

**IMPLEMENTASI ALGORITMA KRIPTOGRAFI RSA  
PADA APLIKASI SMART CARD**

**SKRIPSI**

**oleh:**

**ANUGRAH WIDIASARI**

**NIM. 10650037**



**JURUSAN TEKNIK INFORMATIKA  
FAKULTAS SAINS DAN TEKNOLOGI  
UNIVERSITAS ISLAM NEGERI MAULANA MALIK IBRAHIM  
MALANG  
2014**

**HALAMAN PENGAJUAN**

**IMPLEMENTASI ALGORITMA KRIPTOGRAFI RSA  
PADA APLIKASI *SMART CARD***

**SKRIPSI**

**Diajukan kepada:  
Fakultas Sains dan Teknologi  
Universitas Islam Negeri Maulana Malik Ibrahim Malang  
Untuk Memenuhi Salah Satu Persyaratan Dalam  
Memperoleh Gelar Sarjana Komputer (S.Kom)**

**oleh :  
ANUGRAH WIDIASARI  
NIM. 10650037 / S-1**

**JURUSAN TEKNIK INFORMATIKA  
FAKULTAS SAINS DAN TEKNOLOGI  
UNIVERSITAS ISLAM NEGERI MAULANA MALIK IBRAHIM  
MALANG  
2014**

**HALAMAN PERSETUJUAN**

**IMPLEMENTASI ALGORITMA KRIPTOGRAFI RSA  
PADA APLIKASI SMART CARD**

**SKRIPSI**

**Oleh :**

Nama : Anugrah Widiyari  
NIM : 10650037  
Jurusan : Teknik Informatika  
Fakultas : Sains Dan Teknologi

Telah Diperiksa dan Disetujui  
Tanggal : November 2014

**Dosen Pembimbing I**

**Dosen Pembimbing II**

**Dr. Muhammad Faisal, M.T**  
NIP.19740510 200501 1 007

**Totok Chamidy, M.Kom**  
NIP.19691222 200604 1 001

Mengetahui,  
**Ketua Jurusan Teknik Informatika**

**Dr. Cahyo Crysdiyan**  
NIP. 19740424 200901 1 008

**HALAMAN PENGESAHAN**

**IMPLEMENTASI ALGORITMA KRIPTOGRAFI RSA  
PADA APLIKASI SMART CARD**

**SKRIPSI**

Oleh :  
**ANUGRAH WIDIASARI**  
**NIM. 10650037**

Telah Dipertahankan di Depan Dewan Penguji Skripsi  
Dan Dinyatakan Diterima Sebagai Salah Satu Persyaratan  
Untuk Memperoleh Gelar Sarjana Komputer (S.Kom)  
Tanggal : November 2014

1. Penguji Utama : **Yunifa Miftachul Arif, M.T** ( )  
NIP. 19830616 201101 1 004
2. Ketua Penguji : **Hani Nurhayati, M.T** ( )  
NIP. 19780625 200801 2 006
3. Sekretaris Penguji : **Dr. M. Faisal, M.T** ( )  
NIP. 19740510 200501 1 007
4. Anggota Penguji : **Totok Chamidy, M.Kom** ( )  
NIP. 19691222 200604 1 001

Mengesahkan,  
**Ketua Jurusan Teknik Informatika**

**Dr. Cahyo Crysdiان**  
**NIP. 19740424 200901 1 008**

**HALAMAN PERNYATAAN  
ORISINALITAS PENELITIAN**

Saya yang bertandatangan di bawah ini:

Nama : Anugrah Widiyasari  
NIM : 10650037  
Fakultas/Jurusan : Sains Dan Teknologi / Teknik Informatika  
Judul Penelitian : *Implementasi Algoritma Kriptografi RSA pada Aplikasi Smart Card*

Menyatakan dengan sebenarnya bahwa skripsi yang saya tulis ini benar-benar merupakan hasil karya saya sendiri, bukan merupakan pengambilan data, tulisan atau pikiran orang lain yang saya akui sebagai hasil tulisan atau pikiran saya sendiri, kecuali dengan mencantumkan sumber cuplikan pada daftar pustaka. Apabila dikemudian hari terbukti atau dapat dibuktikan skripsi ini hasil jiplakan, maka saya bersedia menerima sanksi atas perbuatan tersebut.

Malang, November 2014  
Yang membuat pernyataan,

Anugrah Widiyasari  
NIM. 10650037

## MOTTO

*“ Sesungguhnya Allah tidak akan mengubah keadaan suatu kaum sehingga mereka merubah keadaan yang ada pada diri mereka sendiri. Dan apabila Allah menghendaki keburukan kepada suatu kaum, maka tak ada yang dapat menolaknya; dan sekali-kali tak ada pelindung bagi mereka selain Dia.”*

*( QS Ar Ra'd 13 : 11 )*

*” Sesungguhnya sesudah kesulitan itu ada kemudahan. Maka apabila kamu telah selesai (dari sesuatu urusan), kerjakanlah dengan sungguh-sungguh (urusan) yang lain. Dan Hanya kepada Tuhanmulah hendaknya kamu berharap.”*

*(Qs. Alam-Nasyrah 94 : 6-8)*

## HALAMAN PERSEMBAHAN

*Alhamdulillah...*

*Puji syukur yang sebesar-besarnya tercurahkan kepada Allah SWT atas selesainya skripsi ini. Kupersembahkan sebuah karya sederhana untuk orang-orang yang paling aku kasahi dan kusayangi,*

*Papa dan Mama,*

*Hardjoko dan Lu'lu Ulwaroh*

*Yang selalu memberikan semangat, motivasi, dukungan, dan doa selama menyelesaikan studi di UIN Maliki Malang. Terimakasih papa dan mama...*

*Adikku,*

*Kurnia Sari Dewi*

*Yang selalu membuatku semangat dan mendoakanku...*

*Kepada M. Nurul Misbah yang selalu memberikan semangat, dukungan, doa dan selalu ada untukku.*

*Kepada teman seperjuanganku Ade, Dewi, Vina, Balqis, Puspita, Gery, Rizky, Sari, Amel, Amru, Fuad, Dzakiyah, Wati, Aeny, Riris yang selalu saling bersama-sama dan saling mengingatkan jika lalai*

*Kepada Sahabat-sahabat sepen ikan tersayang Icha, Listya, Vina, Elis, Balqis, Firoh, yang selalu kocak dan menghibur. Kalian adalah sahabat terbaikku.*

*Kepada teman-teman infinity (T'10), yang selalu ada untuk membantu sesama*

## KATA PENGANTAR

بِسْمِ اللَّهِ الرَّحْمَنِ الرَّحِيمِ

*Assalamu'alaikum Wr. Wb.*

Segala puji bagi Allah SWT, karena atas rahmat, taufik dan hidayahnya, penulis dapat menyelesaikan studi di Jurusan Teknik Informatika Universitas Islam Negeri Maulana Malik Ibrahim Malang. Sekaligus menyelesaikan skripsi ini dengan baik. Shalawat serta salam tetap tercurahkan kepada junjungan Nabi Muhammad SAW, yang telah membimbing umatnya menuju jalan yang *diridhoi* oleh Allah SWT.

Selanjutnya, penulis haturkan ucapan terima kasih seiring do'a dan harapan kepada semua pihak yang telah membantu terselesaikannya skripsi ini. Ucapan terima kasih ini penulis sampaikan kepada:

1. Dr. Muhamad Faisal, M.T. selaku dosen pembimbing I yang telah memberikan memotivasi, membantu dan memberikan penulis arahan yang baik dan benar dalam menyelesaikan penulisan skripsi ini.
2. Totok Chamidy, M.Kom selaku dosen pembimbing II yang telah bersedia meluangkan waktu untuk memberikan masukan dan arahan mengenai laporan dan permasalahan integrasi Al-Quran.
3. Dr. Cahyo Crysdiyan selaku Ketua Jurusan Teknik Informatika Universitas Islam Negeri Maulana Malik Ibrahim Malang.
4. Seluruh Dosen Universitas Islam Negeri (UIN) Maulana Malik Ibrahim Malang, khususnya Dosen Teknik Informatika dan staf yang telah



memberikan ilmu kepada penulis serta dukungan dalam menyelesaikan penulisan skripsi ini.

5. Semua pihak yang ikut membantu dalam menyelesaikan skripsi ini baik berupa materil maupun moril.

Penulis menyadari bahwa dalam penyusunan skripsi ini masih terdapat kekurangan dan penulis berharap semoga skripsi ini bisa memberikan manfaat kepada para pembaca khususnya bagi penulis secara pribadi. *Amiin Yaa Robbal Alamin.*

*Wassalamu'alaikum Wr. Wb.*

Malang, November 2014  
Penulis

Anugrah Wideasari

## DAFTAR ISI

<b>HALAMAN JUDUL .....</b>	<b>i</b>
<b>HALAMAN PENGAJUAN .....</b>	<b>ii</b>
<b>HALAMAN PERSETUJUAN .....</b>	<b>iii</b>
<b>HALAMAN PENGESAHAN .....</b>	<b>iv</b>
<b>HALAMAN PERNYATAAN.....</b>	<b>v</b>
<b>HALAMAN MOTTO .....</b>	<b>vi</b>
<b>HALAMAN PERSEMBAHAN .....</b>	<b>vii</b>
<b>KATA PENGANTAR.....</b>	<b>viii</b>
<b>DAFTAR ISI.....</b>	<b>x</b>
<b>DAFTAR GAMBAR.....</b>	<b>xiv</b>
<b>DAFTAR TABEL .....</b>	<b>xvi</b>
<b>ABSTRAK .....</b>	<b>vii</b>
<b>ABSTRACT .....</b>	<b>viii</b>
<b>الخلاصة .....</b>	<b>ix</b>
<b>BAB I PENDAHULUAN.....</b>	<b>1</b>
1.1. Latar Belakang .....	1
1.2. Identifikasi Masalah .....	4
1.3. Batasan Masalah.....	4
1.4. Tujuan Penelitian .....	5
1.5. Manfaat Penelitian .....	5
1.6. Metodologi Penelitian .....	6
1.7. Sistematika Penulisan .....	7
<b>BAB II TINJAUAN PUSTAKA.....</b>	<b>9</b>
2.1. Penelitian Terkait .....	9
2.2. <i>Smart Card</i> .....	12
2.3. Kriptografi.....	13
2.3.1. Teori Kriptografi.....	13
2.3.2. Algoritma Kriptografi.....	16

2.3.2.1. Algoritma Kriptografi Simetris.....	16
2.3.2.1. Algoritma Kriptografi Asimetris.....	18
2.4. Algoritma RSA .....	19
<b>BAB III DESAIN DAN PERANCANGAN SISTEM.....</b>	<b>22</b>
3.1. Perancangan Sistem .....	22
3.1.1. Flowchart Sistem Untuk Enkripsi Data.....	23
3.1.2. Flowchart Sistem Untuk Deskripsi Data.....	24
3.1.3. Flowchart Algoritma Kriptografi RSA.....	25
3.2. Perancangan Database .....	30
3.2.1. Konteks Diagram.....	31
3.2.2. <i>Data Flow Diagram</i> Level 1.....	32
3.2.3. <i>Data Flow Diagram</i> Level 2.....	33
3.2.4. <i>Entity Relation Diagram</i> (ERD).....	34
3.3. Perancangan <i>Interface</i> .....	37
3.3.1. Rancangan <i>Interface</i> Halaman Utama.....	37
3.3.2. Rancangan <i>Interface</i> Login Admin.....	37
3.3.3. Rancangan <i>Interface</i> Tambah Admin.....	38
3.3.4. Rancangan <i>Interface</i> Data Mahasiswa.....	39
3.3.5. Rancangan <i>Interface</i> Data Mata Kuliah.....	39
3.3.6. Rancangan <i>Interface</i> Data Dosen.....	40
3.3.7. Rancangan <i>Interface</i> Data Ruang.....	41
3.3.8. Rancangan <i>Interface</i> Data Waktu.....	41
3.3.9. Rancangan <i>Interface</i> Data Jadwal.....	42
3.3.10. Rancangan <i>Interface</i> Data Praktikan.....	43
3.3.11. Rancangan <i>Interface</i> Absensi Mahasiswa.....	43
3.3.12. Rancangan <i>Interface</i> Laporan Absensi.....	44

3.3.13. Rancangan <i>Interface</i> Laporan Praktikan.....	45
<b>BAB IV IMPLEMENTASI DAN HASIL .....</b>	<b>46</b>
4.1. Lingkungan Implementasi.....	46
4.1.1. Lingkungan Perangkat Keras .....	46
4.1.2. Lingkungan perangkat Lunak .....	47
4.2. Implementasi Program .....	47
4.2.1. Implementasi <i>Interface</i> .....	47
4.2.1. <i>Interface</i> Halaman Utama.....	49
4.2.2. <i>Interface</i> Login Admin.....	49
4.2.3. <i>Interface Home</i> Halaman Admin.....	50
4.2.4. <i>Interface</i> Tambah Admin.....	51
4.2.5. <i>Interface</i> Data Mahasiswa.....	52
4.2.6. <i>Interface</i> Data Mata Kuliah.....	53
4.2.7. <i>Interface</i> Data Dosen.....	53
4.2.8. <i>Interface</i> Data Ruang.....	54
4.2.9. <i>Interface</i> Data Waktu.....	55
4.2.10. <i>Interface</i> Data Jadwal.....	56
4.2.11. <i>Interface</i> Data Praktikan.....	57
4.2.12. <i>Interface</i> Absensi Mahasiswa.....	58
4.2.13. <i>Interface</i> Laporan Absensi.....	59
4.2.14. <i>Interface</i> Laporan Praktikan.....	60
4.2.2. Implementasi Prosedural .....	60
4.2.2.1. <i>Source Code</i> Pembangkitan Kunci Algoritma RSA.....	61
4.2.2.2. <i>Source Code</i> Enkripsi Algoritma RSA.....	65
4.2.2.3. <i>Source Code</i> Deskripsi Algoritma RSA.....	66
4.3. Pengujian dan Hasil Uji Coba Sistem.....	66

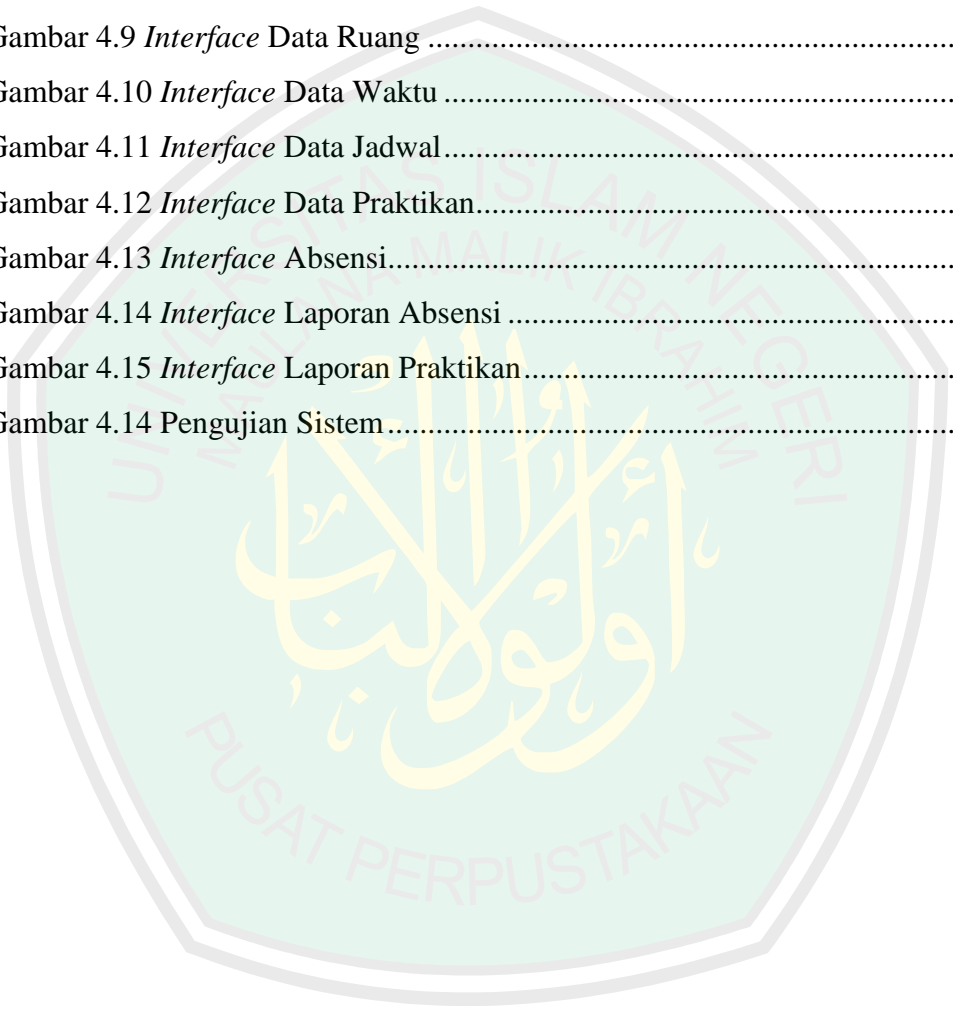
4.3.1. Pengujian Sistem .....	66
4.3.2. Hasil Uji Coba Sistem .....	70
4.3.2.1. Hasil Uji Coba Enkripsi Algoritma RSA .....	70
4.3.2.2. Hasil Uji Coba Autentifikasi <i>Smart Card</i> .....	72
4.3.2.3. Hasil Uji Coba Implementasi Algoritma RSA .....	73
4.4. Integrasi Kriptografi Menurut Kajian dalam Al Qur'an .....	73
<b>BAB V KESIMPULAN DAN SARAN .....</b>	<b>76</b>
A. Kesimpulan .....	76
B. Saran.....	76
<b>DAFTAR PUSTAKA .....</b>	<b>78</b>



## DAFTAR GAMBAR

Gambar 2.1 Diagram Proses Enkripsi dan Deskripsi.....	16
Gambar 2.2 Diagram Proses Enkripsi dan Deskripsi Algoritma Simetris.....	17
Gambar 2.3 Diagram Proses Enkripsi dan Deskripsi Algoritma Asimetris.....	18
Gambar 3.1 <i>Flowchart</i> Sistem (Enkripsi Data).....	23
Gambar 3.2 <i>Flowchart</i> Sistem (Deskripsi Data).....	24
Gambar 3.3 <i>Flowchart</i> Pembangkitan Kunci Algoritma RSA .....	26
Gambar 3.4 <i>Flowchart</i> Enkripsi Algoritma RSA .....	27
Gambar 3.5 <i>Flowchart</i> Deskripsi Algoritma RSA.....	29
Gambar 3.6 Simbol dalam DFD .....	30
Gambar 3.7 Diagram Konteks.....	31
Gambar 3.8 DFD Level 1.....	32
Gambar 3.9 DFD Level 2.....	33
Gambar 3.10 <i>Entity Relation Diagram</i> (ERD).....	34
Gambar 3.11 Rancangan <i>Interface</i> Halaman Utama.....	37
Gambar 3.12 Rancangan <i>Interface Login Admin</i> .....	38
Gambar 3.13 Rancangan <i>Interface Tambah Admin</i> .....	38
Gambar 3.14 Rancangan <i>Interface Data Mahasiswa</i> .....	39
Gambar 3.15 Rancangan <i>Interface Data Matakuliah</i> .....	40
Gambar 3.16 Rancangan <i>Interface Data Dosen</i> .....	40
Gambar 3.17 Rancangan <i>Interface Data Ruang</i> .....	41
Gambar 3.18 Rancangan <i>Interface Data Waktu</i> .....	42
Gambar 3.19 Rancangan <i>Interface Data Jadwal</i> .....	42
Gambar 3.20 Rancangan <i>Interface Data Praktikan</i> .....	43
Gambar 3.21 Rancangan <i>Interface Absensi Mahasiswa</i> .....	44
Gambar 3.22 Rancangan <i>Interface Laporan Absensi</i> .....	44
Gambar 3.23 Rancangan <i>Interface Laporan Praktikan</i> .....	45
Gambar 4.1 Struktur Menu Program.....	48
Gambar 4.2 <i>Interface</i> Halaman Utama .....	49
Gambar 4.3 <i>Interface Login Admin</i> .....	50

Gambar 4.4 <i>Interface Home</i> Halaman Admin .....	50
Gambar 4.5 <i>Interface</i> Tambah Admin .....	51
Gambar 4.6 <i>Interface</i> Data Mahasiswa.....	52
Gambar 4.7 <i>Interface</i> Data Matakuliah.....	53
Gambar 4.8 <i>Interface</i> Data Dosen.....	54
Gambar 4.9 <i>Interface</i> Data Ruang .....	55
Gambar 4.10 <i>Interface</i> Data Waktu .....	55
Gambar 4.11 <i>Interface</i> Data Jadwal.....	56
Gambar 4.12 <i>Interface</i> Data Praktikan.....	57
Gambar 4.13 <i>Interface</i> Absensi.....	58
Gambar 4.14 <i>Interface</i> Laporan Absensi .....	59
Gambar 4.15 <i>Interface</i> Laporan Praktikan.....	60
Gambar 4.14 Pengujian Sistem.....	67



## DAFTAR TABEL

Tabel 4.1 Hasil Uji Coba Enkripsi .....	70
Tabel 4.2 Hasil Uji Coba Autetifikasi <i>Smart Card</i> .....	72
Tabel 4.3 Hasil Uji Coba Implementasi Algoritma RSA.....	73





## ABSTRAK

Widiasari, Anugrah. 2014. Implementasi Algoritma Kriptografi RSA pada Aplikasi *Smart Card*. Skripsi. Jurusan Teknik Informatika Fakultas Sains dan Teknologi Universitas Islam Negeri Maulana Malik Ibrahim Malang. Pembimbing: (I) Dr. Muhammad Faisal, M.T., (II) Totok Chamidy, M.Kom.

