PENERAPAN ALGORITMA ELGAMAL PADA *SMART CARD* UNTUK KEAMANAN DATA DALAM TRANSAKSI JUAL BELI

SKRIPSI

oleh:
ADE DUROTUN NISA'
NIM. 10650111

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

HALAMAN PENGAJUAN

PENERAPAN ALGORITMA ELGAMAL PADA *SMART CARD* UNTUK KEAMANAN DATA DALAM TRANSAKSI JUAL BELI

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 :
ADE DUROTUN NISA'
NIM. 10650111 / S-1

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

2014

HALAMAN PERSETUJUAN

PENERAPAN ALGORITMA ELGAMAL PADA *SMART CARD* UNTUK KEAMANAN DATA DALAM TRANSAKSI JUAL BELI

SKRIPSI

Oleh :

Nama : Ade Durotun Nisa;
NIM : 10650111
Jurusan : Teknik Informatika
Fakultas : Sains Dan Teknologi

Telah Diperiksa dan Disetujui untuk Diuji :
Tanggal : November 2014

Dosen Pembimbing I	**Dosen Pembimbing II**
Totok Chamidy, M.Kom	**Ririen Kusumawati, M.Kom**
NIP.19691222 200604 1 001	**NIP.19720309 200501 2 002**

Mengetahui,
Ketua Jurusan Teknik Informatika

Dr. Cahyo Crysdian
NIP. 19740424 200901 1 008

HALAMAN PENGESAHAN

PENERAPAN ALGORITMA ELGAMAL PADA *SMART CARD* UNTUK KEAMANAN DATA DALAM TRANSAKSI JUAL BELI

SKRIPSI

Oleh :

ADE DUROTUN NISA'
NIM. 10650111

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

Susunan Dewan Penguji :			**Tanda Tangan**
Penguji Utama	**:**	**A'la Syauqi, M.Kom** **NIP.19771201 200801 1 007**	**( )**
Ketua Penguji	**:**	**Dr.Muhammad Faisal, M.T** **NIP.19740510 200501 1 007**	**( )**
Sekretaris Penguji	**:**	**Totok Chamidy, M.Kom** **NIP.19691222 200604 1 001**	**( )**
Anggota Penguji	**:**	**Ririen Kusumawati, M.Kom** **NIP.19720309 200501 2 002**	**( )**

Mengesahkan,
Ketua Jurusan Teknik Informatika

Dr. Cahyo Crysdian
NIP. 19740424 200901 1 008

HALAMAN PERNYATAAN
ORISINALITAS PENELITIAN

Saya yang bertandatangan di bawah ini:

Nama	: Ade Durotun Nisa’
NIM	: 10650111
Fakultas/Jurusan	: Sains Dan Teknologi / Teknik Informatika
Judul Penelitian	: PENERAPAN ALGORITMA ELGAMAL PADA *SMART CARD* UNTUK KEAMANAN DATA DALAM TRANSAKSI JUAL BELI

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,

Ade Durotun Nisa’
NIM. 10650111

MOTTO

The true happiness comes when we are able to make others happy

And

Every successful person must have a failure. Do not be afraid to fail because failur is a part of success

~ Yoong ~

HALAMAN PERSEMBAHAN

Dengan rasa syukur seraya mengharap ridho Ilahi kupersembahkan karya ini kepada :
Ayahanda dan Ibunda tercinta
H. Ach. Zuhro** dan **Hj. Muzdalifah
Serta Kakak saya tercinta
Fitri Zulifiah
Atas Segalanya.

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

*Kepada sahabatku kelompok MMM **Aldita, Puspa, Vivid, agus, Naufal , Syafe'i, Nopi, Haris, Zainal, Dian** yang selalu berbagi suka cita bersama-sama.*

*Kepada sahabatku yang telah berpulang terlebih dahulu, **Alm.Muslih Adlan Agung.***

Kepada para sahabat TI angkatan 2010, yang selalu ada untuk membantu sesama.

Dan kepada teman-temanku semua yang tidak bisa kusebutkan satu persatu yang selalu membantuku dan menyemangatiku di saat aku susah dan terpuruk.

Semoga Allah SWT melindungi, menyayangi dan menempatkan mereka semuanya pada surganya kelak dan melimpahkan rezeki kepada mereka semua...

