary |
| Stambuk | Varchar | 12 | - |
| nama | Varchar | 50 | - |
| Jenis\_kelamin | Varchar | 10 | - |
| No\_hp | Varchar | 12 | - |
| email | Varchar | 50 | - |
| Status | Varchar | 12 | - |
| angkatan | Varchar | 5 | - |

1. Tabel Matakuliah

Tabel matakuliah dapat dilihat pada tabel 4.4 tabel matakuliah digunakan untuk menyimpan matakuliah apa saja yang diajarkan di Program Studi Teknik Informaatika, Jurusan Teknologi Informasi, Universitas Tadulako.

Tabel 4.4 Matakuliah

|  |  |  |  |
| --- | --- | --- | --- |
| ***Field*** | ***Type*** | ***Length/Values*** | ***Index*** |
| Id | Int | 11 | primary |
| Kmk | Varchar | 15 | - |
| Nama\_matkul | Varchar | 100 | - |
| Sks | Int | 11 | - |

1. Tabel Nilai

Tabel nilai dapat dilihat pada tabel 4.5 digunakan untuk menyimpan yang digunakan nantinya pada saat penginputan nilai.

Tabel 4.5 Nilai

|  |  |  |  |
| --- | --- | --- | --- |
| ***Field*** | ***Type*** | ***Length/Values*** | ***Index*** |
| Id | int | 11 | PRIMARY |
| Huruf | Char | 3 | - |
| Angka | Float | - | - |

1. Tabel Rekap Nilai

Tabel nilai dapat dilihat pada tabel 4.6 digunakan untuk menyimpan data-data rekap nilai mahasiswa yang sudah dimasukkan nilai akademiknya.

Tabel 4.6 Rekap Nilai

|  |  |  |  |
| --- | --- | --- | --- |
| ***Field*** | ***Type*** | ***Length/Values*** | ***Index*** |
| id\_rekap | Int | 11 | primary |
| Id\_matakuliah | Varchar | 15 | - |
| Id\_thn\_ajaran | Int | 11 | - |
| Stambuk | Varchar | 15 | - |
| nilai | Varchar | 15 | - |
| Id\_Rsa | Varchar | 15 | - |

1. Tabel RSA

Tabel rsa dapat dilihat pada tabel 4.7 digunakan untuk menyimpan kunci-kunci untuk meng-enkripsi nilai dan sekaligus dekripsi..

Tabel 4.7 RSA

|  |  |  |  |
| --- | --- | --- | --- |
| ***Field*** | ***Type*** | ***Length/Values*** | ***Index*** |
| id\_rsa | Int | 11 | Primary |
| Key\_p | Int | 11 | - |
| Key\_q | Int | 11 | - |
| Key\_e | Int | 11 | - |
| Key\_n | Int | 11 | - |
| Key\_enkrip | Int | 11 | - |
| Key\_dekrip | Int | 11 | - |

1. Tabel Tahun Ajaran

Tabel tahun ajaran yang dapat dilihat pada tabel 4.8 digunakan untuk tahun-tahun ajaran.

Tabel 4.8 Tahun Ajaran

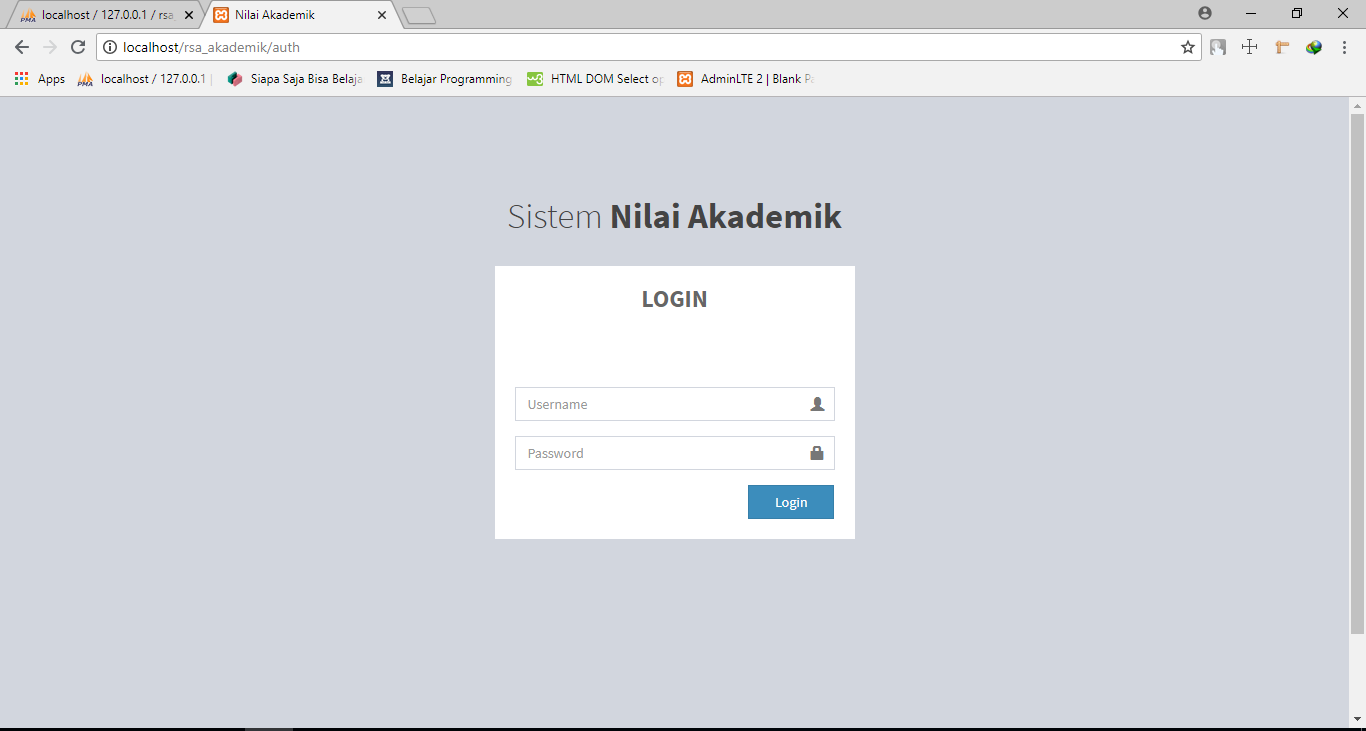
|  |  |  |  |
| --- | --- | --- | --- |
| ***Field*** | ***Type*** | ***Length/Values*** | ***Index*** |
| id\_thn\_ajaran | Int | 11 | Primary |
| Thn\_ajaran | Int | 11 | - |
| deskripsi | Varchar | 50 | - |

* + - 1. **Implementasi *Input***

Pada sistem pengamanan data nilai akademik, terdapat beberapa *form* untuk memasukan data, antara lain sebagai berikut:

1. Halaman *Login*

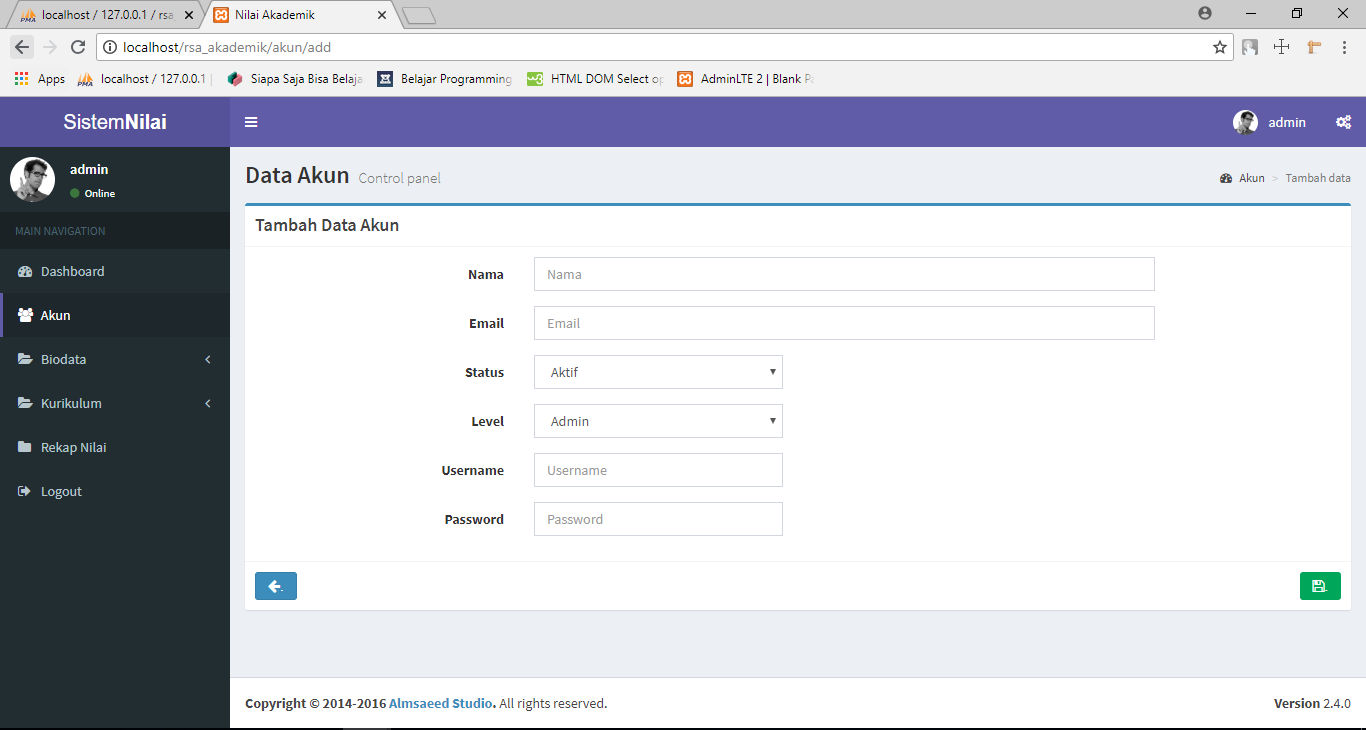
Halamanini digunakan oleh admin, dosendanmahasiswa*,* halaman ini berguna sebagai keamanan untuk masuk ke dalam sistem. Halaman *login* dapat dilihat pada gambar 4.7.



Gambar 4.7 Halaman *Login*

1. Halaman Tambah Akun

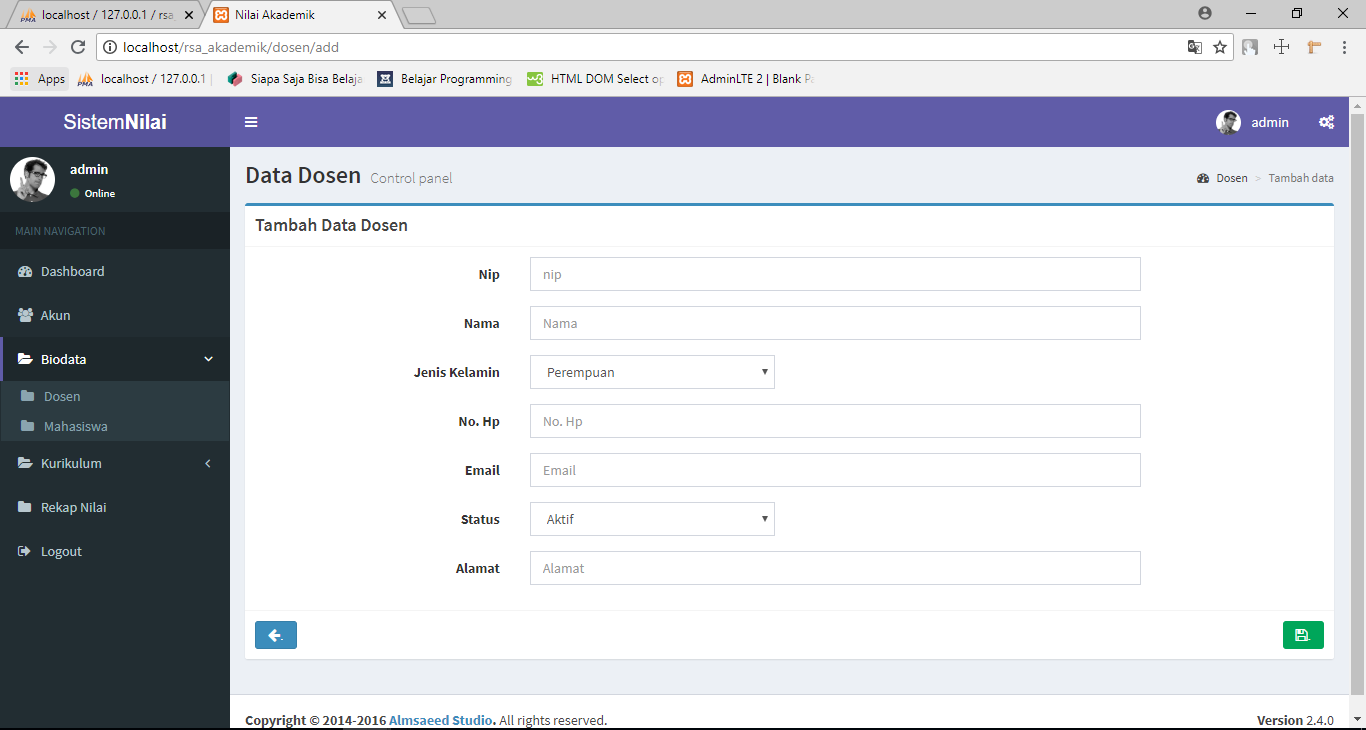
Halamanini digunakan oleh admin*,* untuk menambahkan akun pengguna. Halaman tambah akun dapat dilihat pada gambar 4.8.



Gambar 4.8. Halaman Tambah Akun.