Kata Kunci : *Smart card, Algoritma RSA, keamanan data*

*Smart card* merupakan sebuah teknologi identifikasi yang sedang dikembangkan oleh para ilmuwan. *Smart card* adalah kartu plastik yang berukuran sama dengan kartu kredit yang di dalamnya terdapat *chip* silikon yang mempunyai kemampuan untuk memproses dan menyimpan data tersebut secara aman. *Smart card* merupakan salah satu teknologi yang paling rentan terhadap pencurian informasi/data karena merupakan media pertukaran data yang berbasis kartu. Dalam pertukaran data dapat dimanipulasi isinya oleh pihak ketiga sehingga data dengan isi yang berbeda akan diterima oleh penerima. Oleh karena itu dibutuhkan mekanisme untuk mengamankan data yang disimpan di dalam *smart card*, sehingga data tersebut tidak dapat dibaca ataupun dimanipulasi oleh pihak yang tidak berwenang.

Dalam penelitian ini digunakan algoritma kriptografi RSA untuk mengamankan data yang ada di dalam *smart card*. RSA merupakan algoritma kriptografi asimetris yang menggunakan sepasang kunci, yaitu kunci publik dan kunci pribadi. Keamanan algoritma RSA terletak pada sulitnya memfaktorkan bilangan prima. Dalam penelitian ini pengujian dilakukan dengan memasukkan data id mahasiswa, id jadwal, dan jumlah absen ke dalam *smart card*. Data tersebut dienkripsi menggunakan algoritma kriptografi RSA, sehingga data yang disimpan ke dalam *smart card* berupa data *ciphertext* yang tidak bisa dibaca oleh pihak yang tidak berwenang. Hasil pengujian terhadap implementasi algoritma RSA, menghasilkan nilai akurasi sebesar 100%.

## ABSTRACT

Widiasari, Anugrah. 2014. Implementations of RSA cryptographic algorithms Smart Card Applications. Thesis. Department of Informatics, Faculty of Science and Technology of the State Islamic University of Maulana Malik Ibrahim Malang. Preceptor: (I) Dr. Muhammad Faisal, M.T., (II) Totok Chamidy, M.Kom.

Keyword : *Smart card, RSA algorithms, Data Security*

The Smart Card is an identification technology that is being developed by scientists. Smart cards have the ability to process and store this data securely. Smart cards are one of the technologies that are vulnerable to information theft because it is a data exchange based media cards. Data can be manipulated in exchange of its contents by a third party, so that the data with different content will be accepted by the recipient. Therefore it needs a mechanism to secure the data stored on the smart card, so that the data cannot be read or manipulated by unauthorized parties.

In this research was used RSA Cryptographic algorithms to secure data in a smart card. RSA is an asymmetric cryptographic algorithms that uses a pair of keys, a public key and private key. The security of RSA algorithm in the difficulty factor primes. In this research, testing is done by entering id of student, id of schedule, and the number of absences to the smart card. The Data stored in the smart card encrypted with RSA Cryptographic algorithms, so that the data stored in the smart card is ciphertext form. The test results of the implementation of the RSA algorithm, yielding a value of 100% accuracy.

## الخلاصة

ويديّة ساري، انوغرة 2014. تنفيذ التشفير خوارزمي RSA: للتطبيقات البطاقة الذكية. المقالة. قسم المعلوماتية في كلية العلوم والتكنولوجيا في جامعة الحكومية الإسلامية مولانا الكاثير ااهيم الانج.

المسرف : 1- محمد فيسل 2- توتوك حامدى

كلمات البحث : البطاقة الذكية, خوارزمي RSA

البطاقة الذكية هي تقنية التعرف على الهوية التي يتم تطويرها من قبل العلماء. البطاقة الذكية هي بطاقة بلاستيكية وهذا هو نفس حجم بطاقة الائتمان التي يوجد فيها رقاقة السيليكون التي لديها القدرة على معالجة وتخزين البيانات وتبادل البيانات / البيانات بشكل آمن. تقنية البطاقة الذكية هي واحدة من أكثر عرضة لسرقة المعلومات على بطاقة الوسائط. فيتبادل البيانات يمكن التلاعب بهامن قبل طرف ثالث حيث سيتم استلام محتويات البيانات مع محتويات مختلفة من قبل المستلم. لذلك، فإن يحتاج إلى تأمين البيانات المخزنة في البطاقة الذكية، لذلك أن البيانات لا يمكن قراءة أو التلاعب بهامن قبل أطراف غير مصرح بها.

في هذه الدراسة استخدم خوارزميات التشفير لـ RSA انات الموجودة في البطاقة الذكية. هي خوارزمية RSA غير المتماثلة التي تستخدم زوج مفاتيح، وهما المفتاح العام والمفتاح الخاص. خوارزمية الأمان يمكن RSA العمليّة. في هذا البحث، ويتم اختبار عن طريق إدخال البيانات هوية الطالب، والجدول الزمني الهوية، وعدد الغياب بالبطاقة الذكية. يتم تشفير البيانات باستخدام خوارزمية التشفير، حتى أن البيانات المخزنة في البطاقة الذكية، RSA للنص المشفر البيانات التي لا يمكن قراءتها من قبل أطراف غير مصرح بها. نتائج الاختبار لتنفيذ خوارزمية، مما أسفر عن قيمة RSA، 100% من الدقة.

## BAB I

### PENDAHULUAN

#### 1.1. Latar Belakang

Dewasa ini dunia elektronika semakin berkembang, salah satu perkembangannya adalah teknologi *smart card*. *Smart card* banyak diproduksi untuk menggantikan teknologi kartu data magnetik yang banyak digunakan sebelumnya. *Smart card* adalah kartu plastik yang di dalamnya terdapat *chip* silikon yang disebut mikrokontroler. *Chip* merupakan *integrated circuit* yang terdiri dari prosesor dan memori. *Smart card* mempunyai kemampuan untuk memproses dan menginterpretasikan data, serta menyimpan data tersebut secara aman. Apalagi dengan perkembangan algoritma kriptografi, data yang disimpan akan dienkripsi terlebih dahulu, sehingga tidak mudah dibaca oleh pihak yang tidak berwenang/berhak (Margoselo, 2003).

Dalam beberapa tahun terakhir ini, beberapa institusi di Indonesia telah mencoba menggunakan *smart card* meskipun dalam skala yang masih terbatas. Misalnya Pemerintah Kabupaten Jember yang menerapkan penggunaan *smart card* ke dalam kartu pegawai yang juga diintegrasikan dengan kartu bank yang masih berbasis pada strip magnetis. Beberapa institusi lain juga sudah merencanakan untuk menggunakan *smart card* misalnya kartu tol, Kartu subsidi BBM, dan lain-lainnya (Depkominfo, 2008). Pada tahun 2013 Pertamina sudah menyiapkan anggaran sekitar Rp 2 triliun untuk membuat *smart card* BBM dan infrastruktur, seperti yang dibuat PT AKR Corporindo Tbk (detik.com, 2012).

Pada perkembangannya *smart card* banyak diterapkan dalam berbagai bidang, salah satunya dalam bidang akademik yaitu pada sistem absensi. Absensi memegang peranan penting dalam kegiatan perkuliahan. Absensi merupakan salah satu penunjang yang dapat memotivasi setiap kegiatan serta sebagai informasi kedisiplinan mahasiswa. Informasi mengenai kehadiran mahasiswa menentukan prestasi mahasiswa tersebut dan dapat menjadi parameter kemajuan suatu instansi.

Saat ini proses pengambilan data absen praktikum jurusan Teknik Informatika UIN Maulana Malik Ibrahim Malang masih dilakukan dengan cara manual. Proses pengambilan data absen menggunakan kertas dan alat tulis dapat menjadi faktor yang menyulitkan dalam pemrosesan data absen lebih lanjut karena data harus tetap diketik satu demi satu secara manual. Hal tersebut dapat mengakibatkan terbukanya peluang manipulasi, kesalahan pencatatan, maupun hilangnya catatan kehadiran seorang mahasiswa. Selain itu kelemahan lain dari pencatatan absensi secara manual adalah kurangnya efisiensi waktu dalam melakukan absensi.

Untuk menangani masalah-masalah tersebut, maka dirancanglah sistem pengelolaan kehadiran yang baru dengan memanfaatkan teknologi *smart card*. Akan tetapi seiring dengan kegunaannya, *smart card* mempunyai masalah yang penting untuk diperhatikan yaitu keamanannya. *Smart card* merupakan salah satu teknologi yang paling rentan terhadap pencurian informasi/data karena merupakan media pertukaran data yang berbasis kartu. Dalam pertukaran data dapat dimanipulasi isinya oleh pihak ketiga sehingga data dengan isi yang berbeda akan

diterima oleh penerima. Oleh karena itu dibutuhkan mekanisme untuk mengamankan data sehingga data tersebut tidak dapat dibaca ataupun dimanipulasi oleh pihak yang tidak berwenang.

Menjamin keamanan merupakan hal yang perlu dilakukan untuk menjaga data/informasi dari pihak yang tidak berwenang. Seperti yang dijelaskan dalam Al Qur'an surah Al Waaqi'ah ayat 77-80 sebagai berikut:

إِنَّهُ لَقُرْآنٌ كَرِيمٌ ﴿٧٧﴾ فِي كِتَابٍ مَّكْنُونٍ ﴿٧٨﴾ لَا يَمَسُّهُ إِلَّا الْمُطَهَّرُونَ ﴿٧٩﴾ تَنْزِيلٌ مِّن رَّبِّ الْعَالَمِينَ ﴿٨٠﴾

Artinya : “bahwa sesungguhnya (yang dibacakan kepada kamu) itu ialah Al Qur'an yang mulia. Yang tersimpan dalam Kitab yang cukup terpelihara. Yang tidak disentuh melainkan oleh makhluk-makhluk yang disucikan. Al Qur'an itu diturunkan dari Allah Tuhan sekalian alam.” (QS Al Waaqi'ah (56) : 77-80 )

Dari ayat di atas dijelaskan tentang jaminan Allah SWT terhadap Al Qur'an. Allah memelihara Al Qur'an dari upaya syetan yang ingin mengubah isi dari Al Qur'an, sehingga Al Qur'an tetap terjaga kesucian dan kemurniannya.

Ada beberapa cara untuk mengamankan data, misalnya dengan menggunakan password pada data yang harus diamankan sehingga hanya dapat dibuka oleh orang yang berhak. Tetapi hal tersebut kurang praktis diterapkan pada *smart card*. Cara lain untuk mengamankan data adalah dengan mengimplementasikan kriptografi pada data yang akan diamankan, sehingga data dapat terjaga keamanan rahasianya walaupun terakses oleh pihak yang tidak berwenang. Kriptografi merupakan teknik mengamankan pesan/data sehingga terjaga kerahasiaannya. Dalam teknik kriptografi, data dienkripsi untuk mengubah

*plaintext* menjadi *ciphertext*, sehingga data tersebut tidak dapat dibaca oleh pihak yang tidak berwenang.

Oleh karena itu aplikasi *smart card* untuk absensi kegiatan praktikum ini mengimplementasikan algoritma kriptografi RSA (Rivest Shamir Adleman) sebagai keamanan datanya. RSA merupakan algoritma kriptografi asimetris yang menggunakan sepasang kunci, yaitu kunci publik dan kunci pribadi. Keamanan algoritma RSA terletak pada sulitnya memfaktorkan bilangan prima. Dengan penggunaan teknologi *smart card*, data yang diperlukan disimpan dan diproses lebih aman dengan adanya kriptografi.

## **1.2. Identifikasi Masalah**

Dari uraian latar belakang di atas, maka hal yang dapat diidentifikasi adalah bagaimana mengatasi masalah keamanan pada aplikasi *smart card* menggunakan algoritma kriptografi RSA. Penelitian ini dilakukan untuk mengetahui hasil dari penerapan algoritma kriptografi RSA untuk menjaga keamanan data di *smart card*.

## **1.3. Batasan Masalah**

Dalam penyusunan tugas akhir ini, penyusun perlu untuk membatasi masalah yang akan dibahas. Adapun masalah yang dibatasi oleh penyusun adalah sebagai berikut :

1. Aplikasi yang dibangun adalah aplikasi smart card untuk presensi praktikum.
2. *Smart card reader* yang digunakan adalah ACR38 dan kartu SLE 4428.
3. Bahasa pemrograman yang digunakan adalah *Visual Basic*.
4. Data yang diolah berupa data absensi.
5. Setiap kartu hanya mempunyai satu data identitas.

#### **1.4. Tujuan Penelitian**

Tujuan dari penelitian ini adalah mengamankan data yang tersimpan di dalam *smart card* menggunakan algoritma kriptografi RSA.

#### **1.5. Manfaat Penelitian**

Manfaat dari penelitian ini adalah sebagai berikut :

1. Data yang di simpan di dalam smart card lebih aman dengan adanya kriptografi.
2. Membuat pencatatan absensi kehadiran praktikum mahasiswa menjadi lebih mudah dan efisien.
3. Aplikasi ini diharapkan dapat mengurangi terjadinya kesalahan dalam pencatatan kehadiran mahasiswa pada saat praktikum.
4. Dapat meminimalisasikan waktu yang terbuang pada saat melakukan absensi.



## 1.6. Metodologi Penelitian

Dalam penelitian ini digunakan metode sebagai berikut :

### 1. Pengumpulan data dan studi literature

Pada tahap ini dilakukan pencarian dan pemahaman literatur serta pengumpulan informasi tentang *smart card* dan algoritma kriptografi RSA yang akan diimplementasikan untuk keamanan data pada *smart card*. Literatur yang digunakan meliputi buku referensi, buku Tugas Akhir mahasiswa jurusan Teknik Informatika serta dokumentasi dari internet.

### 2. Perumusan Masalah dan Penyelesaiannya

Tahap ini meliputi perumusan masalah, batasan-batasan masalah dan penyelesaiannya.

### 3. Perancangan dan desain aplikasi

Pada tahap ini akan dilakukan perancangan desain mengenai aplikasi *smart card* untuk absensi kegiatan praktikum yang akan dibangun berdasarkan teori yang telah dipahami.

### 4. Implementasi sistem

Pada tahap ini akan dilakukan pembangunan aplikasi *smart card* untuk absensi kegiatan praktikum, yang mana dalam pembangunan aplikasi tersebut akan diterapkan teori/algoritma yang telah dipelajari yaitu algoritma kriptografi RSA.

## 5. Pengujian aplikasi

Uji coba dilakukan sampai sistem benar – benar *ready to use*, kekurangan yang terjadi diperbaiki dalam lingkup batasan masalah. Evaluasi dilakukan untuk mengetahui apakah sistem yang dibangun sudah sesuai yang diharapkan.

## 6. Penyusunan laporan

Penyusunan laporan akhir merupakan dokumentasi dari keseluruhan pelaksanaan penelitian dan diharapkan bermanfaat bagi penelitian lebih lanjut

## 1.7. Sistematika Penulisan

### **BAB I Pendahuluan**

Bab ini berisi latar belakang, perumusan masalah, tujuan, batasan masalah dan metodologi penelitian tugas akhir ini.

### **BAB II Landasan Teori**

Bab ini menjelaskan konsep dan teori dasar yang mendukung penulisan tugas akhir ini seperti cara kerja *smart card* dan algoritma kriptografi RSA

### **BAB III Analisis dan Perancangan Aplikasi**

Bab ini menjelaskan mengenai analisis dan perancangan aplikasi presensi dengan menggunakan *smart card* serta implementasi algoritma kriptografi RSA sebagai keamanan datanya.

#### **BAB IV Hasil dan Pembahasan**

Bab ini berisi hasil pengujian terhadap pengujian dari aplikasi yang telah dibangun.

#### **BAB V**

Bab ini berisi kesimpulan dan saran terhadap seluruh kegiatan tugas akhir yang telah dilakukan.



## BAB II

### TINJAUAN PUSTAKA

#### 2.1. Penelitian Terkait

Berikut ini adalah beberapa penelitian terdahulu yang berkaitan dengan penelitian yang akan dilakukan :

Pada tahun 2008 penelitian oleh Tri Rahajoeningroem dan Muhammad Riza dari Jurusan Teknik Elektro Universitas Komputer Indonesia pada jurnal penelitian yang berjudul Studi dan Implementasi Algoritma RSA untuk Pengamanan Data Transkrip Akademik Mahasiswa. Penelitian ini membahas proses enkripsi (penyandian data) nilai transkrip akademik mahasiswa menggunakan algoritma RSA, dan proses dekripsi (pengembalian data asli), serta proses pembangkitan kunci. Kinerja yang diukur dari algoritma RSA ini waktu komputasi serta kompleksitas memori yang dibutuhkan dalam melakukan enkripsi dan dekripsi data. Sebuah perangkat lunak berbasis LabVIEW dibangun untuk implementasi algoritma RSA ini. Hasil pengujian menunjukkan bahwa algoritma RSA berhasil diimplementasikan untuk pengamanan data transkrip akademik mahasiswa. Kelebihannya, algoritma RSA merupakan algoritma kriptografi yang memiliki tingkat keamanan cukup tinggi, akan tetapi resource yang dibutuhkan tidak terlalu besar, sehingga cocok diimplementasikan untuk pengamanan data transkrip akademik mahasiswa.

Pada tahun 2008 penelitian oleh Stefanus Astrianto dari Sekolah Tinggi Elektro dan Informatika, Institut Teknologi Bandung pada jurnal penelitian yang berjudul Pembangunan Perangkat Lunak untuk *Security* pada *Contactless Smart Card* dengan Algoritma RC4. Penelitian ini membahas mengenai perangkat lunak yang berfungsi untuk menambah aspek keamanan dalam sebuah *contactless smart card* tipe mifare 1Kb dengan bantuan *card reader device* ACR120U. Perangkat lunak tersebut beroperasi dengan cara mengubah konfigurasi di dalam *smart card* serta mengenkripsi data yang akan ditulis ke dalam kartu . algoritma Enkripsi yang digunakan adalah RC4 dan MD5 Hash. Hasil dari penelitian ini adalah perangkat lunak mampu menambah aspek keamanan dalam Mifare *contactless smart card* yaitu dengan cara mengubah kunci *login* dan mengenkripsi data. Kelebihan dari sistem tersebut adalah perangkat lunak yang dibangun lebih aman dengan mengimplementasikan 2 algoritma kriptografi.