KATA PENGANTAR

بسم الله الرحمن الرحيم

Segala puji bagi Allah SWT yang telah melimpahkan rahmat serta karuniaNya kepada penulis sehingga bisa menyelesaikan skripsi dengan judul "PENERAPAN ALGORITMA ELGAMAL PADA *SMART CARD* UNTUK KEAMANAN DATA DALAM TRANSAKSI JUAL BELI" dengan baik.

Shalawat serta salam semoga tercurah kepada Nabi Agung Muhammad SAW yang telah membimbing umatnya dari gelapnya kekufuran menuju cahaya Islam yang terang benderang.

Penulis menyadari keterbatasan pengetahuan yang penulis miliki, karena itu tanpa keterlibatan dan sumbangsih dari berbagai pihak, sulit bagi penulis untuk menyelesaikan skripsi ini. Maka dari itu dengan segenap kerendahan hati patutlah penulis ucapkan terima kasih kepada:

1. Totok Chamidy, M.Kom, selaku dosen pembimbing I yang telah meluangkan waktu untuk membimbing, memotivasi, mengarahkan dan memberi masukan dalam pengerjaan skripsi ini.
2. Ririen Kusumawati, M.Kom, selaku dosen pembimbing II, yang selalu memberikan masukan, nasehat serta petunjuk dalam penyusunan laporan skripsi ini.
3. Cahyo Crysdian, M.Kom selaku Ketua Jurusan Teknik Informatika Universitas Islam Negeri Maulana Malik Ibrahim Malang, yang mendukung dan mengarahkan dalam pengerjaan skripsi ini.

4. Segenap Dosen Teknik informatika yang telah memberikan bimbingan keilmuan kepada penulis selama masa studi.
5. Semua pihak yang tidak mungkin penulis sebutkan satu-persatu, atas segala yang telah diberikan kepada penulis dan dapat menjadi pelajaran.

Sebagai penutup, penulis menyadari dalam skripsi ini masih banyak kekurangan dan jauh dari sempurna. Semoga apa yang menjadi kekurangan bisa disempurnakan oleh peneliti selanjutnya. Apa yang menjadi harapan penulis, semoga karya ini bermanfaat bagi kita semua. Amin.

Malang, November 2014

Penulis

DAFTAR ISI

HALAMAN JUDUL.....i
HALAMAN PENGAJUAN.....ii
HALAMAN PERSETUJUAN.....iii
HALAMAN PENGESAHAN.....iv
HALAMAN PERNYATAAN.....v
HALAMAN MOTTO.....vi
HALAMAN PERSEMBAHAN.....vii
KATA PENGANTAR.....viii
DAFTAR ISI.....x
DAFTAR GAMBAR.....xiii
DAFTAR TABEL.....xiv
ABSTRAK.....xv
ABSRTACT.....xvi
الملخص.....xvii
BAB I PENDAHULUAN.....1
1.1 Latar Belakang.....1
1.2 Identifikasi Masalah.....3
1.3 Batasan Masalah.....3
1.4 Tujuan Penelitian.....4
1.5 Manfaat Penelitian.....4
1.6 Metode Penelitian.....4
1.7 Sistematika Penulisan.....6
BAB II TINJAUAN PUSTAKA.....8
2.1 Penelitian Terkait.....8
2.2 *Smart card*.....9

2.3 Sistem Keamanan.....10
2.4 Kriptografi.....11
2.5 Algoritma Kriptografi.....13
2.5.1. Algoritma Simetris.....14
2.5.2. Algoritma Asimetris.....14
2.6 Algoritma Elgamal.....16
4.2.1. Proses Pembentukan Kunci.....17
4.2.2. Proses Enkripsi.....17
4.2.3. Proses Deskripsi.....19