1. Halaman Tambah Dosen

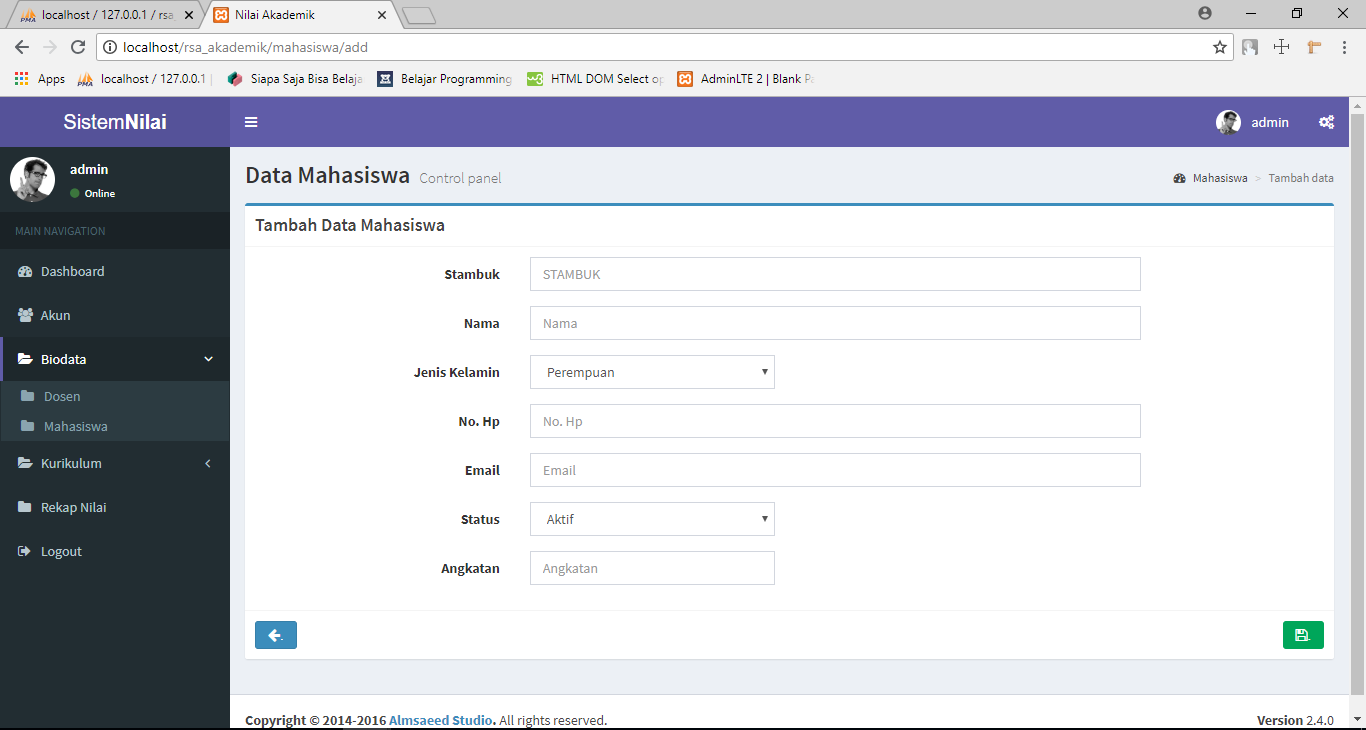
Halaman tambah dosen digunakan oleh *admin* untuk menambah data-data dosen. Halaman tambah dosen dapat dilihat pada gambar 4.9



Gambar 4.9 Halaman TambahDosen

1. Halaman Tambah Mahasiswa

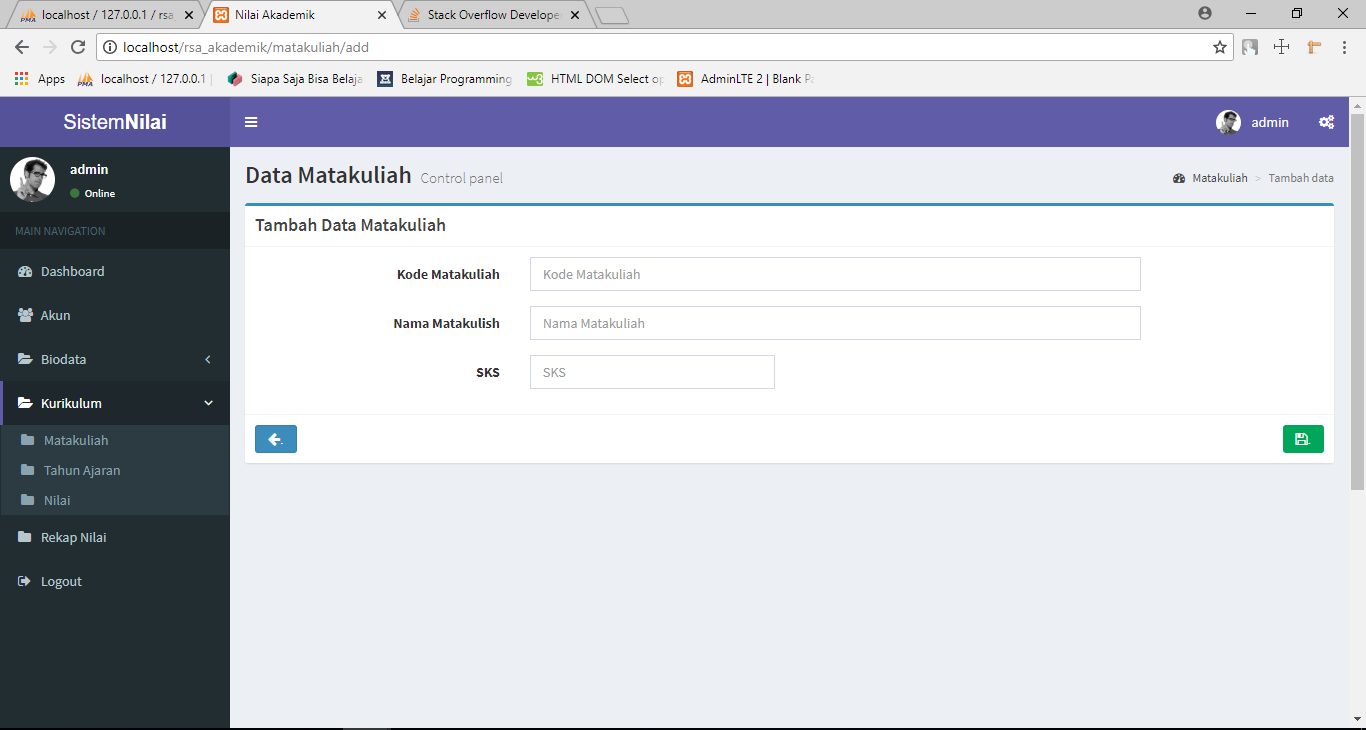
Halaman tambah mahasiswa digunakan oleh admin untuk menambahkan data-data mahasiswa. Halaman tambah mahasisa dapat dilihat pada gambar 4.10



Gambar 4.10 Halaman Tambah Mahasiswa

1. Halaman Tambah Matakuliah

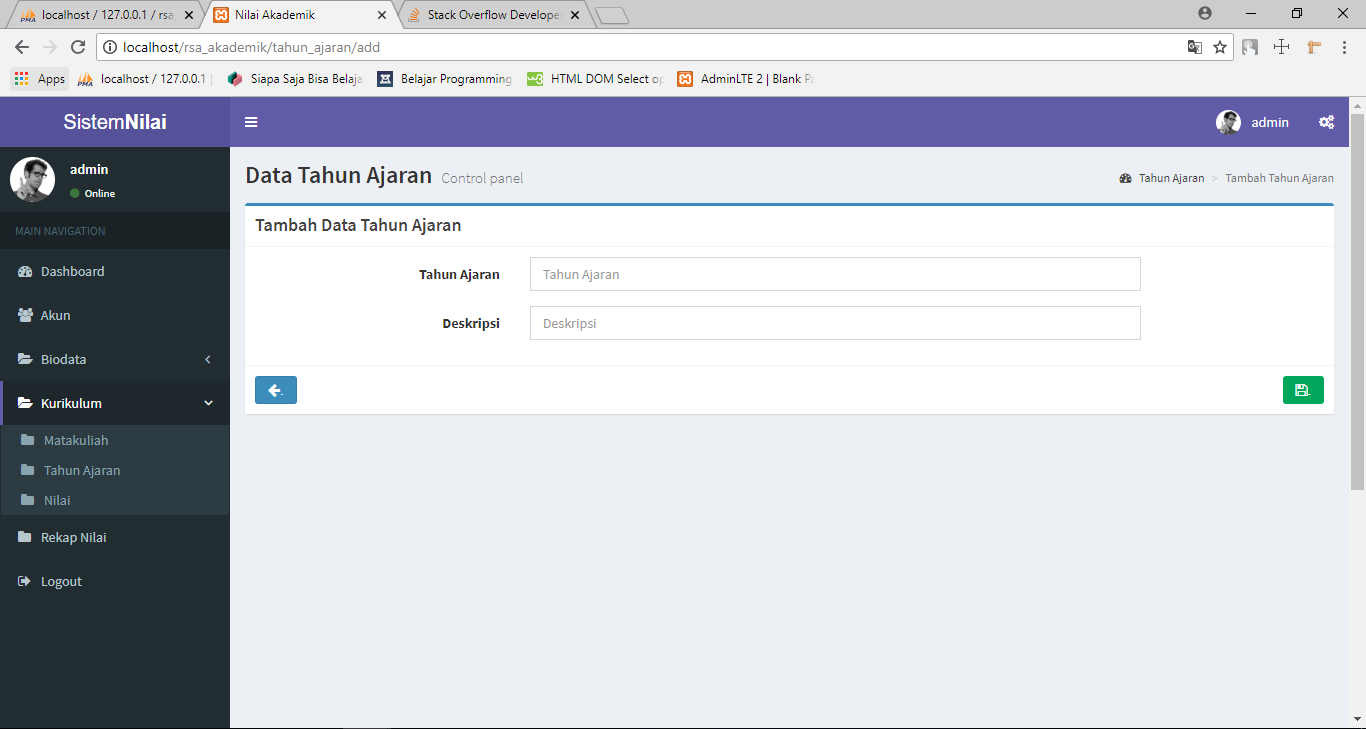
Halaman tambah matakuliah digunakan oleh admin untuk menambah matakuliah baru. Halaman tambah matakuliah dapat dilihat pada gambar 4.11



Gambar 4.11 Halaman Tambah Matakuliah

1. Halaman Tambah Tahun Ajaran

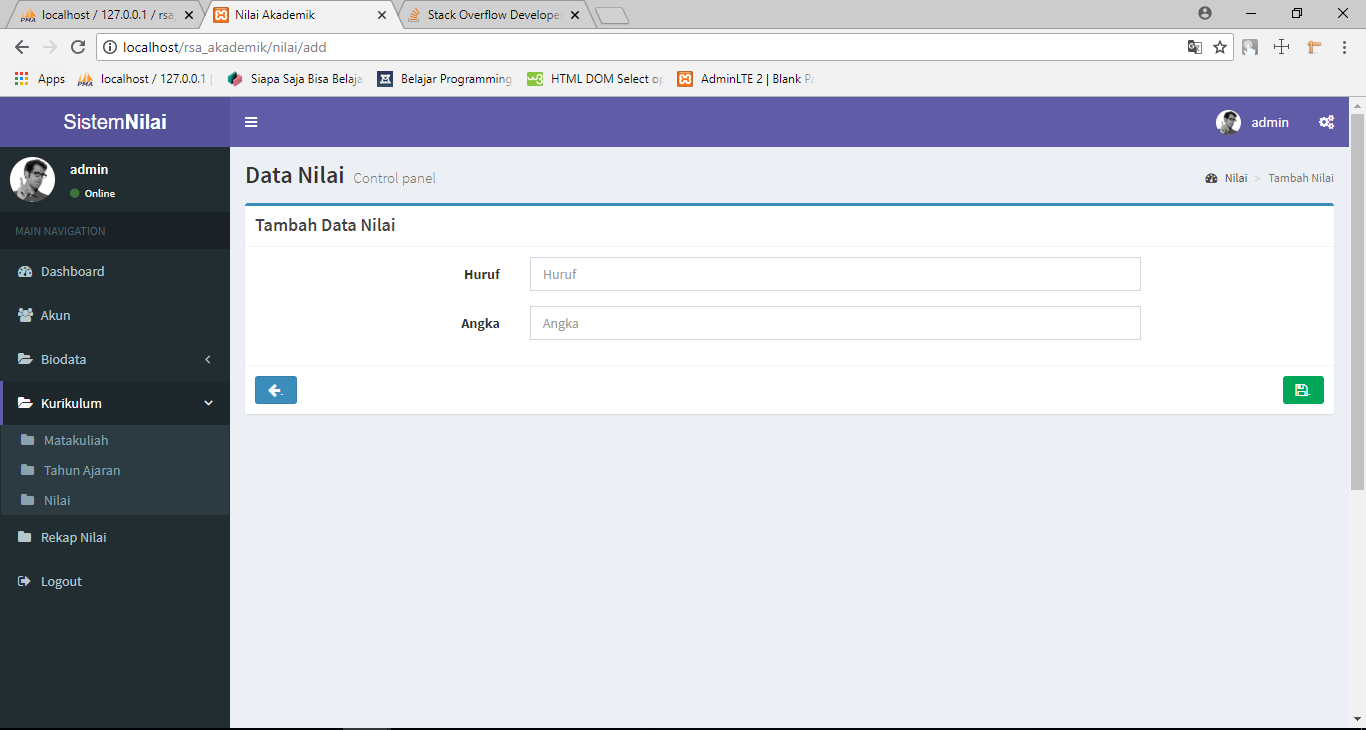
Halaman ini digunakan untuk menambahkan tahun ajaran. Halaman tambah tahun ajarandapat dilihat pada gambar 4.12



Gambar 4.12Halaman Tambah Tahun Ajaran

1. Halaman Tambah Nilai

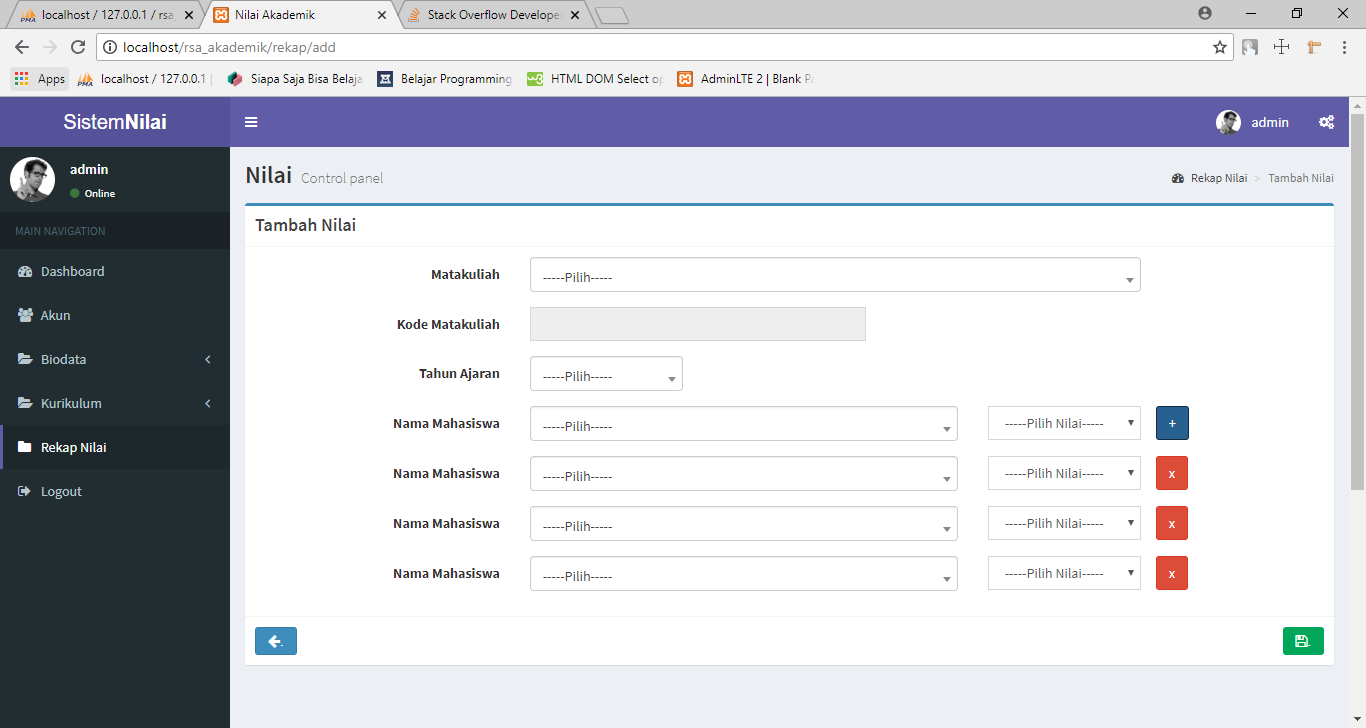
Halaman tambah nilai digunakan oleh admin untuk menambahkan daftar nilai seperti A,B,C,D,E dan sebagainya. Halaman tambah nilai dapat dilihat pada gambar 4.13