Pada tahun 2010 penelitian oleh Adrianus Triorizka dari Sekolah Tinggi Manajemen Informatika dan Komputer AMIKOM Yogyakarta dalam jurnal penelitian yang berjudul Penerapan Algoritma RSA untuk Pengamanan Data dan *Digital Signature* dengan .Net. Penelitian ini membahas mengenai proses enkripsi/dekripsi menggunakan algoritma RSA dan *digital signature* menggunakan kunci *public* dan kunci *private*. Hasil dari penelitian ini adalah sebuah model kriptosistem untuk mengenkripsi dan mendekripsi data. Kelebihan dari sistem tersebut adalah sistem mampu mengamankan data yang penting dan rahasia sekaligus melakukan *digital signature* yang dapat digunakan secara luas di berbagai bidang.

Pada tahun 2013 penelitian oleh Martha Monica dari Sekolah Elektro dan Informatika Institut Teknologi Bandung dalam jurnal penelitian yang berjudul Pemanfaatan Algoritma Kriptografi dalam Pembuatan *Smart Card*. Penelitian ini membahas mengenai perbandingan dari berbagai algoritma kriptografi yang dapat dimanfaatkan dalam menjaga keamanan informasi dalam sebuah *smart card*. Terdapat 3 algoritma kriptografi yang dibandingkan dalam penelitian ini, yaitu algoritma El Gamal, RSA, dan DES. Hasilnya algoritma RSA yang paling cocok digunakan pada sebuah *smart card* dibandingkan algoritma El Gamal dan DES. Walaupun tingkat keamanan pada RSA tidak setinggi algoritma El Gamal, namun masih lebih aman dibandingkan DES. *Resource* yang dibutuhkan juga tidak sebesar algoritma El Gamal sehingga algoritma RSA dapat menjadi pilihan yang tepat untuk penjagaan keamanan informasi yang tersimpan pada *smart card*.

Pada tahun 2013 penelitian oleh Mochamad Julianto Sukarno dalam jurnal penelitian yang berjudul Analisis dan Implementasi Kriptografi El Gamal dan Algoritma Luhn untuk Keamanan Data pada *Smart Card*. Penelitian ini bertujuan untuk membuat sistem penyandian data dengan teknik kriptografi El Gamal dan algoritma Luhn yang digunakan untuk pencegahan penggandaan informasi pada *smart card*. Hasilnya adalah hasil enkripsi dapat secara kuat mempertahankan kerahasiaan data dan sukses ketika diimplementasikan pada *smart card*. Kelebihan dari sistem tersebut adalah sistem mampu memberikan *security* pada *smart card* sehingga kartu yang bersangkutan aman dari penggandaan kartu.

## 2.2. Smart Card

*Smart card* adalah kartu plastik yang berukuran sama dengan kartu kredit yang di dalamnya terdapat *chip* silikon yang disebut mikrokontroler. *Chip* merupakan *integrated circuit* yang terdiri dari prosesor dan memori. *Chip*, seperti layaknya CPU (*CentralProcessingUnit*) di komputer, bertugas melaksanakan perintah dan menyediakan power ke *smart card* (Sariasih, 2009). *Smart card* didesain untuk menyimpan data yang bersifat pribadi dengan tingkat keamanan yang tinggi dan kartu mudah untuk dibawa kemana saja (*portable*).

*Contact smart card* bekerja dengan cara berkomunikasi secara fisik antara *card reader* dan *smart card's pin contact*. *Contact smart card* memiliki chip kecil keemasan pada kartu, saat dibaca oleh *reader*, *chip* tersebut melakukan kontak dengan konektor yang dapat membaca informasi dari *chip*, dan dapat menuliskan informasi kembali kedalam *chip* (Akbar, 2011). *Contact smart card* tidak membutuhkan baterai dan akan aktif ketika terhubung dengan *card reader*. Saat terhubung dengan *reader*, maka *chip* menunggu perintah *request* dari client/host dari aplikasi untuk membaca informasi dari *chip* atau menulis informasi ke *chip*. Aplikasi yang melakukan proses dapat Anda letakkan pada host / komputer, bersamaan dengan database atau tools yang diperlukan oleh aplikasi.

Beberapa jenis *Smart card* masa kini memiliki *chip microprocessor* serta *memory* didalamnya sehingga *Smart card* itu sendiri mampu menjalankan berbagai aplikasi seperti memproses data, melakukan proteksi terhadap data, serta melakukan proses otentifikasi (Rijal Fakhruddin, 2006).

Berlawanan dengan kartu magnetik, atau teknologi otentikasi lainnya, smart card multifungsi yang lebih canggih dewasa ini memiliki fitur pengamanan yang luas. Fungsi pengamanan ini dapat memiliki aturan pengendalian akses yang lebih kompleks, seperti PIN, kunci simetris, biometrik dll seperti berikut:

- Akses kartu yang terlindungi PIN
- Verifikasi pemegang kartu
- Verifikasi kartu dan terminal
- Kriptografi
- Anti gangguan
- Biometrik

## 2.3.KRIPTOGRAFI

### 2.3.1. Teori Kriptografi

*Cryptography* berasal dari dua kata Yunani, yaitu *crypto* yang berarti rahasia dan *grapho* yang berarti menulis. Secara umum *cryptology* dapat diartikan sebagai ilmu dan seni penyandian yang bertujuan untuk menjaga keamanan dan kerahasiaan suatu pesan. *Cryptology* pada dasarnya sudah dikenal sejak lama. Menurut catatan sejarah, *cryptology* sudah digunakan oleh bangsa Mesir sejak 4000 tahun yang lalu oleh raja-raja Mesir pada saat perang untuk mengirimkan pesan rahasia kepada panglima perangnya melalui kurir-kurirnya (Ariyus, 2006).

Kriptografi adalah suatu ilmu yang mempelajari bagaimana cara menjaga agar data atau pesan tetap aman saat dikirimkan, dari pengirim ke



penerima tanpa mengalami gangguan dari pihak ketiga. Teknik untuk mengacak suatu pesan agar tidak dapat diketahui maknanya disebut enkripsi, dan membentuk suatu bidang keilmuan yang disebut Kriptografi. Prinsip dasarnya adalah menyembunyikan informasi sedemikian rupa agar orang yang berhak saja yang dapat mengetahui isi dari informasi yang disembunyi tersebut (Wibowo, 2008).

Prinsip-prinsip yang mendasari kriptografi yakni:

1. *Confidentiality* (kerahasiaan) yaitu layanan agar isi pesan yang dikirimkan tetap rahasia dan tidak diketahui oleh pihak lain (kecuali pihak pengirim, pihak penerima / pihak-pihak memiliki ijin). Umumnya hal ini dilakukan dengan cara membuat suatu algoritma matematis yang mampu mengubah data hingga menjadi sulit untuk dibaca dan dipahami.
2. *Data integrity* (keutuhan data) yaitu layanan yang mampu mengenali/mendeteksi adanya manipulasi (penghapusan, perubahan atau penambahan) data yang tidak sah (oleh pihak lain).
3. *Authentication* yaitu layanan yang berhubungan dengan identifikasi.
4. *Non-repudiation* (anti-penyangkalan) yaitu layanan yang dapat mencegah suatu pihak untuk menyangkal aksi yang dilakukan sebelumnya (menyangkal bahwa pesan tersebut berasal dirinya).

Berbeda dengan kriptografi klasik yang menitikberatkan kekuatan pada kerahasiaan algoritma yang digunakan (yang artinya apabila algoritma

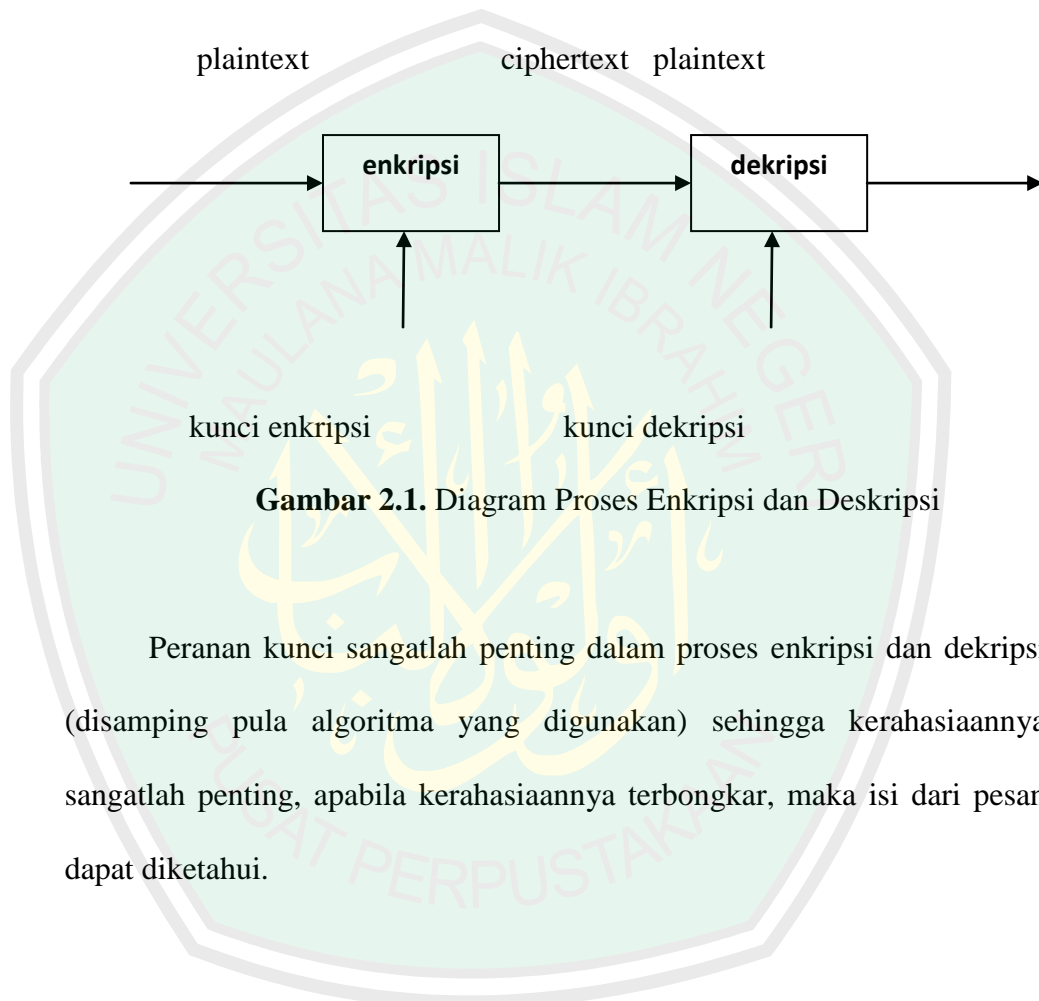
yang digunakan telah diketahui maka pesan sudah jelas "bocor" dan dapat diketahui isinya oleh siapa saja yang mengetahui algoritma tersebut), kriptografi modern lebih menitikberatkan pada kerahasiaan kunci yang digunakan pada algoritma tersebut (oleh pemakainya) sehingga algoritma tersebut dapat saja disebarakan ke kalangan masyarakat tanpa takut kehilangan kerahasiaan bagi para pemakainya.

Berikut adalah istilah-istilah yang digunakan dalam bidang kriptografi:

- a. *Plaintext* (M) adalah pesan yang hendak dikirimkan (berisi data asli).
- b. *Ciphertext*(C) adalah pesan ter-enkrip (tersandi) yang merupakan hasil enkripsi.
- c. Enkripsi (fungsi E) adalah proses perubahan plaintext menjadi *ciphertext*.
- d. Dekripsi (fungsi D) adalah kebalikan dari enkripsi yakni mengubah ciphertext menjadi plaintext, sehingga berupa data awal/asli.
- e. Kunci adalah suatu bilangan yang dirahasiakan yang digunakan dalam proses enkripsi dan dekripsi.

Kriptografi itu sendiri terdiri dari dua proses utama yakni proses enkripsi dan proses dekripsi. Enkripsi adalah suatu proses yang melakukan perubahan dari suatu kode yang bisa dimengerti menjadi tidak bisa dimengerti (tidak terbaca). Dekripsi adalah suatu proses dengan algoritma

yang sama untuk mengembalikan informasi yang tidak bisa dimengerti tadi menjadi bentuk aslinya (WAHANAKomputer, 2003). Pada gambar 2.1. dijelaskan diagram proses enkripsi dan dekripsi



**Gambar 2.1.** Diagram Proses Enkripsi dan Deskripsi

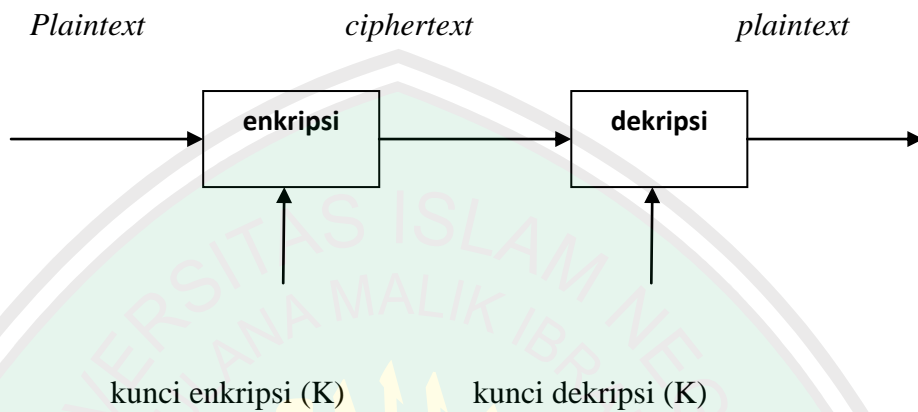
Peranan kunci sangatlah penting dalam proses enkripsi dan dekripsi (disamping pula algoritma yang digunakan) sehingga kerahasiaannya sangatlah penting, apabila kerahasiaannya terbongkar, maka isi dari pesan dapat diketahui.

### 2.3.2. Algoritma Kriptografi

#### 2.3.2.1. Algoritma Kriptografi Simetris

Algoritma simetris (*symmetric algorithm*) adalah suatu algoritma dimana kunci enkripsi yang digunakan sama dengan kunci dekripsi sehingga algoritma ini disebut juga sebagai *single-key algorithm*. Algoritma

ini memiliki kunci enkripsi sama dengan kunci dekripsi. Pada gambar 2.2 dijelaskan diagram proses enkripsi dan dekripsi algoritma simetris.



**Gambar 2.2.**Diagram proses enkripsi dan dekripsi algoritma simetris

Sebelum melakukan pengiriman pesan, pengirim dan penerima harus memilih suatu kunci tertentu yang sama untuk dipakai bersama, dan kunci ini haruslah rahasia bagi pihak yang tidak berkepentingan sehingga algoritma ini disebut juga algoritma kunci rahasia (*secret-key algorithm*).

Kelebihan algoritma kriptografi simetris adalah:

- a. Kecepatan operasi lebih tinggi bila dibandingkan dengan algoritma asimetrik.
- b. Karena kecepatannya yang cukup tinggi, maka dapat digunakan pada sistem *real-time*

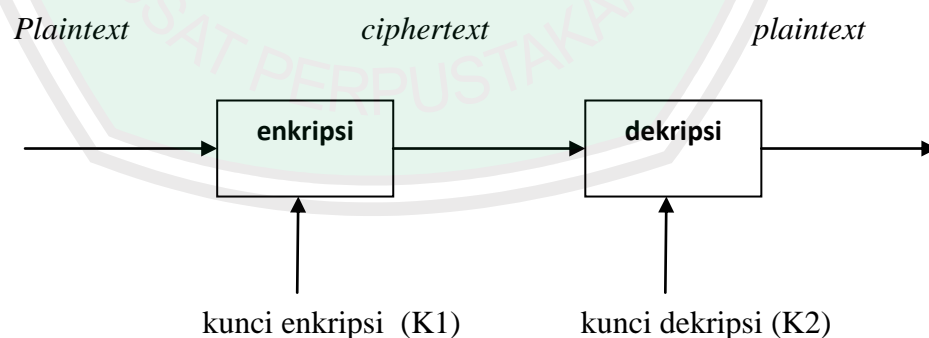
Kelemahan algoritma kriptografi simetris adalah:

- a. Untuk tiap pengiriman pesan dengan pengguna yang berbeda dibutuhkan kunci yang berbeda juga, sehingga akan terjadi kesulitan dalam manajemen kunci tersebut.

Contoh algoritma kriptografi simetris : TwoFish, Rijndael, Camellia

### 2.3.2.2. Algoritma Kriptografi Asimetris

Algoritma asimetris (*asymmetric algorithm*) adalah suatu algoritma dimana kunci enkripsi yang digunakan tidak sama dengan kunci dekripsi. Pada algoritma ini menggunakan dua kunci yakni kunci publik (*public key*) dan kunci privat (*private key*). Kunci publik disebarakan secara umum sedangkan kunci privat disimpan secara rahasia oleh si pengguna. Walau kunci publik telah diketahui namun akan sangat sukar mengetahui kunci privat yang digunakan. Pada gambar 2.3 dijelaskan diagram proses enkripsi dan dekripsi algoritma asimetris.



**Gambar 2.3.** Diagram proses enkripsi dan dekripsi algoritma asimetris

Pada umumnya kunci publik (*public key*) digunakan sebagai kunci enkripsi sementara kunci privat (*private key*) digunakan sebagai kunci dekripsi.

Kelebihan algoritma kriptografi asimetris :

- a. Masalah keamanan pada distribusi kunci dapat lebih baik
- b. Masalah manajemen kunci yang lebih baik karena jumlah kunci yang lebih sedikit

Kelemahan algoritma kriptografi asimetris:

- a. Kecepatan yang lebih rendah bila dibandingkan dengan algoritma simetris
- b. Untuk tingkat keamanan sama, kunci yang digunakan lebih panjang dibandingkan dengan algoritma simetris.

Contoh algoritma : RSA, DSA, ElGamal

#### **2.4. ALGORITMA RSA**

Algoritma RSA diuat oleh 3 orang peneliti dari MIT (*Massachusetts 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. Pemfaktoran dilakukan untuk memperoleh kunci privat. Selama

pemfaktoran bilangan besar menjadi faktor-faktor prima belum ditemukan algoritma yang mangkus, maka selama itu pula keamanan algoritma RSA tetap terjamin (Syaputra, 2012).

RSA memiliki dasar proses enkripsi dan dekripsinya pada konsep bilangan prima dan aritmatika modulo. Kunci dekripsi dan enkripsi keduanya merupakan bilangan bulat. Kunci enkripsi tidak dirahasiakan dan diketahui oleh umum sehingga kunci enkripsi biasa disebut juga dengan kunci publik, namun kunci untuk dekripsi bersifat rahasia. Kunci dekripsi dibangkitkan dari beberapa buah bilangan prima bersama-sama dengan kunci enkripsi. Untuk menemukan kunci dekripsi, terlebih dahulu harus memfaktorkan suatu bilangan non prima menjadi faktor primanya.

Algoritma pembangkitan kunci dalam algoritma RSA dapat dijelaskan sebagai berikut :

1. Pilih dua bilangan prima  $p \neq q$  secara acak dan terpisah untuk tiap-tiap  $p$  dan  $q$ .
2. Hitung  $N$  dengan persamaan:

$$N = p q.$$

3. Hitung  $\phi$  dengan persamaan:

$$\phi = (p-1)(q-1).$$

4. Pilih bilangan bulat (*integer*) antara satu dan  $\phi$  ( $1 < e < \phi$ ) yang juga merupakan *coprime* dari  $\phi$ .