BAB III METODE DAN PERANCANGAN SISTEM.....20

3.1. Blog Diagram.....21
3.2. Diagram Alir Sistem.....21
3.2.1. Diagram Alir Pembuatan ID Pelanggan Baru.....22
3.2.2. Diagram Alir Pengisian Saldo.....22
3.2.3. Diagram Alir Transaksi Jual Beli.....23
3.3. Analisis *Input*.....25
3.4. Analisis *Output*.....25
3.5.Perancangan Data.....25
3.5.1. Perancangan Data *Input*.....26
3.5.2. Perancangan Data *Output*.....26
3.6. Flwchart Sistem.....27
3.7. Flowchart Algoritma.....28
3.4.1 Proses Pembentukan Kunci.....28
3.4.2 Proses Enkripsi.....29
3.4.3 Proses Deskripsi.....31
3.6.Data Flow Diagram.....33
3.6.1. Context Diagram.....33
3.6.2. DFD Level 1.....34
3.6.3. DFD Level 2 *Input* Data Pelanggan.....35
3.6.4. DFD Level 2 Transaksi Jual Beli.....35
3.7. Desain Interface.....36

3.8. Kebutuhan Sistem 42
BAB IV HASIL DAN PEMBAHASAN 46
4.1. Implementasi Sistem 46
4.2. Implementasi Algoritma Elgamal 47
4.2.1. Tahapan Pembentukan Kunci 47
4.2.2. Tahapan Proses Enkripsi.....47
4.2.3. Tahapan Proses Deskripsi 48
4.3. Implementasi *Interface* dan Fungsinya 50
4.4. Evaluasi dan Analisis Hasil Pengujian.....58
4.4.1. Pengujian Proses Enkripsi 58
4.4.2. Pengujian Proses Deskripsi.....62
4.4.3. Pengujian Autentifikasi pada *Smart card* 65
4.5. Hasil Pengujian Algoritma Elgamal.....66
4.6. Integrasi Kriptografi Menurut Kajian dalam Islam.....67
BAB V PENUTUP.....69
5.1. Kesimpulan 69
5.2. Saran.....69
DAFTAR PUSTAKA 70

DAFTAR GAMBAR

Gambar 2.1 Proses Enkripsi Deskripsi....12
Gambar 2.2 Proses Algoritma Simetris....14
Gambar 2.3 Proses Algoritma Asimetris....15
Gambar 2.4 Proses Algoritma Elgamal....16
Gambar 2.5 Kode ASCII....18
Gambar 3.1 Blog Diagram....21
Gambar 3.2 Diagram Alir Proses Pembuatan Id Pelanggan Baru....22
Gambar 3.3 Diagram Alir Proses Pengisian Saldo....23
Gambar 3.4 Diagram Alir Proses Transaksi Jual Beli....24
Gambar 3.5 Flowchart Sistem....27
Gambar 3.6 Flowchart Pembentukan Kunci....28
Gambar 3.7 Flowchart Proses Enkripsi....29
Gambar 3.8 Flowchart Proses Dekripsi....31
Gambar 3.9 Context Diagram....33
Gambar 3.10 DFD Level 1....34
Gambar 3.11 DFD Level 2 *Input* Data Pelanggan....35
Gambar 3.12 DFD Level 2 Transaksi Jual Beli....35
Gambar 3.13 Form *Login*....36
Gambar 3.14 Form *Home*....37
Gambar 3.15 Form Barang....37
Gambar 3.16 Form *Input* Pelanggan....38
Gambar 3.17 Form *Input* Saldo....39
Gambar 3.18 Form Penjualan....40
Gambar 3.19 Form Laporan Barang....40
Gambar 3.20 Form Laporan Pelanggan....41
Gambar 3.21 Form Laporan Penjualan....41
Gambar 3.22 Kartu SLE4428....43
Gambar 3.23 *Smart card Reader Writer*....44
Gambar 4.1 Form Menu *Login*....50
Gambar 4.2 Form Menu *Home*....51
Gambar 4.3 Form Menu *Input* Barang....52
Gambar 4.4 Form Menu *Input* Pelanggan....53
Gambar 4.5 Form Menu *Input* Saldo....54
Gambar 4.6 Form Menu Transaksi Jual Beli....55
Gambar 4.7 Form Menu Laporan Barang....56
Gambar 4.8 Form Menu Laporan Pelanggan....57
Gambar 4.9 Form Menu Laporan Penjualan....58
Gambar 4.10 Form Membaca Data Kartu....61