Gambar 4.13 Halaman Tambah Nilai

1. Halaman Tambah Nilai Akhir

Halaman tambah nilai akhir digunakan untuk menambahkan nilai akhir pada masing-masing mahasiswa yang bersangkutan. Halaman tambah nilai akhirdapat dilihat pada gambar 4.14



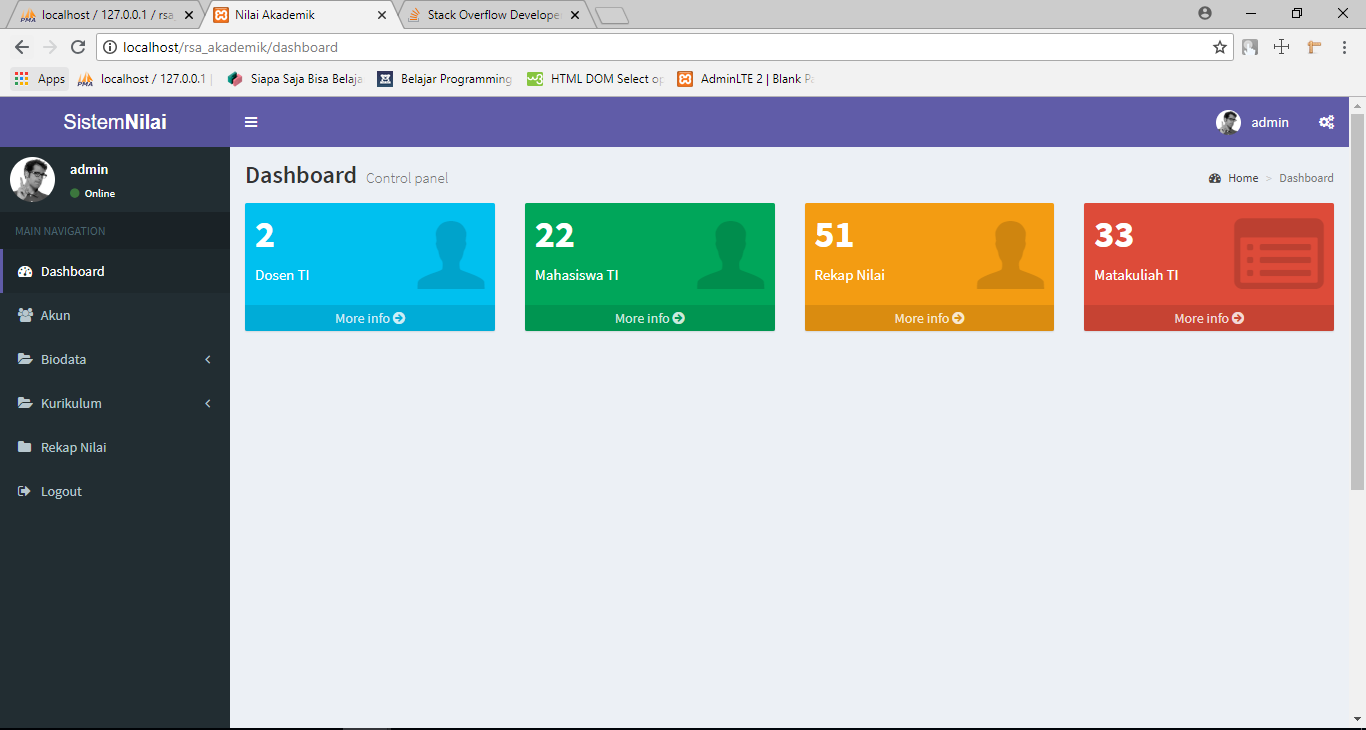
Gambar 4.14 Halaman Tambah Nilai Akhir

* + - 1. **Implementasi *Output***

Pada sistem pengamanan data nilai akademik, terdapat beberapa *form* untuk menampilkan data, antara lain sebagai berikut:

HalamanUtama Admin dan Dosen

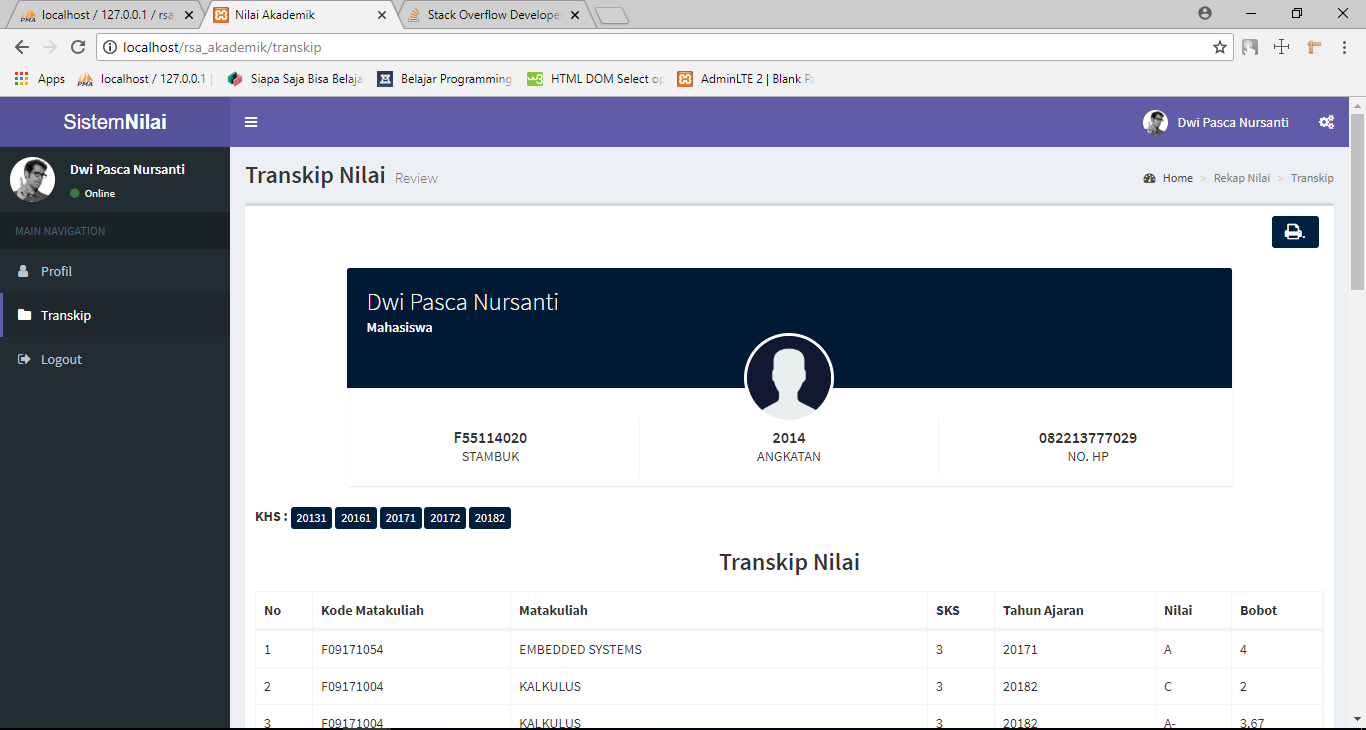
Halaman ini adalah tampilam utama saatpengguna *(*admin, dosen*)* berhasil *login,* fungsi dari halaman utama yaitu melihat jumlah dosen yang mengajar, jumlah mahasiswa, jumlah matakuliah dan jumlah rekap nilai yang sudah ada. Halamanutama dapat dilihat pada gambar 4.15



Gambar 4.15 HalamanAdmin dan Dosen

HalamanUtama Mahasiswa

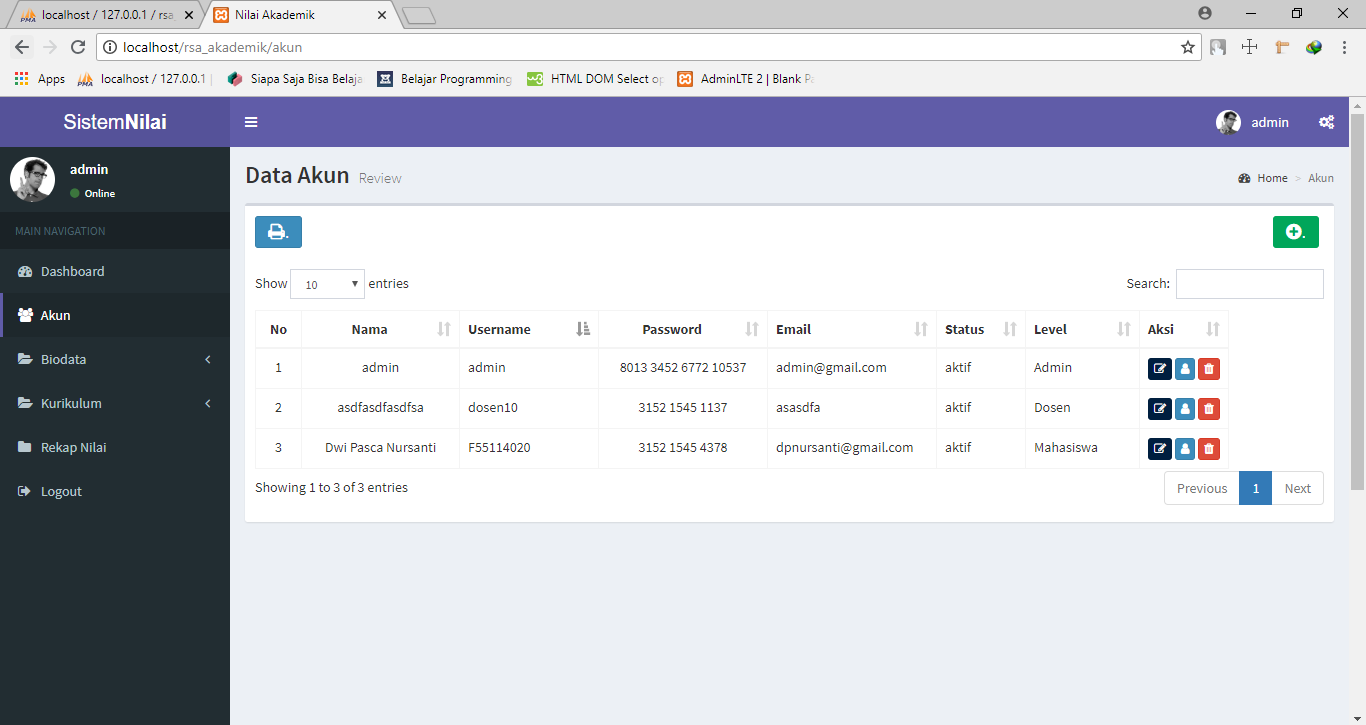
Halaman ini adalah tampilam utama saatpengguna(mahasiswa) berhasil *login,* halaman ini berfungsi untuk melihat nilai-nilai yang sudah dimasukkan oleh dosen yang mengajar mahasiswa tersebut. Halamanini dapat dilihat pada gambar 4.16



Gambar 4.16 HalamanUtama Mahasiswa

HalamanDetail Akun

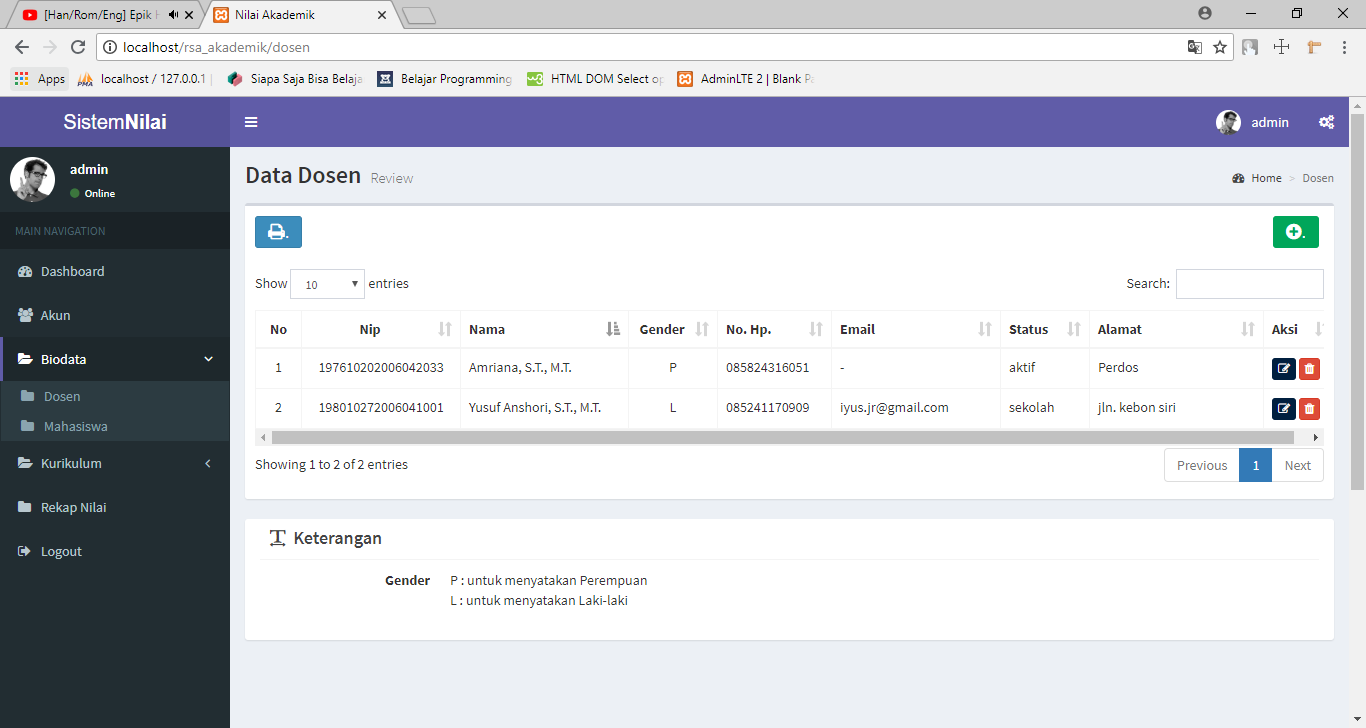
Halaman ini berfungsi melihat semua data akun pengguna. Halmandetail akundapat dilihat pada gambar 4.17