5. Hitung  $d$  dengan persamaan :

$$de \equiv 1 \pmod{\phi}.$$

Hasil dari algoritma ini:

Kunci public : pasangan (N,e)

Kunci privat : pasangan (N,d)

Algoritma enkripsi yang digunakan dalam algoritma RSA dapat dijelaskan sebagai berikut :

1. Susun *plaintext* menjadi blok-blok  $m_1, m_2, \dots, m_n$
2. Hitung *ciphertext*  $c_i$  dengan rumus :

$$C_i = M_i^e \text{ mod } N$$

Algoritma dekripsi yang digunakan dalam algoritma RSA dapat dijelaskan sebagai berikut :

1. Gunakan kunci privat untuk menghitung  $M_i = C_i^d \text{ mod } N$
2. Carilah nilai  $m$  dengan rumus :

$$M_i = C_i^d \text{ mod } N$$



## BAB III

### DESAIN DAN PERANCANGAN SISTEM

Dalam proses pembuatan sebuah aplikasi dibutuhkan perencanaan terlebih dahulu. Hal ini bertujuan agar aplikasi yang dibuat dapat berfungsi dengan baik (sesuai dengan yang diharapkan). Bab ini membahas tentang desain dan perancangan aplikasi *smart card* absensi praktikum dengan mengimplementasikan algoritma kriptografi RSA sebagai keamanan datanya. Desain dan perancangan sistem ini meliputi perancangan sistem, perancangan data, perancangan *database*, dan perancangan *interface*.

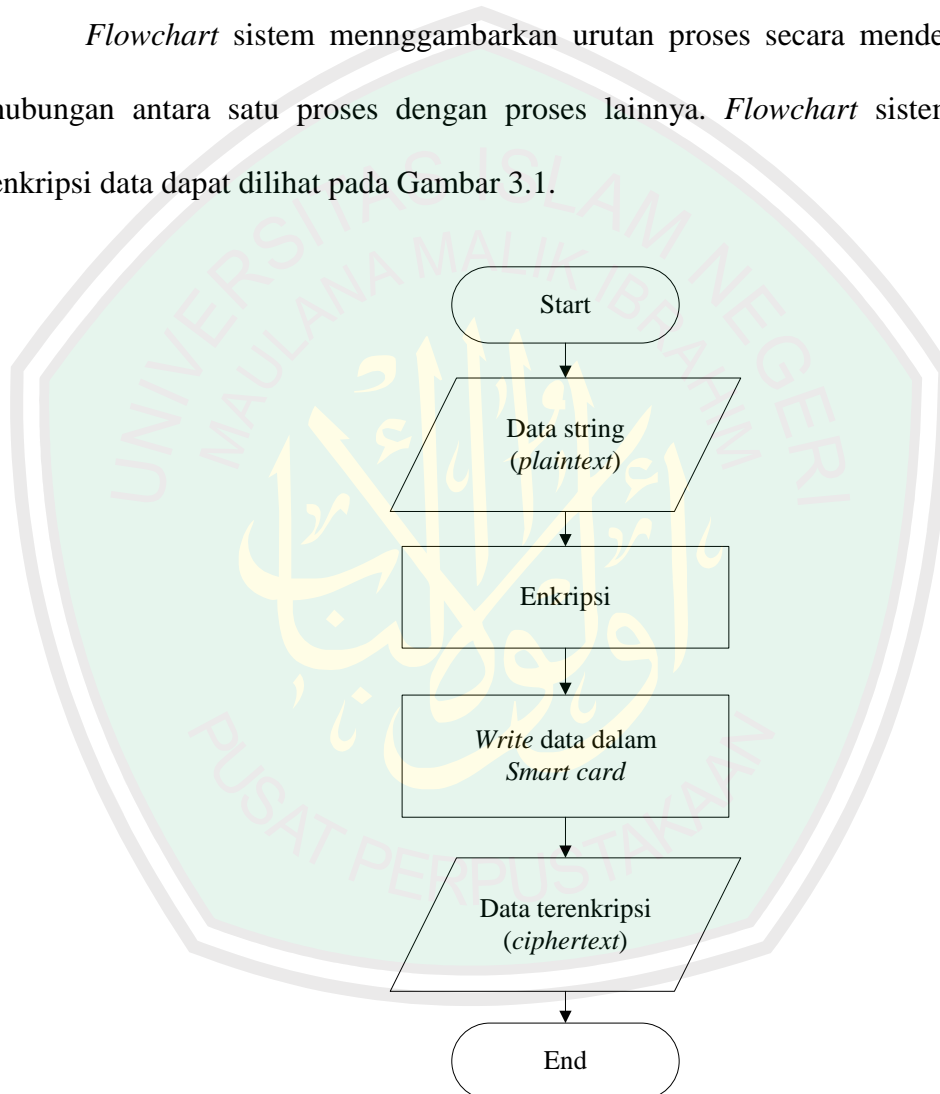
#### 3.1. Perancangan Sistem

Sub bab ini akan membahas mengenai perancangan sistem yang dikerjakan pada skripsi ini. Tujuan pembuatan sistem ini adalah menerapkan algoritma untuk mengamankan data sehingga data tersebut menjadi tidak dapat terbaca. Proses utama pada aplikasi ini adalah melakukan enkripsi pada data yang tersimpan dalam *smart card*, dan melakukan deskripsi pada saat pembacaan data dari *smart card*. Digunakan *Smart Card reader writer* yang merupakan perantara komunikasi antara *smart card* dengan peralatan lain seperti komputer. Komputer dapat membaca atau menulis data melalui *smart card reader writer*, kemudian *smart card reader writer* mengubah perintah membaca/menulis tersebut ke dalam bahasa yang dimengerti *smart card*. Berikut ini merupakan

*flowchart* sistem untuk enkripsi data yang disimpan di dalam *smart card* dan *flowchart* sistem untuk deskripsi data yang diambil (dibaca) dari *smart card*.

### 3.1.1. *Flowchart* Sistem untuk Enkripsi Data

*Flowchart* sistem menngambarkan urutan proses secara mendetail dan hubungan antara satu proses dengan proses lainnya. *Flowchart* sistem untuk enkripsi data dapat dilihat pada Gambar 3.1.



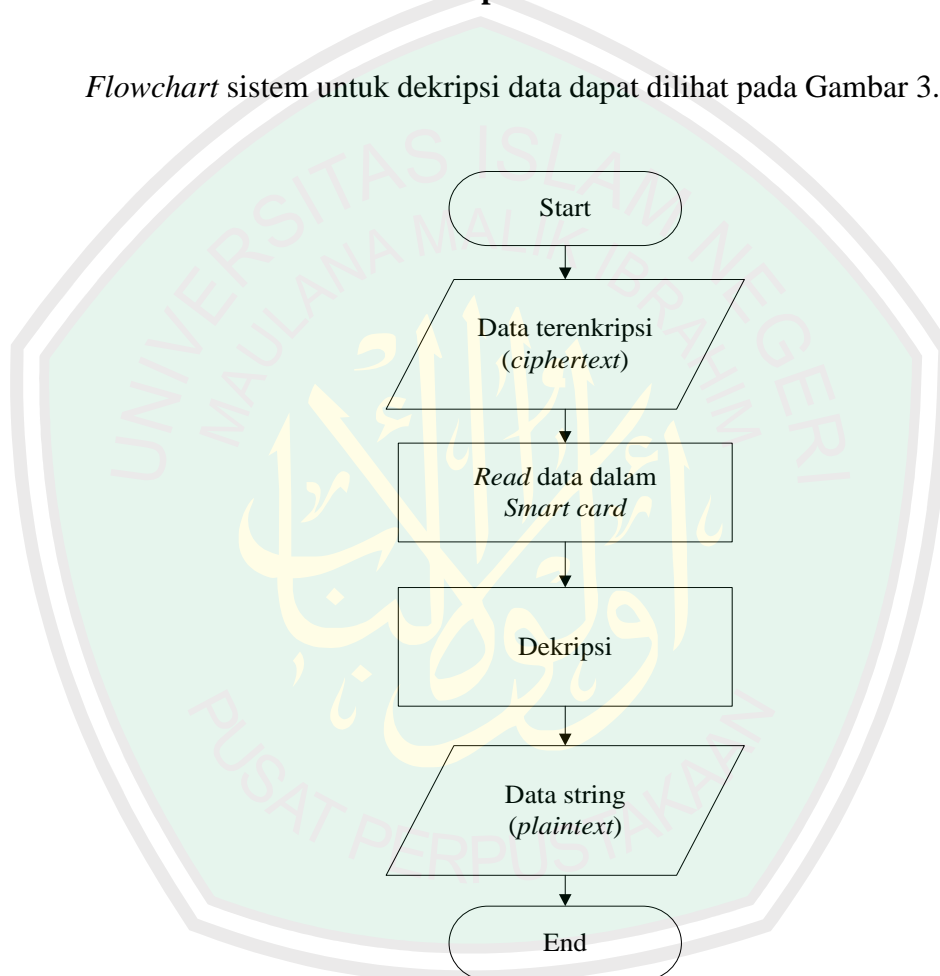
**Gambar 3.1.** *Flowchart* Sistem (enkripsi data)

Berdasarkan Gambar 3.1, pada sistem ini, data *input* yang akan diproses dalam penelitian ini adalah data *string* yang masih berupa *plaintext*. Sebelum dimasukkan ke dalam *smart card*, data *string* tersebut dienkripsi terlebih dahulu

menggunakan algoritma kriptografi. Data yang telah terenkripsi di simpan ke dalam *smart card* menggunakan *smart card reader writer ACR38*. *Ouput* dari proses ini adalah data yang telah terenkripsi (*ciphertext*).

### 3.1.2. Flowchart Sistem untuk Dekripsi Data

*Flowchart* sistem untuk dekripsi data dapat dilihat pada Gambar 3.2.



**Gambar 3.2.** *Flowchart* Sistem (dekripsi data)

Berdasarkan Gambar 3.2, data *input* yang akan diproses adalah data terenkripsi (*ciphertext*) yang tersimpan di dalam *smart card*. Data yang terenkripsi tersebut dibaca menggunakan *smart card reader writer ACR38* kemudian

didekripsi. *Output* dari proses ini adalah data asli yang berupa data string (*plaintext*).

### 3.1.3. Flowchart Algoritma Kriptografi RSA

Algoritma yang digunakan untuk mengenkripsi dan mendekripsi data adalah algoritma kriptografi RSA. Algoritma RSA itu sendiri merupakan algoritma asimetris, sehingga memiliki kunci *public* dan kunci *privat*.

RSA memiliki dasar proses enkripsi dan dekripsinya pada konsep bilangan prima dan aritmatika modulo. Kunci dekripsi dan enkripsi keduanya merupakan bilangan bulat. Kunci enkripsi tidak dirahasiakan dan diketahui oleh umum sehingga kunci enkripsi biasa disebut juga dengan kunci publik, namun kunci untuk dekripsi bersifat rahasia. Kunci deskripsi dibangkitkan dari beberapa buah bilangan prima bersama-sama dengan kunci enkripsi. Semakin besar bilangan non primanya maka semakin sulit pefaktorannya. Semakin sulit pefaktorannya, maka semakin kuat algoritma RSA-nya.

Algoritma pembangkitan kunci dalam algoritma RSA dapat dijelaskan sebagai berikut :

1. Dipilih dua bilangan prima  $p \neq q$  secara acak dan terpisah untuk tiap-tiap  $p$  dan  $q$ .

2. Hitung  $N$  dengan persamaan:

$$N = p q.$$

3. Hitung  $\phi$  dengan persamaan:

$$\phi = (p-1)(q-1).$$

4. dipilih bilangan bulat (*integer*) antara satu dan  $\phi$  ( $1 < e < \phi$ ) yang juga merupakan *coprime* dari  $\phi$ .
5. Hitung  $d$  dengan persamaan :

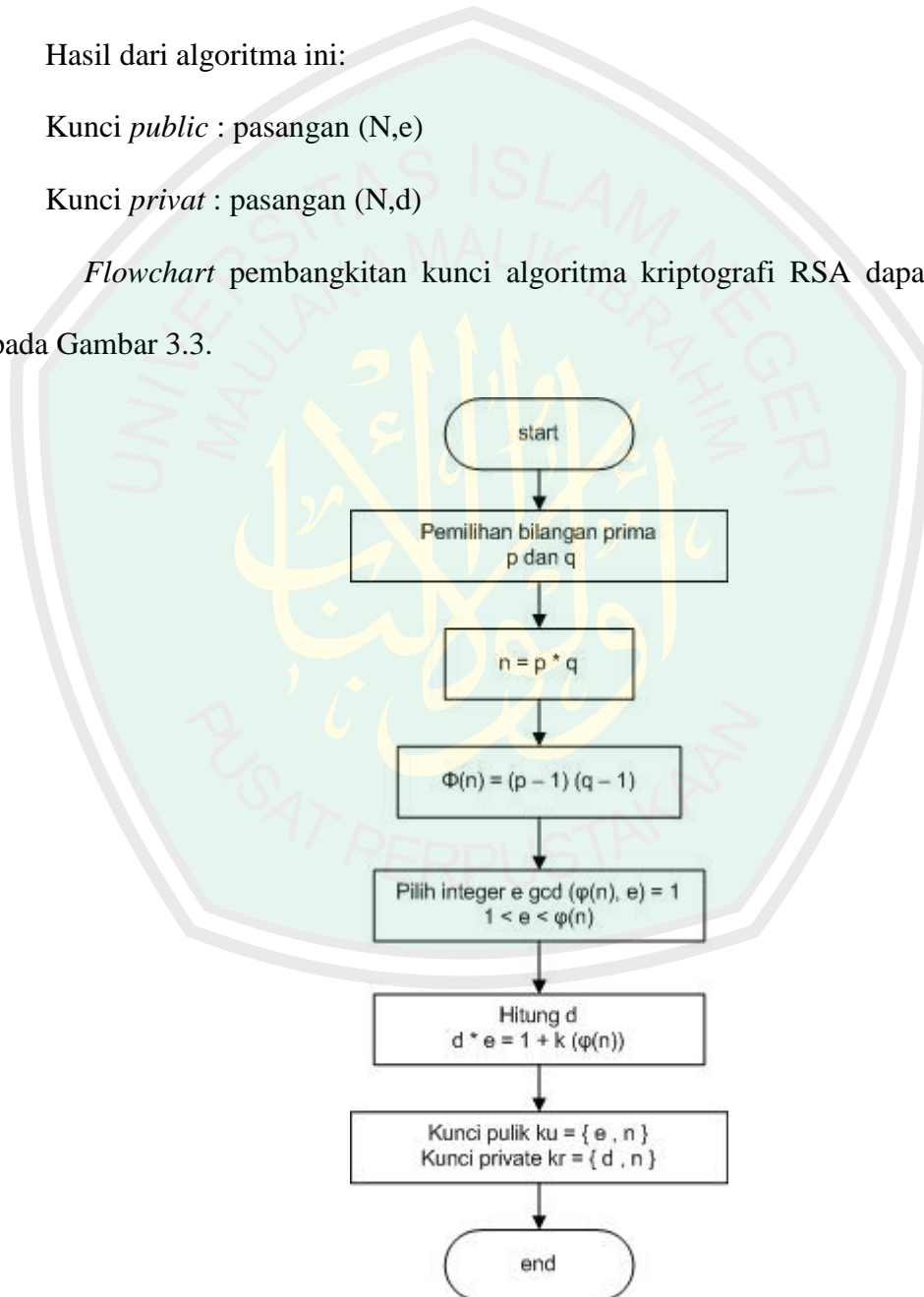
$$de \equiv 1 \pmod{\phi}.$$

Hasil dari algoritma ini:

Kunci *public* : pasangan  $(N,e)$

Kunci *privat* : pasangan  $(N,d)$

*Flowchart* pembangkitan kunci algoritma kriptografi RSA dapat dilihat pada Gambar 3.3.



**Gambar 3.3.** *Flowchart* Pembangkitan Kunci Algoritma RSA

Contoh :

1. Dipilih bilangan prima  $p = 47$  dan  $q = 71$
2. Hitung nilai  $N$  dengan rumus:

$$N = p \cdot q = 3337$$

3. Hitung nilai  $\phi(N)$  dengan persamaan:

$$\phi(N) = (p - 1)(q - 1) = 3220.$$

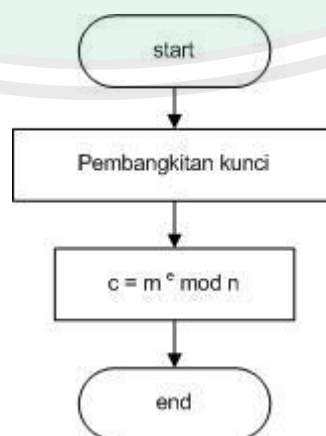
4. Dipilih  $e = 79$ ,
5. Maka  $d = 1019$

Algoritma enkripsi yang digunakan dalam algoritma RSA dapat dijelaskan sebagai berikut :

1. Disusun *plaintext* menjadi blok-blok  $m_1, m_2, \dots, m_i$
2. Hitung *ciphertext*  $c_i$  dengan rumus :

$$C_i = M_i^e \text{ mod } N$$

*Flowchart* proses enkripsi algoritma kriptografi RSA dapat dilihat pada Gambar 3.4.



**Gambar 3.4.** *Flowchart* Enkripsi Algoritma RSA

Contoh :

Misalkan *plaintext* yang akan dienkripsikan adalah  $x = \text{HARI INI}$

1. Mengubah *plaintext* yang akan dienkripsi dalam sistem desimal (pengkodean ASCII)

$$\text{HARI INI} = 7265827332737873$$

2. Memecah  $x$  menjadi blok yang lebih kecil, misalnya  $x$  dipecah menjadi enam blok yang berukuran 3 digit

$$x_1 = 726$$

$$x_4 = 273$$

$$x_2 = 582$$

$$x_5 = 787$$

$$x_3 = 733$$

$$x_6 = 003$$

3. Blok-blok *plaintext* dienkripsikan sebagai berikut :

$$726^{79} \bmod 3337 = 215 = y_1$$

$$582^{79} \bmod 3337 = 776 = y_2$$

$$733^{79} \bmod 3337 = 1743 = y_3$$

$$273^{79} \bmod 3337 = 933 = y_4$$

$$787^{79} \bmod 3337 = 1731 = y_5$$

$$003^{79} \bmod 3337 = 158 = y_6$$

Jadi, *ciphertext* yang dihasilkan adalah  $Y = 215\ 776\ 1743\ 933\ 1731\ 158$ .

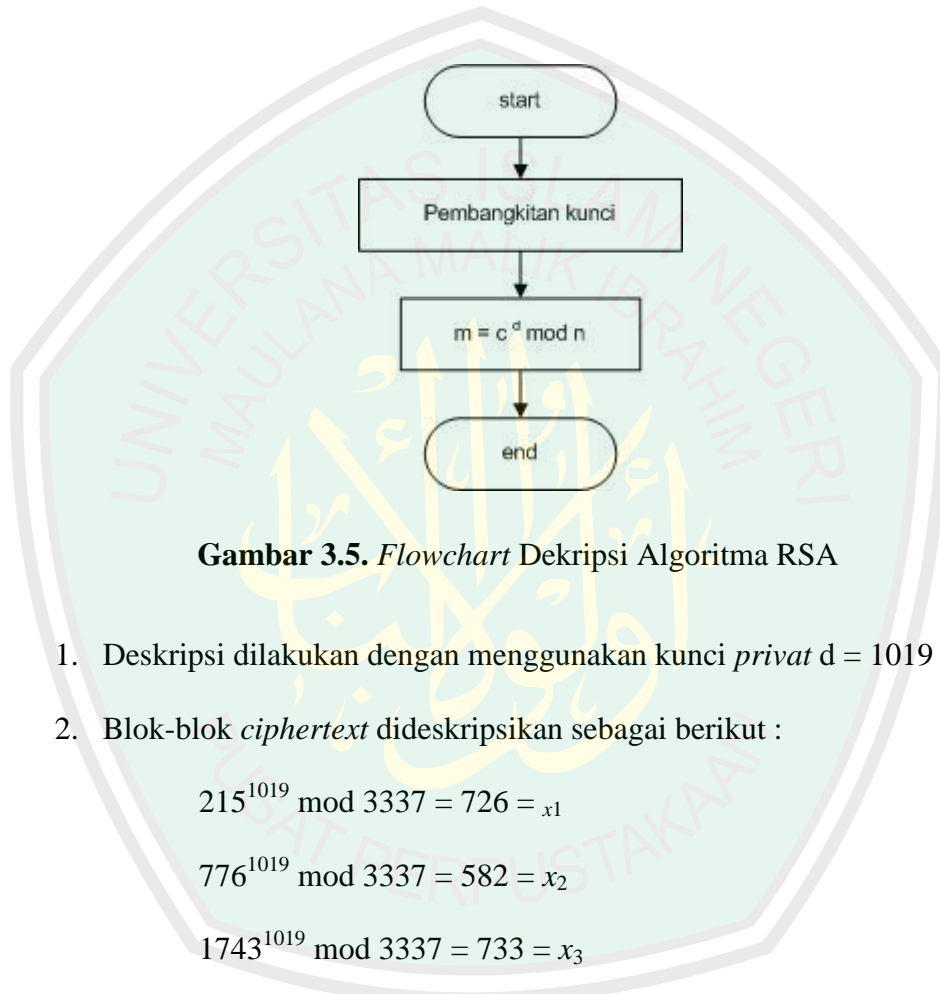
Algoritma dekripsi yang digunakan dalam algoritma RSA dapat dijelaskan sebagai berikut :

1. Gunakan kunci *privat* untuk menghitung  $M_i = C_i^d \bmod N$

2. Carilah nilai  $m$  dengan rumus

$$M_i = C_i^d \text{ mod } N$$

*Flowchart* proses dekripsi algoritma kriptografi RSA dapat dilihat pada Gambar 3.5.