DAFTAR TABEL

Tabel 3.1 Tabel Proses Pembentukan Kunci k.....25
Tabel 3.2 Tabel Proses Pengembalian ASCII ke *Char*.....27
Tabel 3.3 Tabel Perancangan Data *Input*.....28
Tabel 3.4 Tabel Perancangan Data *Output*.....29
Tabel 4.1 Tabel Pembentukan Kunci k pada Data Id Pelanggan.....57
Tabel 4.2 Tabel Pembentukan Kunci k pada Data Saldo Pelanggan.....58
Tabel 4.3 Tabel Pengujian Hasil Proses Enkripsi.....60
Tabel 4.4 Tabel Hasil Deskripsi Id Pelanggan.....62
Tabel 4.5 Tabel Hasil Deskripsi Saldo Pelanggan.....63
Tabel 4.6 Tabel Hasil Pengujian Proses Deskripsi.....64
Tabel 4.7 Tabel Hasil Pengujian Autentifikasi Aplikasi *Smart card*.....65
Tabel 4.8 Tabel Hasil Penerapan Algoritma Elgamal.....66

UNIVERSITAS ISLAM NEGERI MAULANA MALIK IBRAHIM PUSAT PERPUSTAKAAN

ABSTRAK

Durotun Nisa', Ade. 2014. Penerapan Algoritma Elgamal pada *Smart card* untuk Keamanan Data dalam Transaksi Jual Beli. Skripsi. Jurusan Teknik Informatika Fakultas Sains dan Teknologi Universitas Islam Negeri Maulana Malik Ibrahim Malang. Pembimbing: (I) Totok Chamidy, M.Kom., (II).Ririen Kusumawati, M.Kom.

Kata Kunci : *Smart card, Algoritma Elgamal*

Smart card adalah suatu penemuan di bidang IT yang telah mempermudah kehidupan manusia karena mempunyai banyak fungsi dan kemampuannya dalam menyimpan data *cardholder*. *Smart card* merupakan suatu kartu yang mempunyai rangkaian terintegrasi di dalamnya dan mampu memproses serta menyimpan data. Seiring dengan maraknya penggunaan *smart card* untuk identifikasi dan penyimpanan data, *smart card* mempunyai masalah yang penting untuk diperhatikan yaitu keamanannya. Dibutuhkan cara untuk mengamankan agar data penting hanya dapat diakses oleh pihak yang berhak/berwenang.

Dalam penelitian ini digunakan algoritma kriptografi Elgamal untuk mengamankan data yang ada di dalam *memory smart card.* Tingkat keamanan algoritma ini didasarkan atas masalah logaritma diskrit pada grup pergandaan bilangan bulat modulo prima. Algoritma ini termasuk algoritma kriptografi asimetris yang menggunakan dua jenis kunci, yaitu kunci publik dan kunci rahasia. Data yang ada di dalam *memory smart card* diamankan menggunakan metode penyandian algoritma Elgamal, sehingga data yang dimasukkan ke dalam *memory smart card* berupa data *ciphertext*. Dalam penelitian ini pengujian dilakukan dengan memasukkan data pelanggan yakni id pelanggan, dan jumlah saldo pelanggan ke dalam *memory smart card*. Data tersebut dienkripsi menggunakan algortima kriptografi elgamal, sehingga data yang disimpan ke dalam *memory smart card* berupa data *ciphertext* yang tidak bisa dibaca oleh pihak yang tidak berwenang.

ABSTRACT

Durotun Nisa', Ade.2014. The Use of Elgamal Algorithm on Smart card add security of buy and selling transaction. Thesis. Faculty of Science. Teknik Informatika Departmen. Maulana Malik Ibrahim State Islamic University. Advisor : (I) Totok Chamidy, M.Kom., (II).Ririen Kusumawati, M.Kom.

Keyword : Smart card , Elgamal Algorithm

Smart card is a discovery in the field of IT that enables human life because it has many functions and capabilities in the datum store cardholder. Smart card is a card that have integrated series inside that and also be able to processing and saving datum and smart cards have an important issue to consider is safety. For the rise of smart card to identify and saving datum, need a way to secure so important datum can be accessed by the competent side.