Gambar 4.17 HalamanDetail Akun

HalamanDetail Dosen

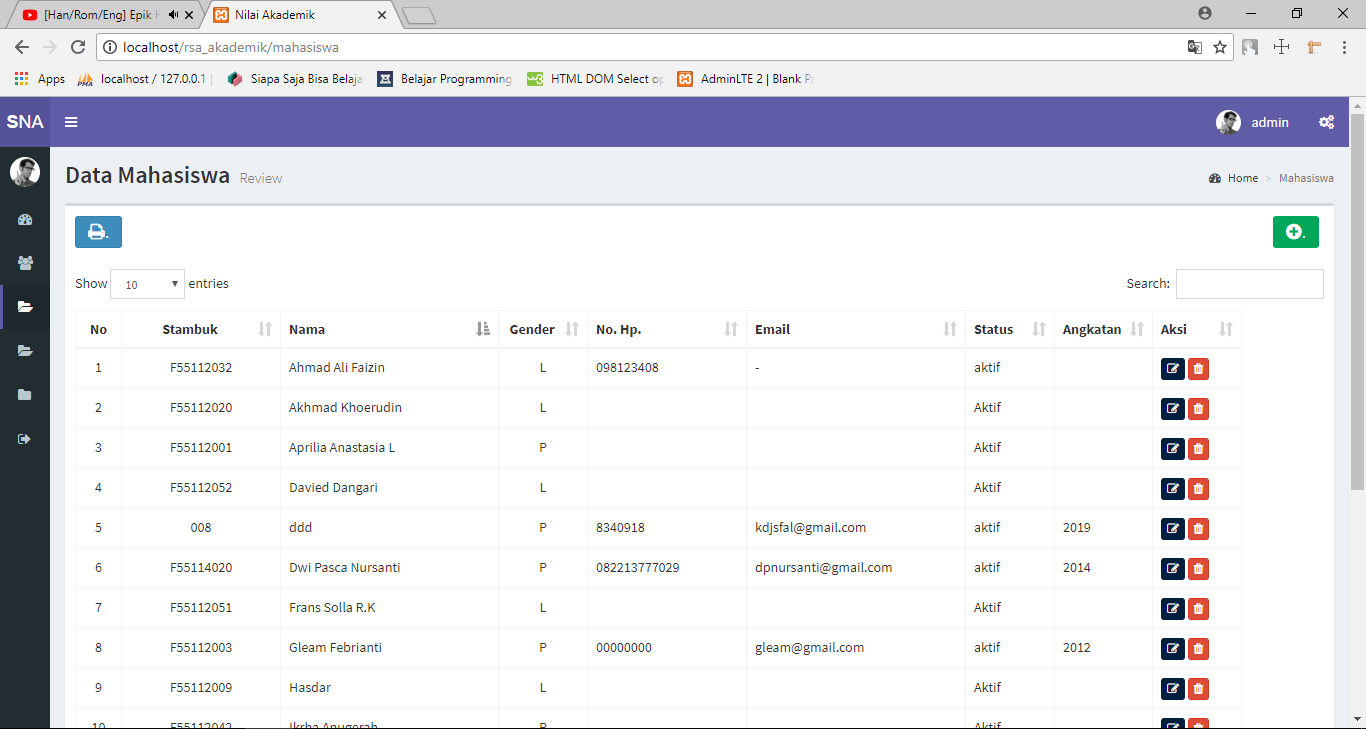
Halaman ini berfungsi melihat semua data-data dosen. Halaman detail dosen dapat dilihat pada gambar 4.18



Gambar 4.18 HalamanDetail Dosen

HalamanDetail Mahasiswa

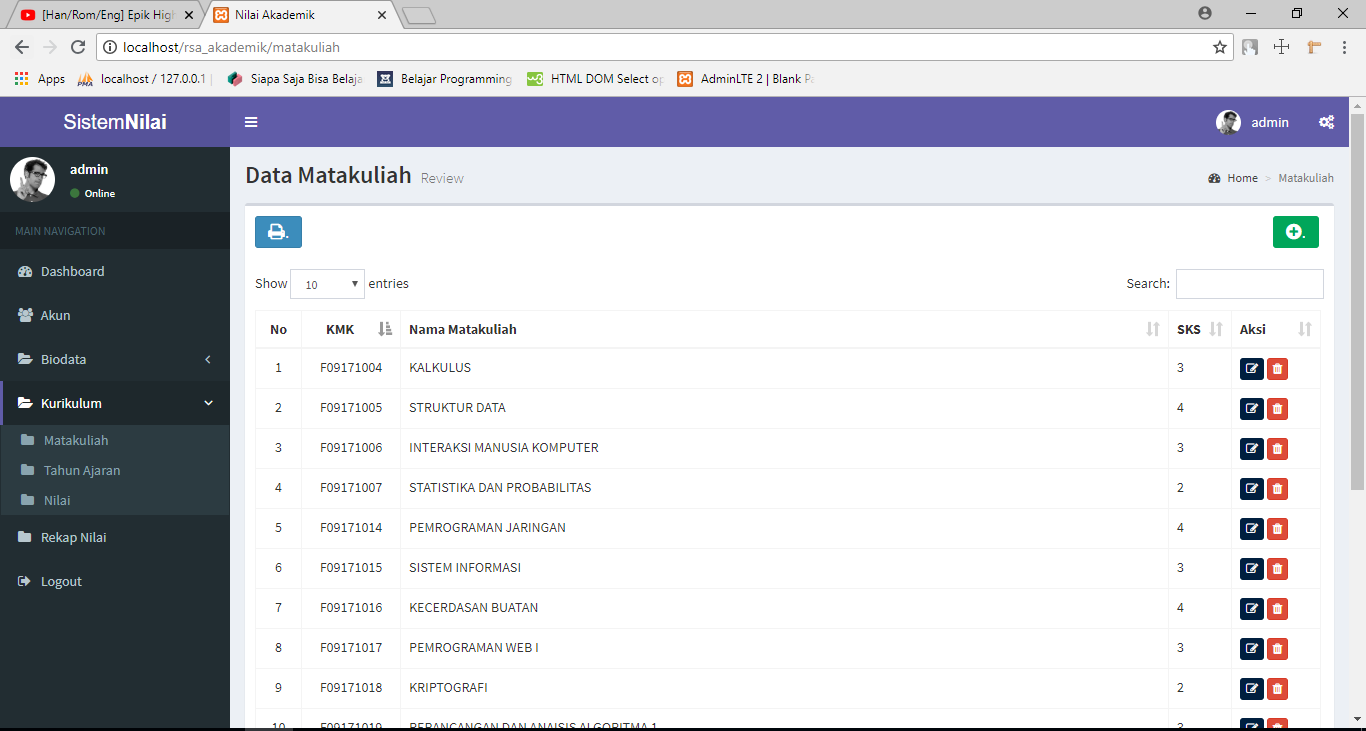
Halaman ini berfungsi melihat data-data mahasiswa. Halaman detail mahasiswa dapat dilihat pada gambar 4.19



Gambar 4.19 HalamanDetail Mahasiswa

HalamanDetail Matakuliah

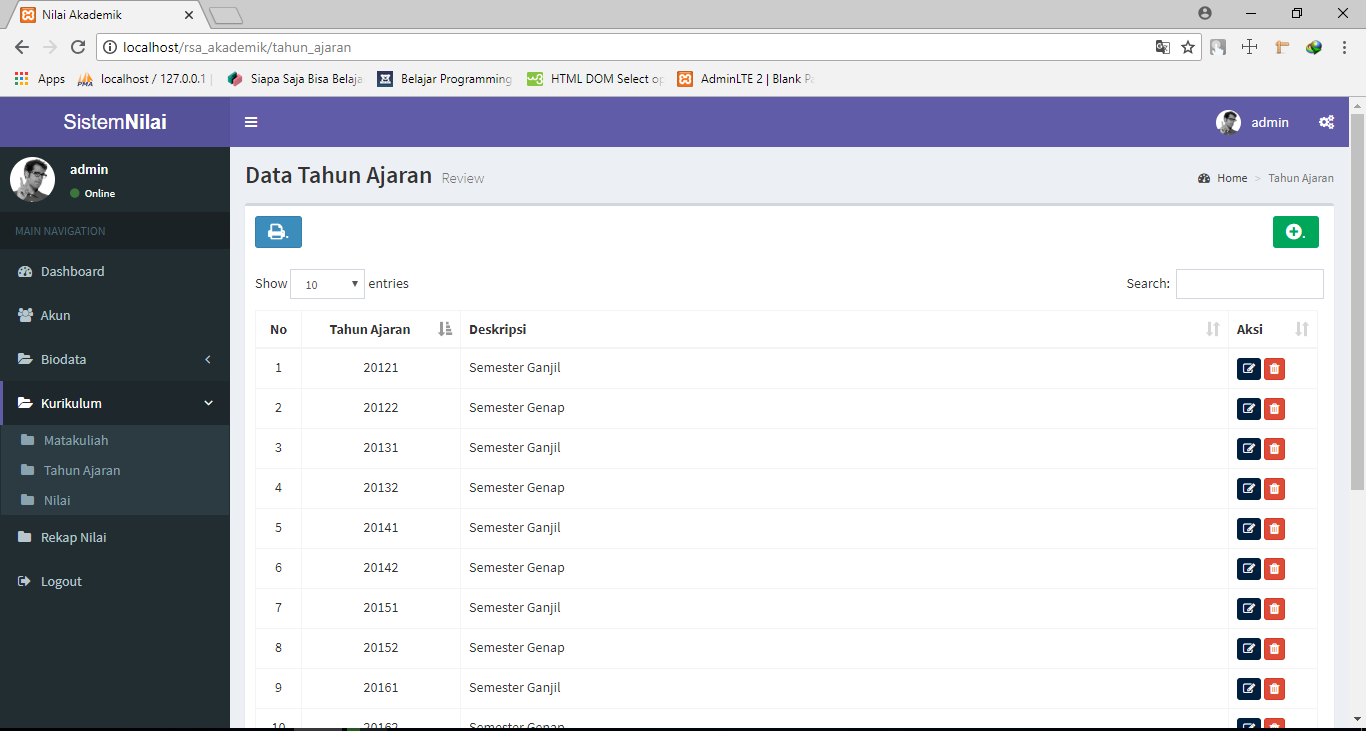
Halaman ini berfungsi untuk melihat matakuliah apa saja yang diajarkan di Program Studi Teknik Informatika Jurusan Teknologi Informasi Fakultas Teknik Universitas Tadulako. Halaman detail matakuliah dapat dilihat pada gambar 4.20



Gambar 4.20 HalamanDetail Mtakuliah

Halaman Detail Tahun Ajaran

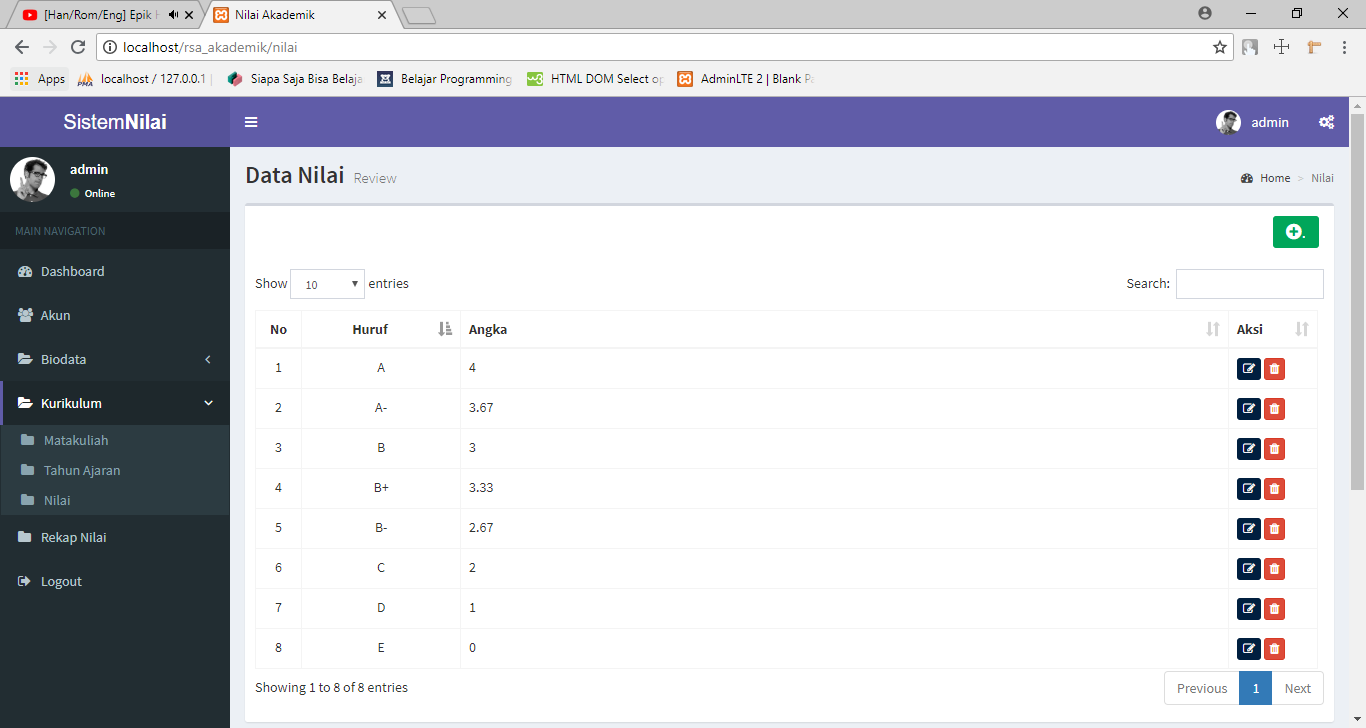
Halaman ini berfungsi untuk melihat tahun ajaran yang ada di Program Studi Teknik Informatika, Jurusan Teknologi Informasi, Fakultas Teknik, Universitas Tadulako. Halaman detail tahun ajaran dapat dilihat pada gambar 4.21