**Gambar 3.5.** *Flowchart* Dekripsi Algoritma RSA

1. Deskripsi dilakukan dengan menggunakan kunci *privat*  $d = 1019$
2. Blok-blok *ciphertext* dideskripsikan sebagai berikut :

$$215^{1019} \text{ mod } 3337 = 726 = x_1$$

$$776^{1019} \text{ mod } 3337 = 582 = x_2$$

$$1743^{1019} \text{ mod } 3337 = 733 = x_3$$

$$933^{1019} \text{ mod } 3337 = 273 = x_4$$

$$1731^{1019} \text{ mod } 3337 = 787 = x_5$$

$$158^{1019} \text{ mod } 3337 = 3 = x_6$$

3. Akhirnya diperoleh kembali *plaintext* semula

$$P = 7265827332737873$$

Dalam karakter ASCII  $P = \text{HARI INI}$

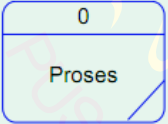
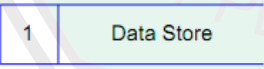
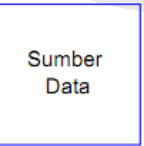



### 3.2. Perancangan *Database*

Aplikasi yang akan dibangun membutuhkan *database* atau basis data untuk menyimpan data-data yang terkait dengan aplikasi absensi. Agar basis data yang dibangun dapat diimplementasikan dengan baik, maka terlebih dahulu dilakukan proses perancangan basis data. Untuk melakukan proses desain secara umum digunakan DFD (Data Flow Diagram).

Data flow diagram menjelaskan kepada user bagaimana nantinya fungsi-fungsi di sistem secara logika akan bekerja. Data flow diagram akan menginterpretasikan *Logical Model* dari suatu sistem.

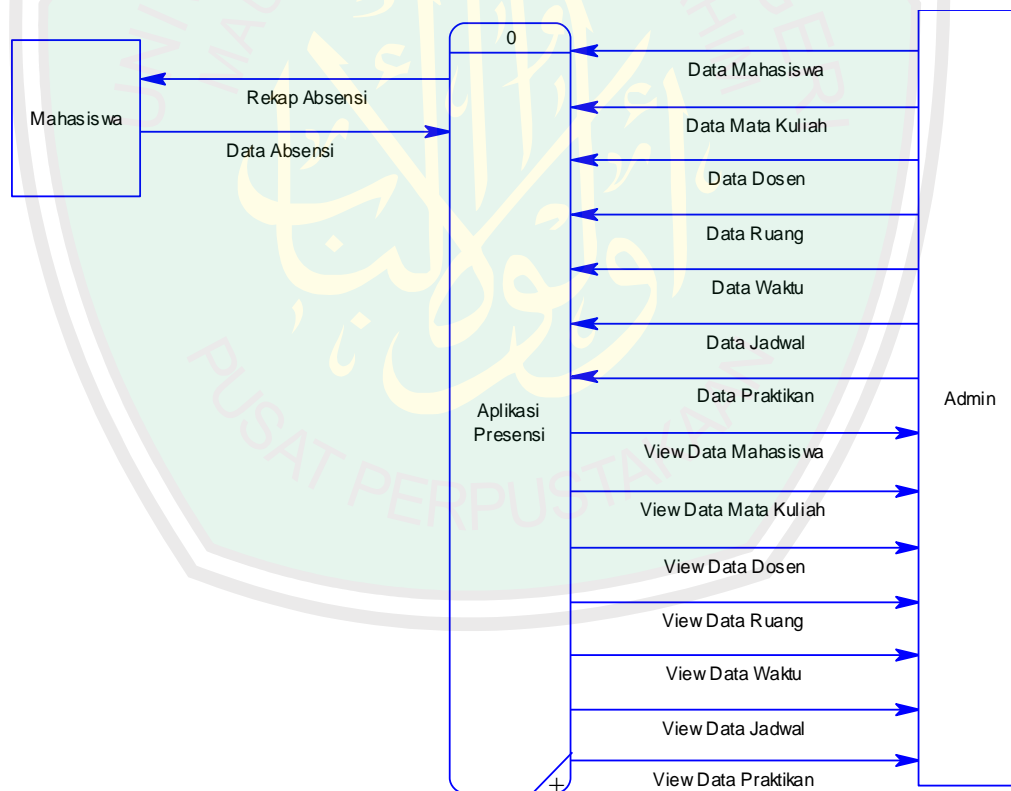
Terdapat beberapa simbol yang digunakan dalam DFD, antara lain dapat dilihat pada Gambar 3.6.

	Sumber data / tujuan data
	Penyimpanan Data
	Proses
	Aliran Data

**Gambar 3.6.** Simbol dalam DFD

### 3.2.1. Diagram Konteks

DFD Level 0 atau disebut juga dengan diagram konteks merupakan DFD yang menggambarkan garis besar operasional sistem. Diagram konteks adalah diagram yang menggambarkan secara umum konteks yang terjadi dalam sistem antara dunia internal dan dunia eksternal. Diagram konteks dari Aplikasi Presensi adalah gambaran suatu proses hubungan *input / output* antara Aplikasi Presensi dengan entitas luarnya, yaitu admin dan mahasiswa. Diagram konteks dari aplikasi absensi ini dapat dilihat pada Gambar 3.7.



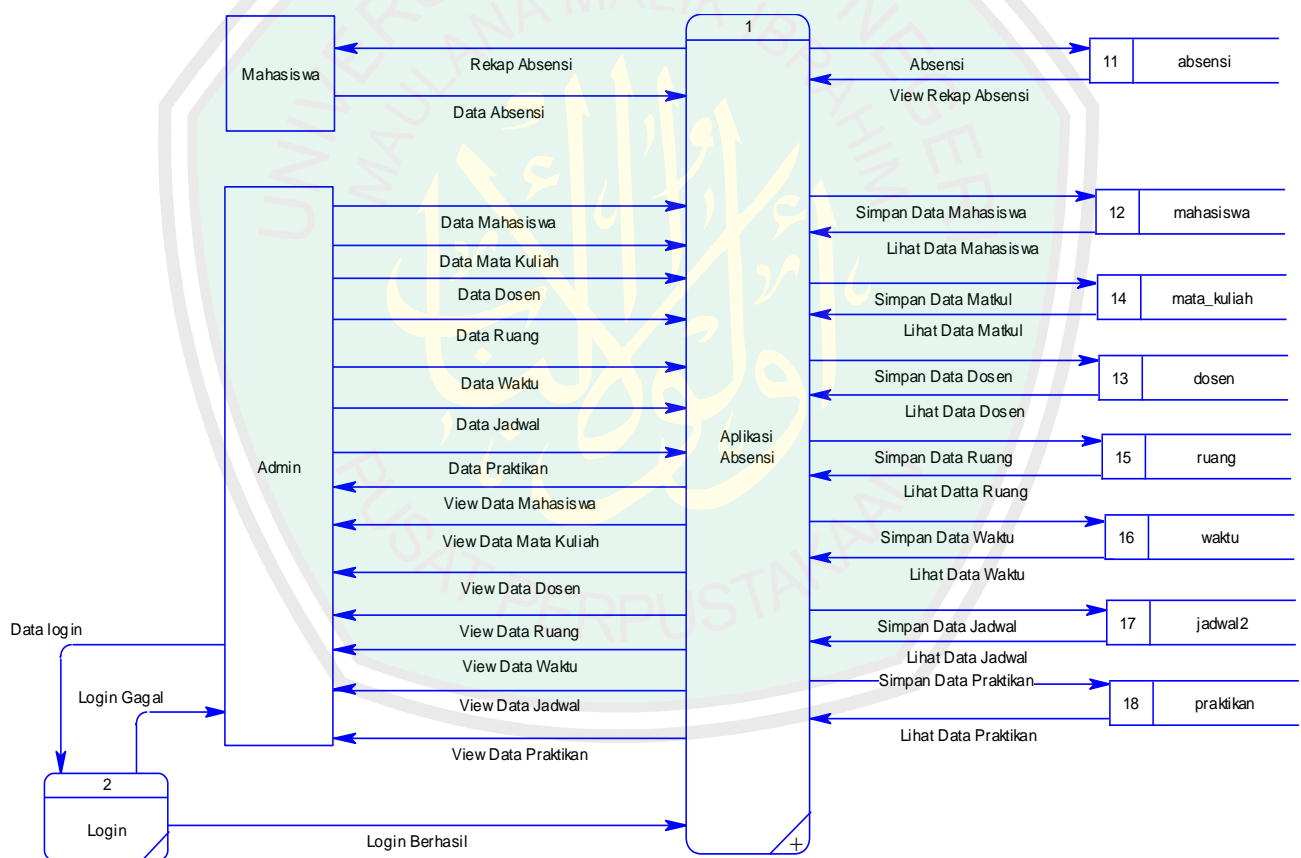
**Gambar 3.7.** Diagram Konteks

Berdasarkan gambar 3.7, dalam sistem ini terdapat 2 entitas yaitu admin dan mahasiswa. Bagian admin bertugas mengelola data mahasiswa, data

matakuliah, data dosen, data ruang, data waktu, data jadwal, dan data praktikan. Dari pengelolaan tersebut aplikasi akan menampilkan data mahasiswa, data matakuliah, data dosen, data ruang, data waktu, data jadwal, dan data praktikan.

### 3.2.2. Data Flow Diagram (DFD) Level 1

Data flow diagram (DFD) level 1 pada sistem ini dapat dilihat pada Gambar 3.8.



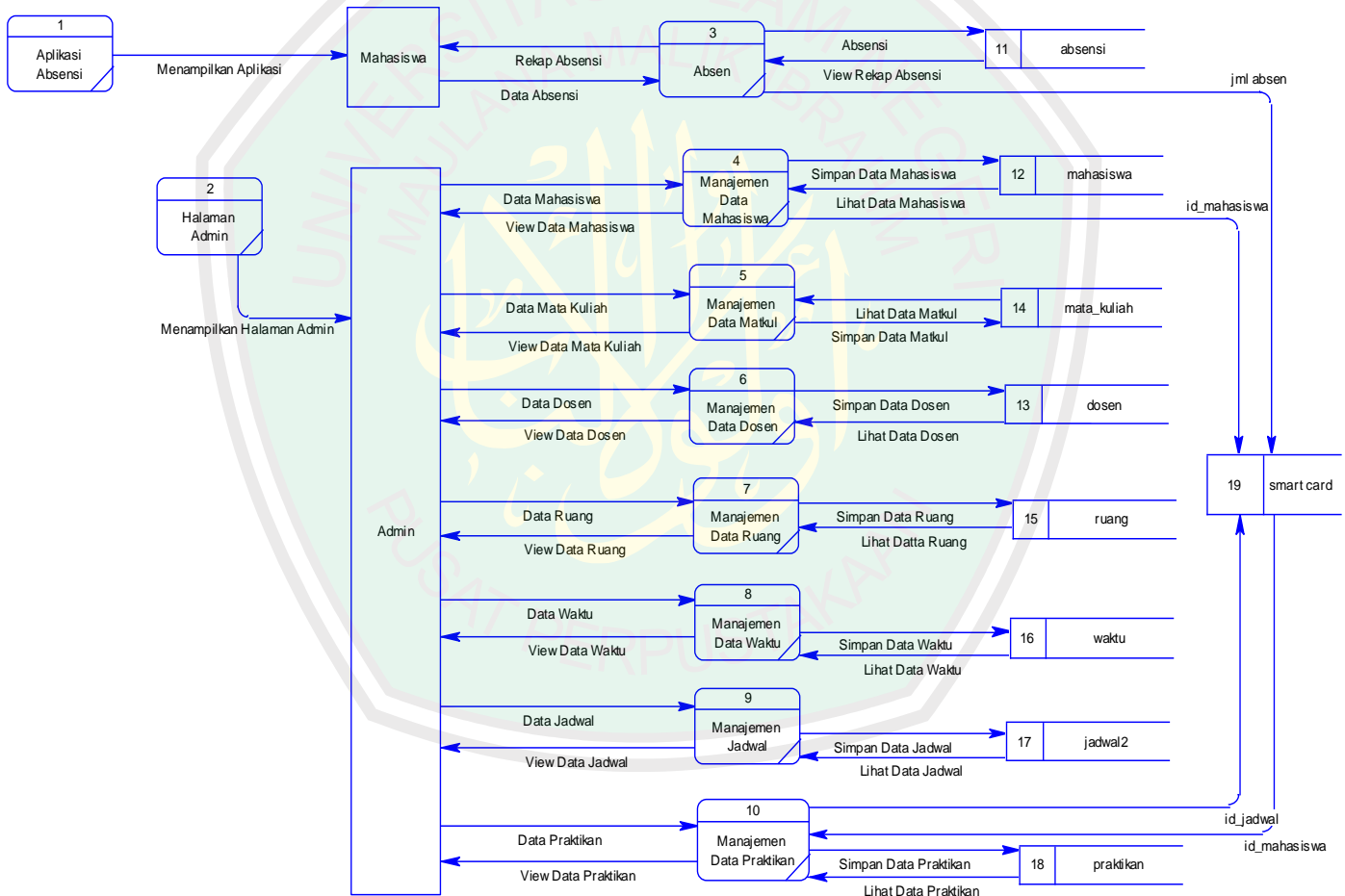
**Gambar 3.8.** DFD Level 1

Gambar 3.8 merupakan gambar DFD level 1. Data flow diagram Level 1 merupakan *decompose* dari diagram konteks. Pada DFD level 1 dijelaskan bagian proses yang lebih rinci dari proses yang ada pada diagram konteks sebelumnya.

Berdasarkan gambar diatas terdapat dua proses pada data flow diagram level 1 tersebut. Yaitu proses *login* dan aplikasi absensi.

### 3.2.3. Data Flow Diagram (DFD) Level 2

Data flow diagram (DFD) level 2 pada sistem ini dapat dilihat pada Gambar 3.9.



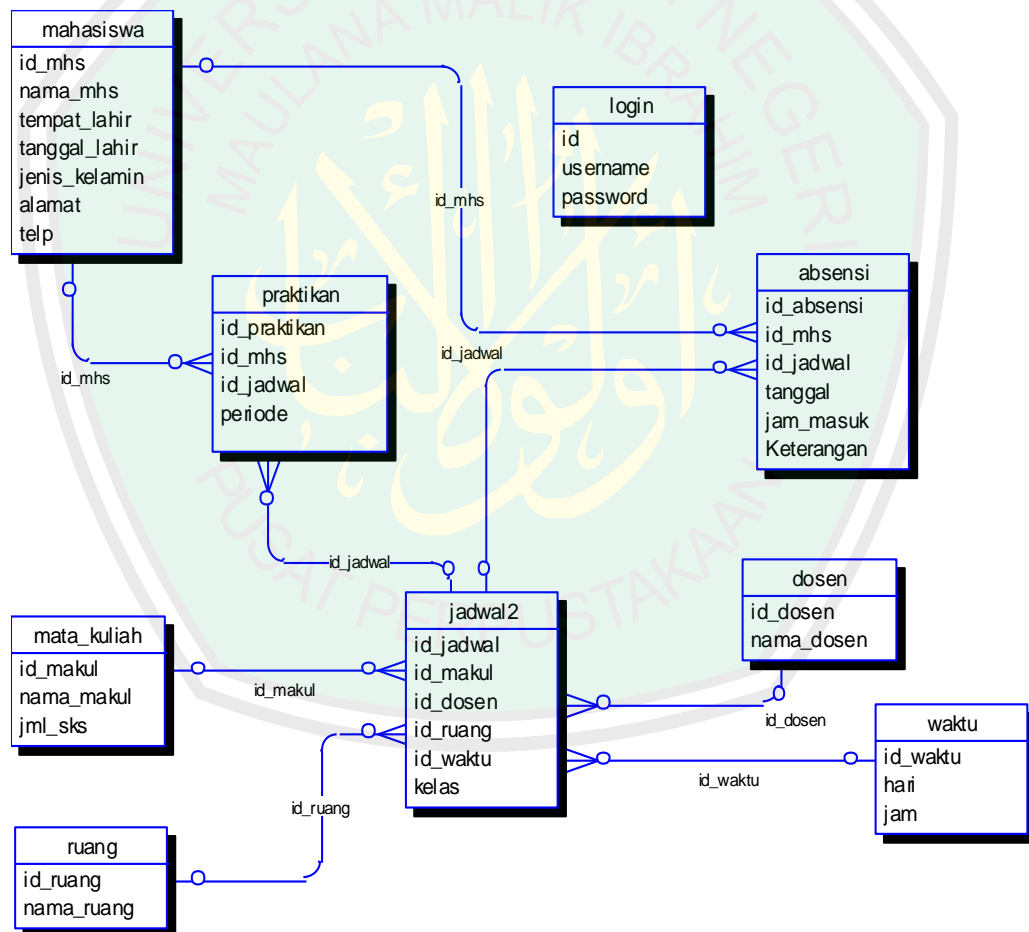
**Gambar 3.9. DFD Level 2**

Gambar 3.9 merupakan gambar data flow diagram level 2. Terdapat 10 proses diantaranya aplikasi presensi, halaman admin, absen, manajemen data mahasiswa, manajemen data matakuliah, manajemen data dosen, manajemen data

ruang, manajemen data waktu, manajemen data jadwal, dan manajemen data praktikan.

### 3.2.4. Entity Relationship Diagram (ERD)

*Entity Relationship Diagram* (ERD) adalah suatu model untuk menjelaskan hubungan antar data dalam suatu basis data. ERD dalam sistem ini dapat dilihat pada Gambar 3.10.



**Gambar 3.10.** Entity Relation Diagram

a. Tabel *mahasiswa*

Tabel *mahasiswa* adalah tabel yang berisi data mahasiswa. Dalam tabel ini terdapat data-data mahasiswa, yaitu : nama, tanggal lahir, tempat lahir, jenis kelamin, alamat dan nomer telepon.

b. Tabel *mata\_kuliah*

Tabel *mata\_kuliah* adalah tabel yang berisi data mata kuliah. Tabel ini merupakan tabel master yang mana isi tabel ini akan diambil dan dimasukkan ke dalam tabel *jadwal2*.

c. Tabel *dosen*

Tabel *dosen* adalah tabel master yang di dalamnya berisi data dosen, yang nantinya juga akan dimasukkan ke dalam tabel *jadwal2*.

d. Tabel *absensi*

Tabel *absensi* adalah tabel yang berisi data absensi mahasiswa. Tabel ini mengambil data dari 2 tabel, yaitu: tabel *mahasiswa* dan tabel *jadwal2*. Tabel ini berfungsi untuk menyimpan data absensi yang dilakukan oleh mahasiswa.

e. Tabel *jadwal2*

Tabel *jadwal* adalah tabel yang berisi data jadwal praktikum. Tabel ini terkoneksi dengan 4 tabel yang nantinya isi dari tabel ini akan mengambil

data dari 4 tabel tersebut. Tabel tersebut diantaranya adalah tabel *mata\_kuliah*, *dosen*, *waktu* dan tabel *ruang*.

f. Tabel *praktikan*

Tabel *praktikan* adalah tabel yang berisi data mahasiswa yang mengikuti praktikum. Data mahasiswa yang ada di tabel ini diambil dari tabel *mahasiswa*. Tabel *praktikan* meliputi id *praktikan*, id mahasiswa, id *jadwal*, dan *periode*.

g. Tabel *login*

Tabel *login* adalah tabel yang berisi data user yaitu admin yang nantinya tabel ini berfungsi untuk menyimpan data *username* dan *password* user.

h. Tabel *waktu*

Tabel *waktu* adalah tabel master yang berisi data hari dan jam. Tabel ini merupakan tabel master dimana data dari tabel ini akan diambil dan dimasukkan ke dalam tabel *jadwal2*.