In this research the use of elgamal cryptography are to secure datum inside memory of smart card, security level of this algorithm based on the problems discrete algorithm on the doubling of first rate modulo interger group. This algorithm include asymmetric cryptography that use teo keys those are public and secret key, datum that inside the memory of smart card secure using encoding algorithm method so datum that saved on memory of smart card is ciphertext form. In this research, testing is done by entering the customer data customer id, and the number of customer balances in the smart card memory. The datum is encrypted using ElGamal cryptography algorithms, so the data is stored into the memory of the smart card in the form of datum ciphertext that can not be read by unauthorized parties.

الملخص

دورة نساء. اد.2014. تطبيق خوارزمية الجمل على بطاقة الذكية لالبيانات في بيع وشراء المعاملات. أطروحة. . قسم المعلوماتية الكلية العلوم والتكنولوجي الجامعة الحكومية الإسلامية مولانا مالك إبراهيم مالانج. المشرف : 1- توتوك حامدى 2- ريرين كوسومواتى الما جستير.

الكلمات البحث : بطاقة الذكية, خوارزمية الجمل.

البطاقة الذكية هي اكتشاف في مجال تكنولوجيا المعلومات التي تمكن حياة الإنسان لأنه لديه العديد من الوظائف والقدرات في حامل البطاقة مخزن البيانات. لبطاقة الذكية هي البطاقة التي تمت الدوائر المتكاملة فيها, وغير قادرة على تجهيز وتخزين البيانات. جنبا إلى جنب مع الاستخدام الواسع النطاق للبطاقات الذكية لتحديد وتخزين البيانات, والبطاقات الذكية لديها قضية هامة للنظر هو السلامة. يستغرق وسيلة لتأمين تلك البيانات الهامة لا يمكن الوصول إليها من قبل الحزب بعنوان / المعتمدين لديها.

في هذه الدراسة استخدام الجمل خوارزميات التشفير لحماية البيانات في ذاكرة البطاقة الذكية. ويستند خوارزمية مستوى الأمان على مشكلة اللوغاريتم منفصلة على مجموعة تكاثر الأعداد الصحيحة رئيس الحكومة. وتشمل هذه الخوارزميات خوارزمية التشفير غير المتماثلة التي تستخدم نوعين من المفاتيح, أي المفتاح العام والمفتاح السري. يتم تأمين البيانات الموجودة على بطاقة الذاكرة الذكية باستخدام خوارزمية تشفير الجمل, بحيث يتم إدخال البيانات إلى ذاكرة البطاقة الذكية في شكل النص المشفر البيانات. في هذا البحث, ويتم اختبار عن طريق إدخال هوية العملاء بيانات العملاء, وعدد من أرصدة العملاء في ذاكرة البطاقة الذكية. يتم تشفير البيانات باستخدام الجمل خوارزميات التشفير, بحيث يتم تخزين البيانات في الذاكرة لبطاقة الذكية في شكل النص المشفر البيانات التي لا يمكن قراءتها من قبل الأطراف غير مصرح بها.

الملخص

دورة نساء. اد.2014. تطبيق خوارزمية الجمل على بطاقة الذكية لالبيانات في بيع وشراء المعاملات. أطروحة. . قسم المعلوماتية الكلية العلوم والتكنولوجي الجامعة الحكومية الإسلامية مولانا مالك إبراهيم مالانج. المشرف : 1- توتوك حامدى 2- ريرين كوسومواتى الما جستير.

الكلمات البحث : بطاقة الذكية, خوارزمية الجمل.

البطاقة الذكية هي اكتشاف في مجال تكنولوجيا المعلومات التي تمكن حياة الإنسان لأنه لديه العديد من الوظائف والقدرات في حامل البطاقة مخزن البيانات. لبطاقة الذكية هي البطاقة التي تمت الدوائر المتكاملة فيها, وغير قادرة على تجهيز وتخزين البيانات. جنبا إلى جنب مع الاستخدام الواسع النطاق للبطاقات الذكية لتحديد وتخزين البيانات, والبطاقات الذكية لديها قضية هامة للنظر هو السلامة. يستغرق وسيلة لتأمين تلك البيانات الهامة لا يمكن الوصول إليها من قبل الحزب بعنوان / المعتمدين لديها.