Gambar 4.21 HalamanDetail Tahun Ajaran

Halaman Detail Nilai

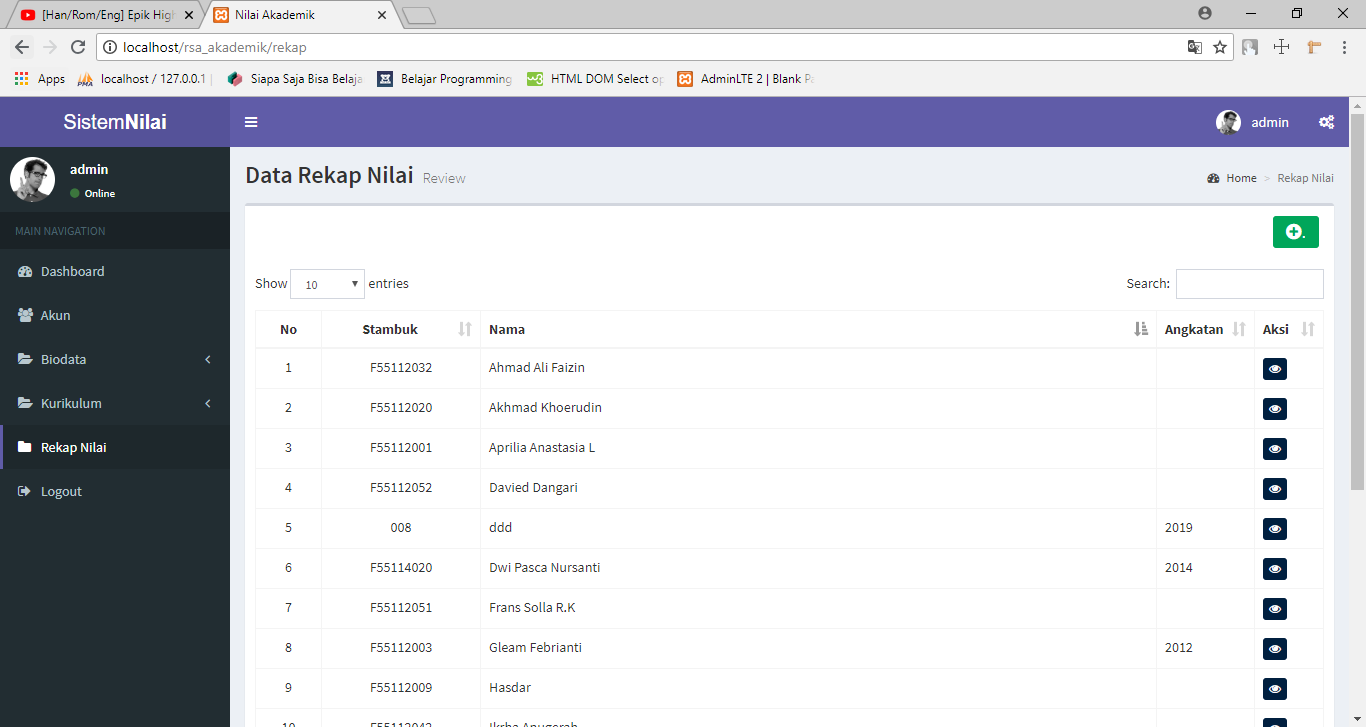
Halaman ini berfungsi melihat data nilai. Halaman detail nilai dapat dilihat pada gambar 4.22



Gambar 4.22 HalamanDetail Nilai

Halaman *List* Mahasiswa Rekap Nilai

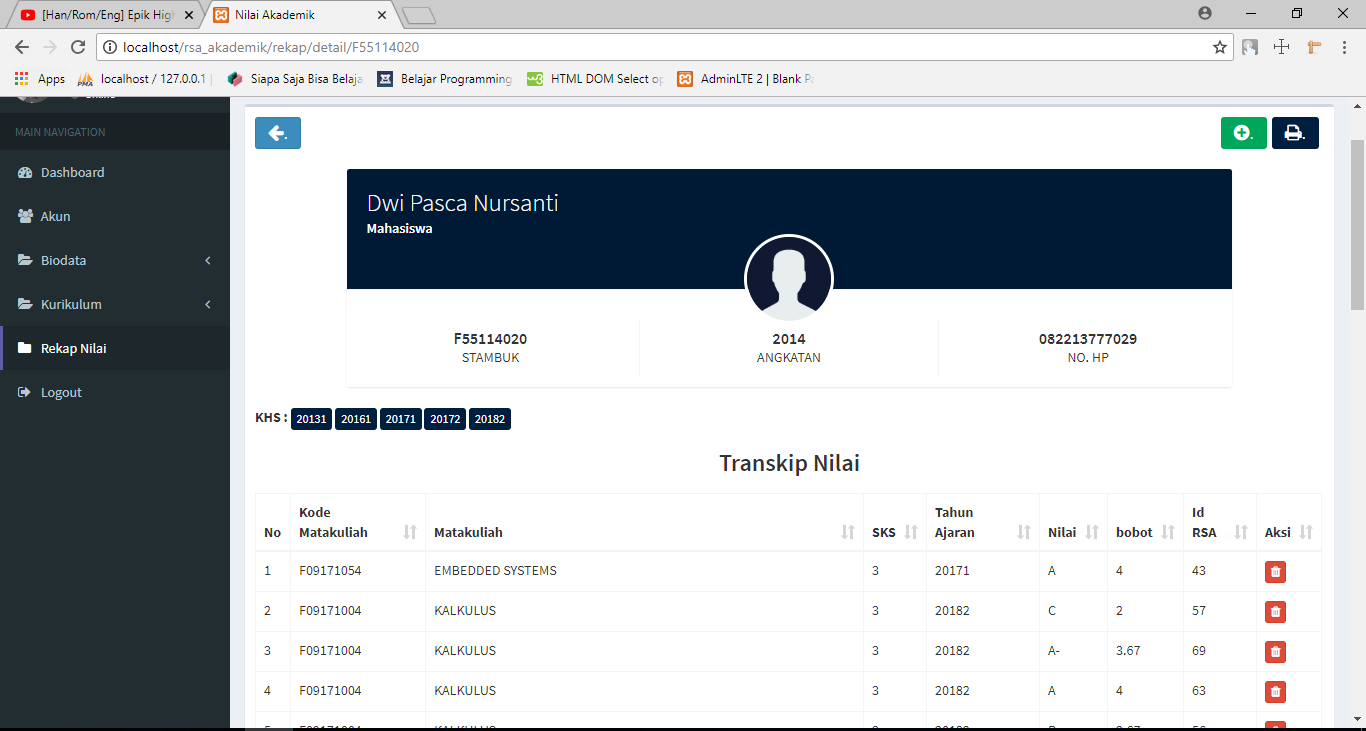
Halaman ini berfungsi melihat mahasiswa-mahasiswa yang memiliki rekap nilai. Halaman *list* mahasiswa rekap nilai dapat dilihat pada gambar 4.23



Gambar 4.23 Halaman *list* mahasiswa rekap nilai

Halaman Transkip Nilai dari sisi Admin

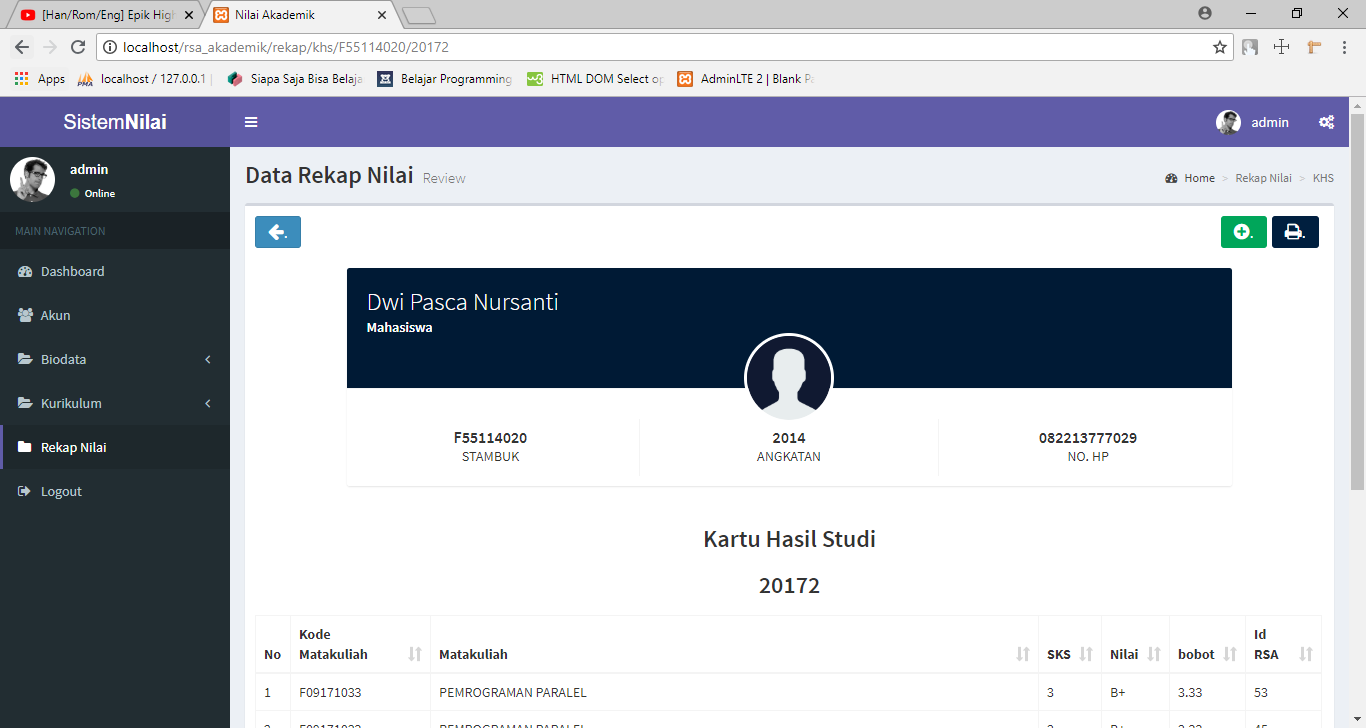
Halaman ini berfungsi nilai-nilai per-mahasiswa. Halaman ini dapat dilihat pada gambar 4.24



Gambar 4.24 Halamantranskip nilai dari sisi admin

Halaman Kartu Hasil Studi (KHS)

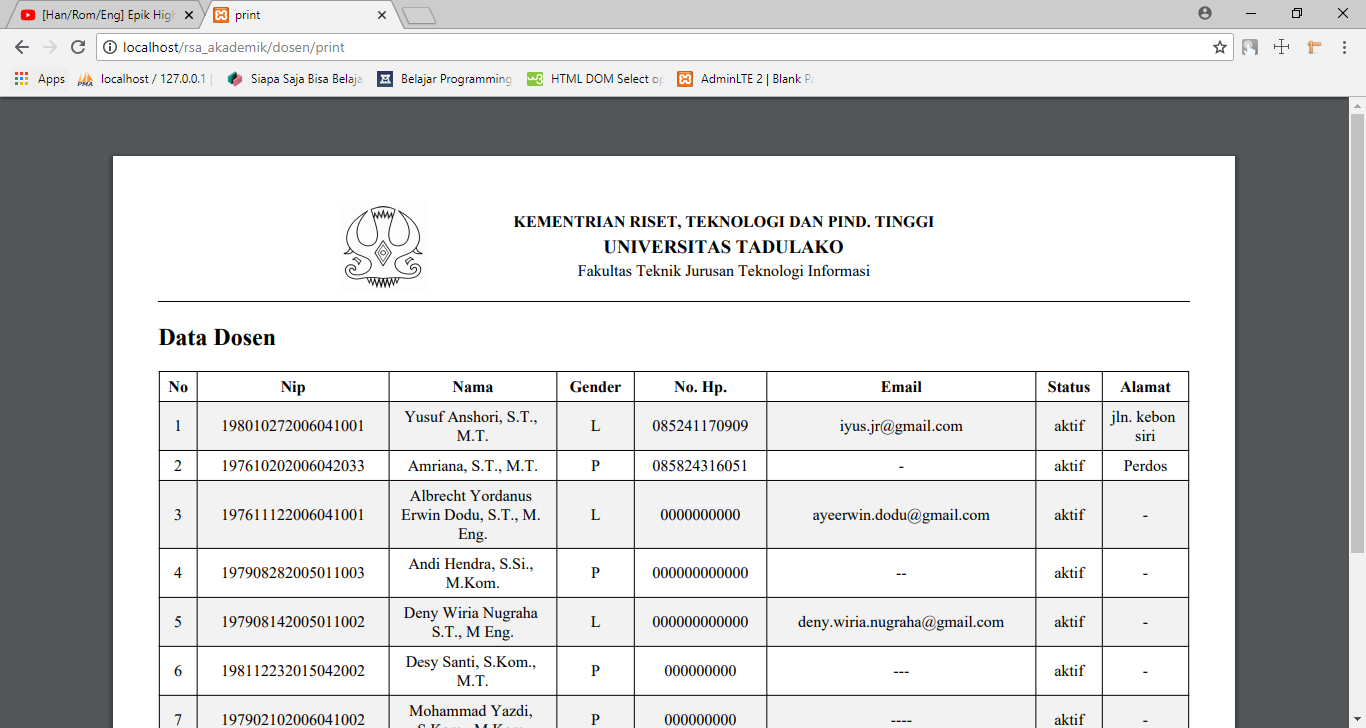
Halaman ini berfungsi untuk menampilkan nilai-nilai mahasiswa dalam satu semester. Halaman ini dapat dilihat pada gambar 4.25



Gambar 4.25 Halaman Kartu Hasil Studi (KHS)