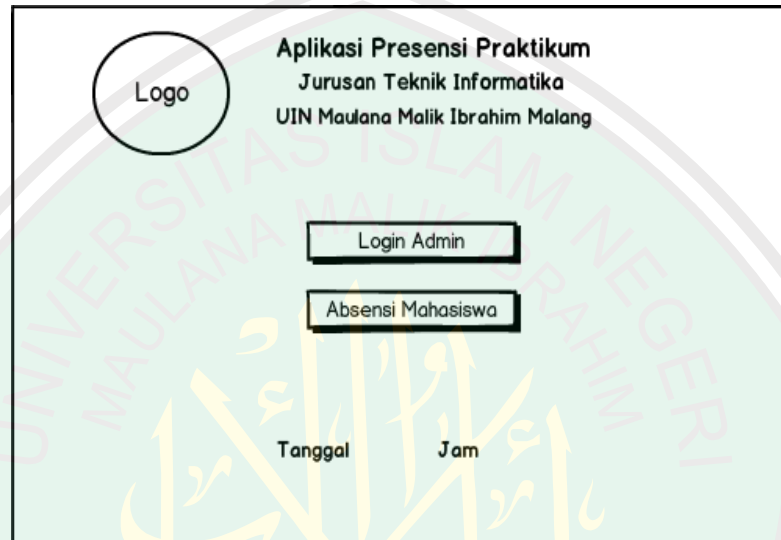
i. Tabel *ruang*

Tabel *ruang* adalah tabel yang berisi data ruang yang akan digunakan untuk melaksanakan kegiatan praktikum. Tabel ini merupakan tabel master, data dari tabel ini akan dimasukkan ke dalam tabel *jadwal2*.

### 3.3. Perancangan *Interface*

#### 3.3.1. Rancangan *Interface* Halaman Utama

Rancangan *interface* halaman utama ditunjukkan pada Gambar 3.11.



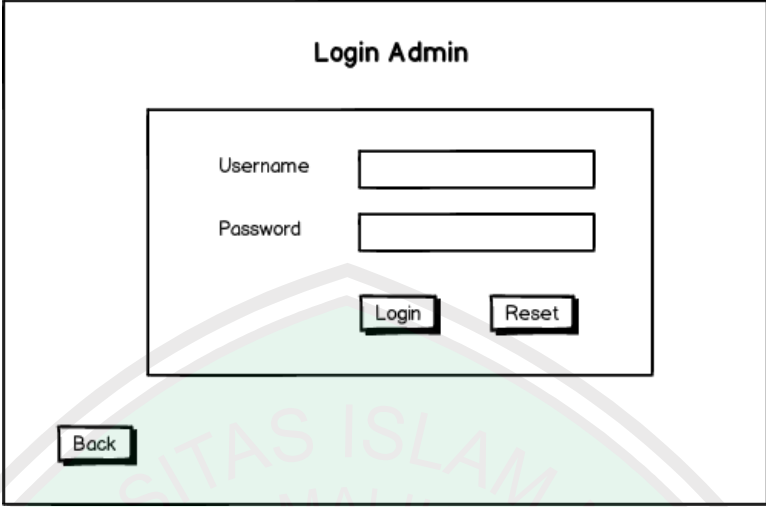
**Gambar 3.11.** Rancangan *Interface* Halaman Utama

Gambar 3.11 merupakan rancangan tampilan pertama ketika aplikasi dijalankan. Terdapat 2 tombol menu yang dapat dipilih *user* untuk menuju halaman lain, yaitu tombol *login* admin dan tombol absensi mahasiswa. Tombol *login* admin digunakan oleh admin untuk masuk ke dalam sistem. Tombol absensi mahasiswa digunakan mahasiswa untuk absen praktikum.

#### 3.3.2. Rancangan *Interface* Login Admin

Rancangan *interface* untuk *login* admin dapat dilihat pada Gambar 3.12.





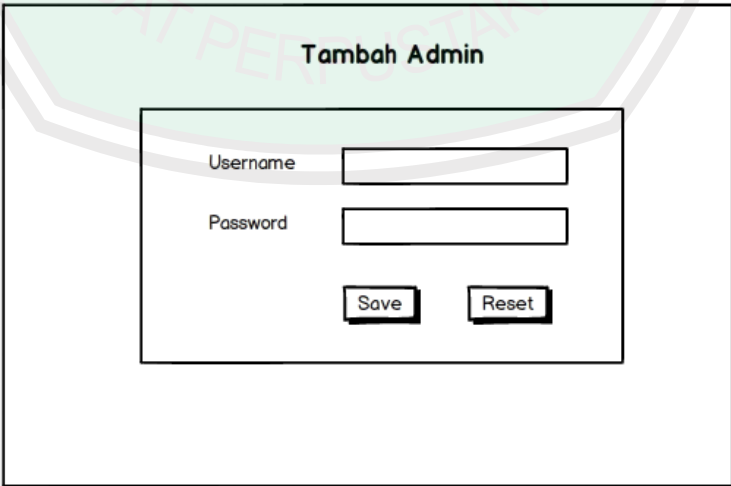
The image shows a wireframe for an admin login page. At the top center, the text "Login Admin" is displayed. Below this, there is a central rectangular box containing two input fields: "Username" and "Password". To the right of each label is a rectangular input field. Below the "Password" field are two buttons: "Login" and "Reset". Below the main box, at the bottom left, is a "Back" button. The entire form is enclosed in a larger rectangular border.

**Gambar 3.12.** Rancangan *Interface Login Admin*

Pada Gambar 3.12 ditampilkan rancangan *interface login* admin. Halaman *login* digunakan admin untuk masuk ke dalam sistem. Agar dapat masuk ke dalam sistem admin harus memasukkan *username* dan *password* yang benar.

### 3.3.3. Rancangan *Interface Tambah Admin*

Rancangan *interface* tambah admin dapat dilihat pada Gambar 3.13.



The image shows a wireframe for an admin addition page. At the top center, the text "Tambah Admin" is displayed. Below this, there is a central rectangular box containing two input fields: "Username" and "Password". To the right of each label is a rectangular input field. Below the "Password" field are two buttons: "Save" and "Reset". The entire form is enclosed in a larger rectangular border.

**Gambar 3.13.** Rancangan *Interface Tambah Admin*

Gambar 3.13 merupakan rancangan *interface* tambah admin. Halaman tambah admin digunakan untuk menambah admin dengan menyimpan *username* dan *password* yang akan digunakan untuk *login* admin.

### 3.3.4. Rancangan *Interface* Data Mahasiswa

Rancangan *interface* data mahasiswa dapat dilihat pada Gambar 3.14.

**Tambah Data Mahasiswa**

Id Mahasiswa  Jenis Kelamin  L  P

Nama  Alamat

Tempat Lahir  No Tlp / Hp

Tanggal Lahir

Save Reset

Search Update Delete

Id Mahasiswa	Nama	Tnp Lahir	Tgl Lahir	L/P	Alamat	Tlp

**Gambar 3.14.** Rancangan *Interface* Data Mahasiswa

Gambar 3.14 merupakan rancangan *interface* data mahasiswa. Halaman data mahasiswa merupakan halaman untuk mengelola data mahasiswa. Pada halaman data mahasiswa, admin dapat menyimpan, mengedit, dan menghapus data mahasiswa. Data mahasiswa yang telah dimasukkan admin akan tampil pada tabel di bawahnya.

### 3.3.5. Rancangan *Interface* Data Mata Kuliah

Rancangan *interface* data mata kuliah dapat dilihat pada Gambar 3.15.

**Data Matakuliah**

Id Matakuliah	<input type="text"/>		<input type="button" value="Save"/>	<input type="button" value="Search"/>
Nama	<input type="text"/>		<input type="button" value="Reset"/>	<input type="button" value="Update"/>
Jumlah sks	<input type="text"/>			<input type="button" value="Delete"/>

Id Matakuliah	Nama Matakuliah	Jumlah sks

**Gambar 3.15.** Rancangan *Interface* Data Mata Kuliah

Gambar 3.15 merupakan rancangan *interface* data mata kuliah. Halaman data mata kuliah merupakan halaman untuk mengelola data mata kuliah. Pada halaman ini, admin dapat menyimpan, mengedit, dan menghapus data mata kuliah. Data yang telah dimasukkan admin akan tampil pada tabel di bawahnya.

### 3.3.6. Rancangan *Interface* Data Dosen

Rancangan *interface* data dosen dapat dilihat pada Gambar 3.16.

**Dosen Dosen**

Id Dosen	<input type="text"/>		<input type="button" value="Save"/>	<input type="button" value="Search"/>
Nama Dosen	<input type="text"/>		<input type="button" value="Reset"/>	<input type="button" value="Update"/>
				<input type="button" value="Delete"/>

Id Dosen	Nama Dosen

**Gambar 3.16.** Rancangan *Interface* Data Dosen

Gambar 3.16 merupakan rancangan *interface* data dosen. Halaman data dosen merupakan halaman untuk mengelola data dosen. Pada halaman ini, admin dapat menyimpan, mengedit, dan menghapus data dosen. Data yang telah dimasukkan admin akan tampil pada tabel di bawahnya.

### 3.3.7. Rancangan *Interface* Data Ruang

Rancangan *interface* data ruang dapat dilihat pada Gambar 3.17.

The image shows a web interface titled "Data Ruang". It features two input fields: "Id Ruang" and "Nama Ruang". To the right of these fields are five buttons: "Save", "Search", "Reset", "Update", and "Delete". Below the input fields is a table with two columns: "Id Ruang" and "Nama Ruang". The table has three rows, with the first row being a header and the subsequent two rows being empty data rows.

Id Ruang	Nama Ruang

**Gambar 3.17.** Rancangan *Interface* Data Ruang

Gambar 3.17. merupakan rancangan *interface* data ruang. Halaman data ruang merupakan halaman untuk mengelola data ruang. Pada halaman ini, admin dapat menyimpan, mengedit, dan menghapus data ruang. Data yang telah dimasukkan admin akan tampil pada tabel di bawahnya.

### 3.3.8. Rancangan *Interface* Data Waktu

Rancangan *interface* data waktu dapat dilihat pada Gambar 3.18.

The screenshot shows a web interface titled "Data Waktu". It contains three input fields: "Id Waktu" (text), "Hari" (dropdown menu with "Pilih Hari"), and "Jam" (dropdown menu with "Pilih Jam"). To the right of these fields are five buttons: "Save", "Search", "Reset", "Update", and "Delete". Below the form is a table with three columns: "Id Waktu", "Hari", and "Jam".

Id Waktu	Hari	Jam

**Gambar 3.18.** Rancangan *Interface* Data Waktu

Gambar 3.18 merupakan rancangan *interface* data waktu. Halaman data waktu merupakan halaman untuk mengelola data waktu. Pada halaman ini, admin dapat menyimpan, mengedit, dan menghapus data waktu. Data yang telah dimasukkan admin akan tampil pada tabel di bawahnya.

### 3.3.9. Rancangan *Interface* Data Jadwal

Rancangan *interface* data jadwal dapat dilihat pada Gambar 3.19.

The screenshot shows a web interface titled "Data Jadwal". It contains six input fields: "Id Jadwal" (text), "Mata Kuliah" (dropdown menu with "▼"), "Kelas" (dropdown menu with "▼"), "Dosen" (dropdown menu with "▼"), "Ruang" (dropdown menu with "▼"), and "Waktu" (dropdown menu with "▼"). To the right of these fields are five buttons: "Save", "Search", "Reset", "Update", and "Delete". Below the form is a table with six columns: "Id Jadwal", "Matakuliah", "Kelas", "Dosen", "Ruang", and "Waktu".

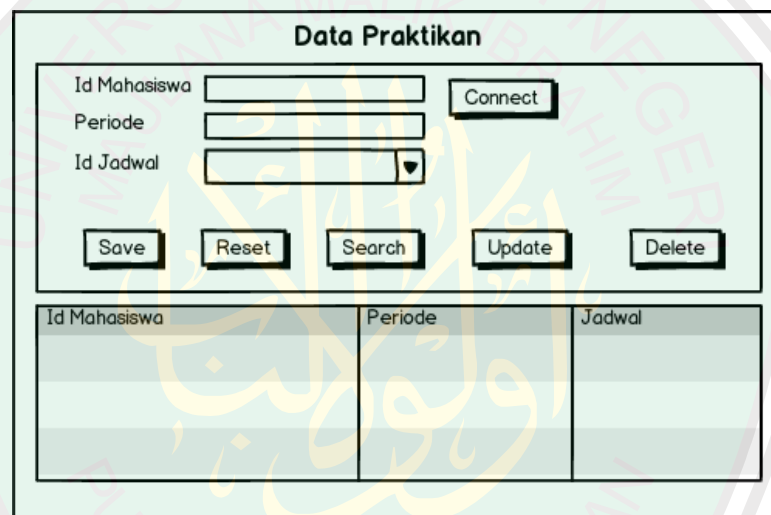
Id Jadwal	Matakuliah	Kelas	Dosen	Ruang	Waktu

**Gambar 3.19.** Rancangan *Interface* Data Jadwal

Gambar 3.19 merupakan rancangan *interface* data jadwal. Halaman data jadwal merupakan halaman untuk mengelola data jadwal. Pada halaman ini, admin dapat menyimpan, mengedit, dan menghapus data jadwal. Data yang telah dimasukkan admin akan tampil pada tabel di bawahnya.

### 3.3.10. Rancangan *Interface* Data Praktikan

Rancangan *interface* data praktikan dapat dilihat pada gambar 3.20.



The image shows a web interface titled "Data Praktikan". It contains three input fields: "Id Mahasiswa", "Periode", and "Id Jadwal" (with a dropdown arrow). A "Connect" button is positioned to the right of the "Id Mahasiswa" field. Below the input fields are five buttons: "Save", "Reset", "Search", "Update", and "Delete". At the bottom, there is a table with three columns: "Id Mahasiswa", "Periode", and "Jadwal". The table is currently empty.

Id Mahasiswa	Periode	Jadwal

**Gambar 3.20.** Rancangan *Interface* Data Praktikan

Gambar 3.20 merupakan rancangan *interface* data praktikan. Halaman data praktikan merupakan halaman untuk mengelola data praktikan. Pada halaman ini, admin dapat menyimpan, mengedit, dan menghapus data praktikan. Data yang telah dimasukkan admin akan tampil pada tabel di bawahnya.

### 3.3.11. Rancangan *Interface* Absensi Mahasiswa

Perancangan *interface* absensi mahasiswa dapat dilihat pada Gambar 3.21.

**Gambar 3.21.** Rancangan *Interface* Absensi Mahasiswa

Gambar 3.21 merupakan rancangan *interface* absensi mahasiswa. Halaman Absensi mahasiswa digunakan untuk absensi praktikum mahasiswa. Terdapat tombol connect yang digunakan untuk mengambil data Id Mahasiswa dan jadwal dengan cara *read* data yang ada di dalam smart card, kemudian data akan muncul pada halaman tersebut. Mahasiswa melakukan absensi dengan meng-klik tombol absen, lalu data akan tersimpan ke dalam database.

### 3.3.12. Rancangan *Interface* Laporan Absensi

Rancangan interface laporan absensi dapat dilihat pada Gambar 3.22.

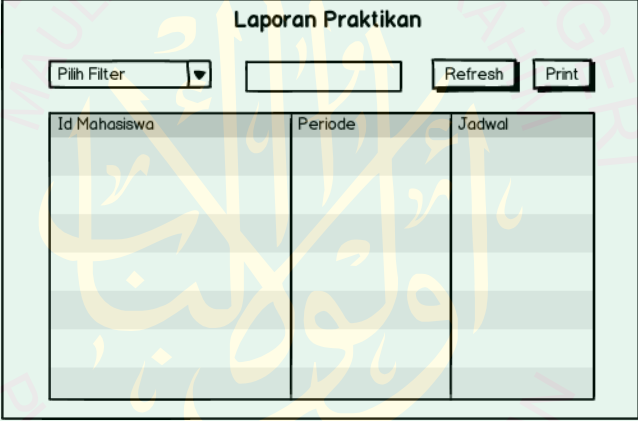
Id Absensi	Id Mahasiswa	Id Jadwal	Tanggal	Jam Masuk	Keterangan

**Gambar 3.22.** Rancangan *Interface* Laporan Absensi

Gambar 3.22 merupakan rancangan *interface* laporan absensi. Halaman laporan absensi digunakan admin untuk melihat laporan absensi. Terdapat filter berdasarkan id mahasiswa, id jadwal, dan tanggal untuk mem-filter data yang dibutuhkan untuk ditampilkan. Hasil yang ditampilkan dapat langsung dicetak.

### 3.3.13. Rancangan *Interface* Laporan Praktikan

Berikut rancangan *interface* laporan praktikan yang ditunjukkan pada gambar 3.23.



The screenshot shows a web interface titled "Laporan Praktikan". At the top left, there is a dropdown menu labeled "Pilih Filter" with a downward arrow. To its right is a text input field. Further right are two buttons: "Refresh" and "Print". Below these elements is a table with three columns: "Id Mahasiswa", "Periode", and "Jadwal". The table has several rows, but they are currently empty.

**Gambar 3.23.** Rancangan *Interface* Laporan Praktikan

Gambar 3.23 merupakan rancangan *interface* laporan praktikan. Halaman laporan praktikan digunakan admin untuk melihat laporan praktikan. Terdapat filter berdasarkan id mahasiswa dan periode untuk mem-filter data yang dibutuhkan untuk ditampilkan. Hasil yang ditampilkan dapat langsung dicetak.



## **BAB IV**

### **IMPLEMENTASI DAN HASIL**

Pada bab ini dibahas tentang implementasi dari perancangan yang dibuat. Serta melakukan pengujian terhadap aplikasi untuk mengetahui apakah aplikasi tersebut telah berjalan sesuai yang diharapkan.

#### **4.1. Lingkungan Implementasi**

Lingkungan implementasi yang akan dipaparkan disini meliputi lingkungan perangkat keras dan lingkungan perangkat lunak.