في هذه الدراسة استخدام الجمل خوارزميات التشفير لحماية البيانات في ذاكرة البطاقة الذكية. ويستند خوارزمية مستوى الأمان على مشكلة اللوغاريتم منفصلة على مجموعة تكاثر الأعداد الصحيحة رئيس الحكومة. وتشمل هذه الخوارزميات خوارزمية التشفير غير المتماثلة التي تستخدم نوعين من المفاتيح, أي المفتاح العام والمفتاح السري. يتم تأمين البيانات الموجودة على بطاقة الذاكرة الذكية باستخدام خوارزمية تشفير الجمل, بحيث يتم إدخال البيانات إلى ذاكرة البطاقة الذكية في شكل النص المشفر البيانات. في هذا البحث, ويتم اختبار عن طريق إدخال هوية العملاء بيانات العملاء, وعدد من أرصدة العملاء في ذاكرة البطاقة الذكية. يتم تشفير البيانات باستخدام الجمل خوارزميات التشفير, بحيث يتم تخزين البيانات في الذاكرة لبطاقة الذكية في شكل النص المشفر البيانات التي لا يمكن قراءتها من قبل الأطراف غير مصرح بها.

ABSTRACT

Durotun Nisa', Ade.2014. The Use of Elgamal Algorithm on Smart card add security of buy and selling transaction. Thesis. Faculty of Science. Teknik Informatika Departmen. Maulana Malik Ibrahim State Islamic University. Advisor : (I) Totok Chamidy, M.Kom., (II).Ririen Kusumawati, M.Kom.

Keyword : Smart card , Elgamal Algorithm

Smart card is a discovery in the field of IT that enables human life because it has many functions and capabilities in the datum store cardholder. Smart card is a card that have integrated series inside that and also be able to processing and saving datum and smart cards have an important issue to consider is safety. For the rise of smart card to identify and saving datum, need a way to secure so important datum can be accessed by the competent side.

In this research the use of elgamal cryptography are to secure datum inside memory of smart card, security level of this algorithm based on the problems discrete algorithm on the doubling of first rate modulo interger group. This algorithm include asymmetric cryptography that use teo keys those are public and secret key, datum that inside the memory of smart card secure using encoding algorithm method so datum that saved on memory of smart card is ciphertext form. In this research, testing is done by entering the customer data customer id, and the number of customer balances in the smart card memory. The datum is encrypted using ElGamal cryptography algorithms, so the data is stored into the memory of the smart card in the form of datum ciphertext that can not be read by unauthorized parties.

ABSTRAK

Durotun Nisa', Ade. 2014. Penerapan Algoritma Elgamal pada *Smart card* untuk Keamanan Data dalam Transaksi Jual Beli. Skripsi. Jurusan Teknik Informatika Fakultas Sains dan Teknologi Universitas Islam Negeri Maulana Malik Ibrahim Malang. Pembimbing: (I) Totok Chamidy, M.Kom., (II).Ririen Kusumawati, M.Kom.

Kata Kunci : *Smart card, Algoritma Elgamal*

Smart card adalah suatu penemuan di bidang IT yang telah mempermudah kehidupan manusia karena mempunyai banyak fungsi dan kemampuannya dalam menyimpan data *cardholder*. *Smart card* merupakan suatu kartu yang mempunyai rangkaian terintegrasi di dalamnya dan mampu memproses serta menyimpan data. Seiring dengan maraknya penggunaan *smart card* untuk identifikasi dan penyimpanan data, *smart card* mempunyai masalah yang penting untuk diperhatikan yaitu keamanannya. Dibutuhkan cara untuk mengamankan agar data penting hanya dapat diakses oleh pihak yang berhak/berwenang.

Dalam penelitian ini digunakan algoritma kriptografi Elgamal untuk mengamankan data yang ada di dalam *memory smart card*. Tingkat keamanan algoritma ini didasarkan atas masalah logaritma diskrit pada grup pergandaan bilangan bulat modulo prima. Algoritma ini termasuk algoritma kriptografi asimetris yang menggunakan dua jenis kunci, yaitu kunci publik dan kunci rahasia. Data yang ada di dalam *memory smart card* diamankan menggunakan metode penyandian algoritma Elgamal, sehingga data yang dimasukkan ke dalam *memory smart card* berupa data *ciphertext*. Dalam penelitian ini pengujian dilakukan dengan memasukkan data pelanggan yakni id pelanggan, dan jumlah saldo pelanggan ke dalam *memory smart card*. Data tersebut dienkripsi menggunakan algortima kriptografi elgamal, sehingga data yang disimpan ke dalam *memory smart card* berupa data *ciphertext* yang tidak bisa dibaca oleh pihak yang tidak berwenang.