Halaman Laporan Data Dosen

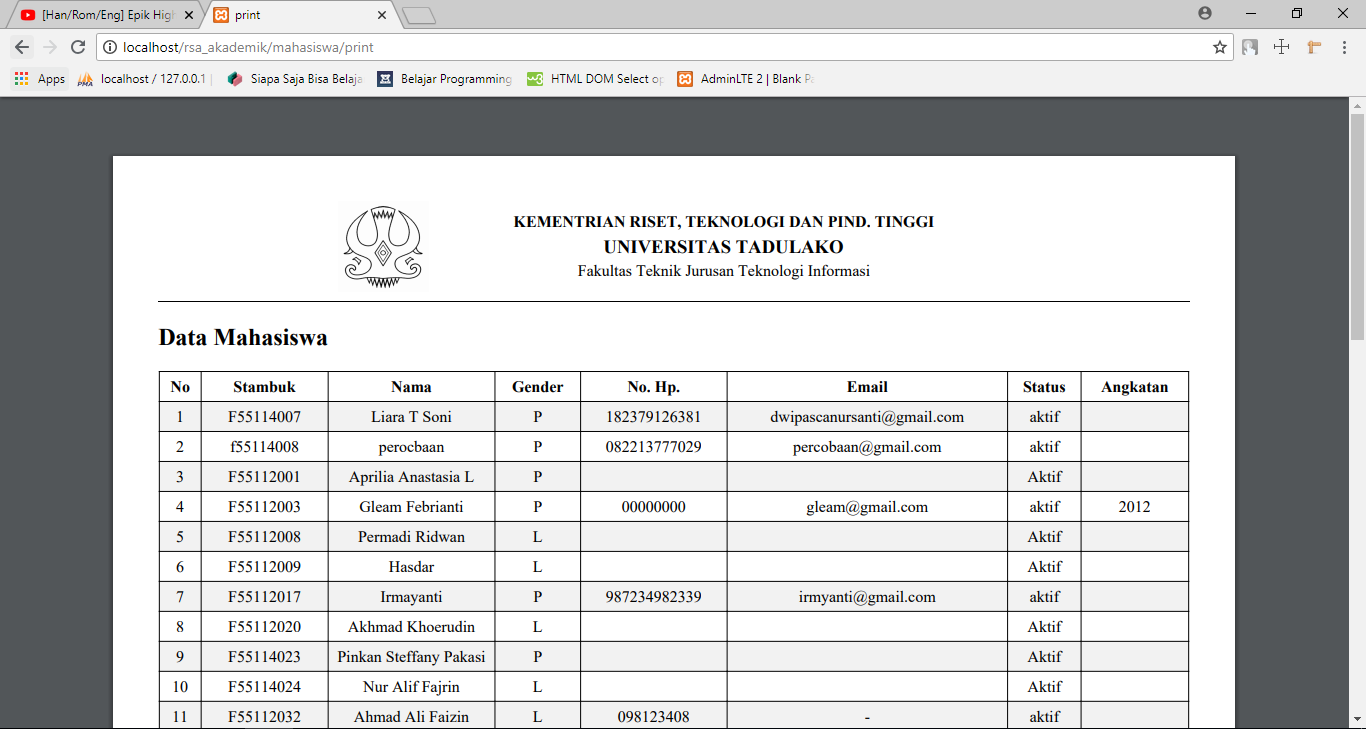
Halaman ini berfungsi untuk menampilkan laporan data-data dosen. Halaman ini dapat dilihat pada gambar 4.26



Gambar 4.26 Halaman Laporan Data Dosen

Halaman Laporan Data Mahasiswa

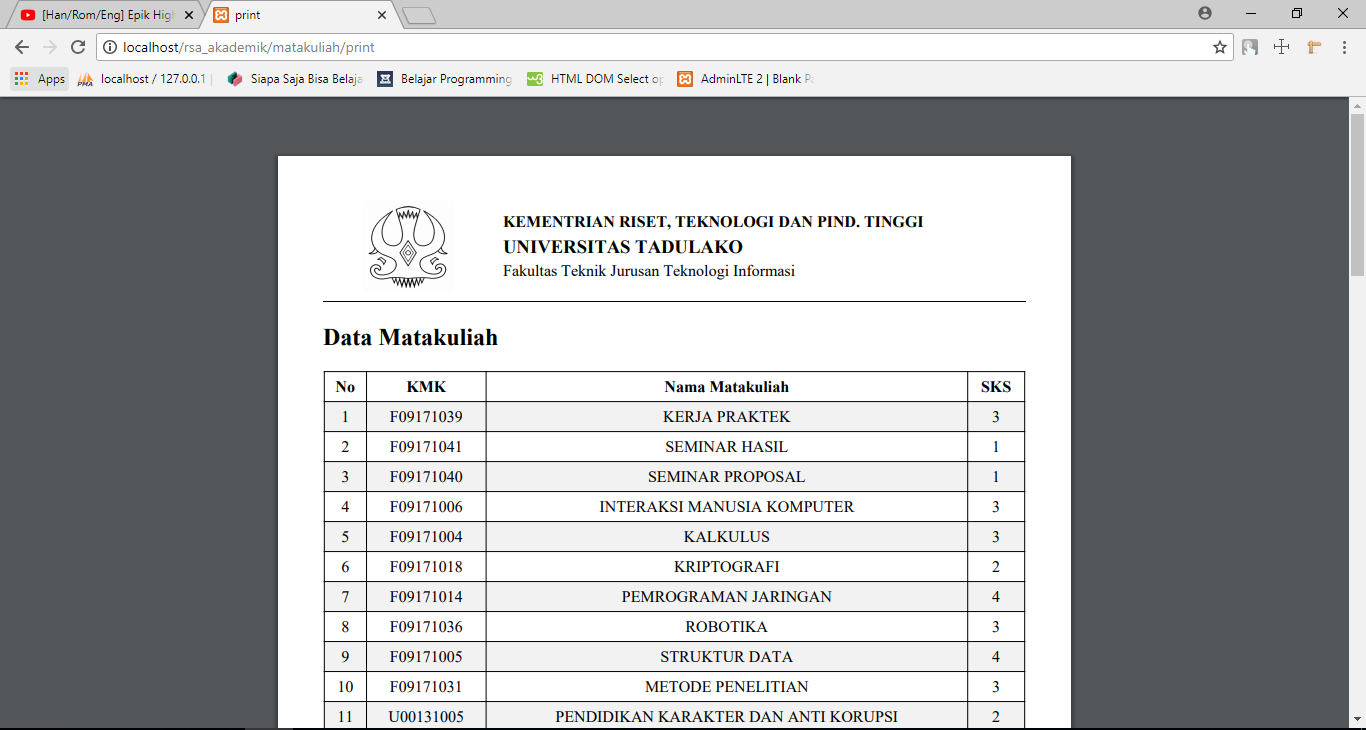
Halaman ini berfungsi untuk menampilkan laporan data-data mahasiswa. Halaman ini dapat dilihat pada gambar 4.27



Gambar 4.27 Halaman Laporan Data Mahasiswa

Halaman Laporan Data Matakuliah

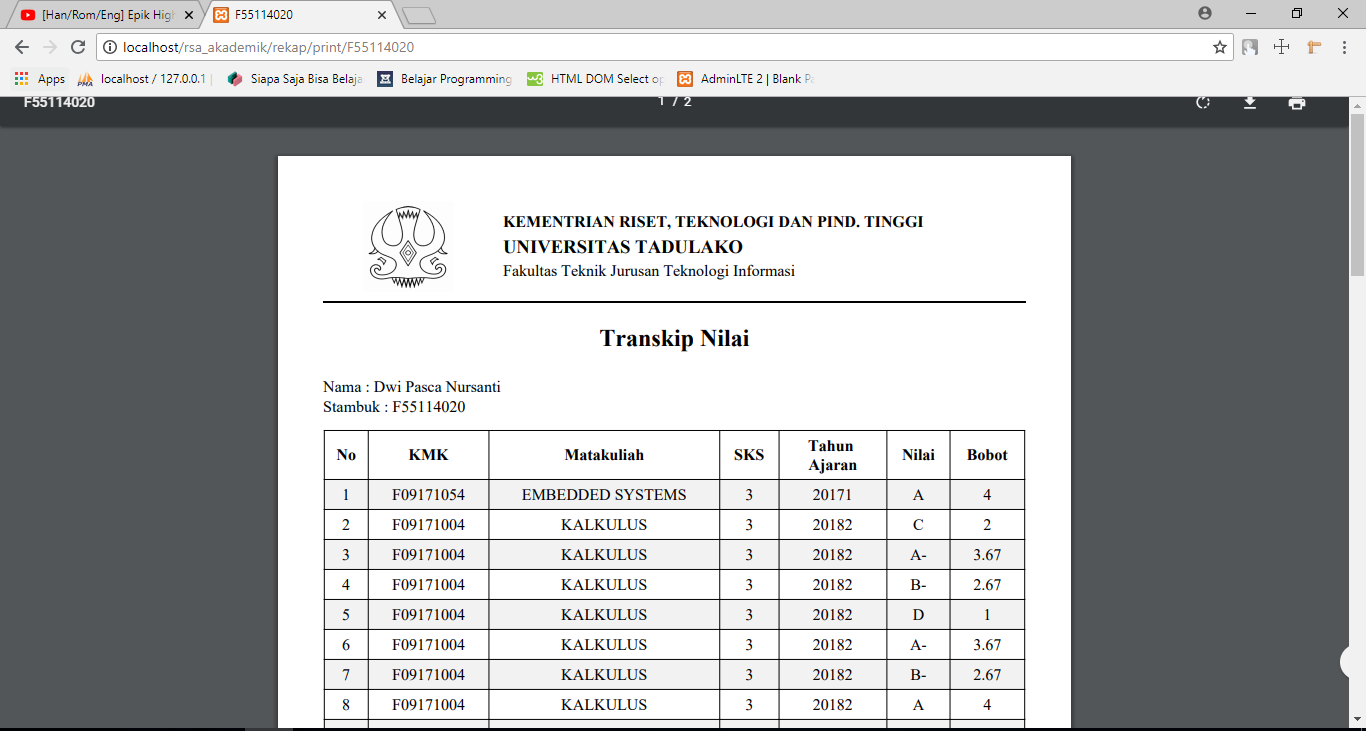
Halaman ini berfungsi untuk menampilkan laporan daftar matakuliah. Halaman ini dapat dilihat pada gambar 4.28



Gambar 4.28 Halaman Laporan Data Matakuliah

Halaman Laporan Transkip Nilai

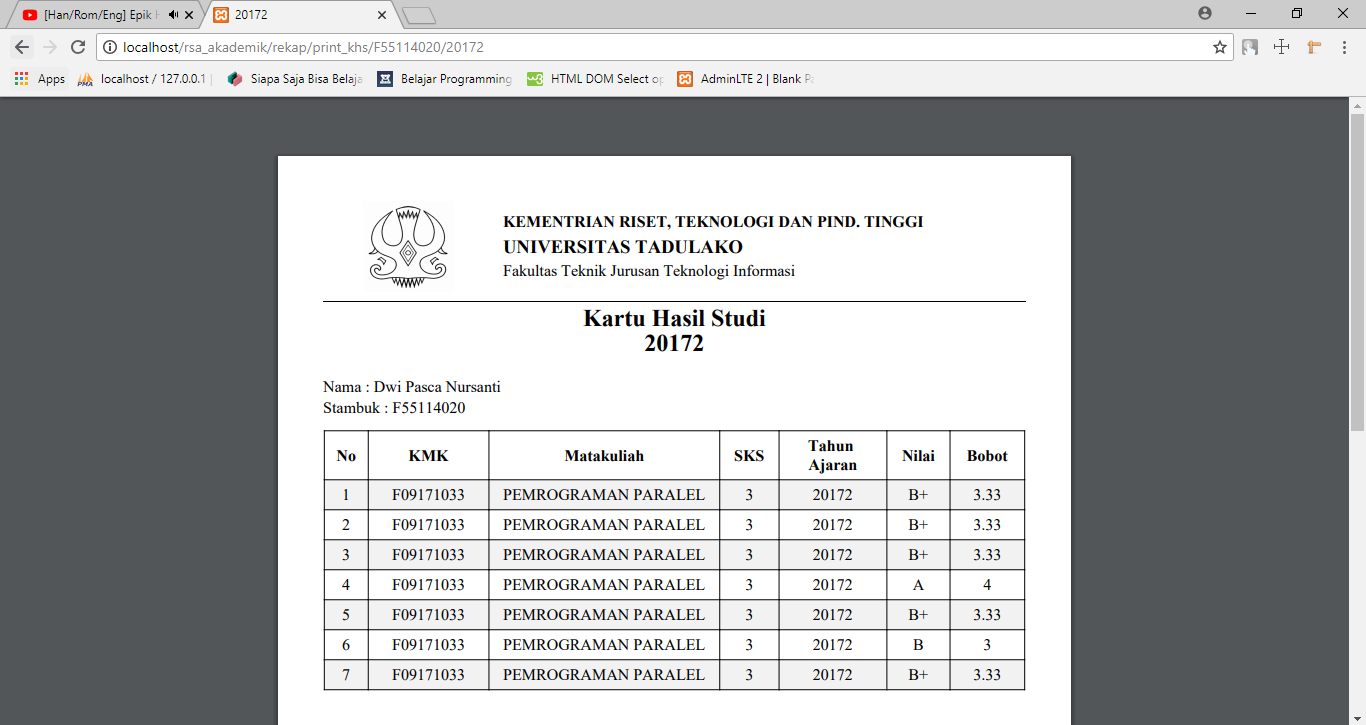
Halaman ini berfungsi untuk menampilkan laporan transkip nilai mahasiswa yang bersangkutan. Halaman ini dapat dilihat pada gambar 4.29



Gambar 4.29 Halaman Laporan Transkip Nilai

Halaman Laporan Kartu Hasil Studi (KHS)

Halaman ini berfungsi untuk menampilkan laporan KHS mahasiswa yang bersangkutan. Halaman ini dapat dilihat pada gambar 4.30



Gambar 4.30 Halaman Laporan Kartu Hasil Studi (KHS)

* + 1. **Pengujian Sistem**

Setelah pembuatan sistem telah selesai, maka dilakukan pengujian terhadap sistem. Pengujian sistem yang dilakukan merupakan pengujian terhadap Sistem pengamanan data nilai akademik. Pengujian fungsi sistem dilakukan dengan metode *blackbox* untuk mengetahui apakah fungsi-fungsi yang terdapat dalam sistem berjalan dengan baik atau tidak.