##### **4.1.1. Lingkungan Perangkat Keras**

Perangkat keras (*hardware*) yang digunakan dalam pembuatan aplikasi ini adalah sebagai berikut :

1. *Prosesor intel core i3, 2.26 GHZ*
2. *RAM 1024 MB*
3. *HardDisk dengan kapasitas 320*
4. *Monitor 14"*
5. *Keyboard*
6. *Smart card reader writer ACR35*
7. *Kartu SLE4428*

#### 4.1.2. Lingkungan Perangkat Lunak

Perangkat lunak (*software*) yang digunakan dalam pembuatan aplikasi ini adalah sebagai berikut :

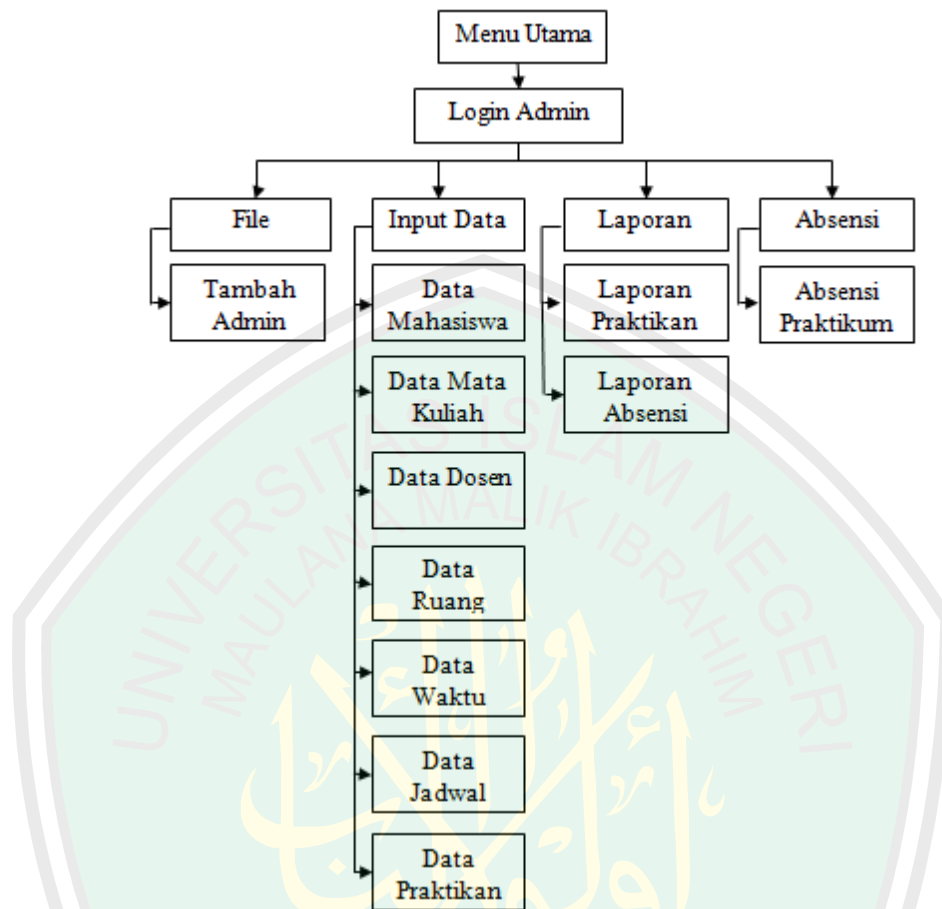
1. Sistem operasi *windows XP*
2. *Visual Basic 6.0*
3. *Microsoft Access*
4. SDK ACR38

#### 4.2. Implementasi Program

Di dalam sub bab ini dijelaskan tentang implementasi program yang meliputi implementasi *interface*, dan implementasi prosedural dari algoritma kriptografi RSA yang diimplementasikan beserta kegunaan dari program yang dibuat. Selain itu akan dibahas hasil implementasi algoritma RSA yang dibuat beserta tampilan sistemnya.

##### 4.2.1. Implementasi *Interface*

Implementasi *interface* memaparkan implementasi dari hasil perancangan *interface*. Berikut ini struktur menu program yang menggambarkan tampilan-tampilan halaman yang ada di dalam program yang dapat dilihat pada Gambar 4.1.



**Gambar 4.1.** Struktur Menu Program

Gambar 4.1 merupakan struktur menu program dari sistem yang telah dibuat. Terdapat 4 menu, yaitu menu *file*, menu *input*, menu laporan, dan menu absensi. Menu *file* terdiri dari sub menu tambah data admin. Menu *input* terdiri dari sub menu data mahasiswa, data mata kuliah, data dosen, data ruang, data waktu, data jadwal, dan data praktikan. Menu laporan terdiri dari 2 sub menu yaitu sub menu laporan absensi dan laporan praktikum. Menu absensi berisi sub menu absensi.

#### 4.2.1.1. *Interface* Halaman Utama

Interface halaman utama dapat dilihat pada Gambar 4.2.



**Gambar 4.2.** *Interface* Halaman Utama

Gambar 4.2 merupakan *interface* halaman utama. Halaman utama merupakan tampilan pertama ketika aplikasi dijalankan. Terdapat 2 tombol menu yang dapat dipilih *user* untuk menuju halaman lain, yaitu tombol *login* admin dan tombol absensi mahasiswa. Tombol *login* admin digunakan oleh admin untuk masuk ke dalam sistem. Tombol absensi mahasiswa digunakan mahasiswa untuk melakukan absen praktikum.

#### 4.2.1.2. *Interface* Login Admin

*Interface* login admin dapat dilihat pada Gambar 4.3.



**Gambar 4.3.** *Interface Login Admin*

Gambar 4.3 merupakan *interface login* admin. Halaman *login* digunakan admin untuk masuk ke dalam sistem. Agar dapat masuk ke dalam sistem admin harus memasukkan *username* dan *password* yang benar.

#### 4.2.1.3. *Interface Home* Halaman Admin

*Interface home* halaman admin dapat dilihat pada Gambar 4.4.



**Gambar 4.4.** *Interface Home* Halaman Admin

Gambar 4.4 merupakan *interface home* halaman admin. Setelah admin berhasil login maka akan masuk ke home halaman admin. Pada toolbar home halaman admin terdapat menu-menu yang dapat dipilih admin untuk mengolah seluruh data. Menu-menu tersebut diantaranya file, input, laporan dan absensi. Menu file terdiri dari sub menu tambah data admin dan login. Menu input terdiri dari sub menu data mahasiswa, data matakuliah, data dosen, data ruang, data waktu, data jadwal, dan data praktikan. Menu laporan terdiri dari sub menu laporan absensi dan laporan praktikum.

#### 4.2.1.4. *Interface Tambah Admin*

*Interface* tambah admin dapat dilihat pada gambar 4.5.



The image shows a screenshot of a software application window titled "MDIForm1 - [Form9]". The window has a menu bar with "File", "Input", "Laporan", and "Absensi". The main content area has a green background with the text "TAMBAH DATA ADMIN" centered. Below this text is a form with two input fields labeled "Username" and "Password", and two buttons labeled "Save" and "Reset".

**Gambar 4.5.** *Interface Tambah Admin*

Gambar 4.5. adalah *interface* tambah admin digunakan untuk menambah admin dengan menyimpan *username* dan *password* yang akan digunakan untuk *login* admin.

#### 4.2.1.5. Interface Data Mahasiswa

Pada halaman data mahasiswa admin dapat mengolah data mahasiswa pada halaman data mahasiswa. Data yang diolah yaitu id mahasiswa, nama mahasiswa, tempat lahir, tanggal lahir, jenis kelamin, alamat, dan nomor tlp/hp.

Interface data mahasiswa dapat dilihat pada Gambar 4.6.

ID MHS	NAMA	TEMPAT LAHIR	TANGGAL LAHIR	L/P	ALAMAT	NO TELP
10650037	anugrah widasari	jombang	16-08-1992	P	malang	085645539972
10650041	Nur Aisyah	bengkulu	25-07-1991	P	malang	08728726625
10650089	Ade Durotun	gresik	10-12-1992	P	malang	087654764876
10650056	Dewi Chumaroh	malang	17-05-1992	P	malang	0863764578865
10650001	Kurnia Sari Dewi	Tulungagung	01/03/1994	P	malang	085676543234
10650002	Nurul Misbah	Jombang	29/12/1991	L	malang	088763755635
10650007	Alvina Fitna	Bitar	31/12/1992	P	malang	08387654567
10650008	anugrah	jombang	31/12/1993	P	malang	08567655222

**Gambar 4.6.** Interface Data Mahasiswa

Gambar 4.6 merupakan *interface* data mahasiswa. Terdapat tombol *save* untuk menyimpan data ke database serta menyimpan id mahasiswa ke dalam *smart card*. Id mahasiswa yang disimpan ke dalam *smart card* dienkripsi terlebih dahulu menggunakan algoritma kriptografi RSA, sehingga data yang tersimpan dalam *smart card* berupa data yang telah terenkripsi (*chipertext*). Tombol *reset* digunakan untuk mereset data yang telah di tulis di dalam *form*, tombol *update* untuk menyimpan hasil edit ke dalam database, tombol *delete* untuk menghapus

data yang telah tersimpan dalam database, dan tombol *search* untuk mencari data berdasarkan id mahasiswa.

#### 4.2.1.6. Interface Data Mata kuliah

Interface data mata kuliah dapat dilihat pada Gambar 4.7.

The screenshot shows a software interface titled "DATA MATA KULIAH". It features a form with three input fields: "Id Mata Kuliah" (containing "118"), "Nama Mata Kuliah" (containing "Manajemen Basis Data"), and "Jumlah SKS" (containing "2"). To the right of these fields are buttons for "Save", "Search", "Update", "Reset", and "Delete". Below the form is a table with three columns: "ID Mata Kuliah", "Nama Mata Kuliah", and "Jumlah SKS". The table contains the following data:

ID Mata Kuliah	Nama Mata Kuliah	Jumlah SKS
1111	Dasar Pemrograman	3
1112	Dasain Basis Data	3
1113	Jaringan Komputer	3
1114	Gratika Komputer	2
1115	Metode Penertilian	2
1116	Keamanan Jaringan Komputer	3
1117	Sistem Operasi	2

**Gambar 4.7.** Interface Data Mata kuliah

Gambar 4.7 merupakan *interface* data mata kuliah. Pada halaman data mata kuliah admin dapat mengolah data mata kuliah. Data yang diolah admin yaitu id mata kuliah, nama mata kuliah, dan jumlah sks. Terdapat pula tabel yang menampilkan data matakuliah yang telah tersimpan di dalam *database*.

#### 4.2.1.7. Interface Data Dosen

Interface data dosen dapat dilihat pada Gambar 4.8.



ID DOSEN	NAMA DOSEN
111111111	Dr. Muhammad Faisal M.T.
111111112	Totok Chamidy, M.T.
111111113	Rini Kusumawati
111111114	Yunifa Miftachul Anif
111111115	Ainul Yagim
111111116	Cahyo Crysdiyan
111111117	Alfa Syauci

**Gambar 4.8.** *Interface Data Dosen*

Gambar 4.8 merupakan *interface* data dosen. Halaman data dosen merupakan halaman untuk mengelola data dosen. Pada halaman ini, admin dapat menyimpan, mengedit, dan menghapus data dosen. Data yang diolah yaitu id dosen dan nama dosen. Data yang telah dimasukkan admin akan tampil pada tabel di bawahnya.

#### **4.2.1.8. *Interface Data Ruang***

Halaman data ruang merupakan halaman untuk mengelola data ruang. Pada halaman ini, admin dapat menyimpan, mengedit, dan menghapus data ruang. Data yang diolah yaitu id ruang dan nama ruang. Data yang telah dimasukkan admin akan tampil pada tabel di bawahnya. *Interface* data ruang dapat dilihat pada Gambar 4.9.

ID RUANG	NAMA RUANG
1	laboratorium pemrograman
2	Laboratorium Database
3	Laboratorium Multimedia
4	Laboratorium Internet
5	Laboratorium Jaringan

**Gambar 4.9.** *Interface Data Ruang*

#### 4.2.1.9. *Interface Data Waktu*

*Interface data waktu dapat dilihat pada Gambar 4.10.*

ID WAKTU	HARI	JAM
1	senin	08.50-09.50
2	senin	09.50-10.50
3	senin	13.10-14.10
4	selasa	08.50-09.50
5	selasa	09.50-10.50
6	selasa	13.10-14.10
7	rabu	08.50-09.50
8	rabu	09.50-10.50
9	rabu	13.10-14.10
10	kamis	08.50-09.50
11	kamis	09.50-10.50

**Gambar 4.10.** *Interface Data Waktu*

Gambar 4.10 merupakan *interface* data waktu. Halaman data waktu merupakan halaman untuk mengelola data waktu. Admin memasukkan id waktu, jam dan hari. Pada halaman ini, admin dapat menyimpan, mengedit, dan menghapus data waktu. Data yang telah dimasukkan admin akan tampil pada tabel di bawahnya.

#### 4.2.1.10. *Interface* Data Jadwal

*Interface* data jadwal dapat dilihat pada Gambar 4.11.

The screenshot shows a software window titled 'MDIForm1 - [Form8]' with a menu bar containing 'File', 'Input', 'Laporan', and 'Absensi'. The main area is titled 'DATA JADWAL' and contains a form with the following fields:

- Id Jadwal:** Text input field containing '11'.
- Mata Kuliah:** Dropdown menu.
- Kelas:** Dropdown menu.
- Dosen:** Dropdown menu.
- Ruang:** Dropdown menu.
- Waktu:** Dropdown menu.

Buttons for 'Save', 'Search', 'Update', 'Reset', and 'Delete' are located to the right of the form fields.

Below the form is a table with the following data:

ID JADWAL	MATA KULIAH	KELAS	DOSEN	RUANG	WAKTU
1	Dasar Pemrograman	A	Dr. Muhammad Faisal M.T.	laboratorium pemrograman	1
2	Dasar Pemrograman	B	Totok Chamidy, M.T.	Laboratorium Database	2
3	Dasar Pemrograman	C	Dr. Muhammad Faisal M.T.	laboratorium pemrograman	3
4	Desain Basis Data	A	Rinen Kusumawati	Laboratorium Database	4
5	Desain Basis Data	B	Rinen Kusumawati	Laboratorium Database	5
6	Desain Basis Data	C	Yunifa Miftachul Arif	Laboratorium Database	6
7	Jaringan Komputer	A	Yunifa Miftachul Arif	Laboratorium Jaringan	1
8	Jaringan Komputer	B	Totok Chamidy, M.T.	Laboratorium Jaringan	2
9	Jaringan Komputer	C	Dr. Muhammad Faisal M.T.	Laboratorium Jaringan	3

**Gambar 4.11.** *Interface* Data Jadwal

Gambar 4.11 merupakan *interface* data jadwal. Halaman data jadwal merupakan halaman untuk mengelola data jadwal. Pada halaman ini admin dapat menyimpan, mengedit, dan menghapus data jadwal. Admin menginputkan id jadwal, matakuliah, kelas, dosen, ruang, dan waktu. Dalam *combobox* matakuliah,

dosen, ruang dan waktu diambil dari data yang telah tersimpan dalam *database*. Data yang telah dimasukkan admin akan tampil pada tabel di bawahnya.

#### 4.2.1.11. Interface Data Praktikan

Interface data praktikan dapat dilihat pada Gambar 4.12.

ID PRAKTIKAN	ID MAHASISWA	PERIODE	ID JADWAL
10	10650001	2010	2
11	10650001	2010	3
12	10650001	2010	4
14	10650037	2010	1
18	10650001	2010	4
19	10650009	2010	7
21	10650009	2010	5

**Gambar 4.12.** Interface Data Praktikan

Gambar 4.12 merupakan *interface* data praktikan. Halaman data praktikan merupakan halaman untuk mengelola data praktikan. Pada halaman ini, admin dapat menyimpan, mengedit, dan menghapus data praktikan. Sebelum mengisi data praktikan admin terlebih dahulu meng-klik tombol *connect* untuk mengambil id mahasiswa yang tersimpan di dalam *smart card* dengan cara *read* data dalam kartu. Setelah data dibaca, data tersebut didekripsi terlebih dahulu menggunakan algoritma kriptografi RSA. Hasilnya akan tampil id mahasiswa yang sudah

terdekripsi pada textbox id mahasiswa. Setelah id mahasiswa terbaca, admin memasukkan periode dan jadwal kemudian klik tombol *save* untuk menyimpan data. Terdapat 2 proses penyimpanan data. Penyimpanan data ke dalam *database* dan penyimpanan data ke dalam *smart card*. Data yang disimpan ke dalam *smart card* yaitu id jadwal, dimana id jadwal dienkripsi terlebih dahulu sebelum dimasukkan ke dalam *smart card*. Kemudian *write* data yang telah terenkripsi ke dalam *smart card*..

#### 4.2.1.12. Interface Absensi Mahasiswa

Interface absensi mahasiswa dapat dilihat pada Gambar 4.13.



**Gambar 4.13.** Interface Absensi Mahasiswa

Gambar 4.13 merupakan *interface* absensi mahasiswa. Halaman absensi mahasiswa digunakan untuk absensi praktikum mahasiswa. Terdapat tombol *connect* yang digunakan untuk mengambil data id Mahasiswa dan jadwal dengan

cara *read* data yang ada di dalam *smart card*. Sebelum data ditampilkan data didekripsi terlebih dahulu menggunakan algoritma RSA, kemudian data akan muncul pada halaman tersebut. Mahasiswa melakukan absensi dengan memilih tombol absen, lalu muncul di dalam *message box* jumlah absen.

#### 4.2.1.13. Interface Laporan Absensi

Interface laporan absensi dapat dilihat pada Gambar 4.14.

ID ABSENSI	ID MAHASISWA	ID JADWAL	TANGGAL	JAM MASUK	KETERANGAN
7	10650009		10-Jan-2010	0:38:14	
27	10650009	5	10-Jan-2010	1:31:27	10
28	10650016	5	10-Jan-2010	1:49:08	1
29	10650016	2	10-Jan-2010	1:49:14	1
30	10650016	5	10-Jan-2010	1:49:19	1
31	10650016	5	10-Jan-2010	1:49:58	2
32	10650016	2	10-Jan-2010	1:50:07	2
33	11111111	6	10-Jan-2010	0:40:17	1
34	11111111	6	10-Jan-2010	0:41:59	2
35	11111111	6	24-Nov-2014	8:33:11	3
36	11111111	6	24-Nov-2014	8:33:16	3
37	11111111	6	24-Nov-2014	8:33:21	3
38	11111111	6	24-Nov-2014	8:33:49	4
39	11111111	6	24-Nov-2014	8:34:03	5
40	11111111	6	24-Nov-2014	8:34:17	6
41	11111111	6	24-Nov-2014	8:34:31	7
42	11111111	6	24-Nov-2014	8:34:43	8
43	11111111	6	24-Nov-2014	8:34:56	9
44	11111111	6	24-Nov-2014	8:35:10	10
45	11111111	6	24-Nov-2014	8:45:27	21
46	11111111	6	24-Nov-2014	8:45:45	22
47	11111111	6	24-Nov-2014	8:46:56	99
48	11111111	6	24-Nov-2014	8:47:14	100

Gambar 4.14. Interface Laporan Absensi

Gambar 4.14 merupakan *interface* laporan absensi. Pada halaman laporan absensi berisi laporan kegiatan absensi praktikum. Data absensi yang dilaporkan yaitu id absensi, id mahasiswa, id jadwal, jam masuk, dan keterangan jumlah absen. Terdapat filter berdasarkan id mahasiswa dan id jadwal. Terdapat tombol *print* untuk mencetak seluruh data laporan absensi.



#### 4.2.1.14. Interface Laporan Praktikan

Interface laporan absensi dapat dilihat pada Gambar 4.15.

ID CARD	ID MAHASISWA	PERIODE	ID JADWAL
10	10650001	2010	2
11	10650001	2010	3
12	10650001	2010	4
14	10650037	2010	1
18	10650001	2010	4
19	10650009	2010	7
21	10650009	2010	5
23	10650016	2009	1
24	10650016	2009	5
25	10650016	2009	2
27	10650040	2012	1
28	10650040	2012	1
29	10650040	2012	4
30	10650040	2012	7
31	10650040	2012	1

**Gambar 4.15.** Interface Laporan Praktikan

Gambar 4.15 merupakan *interface* laporan praktikan. Pada halaman laporan praktikan berisi laporan data praktikan. Data praktkan yang dilaporkan yaitu id mahasiswa, periode, dan id jadwal. Terdapat filter berdasarkan id mahasiswa dan periode. Terdapat tombol *print* untuk mencetak seluruh data laporan praktikan.

#### 4.2.2. Implementasi Prosedural

Implementasi prosedural berisi *source code* implementasi algoritma kriptografi RSA yang terdiri dari 3 proses, yaitu : pembangkitan kunci, enkripsi, dan dekripsi.