UNIVERSITAS ISLAM NEGERI
MAULANA MALIK IBRAHIM
PUSAT PERPUSTAKAAN

"Orang-orang yang beriman dan tidak mencampuradukkan iman mereka dengan kezaliman, mereka itulah yang mendapat keamanan dan mereka itu adalah orang-orang yang mendapat petunjuk."(Qs.al An'am : 82)

Dalam surat Al-An'am ayat 82 ini menjelaskan tentang cara mendapatkan keamanan, salah satunya dengan cara tidak mencampur adukkan iman dengan kedzaliman. Maksud iman berarti berbuat yang baik yang menjadikan keamanan bagi lingkungan. Hubungan ayat ini dengan kriptografi yaitu adanya anjuran untuk mendapatkan keamanan. Seperti halnya penelitian ini, dilakukan untuk mendapatkan keamanan data pada aplikasi *smart card*.

Ada berbagai macam cara untuk mendapatkan keamanan dalam aplikasi *smart card*, salah satunya dengan cara mengimplementasikan metode penyandian algoritma kriptografi pada data yang ada didalam *smart card*. Dengan mengimplementasikan algoritma kriptografi, data yang ada di dalam *smart card* dapat terjaga keamanan rahasianya. Algoritma kriptografi merupakan algoritma penyandian dengan teknik enkripsi untuk mengubah data *plaintext* menjadi data *ciphertext*, sehingga pihak yang tidak berwenang tidak dapat membaca data tersebut.

Maka dari itu digunakan metode algoritma kriptografi elgamal untuk mengamankan data *smart card* pada proses transaksi jual beli. Algoritma Elgamal merupakan salah satu algoritma asimetris yang memiliki metode penyandian kunci publik. Kekuatan algoritma ini terletak pada sulitnya menghitung logaritma diskret pada grup bilangan bulat prima yang di

dalamnya dilakukan operasi perkalian. Disebut logaritma diskret karena nilainya berhingga dan bergantung pada bilangan prima yang digunakan. Karena bilangan prima yang digunakan adalah bilangan prima yang besar, maka sangat sulit bahkan tidak mungkin menurunkan kunci privat dari kunci publik yang diketahui. Dengan digunakan algoritma kriptografi, data yang ada di dalam *smart card* menjadi lebih aman.

1.2 Identifikasi Masalah

Smart card merupakan salah satu alat dalam transaksi baik jual beli maupun transaksi lainnya yang memang sudah sering digunakan, keamanan dalam proses transaksi tersebut memang dirasa sangat penting untuk diteliti. Maka dari itu digunakan algoritma elgamal untuk menjaga keamanan data *smart card* dalam proses transaksi jual beli.

Dalam penelitian ini dilakukan penelitian untuk mengetahui hasil dari penerapan algoritma elgamal untuk menjaga keamanan pada data *smart card* dalam transaksi jual beli.

1.3 Batasan Masalah

Agar diperoleh hasil pembahasan yang sesuai dengan tujuan yang diharapkan, maka perlu diberikan batasan-batasan masalah yaitu :

1. Aplikasi Perangkat lunak ini menggunakan algoritma elgamal.
2. Alat yang digunakan *smart card* SLE4428 dan *smart card reader writer* ACR38.

3. Aplikasi ini dibuat dengan menggunakan bahasa pemrograman *Visual Basic* 6

1.4 Tujuan Penelitian

Berdasarkan penjelasan pada latar belakang maka tujuan dari penelitian ini adalah untuk mengamankan data yang ada di dalam *smart card* dengan menggunakan metode penyandian algoritma elgamal serta menerapkan aplikasi *smart card* pada program aplikasi jual beli.

1.5 Manfaat Penelitian

Penelitian ini dilakukan agar dapat menerapkan aplikasi *smart card* dalam transaksi jual beli serta menerapkan algoritma elgamal dalam keamanan data pada *smart card* .