Hasil pengujian fungsi sistem dan pengujian lapangan dapat dilihat pada tabel berikut:

1. Pengujian *Login Web*

Tabel 4.9 Tabel Pengujian Fungsi *Login*

|  |  |  |  |
| --- | --- | --- | --- |
| **Data Masukan** | **Yang diharapkan** | **Pengamatan** | **Simpulan** |
| *Login* | Tampil *form login* | Menampilkan *username, password* | Baik |
| Memasukkan data login, contoh masukan :  Username: admin  Password: \*\*\*\*\* | Data yang dimasukan benar  lalu masuk ke utama | Form login terisi  atau benar dalam  pengisian, maka  akan dapat  melanjutkan proses  kehalaman dashboard | Baik |
| Memasukkan Sql Injection contoh masukkan :  Username = ' or '1'='1  Password = \*\*\*\*\* | Tampil pesan *error* | Menampilkan peringatan bahwa username atau password salah | Baik |

1. Pengujian Menu Akun

Tabel 4.10 Tabel Pengujian Menu Akun

|  |  |  |  |
| --- | --- | --- | --- |
| **Data Masukan** | **Yang diharapkan** | **Pengamatan** | **Simpulan** |
| Menu Akun | Tampil halaman data tabel akun | Menampilkan halaman seluruh data akun | Baik |
| Menekan tombol tambah pada menu akun | Tampil halaman tambah akun beserta kolom pengisian | Menampilkan halaman tambah akun dengan kolom nama, email, status, level, *username* dan *password.* | Baik |
| Tidak memasukkan nama, email, status, level, *username* dan *password* ketika menekan tombol simpan | Tampil pesan *error* | Menampilkan peringatan bahwa nama, email, status, level, *username* dan *password* wajib di isi | Baik |
| Memasukkan seluruh data yang dibutuhkan berjalan dengan baik saat menekan tombol simpan | Data berhasil tersimpan | Menampilkan pesan berhasil disimpan dan menuju halaman menu akun | Baik |
| Menekan tombol edit akun | Tampil halaman edit akun | Menampilkan halaman edit akun berdasarkan id akun yang dipilih serta data muncul dikolom edit text yang disediakan | Baik |
| Menekan tombol simpan tanpa melakukan perubahan data | Tidak ada data yang terubah | Kembali Kehalaman menu akun | Baik |
| Melakukan perubahan data dan menekan tombol simpan | Data berita baru tersimpan | Menampilkan pesan data berhasil di ubahdan meuju halaman menu akun | Baik |
| Menekan tombol edit password | Tampil halaman edit password akun | Menampilkan halaman memasukkan password baru dengan kolom konfirmasi password baru | Baik |
| Tidak memasukkan password baru dan konfirmasi password saat menekan tombol  Simpan | Tampil pesan *error* | Menampilkan peringatan bahwa kolom password baru dan kolom konfirmasi password kosong | Baik |
| Menekan tombol hapus pada menu akun | Data terhapus | Menampilkan pesan konfirmasi penghapusan data, jika menekan tombol ok, data akan terhapus | Baik |
| Menekan tombol Print | Print Data Akun | Menampilkan semu data akun dalam bentuk PDF | Baik |

1. Pengujian Menu Dosen

Tabel 4.11 Tabel pengujian menu dosen

|  |  |  |  |
| --- | --- | --- | --- |
| **Data Masukan** | **Yang diharapkan** | **Pengamatan** | **Simpulan** |
| Menu Dosen | Tampil halaman dosen | Menampilkan halaman dosen, beserta data tabel dosen | Baik |
| Menekan tombol tambah pada menu dosen | Tampil halaman tambah dosen beserta kolom pengisian | Menampilkan halaman tambah dosen beserta kolom nip, nama, jenis kelamin, nomor hp, email status, dan alamat. | Baik |
| Tidak memasukkan data yang dibutuhkan dan menekan tombol simpan | Tampil pesan *error* | Menampilkan peringatan bahwa kolom wajib di isi | Baik |
| Memasukkan seluruh data yang dibutuhkan dan menekan tombol simpan | Data berhasil tersimpan | Menampilkan pesan berhasil disimpan dan menuju halaman menu dosen | Baik |
| Menekan tombol edit pada data tabel dosen | Tampil halaman edit dosen | Menampilkan halaman edit dosen berdasarkan id dosen serta data muncul dikolom edit text yang disediakan | Baik |
| Menekan tombol simpan tanpa melakukan perubahan data | Tidak ada yang terubah | Kembali Kehalaman menu dosen | Baik |
| Mengedit data dosen | Data dosen baru tersimpan | Menampilkan pesan data berhasil di ubah dan meuju halaman menu dosen | Baik |
| Menekan tombol hapus pada data tabel dosen | Data terhapus | Menampilkan pesan konfirmasi penghapusan data, jika menekan tombol ok, data akan terhapus | Baik |
| Menekan tombol Print | Print data dosen | Menampilkan semu data dosen dalam bentuk PDF | Baik |

1. Pengujian Menu Mahasiswa

Tabel 4.12 Tabel pengujian menu mahasiswa

|  |  |  |  |
| --- | --- | --- | --- |
| **Data Masukan** | **Yang diharapkan** | **Pengamatan** | **Simpulan** |
| Menu mahasiswa | Tampil halaman mahasiswa dan datanya | Menampilkan halaman mahasiswa, beserta data tabel mahasiswa | Baik |
| Menekan tombol tambah pada tabel mahasiswa | Tampil halaman tambah mahasiswa | Menampilkan halaman tambah mahasiswa berserta kolom inputannya seperti stambuk, nama, jenis kelamin, no hp, email, status, dan angkatan. | Baik |
| Tidak memasukkan data yang dibutuhkan dan menekan tombol simpan | Tampil pesan *error* | Menampilkan peringatan bahwa kolom wajib di isi | Baik |
| Memasukkan seluruh data yang dibutuhkan dan menekan tombol simpan | Data berhasil tersimpan | Menampilkan pesan berhasil disimpan dan menuju halaman menu mahasiswa | Baik |
| Menekan tombol edit pada data tabel mahasiswa | Tampil halaman edit mahasiswa | Menampilkan halaman edit mahasiswa berdasarkan id mahasiswa serta data muncul dikolom edit text yang disediakan | Baik |
| Menekan tombol simpan tanpa melakukan perubahan data | Tidak ada yang terubah | Kembali kehalaman menu mahasiswa | Baik |
| Mengedit data mahasiswa dan melakukan perubahan data | Data mahasiswa baru tersimpan | Menampilkan pesan data berhasil di ubah dan meuju halaman menu mahasiswa | Baik |
| Menekan tombol hapus pada data tabel mahasiswa | Data terhapus | Menampilkan pesan konfirmasi penghapusan data, jika menekan tombol ok, data akan terhapus | Baik |
| Menekan tombol Print | Print data mahasiswa | Menampilkan semu data mahasiswa dalam bentuk PDF | Baik |

1. Pengujian Menu Matakuliah

Tabel 4.13 Tabel pengujian menu matakuliah

|  |  |  |  |
| --- | --- | --- | --- |
| **Data Masukan** | **Yang diharapkan** | **Pengamatan** | **Simpulan** |
| Menu matakuliah | Tampil halaman menu matakuliah | Menampilkan halaman matakuliah beserta tabel matakuliah | Baik |
| Menekan tombol tambah pada tabel matakuliah | Tampil halaman tambah matakuliah | Menampilkan halaman tambah matakuliah berserta kolom inputannya seperti kode matakuliah, nama matakuliah dan sks | Baik |
| Tidak memasukkan data yang dibutuhkan dan menekan tombol simpan | Tampil pesan *error* | Menampilkan peringatan bahwa kolom wajib di isi | Baik |
| Memasukkan seluruh data yang dibutuhkan dan menekan tombol simpan | Data berhasil tersimpan | Menampilkan pesan berhasil disimpan dan menuju halaman menu matakuliah | Baik |
| Menekan tombol edit pada data tabel matakuliah | Tampil halaman edit matakuliah | Menampilkan halaman edit matakuliah berdasarkan id matakuliah serta data muncul dikolom edit text yang disediakan | Baik |
| Menekan tombol simpan tanpa melakukan perubahan data | Tidak ada yang terubah | Kembali kehalaman menu matakuliah | Baik |
| Mengedit data matakuliah dan melakukan perubahan data | Data matakuliah baru tersimpan | Menampilkan pesan data berhasil di ubah dan meuju halaman menu matakuliah | Baik |
| Menekan tombol hapus pada data tabel matakuliah | Data terhapus | Menampilkan pesan konfirmasi penghapusan data, jika menekan tombol ok, data akan terhapus | Baik |
| Menekan tombol Print | Print data matakuliah | Menampilkan semu data matakuliah dalam bentuk PDF | Baik |

1. Pengujian Menu Tahun Ajaran

Tabel 4.14 Tabel pengujian menu tahun ajaran

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **Data Masukan** | | **Yang diharapkan** | | **Pengamatan** | | **Simpulan** |
| Menu Tahun Ajaran | | Tampil halaman menu tahun ajaran | | Menampilkan halaman tahun ajaran beserta tabel tahun ajaran | | Baik |
| Menekan tombol tambah pada tabel tahun ajaran | | Tampil halaman tambah tahun ajaran | | Menampilkan halaman tambah tahun ajaran berserta kolom inputannya seperti tahun ajaran dan deskripsinya. | | Baik |
| Tidak memasukkan data yang dibutuhkan dan menekan tombol simpan | | Tampil pesan *error* | | Menampilkan peringatan bahwa kolom wajib di isi | | Baik |
| Memasukkan seluruh data yang dibutuhkan dan menekan tombol simpan | | Data berhasil tersimpan | | Menampilkan pesan berhasil disimpan dan menuju halaman menu tahun ajaran | | Baik |
| Menekan tombol edit pada data tabel tahun ajaran | | Tampil halaman edit tahun ajaran | | Menampilkan halaman edit tahun ajaran berdasarkan id tahun ajaran serta data muncul dikolom edit text yang disediakan | | Baik |
| Menekan tombol simpan tanpa melakukan perubahan data | | Tidak ada yang terubah | | Kembali kehalaman menu tahun ajaran | | Baik |
| Mengedit data tahun ajaran dan melakukan perubahan data | | Data tahun ajaran baru tersimpan | | Menampilkan pesan data berhasil di ubah dan meuju halaman menu tahun ajaran | Baik | |
| Menekan tombol hapus pada data tabel tahun ajaran | | Data terhapus | | Menampilkan pesan konfirmasi penghapusan data, jika menekan tombol ok, data akan terhapus | Baik | |

1. Pengujian Menu Nilai

Tabel 4.15 Tabel pengujian menu nilai

|  |  |  |  |
| --- | --- | --- | --- |
| **Data Masukan** | **Yang diharapkan** | **Pengamatan** | **Simpulan** |
| Menu nilai | Tampil halaman menu nilai | Menampilkan halaman nilai beserta tabel nilai | Baik |
| Menekan tombol tambah pada menu nilai | Tampil halaman tambah nilai | Menampilkan halaman tambah nilai berserta kolom inputannya seperti huruf dan angka | Baik |
| Tidak memasukkan data yang dibutuhkan dan menekan tombol simpan | Tampil pesan *error* | Menampilkan peringatan bahwa kolom wajib di isi | Baik |
| Memasukkan seluruh data yang dibutuhkan dan menekan tombol simpan | Data berhasil tersimpan | Menampilkan pesan berhasil disimpan dan menuju halaman menu nilai | Baik |
| Menekan tombol edit pada data tabel nilai | Tampil halaman edit nilai | Menampilkan halaman edit nilai berdasarkan id nilai serta data muncul dikolom edit text yang disediakan | Baik |
| Menekan tombol simpan tanpa melakukan perubahan data | Tidak ada yang terubah | Kembali kehalaman menu nilai | Baik |
| Mengedit data nilai dan melakukan perubahan data | Data nilai baru tersimpan | Menampilkan pesan data berhasil di ubah dan meuju halaman menu nilai | Baik |
| Menekan tombol hapus pada data tabel nilai | Data terhapus | Menampilkan pesan konfirmasi penghapusan data, jika menekan tombol ok, data akan terhapus | Baik |

1. Pengujian Menu Rekap Nilai

Tabel 4.16 Tabel pengujian menu rekap nilai

|  |  |  |  |
| --- | --- | --- | --- |
| **Data Masukan** | **Yang diharapkan** | **Pengamatan** | **Simpulan** |
| Menu rekap nilai | Tampil halaman rekap nilai | Menampilkan halaman rekap nilai beserta tabel daftar mahasiswa | Baik |
| Menekan tombol detail pada tabel daftar mahasiswa | Tampil halaman transkip nilai dari mahasiswa yang dipilih pada tabel daftar mahasiswa | Menampilkan transkip nilai mahasiswa yang pernah dimasukkan oleh admin/dosen. | Cukup Baik  (Menunggu beberapa detik karena adanya proses dekripsi nilai mahasiswa) |
| Menekan tombol tambah pada transkip nilai | Tampil halaman tambah nilai akhir | Menampilkan halaman tambah nilai akhir berserta kolom inputannya seperti nama matakuliah, kode matakuliah, tahun ajaran, nama  mahasiswa, stambuk dan nilai | Baik |
| Tidak memasukkan data yang dibutuhkan dan menekan tombol simpan | Tampil pesan *error* | Menampilkan peringatan bahwa kolom wajib di isi | Baik |
| Memasukkan seluruh data yang dibutuhkan dan menekan tombol simpan | Data berhasil tersimpan | Menampilkan pesan berhasil disimpan dan menuju halaman rekap nilai | Baik |
| Menekan tombol hapus pada data tabel rekap nilai | Data terhapus | Menampilkan pesan konfirmasi penghapusan data, jika menekan tombol ok, data akan terhapus | Baik |
| Menekan link tahun ajaran diatas transkip nilai | Tampil halaman KHS | Menampilkan halaman KHS dari tahun ajaran yang dipilih | Cukup Baik  (Menunggu beberapa detik karena adanya proses dekripsi nilai mahasiswa) |
| Menekan tombol Print di transkip nilai | Print trnskip nilai | Menampilkan transkip nilai mahasiswa dalam bentuk PDF | Baik |
| Menekan tombol Print di khs | Print khs | Menampilkan khs mahasiswa dalam bentuk PDF | Baik |

1. Pengujian Menu *Logout*

Tabel 4.17 Tabel pengujian menu *logout*

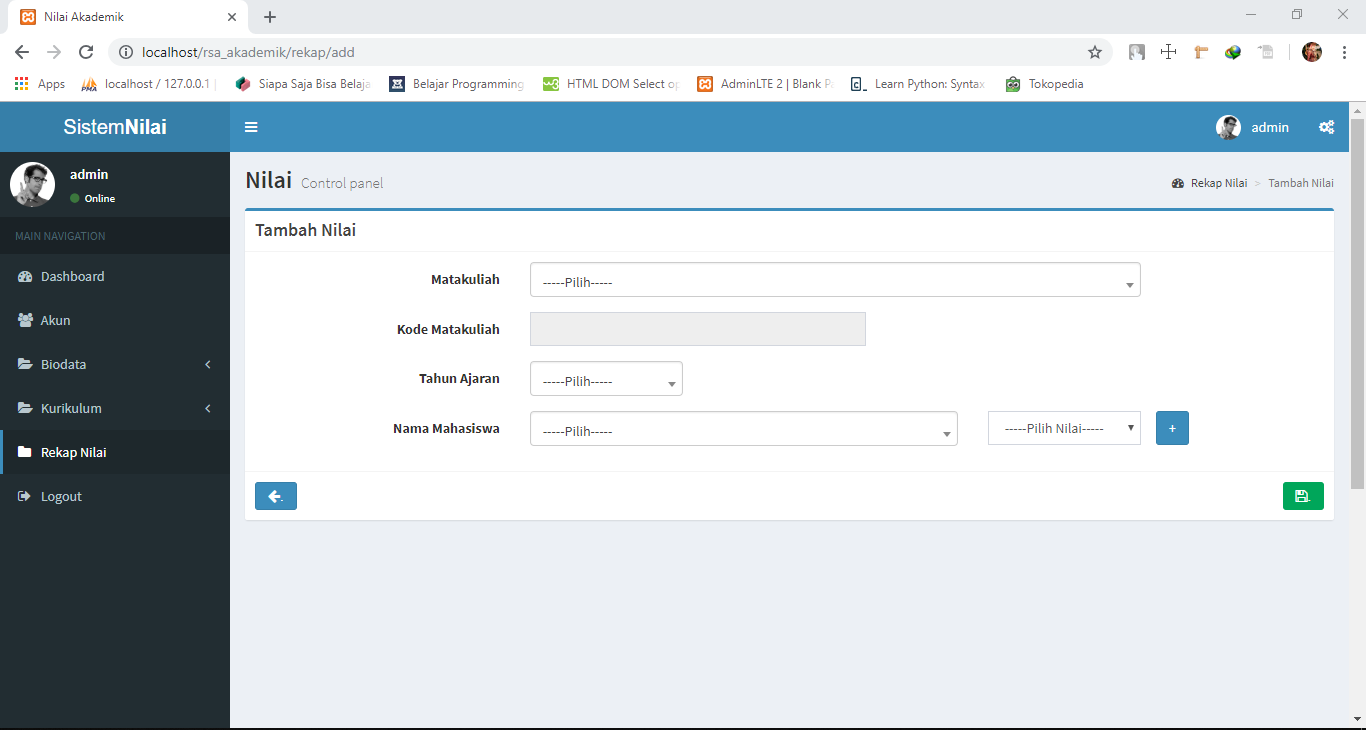
|  |  |  |  |
| --- | --- | --- | --- |
| **Data Masukan** | **Yang diharapkan** | **Pengamatan** | **Simpulan** |
| Klik Logout | Dapat keluar dan menghapus session pengguna | Keluar dari halaman admin dan menuju ke halaman utama | Baik |

1. **Pembahasan**

Terdapat beberapa tahapan yang dilakukan dalam penelitian pembuatan sistem pengamanan data nilai akademik. Tahapan-tahapan tersebut digambarkan pada tahapan sebagai berikut:

1. Penginputan nilai akhir pada setiap mahasiswa

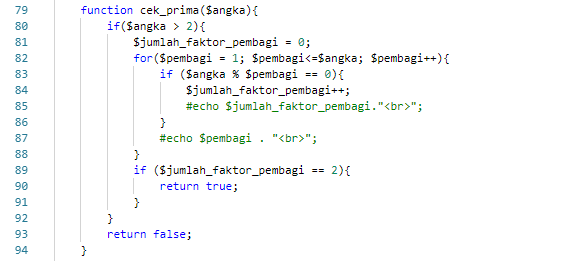
Penginputan nilai akhir pada setiap mahasiswa didapat melalui data yang diperoleh dari objek penelitian. Dimana sumber data yang diperlukan berasal dari Program Studi Teknik Informatika, Jurusan Teknologi Informasi, Fakultas Teknik Universitas Tadulako. Berikut adalah tampilan *form* pengimputan nilai mahasiswa pada gambar 4.31.