#### 4.2.2.1. Source Code Pembangkitan Kunci RSA

```
Public P As Double, Q As Double, phi As Double, E As Double, D As Double

Public key(4) As Double

Public Sub keygen()

    P = 47
    Q = 71
    E = 79

    If (IsPrime(P)) And (IsPrime(Q)) Then

        N = P * Q
        phi = (P - 1) * (Q - 1)

        If (gcd(E, phi)) Then

            D = 1019

            If euler(phi, E, D) Then

                End If

            End If

        End If

        key(1) = E
        key(2) = D
        key(3) = N

    End Sub
```



```
Private Function euler(phi As Double, E As Double, D  
As Double) As Boolean
```

```
    k = 1
```

```
    While f < D
```

```
        f = (1 + (k * phi)) / E
```

```
        If f = D Then
```

```
            euler = True
```

```
        Else
```

```
            euler = False
```

```
        End If
```

```
        k = k + 1
```

```
    Wend
```

```
End Function
```

```
Private Function gcd(a As Double, b As Double) As  
Boolean
```

```
    hasil = 999
```

```
    c = a
```

```
    d = b
```

```
    While hasil > 0
```

```
        hasil = c Mod d
```

```
        If hasil = 0 Then
```

```
            If d = 1 Then
```

```
                gcd = True
```

```
Else
    gcd = False
End If
c = d
d = hasil
Wend
End Function
Private Function IsPrime(lngNumber As Double) As Boolean
On Error Resume Next
Dim lngCount#
Dim lngSqr#
Dim x#
lngSqr = Int(Sqr(lngNumber))
If lngNumber < 2 Then
    IsPrime = False
    Exit Function
End If
lngCount = 2
IsPrime = True
If lngNumber Mod lngCount = 0 Then
    IsPrime = False
    Exit Function
End If
```

```

IngCount = 3

    End If

For x = IngCount To IngSqr Step 2
    If IngNumber Mod x = 0 Then
        IsPrime = False
        Exit Function
    End If
Next
End Function

Private Function nMod(x As Double, y As Double) As Double
    On Error Resume Next
    Dim z#
    z = x - (Int(x / y) * y)
    nMod = z
End Function

Public Function Mult(ByVal x As Double, ByVal p As Double, ByVal m As Double) As Double
    On Error GoTo error1
    y = 1
    Do While p > 0
        Do While (p / 2) = Int((p / 2))
            x = nMod((x * x), m)
            p = p / 2
        Loop
    Loop

```

```
y = nMod((x * y), m)
```

```
p = p - 1
```

```
End If
```

```
Loop
```

```
  Mult = y
```

```
  Exit Function
```

```
error1:
```

```
y = 0
```

```
... ..
```

#### 4.2.2.2. Source Code Enkripsi Algoritma RSA

```
Public Function enc(tIp As String, eE As Double, eN  
As Double) As String
```

```
On Error Resume Next
```

```
Dim encSt As String
```

```
encSt = ""
```

```
e2st = ""
```

```
If tIp = "" Then Exit Function
```

```
For i = 1 To Len(tIp)
```

```
  encSt = encSt & Mult(CLng(Asc(Mid(tIp, i,  
1))), eE, eN) & "+"
```

```
Next i
```

```
enc = encSt
```

```
End Function
```

#### 4.2.2.3. Source Code Dekripsi Algoritma RSA

```

Public Function dec(tIp As String, dD As Double, dN
As Double) As String

    On Error Resume Next

    Dim decSt As String
    decSt = ""
    For z = 1 To Len(tIp)
        ptr = InStr(z, tIp, "+")
        tok = Val(Mid(tIp, z, ptr))
        decSt = decSt + Chr(Mult(tok, dD, dN))
        z = ptr
    Next z
    dec = decSt

End Function

```

### 4.3. Pengujian dan Hasil Uji Coba Sistem

#### 4.3.1. Pengujian Sistem

Pada sub bab ini akan dibahas tentang pengujian sistem yang telah berjalan. Pengujian dilakukan untuk mengetahui apakah sistem telah berjalan sesuai yang diharapkan. Pengujian sistem yang dilakukan dapat dilihat pada Gambar 4.16.

**Gambar 4.16.** Pengujian Sistem

Gambar 4.16 menunjukkan pengujian sistem terhadap implementasi algoritma kriptografi RSA untuk mengenkripsi data yang tersimpan di dalam *smart card*. Hasilnya ketika *read* data yang ada di dalam *smart card*, data yang terbaca berupa *ciphertext*. Diperlukan proses dekripsi untuk menampilkan data aslinya (*plaintext*).

#### 4.3.1.1. Pengujian Enkripsi Algoritma RSA

Data yang digunakan untuk pengujian enkripsi ini adalah data yang disimpan ke dalam *smart card* yaitu: id mahasiswa, id jadwal beserta rekap absen.

Data *input* 1 (id mahasiswa) = 10650009

1. 10650009 diubah ke format ASCII menjadi 49 48 54 53 48 48 48 57
2. Melakukan proses enkripsi dengan rumus  $C_i = M_i^e \bmod N$

$$C_1 = 49^{79} \bmod 3337 = 789$$

$$C_2 = 48^{79} \bmod 3337 = 2304$$

$$C_3 = 54^{79} \bmod 3337 = 1019$$

$$C_4 = 53^{79} \bmod 3337 = 65$$

$$C_5 = 48^{79} \bmod 3337 = 2304$$

$$C_6 = 48^{79} \bmod 3337 = 2304$$

$$C_7 = 48^{79} \bmod 3337 = 2304$$

$$C_8 = 57^{79} \bmod 3337 = 2987$$

Hasil enkripsi dari 10650037 adalah 789 2304 1019 65 2304 2304 2304 2987

Data *input* 2 (id jadwal | rekap absen) = 5|10 (id jadwal = 5 | rekap absen = 10)

1. 5|10 diubah ke format ASCII menjadi 53 124 49 48
2. Melakukan proses enkripsi dengan rumus  $C_i = M_i^e \bmod N$

$$C_1 = 53^{79} \bmod 3337 = 65$$

$$C_2 = 124^{79} \bmod 3337 = 207$$

$$C_3 = 49^{79} \bmod 3337 = 789$$

$$C_4 = 48^{79} \bmod 3337 = 2304$$

Hasil enkripsi dari 5|10 adalah 65 207 789 2304

#### 4.3.1.2. Pengujian Dekripsi Algoritma RSA

Deskripsi dilakukan untuk mengubah data yang tidak bisa terbaca berupa *ciphertext* ke data asli (*plaintext*). Data *input* yang akan diproses pada proses deskripsi ini adalah id mahasiswa, id jadwal beserta rekap absen yang telah terenkripsi.

Hasil enkripsi id mahasiswa = 789 2304 1019 65 2304 2304 2304 2987

1. Melakukan proses dekripsi dengan rumus  $M_i = C_i^d \text{ mod } N$

$$M_1 = 789^{1019} \text{ mod } 3337 = 49$$

$$M_1 = 789^{1019} \text{ mod } 3337 = 49$$

$$M_2 = 2304^{1019} \text{ mod } 3337 = 48$$

$$M_3 = 1019^{1019} \text{ mod } 3337 = 54$$

$$M_4 = 65^{1019} \text{ mod } 3337 = 53$$

$$M_5 = 2304^{1019} \text{ mod } 3337 = 48$$

$$M_6 = 2304^{1019} \text{ mod } 3337 = 48$$

$$M_7 = 2304^{1019} \text{ mod } 3337 = 48$$

$$M_8 = 2987^{1019} \text{ mod } 3337 = 57$$

2. 49 48 54 53 48 48 48 57 dirubah dengan menggunakan format ASCII menjadi 10650037

Hasil enkripsi id jadwal | rekap absen = 65 207 789 2304

1. Melakukan proses dekripsi dengan rumus  $M_i = C_i^d \text{ mod } N$

$$M_1 = 65^{1019} \text{ mod } 3337 = 53$$



$$M_2 = 207^{1019} \bmod 3337 = 124$$

$$M_3 = 789^{1019} \bmod 3337 = 49$$

$$M_4 = 2304^{1019} \bmod 3337 = 48$$

2. 53 124 49 48 dirubah dengan menggunakan format ASCII menjadi 5|10

### 4.3.2. Hasil Uji Coba Sistem

#### 4.3.2.1. Hasil Uji Coba Enkripsi Algoritma RSA

Hasil uji coba enkripsi algoritma RSA dapat dilihat pada Tabel 4.1.

**Tabel 4.1.** Hasil Uji Coba Enkripsi

Data yang Diuji	Jumlah Karakter	Hasil Enkripsi	Kesimpulan
10650009	8	789+2304+1019+65+2304+ 2304+2304+ 2987	<input checked="" type="checkbox"/> Sukses <input type="checkbox"/> Gagal
10650037	8	789+2304+1019+65+2304+ 2304+523+1773	<input checked="" type="checkbox"/> Sukses <input type="checkbox"/> Gagal
10650041	8	789+2304+1019+65+2304+ 2304+3137+789	<input checked="" type="checkbox"/> Sukses <input type="checkbox"/> Gagal

10650117	8	789+2304+1019+65+2304+ 789+789+1773	<input checked="" type="checkbox"/> Sukses <input type="checkbox"/> Gagal
10650010	8	789+2304+1019+65+2304+ 2304+789+2304	<input checked="" type="checkbox"/> Sukses <input type="checkbox"/> Gagal
5 10	4	65 207 789 2304	<input checked="" type="checkbox"/> Sukses <input type="checkbox"/> Gagal
2 5	3	1662+207+65	<input checked="" type="checkbox"/> Sukses <input type="checkbox"/> Gagal
1 3	3	789+207+523	<input checked="" type="checkbox"/> Sukses <input type="checkbox"/> Gagal
1 18	4	789+207+789+2780	<input checked="" type="checkbox"/> Sukses <input type="checkbox"/> Gagal
2 23	4	1662+207+1662+523	<input checked="" type="checkbox"/> Sukses <input type="checkbox"/> Gagal

#### 4.3.2.2. Hasil Uji Coba Autentifikasi *Smart Card*

Hasil uji coba autentifikasi *smart card* dapat dilihat pada Tabel 4.2.

**Tabel 4.2.** Hasil Uji Coba Autentifikasi Smart Card

Butir Uji	Hasil yang diharapkan	Hasil yang diamati	Kesimpulan
Masukkan kartu	Sistem mampu mendeteksi keberadaan kartu.	Sistem dapat mendeteksi keberadaan kartu.	<input checked="" type="checkbox"/> Sukses <input type="checkbox"/> Gagal
<i>Write data ke smart card</i>	Memasukkan data kedalam <i>smart card</i>	Data berhasil dimasukkan ke dalam <i>smart card</i>	<input checked="" type="checkbox"/> Sukses <input type="checkbox"/> Gagal
<i>Read data smart card</i>	Membaca data <i>smart card</i>	Data berhasil dibaca oleh sistem	<input checked="" type="checkbox"/> Sukses <input type="checkbox"/> Gagal

#### 4.3.2.3. Hasil Uji Coba Implementasi Algoritma RSA

Hasil uji coba implementasi algoritma RSA dapat dilihat pada Tabel 4.3.

**Tabel 4.3.** Hasil Uji Coba Implementasi Algoritma RSA

Butir Uji	Hasil yang diharapkan	Hasil yang diamati	Kesimpulan
Proses enkripsi	Data dapat dienkripsi sehingga menghasilkan output <i>ciphertext</i>	Data berhasil dienkripsi tampil hasil enkripsi yaitu <i>ciphertext</i>	[ <input checked="" type="checkbox"/> ] Sukses [ ] Gagal
Proses dekripsi	Data dapat dideskripsi sehingga menghasilkan output <i>plaintext</i>	Data berhasil dideskripsi tampil hasil deskripsi yaitu <i>plaintext</i>	[ <input checked="" type="checkbox"/> ] Sukses [ ] Gagal

#### 4.4. Integrasi Kriptografi Menurut Kajian dalam Al Qur'an

Menjamin keamanan data merupakan hal yang perlu dilakukan untuk menjaga data/informasi dari pihak yang tidak berwenang. Seperti yang dijelaskan dalam Al Qur'an surah Al Waaqi'ah (56) ayat 77-80 sebagai berikut:

إِنَّهُ لَقُرْآنٌ كَرِيمٌ ﴿٧٧﴾ فِي كِتَابٍ مَّكْنُونٍ ﴿٧٨﴾ لَا يَمَسُّهُ إِلَّا الْمُطَهَّرُونَ ﴿٧٩﴾  
 تَنْزِيلٌ مِّن رَّبِّ الْعَالَمِينَ ﴿٨٠﴾

Artinya : “bahwa sesungguhnya (yang dibacakan kepada kamu) itu ialah Al Qur’an yang mulia. Yang tersimpan dalam Kitab yang cukup terpelihara. Yang tidak disentuh melainkan oleh makhluk-makhluk yang disucikan. Al Qur’an itu diturunkan dari Allah Tuhan sekalian alam.” (QS Al-Waqiah (56) : 77-80)

Dari ayat di atas dijelaskan tentang jaminan Allah SWT terhadap Al Qur’an. Allah memelihara Al Qur’an dari upaya syetan yang ingin mengubah isi dari Al Qur’an, sehingga Al Qur’an tetap terjaga kesucian dan kemurniannya. Sama halnya dengan menjaga keamanan data. Keamanan merupakan aspek yang penting sehingga informasi yang dirahasiakan tetap aman dari orang-orang yang tidak berwenang untuk mengetahuinya. Berbagai cara dapat dilakukan untuk menjamin keamanan data, salah satunya dengan teknik kriptografi. Kriptografi adalah seni untuk mengamankan dan merahasiakan informasi.

يَأْتِيهَا الَّذِينَ ءَامَنُوا لَا تَخُونُوا اللَّهَ وَالرَّسُولَ وَتَخُونُوا أَمْنَتِكُمْ وَأَنْتُمْ تَعْلَمُونَ ﴿٧٧﴾

Artinya: “Sesungguhnya Allah menyuruh kamu menyampaikan amanat kepada yang berhak menerimanya, dan (menyuruh kamu) apabila menetapkan hukum di antara manusia supaya kamu menetapkan dengan adil. Sesungguhnya Allah memberi pengajaran yang sebaik-baiknya kepadamu. Sesungguhnya Allah adalah Maha mendengar lagi Maha melihat.” (QS Al-Anfaal: 27)

Dari ayat di atas menurut Yahya Kurniawan dalam tafsir Jalalain dijelaskan, bahwa Allah menyuruh kita agar senantiasa menyampaikan amanat kepada orang yang berhak menerimanya. Sehingga ayat tersebut menganjurkan agar kita menjaga amanat yang dititipkan kepada kita dan tidak memberitahukan amanat

tersebut kepada orang yang tidak berhak menerimanya, dan salah satu jenis dari amanat tersebut adalah rahasia. Dikarenakan rahasia merupakan amanat, maka kita juga berkewajiban menjaga rahasia yang telah dititipkan kepada kita dan janganlah mengkhianati dengan memberitahukan amanat tersebut kepada yang tidak berhak.

Menjamin keamanan data merupakan salah satu bentuk menjaga rahasia terhadap data yang diamankan agar tidak dapat dibaca oleh orang yang tidak berhak membacanya.

Hasil yang telah diperoleh dari skripsi ini adalah perangkat lunak yang dibangun telah berhasil mengenkripsi data menggunakan algoritma kriptografi RSA sehingga data tersebut tidak bisa dibaca oleh orang yang tidak berwenang. Hal ini sudah memenuhi keamanan yang menjadi salah satu aspek dari kriptografi. Kaitannya dengan keislaman bahwa keamanan merupakan pemberian dari Allah SWT yang dengan keamanan akan tercapai segala kemaslahatan dan kebaikan yang dibutuhkan manusia.

## BAB V

### KESIMPULAN DAN SARAN

#### 5.1. Kesimpulan

Berdasarkan pembahasan mengenai implementasi algoritma kriptografi RSA pada aplikasi *smart card* dapat diambil kesimpulan sebagai berikut :

1. Algoritma kriptografi RSA dapat diimplementasikan pada aplikasi *smart card* untuk mengamankan data yang ada di dalam *smart card*.
2. Data yang disimpan di dalam *smart card* berupa *ciphertext* yang merupakan hasil enkripsi menggunakan algoritma kriptografi RSA, sehingga pihak yang tidak berwenang tidak dapat mengambil, membaca, atau memanipulasi data tersebut.
3. Berdasarkan hasil pengujian terhadap implementasi algoritma RSA, didapatkan nilai akurasi sebesar 100%.
4. Berdasarkan hasil pengujian terhadap *smart card*, didapatkan batas maksimal penyimpanan data (*record*) adalah 7 alamat.

#### 5.2. Saran

Beberapa saran untuk penelitian dan pengembangan aplikasi selanjutnya adalah sebagai berikut:

1. Pengembangan aplikasi yang telah dilakukan masih perlu dilakukan studi, penyesuaian, dan perbaikan lebih lanjut. Hal ini diperlukan aplikasi yang dikembangkan dapat mengakomodasi semua kebutuhan yang diperlukan.
2. Dapat digunakan berbagai macam metode kriptografi lain untuk mengamankan data pada *smart card*.





**DAFTAR PUSTAKA**

- Akbar, Fiqri, dkk. 2011. *Pembuatan Report dan Pengaksesan Presensi Smart Card Melalui SMS Gateway*. Politeknik Elektronika Negeri Surabaya Institut Teknologi Sepuluh Nopember (ITS) Surabaya
- Ariyus, Dony. 2006. *Kriptografi Keamanan Data dan Komunikasi*. Yogyakarta: Graha Ilmu.
- Astrianto, Stefanus. 2008. *Pembangunan Perangkat Lunak untuk Security pada Contactless Smart Card dengan Algoritma RC4*. Sekolah Tinggi Elektro dan Informatika, Institut Teknologi Bandung
- Burnett, Steve, dkk. 2004. *RSA Security's Official Guide to Cryptography*. Calofornia: RSA Press
- Depkominfo. 2008. *Laporan Studi Penyusunan Kebijakan Pemerintah mengenai Kerangka Kerja (Framework) Penerapan Kartu Pintar (Smart Card) Di Indonesia*. Pusat Penelitian dan Pengembangan APTEL SKDI.
- Fakhrudin, Rijal, dkk. *Implementasi Portable Smart Card Reader untuk Absensi*. Sekolah Tinggi Elektro dan Informatika, Institut Teknologi Bandung
- Kurniawan, Yahya. 2001. *Singkat Tepat Jelas VBScript*. Jakarta : PT Gramedia
- Margoselo, Bambang. 2003. *Tinjauan Smart Card untuk Pengamanan Database Di Sekolah Berbasis Komputer*. Institut Teknologi Bandung.
- Monica, Martha. 2013. *Pemanfaatan Algoritma Kriptografi Dalam Pembuatan Smart Card*. Institut Teknologi Bandung.

Rahajoeningroem, Tri dkk. 2008. *Studi dan Implementasi Algoritma RSA untuk Pengamanan Data Transkrip Akademik Mahasiswa*. Jurusan Teknik Elektro Universitas Komputer Indonesia.

Sariasih, Christine. 2009. *Rancangan Keamanan Data Sistem Smart Card Kesehatan Sesuai Kebutuhan di Indonesia*. Fakultas Ilmu Komputer Universitas Indonesia.

Stallings, William. 2003. *Cryptography and Network Security : Principles and Practice*. Prentice-Hall, New Jersey.

Syaputra, Hendri dkk. 2012. *Aplikasi Enkripsi Data pada File Text dengan Algoritma RSA*. Jurusan Teknik Informatika, Sekolah Tinggi Teknik Musi, Palembang.

Triorizka, Adrianus. 2010. *Penerapan Algoritma RSA untuk Pengamanan Data dan Digital Signature dengan .Net*. Sekolah Tinggi Manajemen Informatika dan Komputer AMIKOM, Yogyakarta.

WAHANAKomputer Semarang. 2003. *Memahami Model Enkripsi dan Security Data*. Yogyakarta: ANDI.

Wibowo, Ivan dkk. 2008. *Penerapan Algoritma Kriptografi Asimetris RSA untuk Keamanan Data di Oracle*. Fakultas Teknik, Universitas Kristen Duta Wacana.

Dahlan Iskan : Pertamina Siapkan Rp 2 Triliun Buat *Smartcard*, diakses dari <http://detik.com/finance/read/2012/06/27/200839/1952581/1034/>, pada tanggal 15 Mei 2014 pukul 20.00 WIB