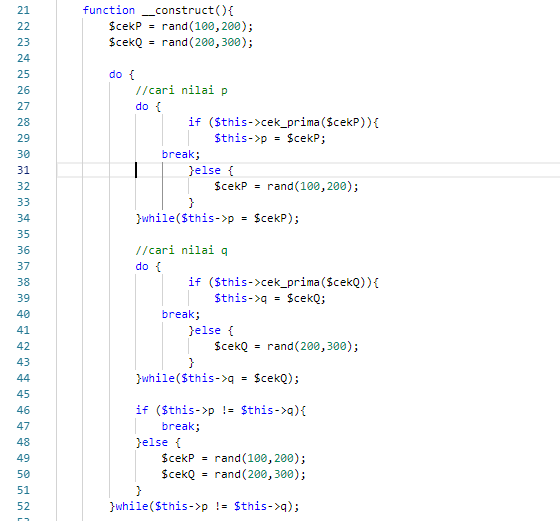
Gambar 4.31. Tampilan *form* pengimputan nilai mahasiswa

1. Proses pembangkitan kunci algoritma RSA

Tahap-tahap untuk mendapatkan pembangkit kunci ada beberapa langkah yang harus dilakukan yaitu menentukan nilai kunci p dan q dimana nilai p dan q harus bernilai prima positif. Pada sistem telah ditetapkan bahwa nilai dari kunci p adalah nilai random yang *range*nya antara 100 sampai 200 sedangkan untuk kunci q *range*nya antara 200 sampai 300. Berikut adalah implementasi langkah-langkah penentuan nilai p dan q prima positif dan rangenya sesuai dengan yang ditetapkan kedalam program.



Gambar 4.32. Mengecek bilangan prima

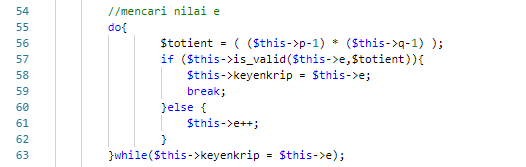


Gambar 4.33. Menentukan nilai p dan q secara random dengan rangenya sesuai dengan yang ditetapkan

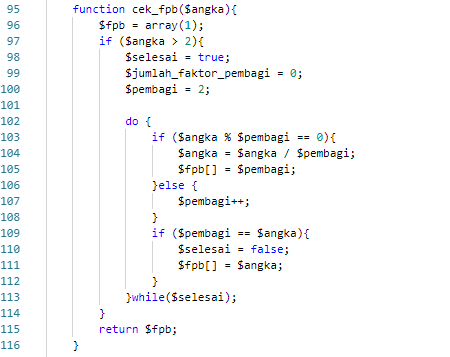
Kemudian menentukan kunci n yang didapat dari hasil perkalian dari kunci p dan q. Menentukan kunci phi(n) yang didapat dari (p-1) x (q-1). Menentukan kunci e dimana kunci e harus bernilai bilangan bulat positif dan FPB dari kunci e dan kunci phi(n) harus sama dengan 1. Berikut adalah implementasi langkah-langkah penentuan kunci phi(n) dan e kedalam program.



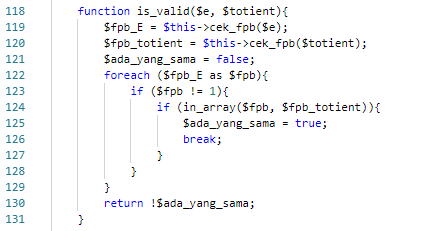
Gambar 4.34. Menentukan kunci n



Gambar 4.35. Menentukan kunci phi(n) dan e

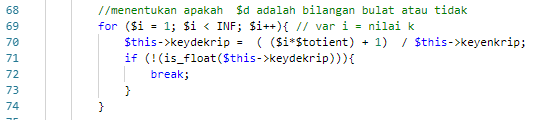


Gambar 4.36. Mengecek bilangan fpb sama dengan satu atau tidak



Gambar 4.37. Mengecek fpb kunci e dan phi(n) sama dengan satu

Menentukan kunci k dimana kunci k harus bernilai bilangan bulat positif. Menentukan kunci d yang di dapat dari perhitungan 1+(k\*(phi(n)) / e yang hasilnya harus bilangan bulat positif.



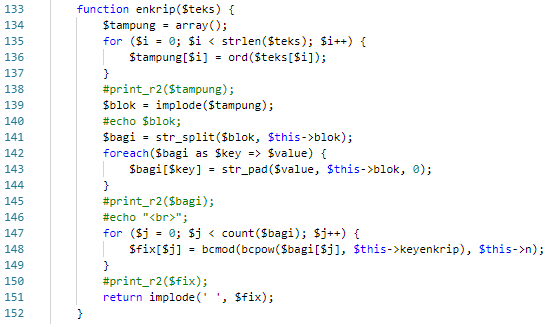
Gambar 4.38. Menentukan kunci k dan d



Gambar 4.39. Pembangkit kunci algoritma RSA

1. Proses enkripsi nilai akhir dengan algoritma RSA

Tahap-tahap enkripsi nilai akhir dengan algoritma RSA akan memerlukan kunci-kunci pembangkit seperti kunci enkripsi (e) dan kunci n yang didapat dari proses pembangkitan kunci. Kemudian plainteks yaitu nilai mahasiswa (A/B/C/D/E) diubah ke kode ASCII (desimal). Kemudian chiperteks tersebut dibagi menjadi beberapa blok yang telah ditentukan yaitu 4. Blok-blok tersebut sebut saja m, akan masuk dalam proses enkripsi dengan rumus m^e mod n. Berikut adalah implementasi langkah-langkah enkripsi nilai kedalam program.



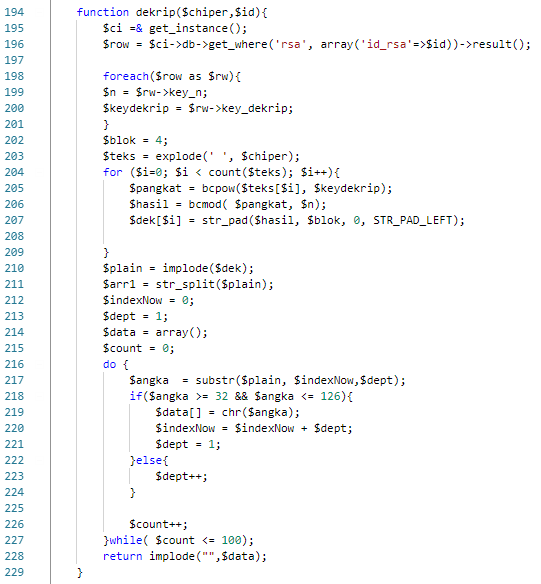
Gambar 4.40. Enkripsi nilai menggunakan algoritma RSA



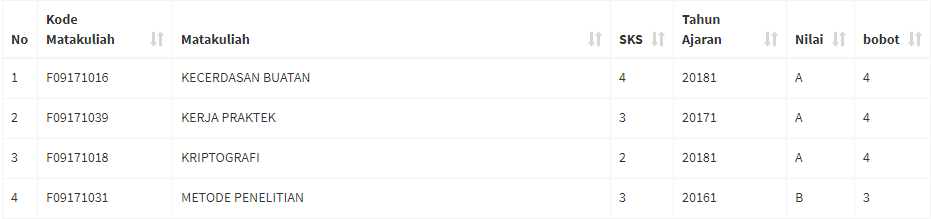
Gambar 4.41. Nilai mahasiswa setelah di enkripsi

1. Proses dekripsi nilai akhir dengan algoritma RSA

Tahap-tahap dekripsi nilai akhir dengan algoritma RSA akan memerlukan kunci-kunci pembangkit seperti kunci dekripsi (d) dan kunci n yang didapat dari proses pembangkitan kunci. Kemudian chiperteks yang didapat diproses dengan menggunakan rumus c^d mod n. Setelah itu baru chiperteks tersebut diubah kedalam plainteks. Berikut adalah implementasi langkah-langkah dekripsi nilai kedalam program.



Gambar 4.42. Dekripsi nilai menggunakan algoritma RSA



Gambar 4.43. Nilai mahasiswa setelah di dekripsi

**BAB V**

**PENUTUP**

**5.1. Kesimpulan**

Berdasarkan pengujian dan analisis Penerapan algoritma RSA (*Rivest-Shamir-Adleman*) pada sistem pengamanan data nilai akademik, maka dapat diambil kesimpulan sebagai berikut:

1. Pada sistem pengamanan data nilai akademik, dibuat fungsi atau *library* RSA yang diletakkan pada *library codeigniter,* fungsi tersebut digunakan untuk meng-enkripsi nilai sebelum dimasukkan kedalam *database* oleh admin/dosen. Fungsi RSA juga digunakan pada saat admin memasukkan data-data dosen/mahasiswa, dimana pada saat admin memasukkan data-data tersebut maka secara otomatis akun dari mahasiswa/dosen akan terbuat dan *password* dari akun tersebut menggunakan fungsi RSA.
2. Sistem pengamanan data nilai akademik dapat mengamankan nilai akademik dengan cara meng-enkripsi nilai tersebut dengan menggunakan algoritma RSA dan nilai-nilai tersebut berbeda dengan satu dan yang lain karena kunci untuk meng-enkripsi nilai tersebut random.
3. Sistem pengamanan data nilai akademik menggunakan *framework codeigniter* dapat menangkal *Sql Injection* dengan menggunakan *form-validation* *(alpha-numeric) library* dari *codeigniter* yang digunakan pada *controller Auth*.

**5.2 Saran**

Pada Sistem pengamanan data nilai akademik belum sepenuhnya sempurna masih ada beberapa yang dapat dikembangkan lagi. Berikut adalah saran yang harus diperhatikan oleh pengembang yang lain jika ingin mengembangkan sistem ini nantinya:

Karena nilai akademik di enkripsi dengan menggunakan algoritma RSA maka perlu waktu beberapa detik untuk menampilkan nilai yang sudah didekripsi kepada pengguna. Semoga kedepannya proses dekripsi nilai dapat memerlukan waktu yang lebih cepat.

Dengan adanya sistem ini, penulis mengharapkan sistem ini dapat berguna dalam sistem penginputan nilai akademik, dan menjadi nilai akademik tersebut.

# **DAFTAR PUSTAKA**

Benny, L. 2017. *Analisis dan Perancangan Aplikasi Kriptografi Keamanan File Berbasis Teks Dengan Menggunakan Metode RSA*, STIMIK ITMI, Medan.

Diarse, N.N. dan Bendi, K.J. 2016. *Penerapan Algoritma RSA Pada Sistem Kriptografi File Audio Mp3*, Universitas Katolik Musi Charitas, Palembang.

Hutahaean, J. 2014. Konsep Sistem Informasi, *Deepublish*, Yogyakarta.

Kharisma, R.S.,dan Rachman M.A.F. 2017. *Pembuatan Aplikasi Notes Menggunakan Algoritma Kriptografi Polyalphabetic Substitution Chiper Kombinasi Kode ASCII dan Operasi XOR Berbasis Android*, Universitas AMIKOM, Yogyakarta.

Linarwati, dkk, 2016. *Studi deskriptif pelatihan dan pengembangan sumberdaya manusia serta penggunaan metode behavioral event interview dalam merekrut karyawan baru di bank mega cabang kudus*, Journal of Management Vol.2 No.2, Universitas Pandanaran, Semarang.

Martono. 2017. *Model Modifikasi Kriptografi Algoritma RSA Untuk Keamanan Data Pada Database E-Voting*, MEDIASISFO Vol.11 No.2, STIKOM Dinamika Bangsa, Jambi.

Miftah, F., 2015. *Fitur Dahsyat Sublime Text 3*, STIKOM, Surabaya.

Natsir M., 2017. *Pengembangan Prototype Sistem Kriptografi Untuk Enkripsi Dan Dekripsi Data Office Menggunakan Metode Blowfish Dengan Bahasa Pemrograman Java*, Universitas Mercu Buana, Jakarta.

Pahrizal dan Pratama, D. 2016. *Implementasi Algoritma RSA Untuk Pengamanan Data Berbentuk Teks,* Universitas Muhammadiyah, Bengkulu.

Pabokory, F.N. dkk. 2015. *Implementasi Kriptografi Pengamanan Data Pada Pesan Teks, Isi File Dokumen, Dan File Dokumen Menggunakan Algoritma Advanced Encryption Standard*. Jurnal Informatika Mulawarman. Vol. 10, No.1.

Rahardjo, M. 2017. *Studi kasus dalam penelitian kualitatif: Konsep dan Prosedurnya*, Universitas Islam Negri Maulana Malik Ibrahim, Malang.

Riski dan Evayanti, 2016. *Analisis dan perancangan sistem informasi akuntansi berbasis data pada sistem persediaan dan penjualan (studi kasus pada cv prima motor, banda aceh)*, Universitas Syiah Kuala, Banda Aceh.