1.6 Metode Penelitian

Adapun tahap-tahap yang dilakukan dalam penelitian, yaitu :

1. Metode Identifikasi Masalah

   Pada tahap ini peneliti mengidentifikasi permasalahan yang ada serta menganalisanya. Masalah yang diidentifikasi yaitu proses keamanan data dalam transaksi pada aplikasi *smart card.* Data disini berupa string dimana berisikan tentang informasi pemilik kartu. Maka dari itu perlu sebuah penelitian dalam hal kemanan data yang lebih aman dan efisien.

2. Studi Pustaka

   Studi literatur bertujuan untuk menggali informasi mengenai teori-teori dan literatur yang berkaitan dengan permasalahan yang akan diteliti. Sehingga peneliti mencari informasi tentang *smart card* dan kriptografi sebagai pengaman data *smart card*.

3. Perancangan dan desain aplikasi

   Perancangan aplikasi terdiri atas perancangan proses-proses utama dan desain aplikasi. Adapun proses utama tersebut adalah perancangan algoritma ELGamal untuk proses keamanan data. Sedangkan desain aplikasi adalah pembuatan desain menu serta tampilan.

4. Pengujian Metode

   Menguji metode algoritma elgamal pada pengamanan data *smart card.*

5. Pembuatan aplikasi

   Mengimplementasikan rancangan dan desain aplikasi dalam bahasa VB6.

6. Uji coba dan evaluasi

   Uji coba dilakukan untuk mengetahui kinerja dari aplikasi yang telah dibuat, kekurangan yang terjadi diperbaiki dalam lingkup batasan masalah. Evaluasi dilakukan untuk mengetahui apakah sistem yang dibangun sudah mendekati yang diharapkan.

7. Dokumentasi

   Penulisan laporan skripsi merupakan dokumentasi dari keseluruhan pelaksanaan penelitian. Diharapkan dokumentasi penelitian berguna dan bermanfaat untuk penelitian dan pengembangan lebih lanjut.

1.7 Sistematika Penulisan

Penulisan Tugas Akhir ini terbagi atas beberapa bab, yaitu :

BAB I : PENDAHULUAN

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

BAB II : DASAR TEORI

Bab ini berisi tentang teori-teori yang menjadi acuan dalam pembuatan analisa dan pemecahan dari permasalahan yang dibahas, sehingga mempermudah penulis dalam menyelesaikan masalah yang diteliti.

BAB III : DESAIN DAN PERANCANGAN SISTEM

Bab ini menjelaskan tentang tahapan-tahapan yang dilalui dalam penyelesaian tugas akhir, mulai dari perancangan input dan output sistem serta perancangan tampilan aplikasi secara keseluruhan.

BAB IV : HASIL DAN PEMBAHASAN

Bab ini membahas tentang implementasi dari aplikasi yang dibuat secara keseluruhan. Serta melakukan pengujian terhadap aplikasi yang dibuat untuk mengetahui aplikasi tersebut telah dapat menyelesaikan permasalahan yang dihadapi.

BAB V : PENUTUP

Bab ini berisi kesimpulan dari seluruh rangkaian penelitian serta saran tentang kemungkinan pengembangan dari hasil pembahasan masalah.

UNIVERSITAS ISLAM NEGERI MAULANA MALIK IBRAHIM PUSAT PERPUSTAKAAN

BAB II

TINJAUAN PUSTAKA

2.1 Penelitian Terkait

Penelitian oleh Muhammad Iffanto(2009) mengenai *Metode Enkripsi dan Dekripsi dengan Menggunakan Algoritma Elgamal.* Penelitian ini menjelaskan tentang kelebihan dan tata cara metode enkripsi dan dekripsi menggunakan algoritma elgamal. Salah satu kelebihannya yaitu tingkat keamanan algoritma ini didasarkan pada kesulitan pemecahan masalah logaritma diskret.

Penelitian oleh Mohammad Gilang Kautzar(2009) mengenai *Implementasi Sistem Enkripsi Pengirim Pesan Instan Java dengan Algoritma Blowfish.* Penelitian ini menjelaskan tentang pengamanan pesan dalam proses pengiriman pesan dengan menggunakan metode *Blowfish*. Penerapan metode *Blowfish* ini memiliki kelebihan yaitu dalam proses enkripsi ini tidak menurunkan performa perangkat lunak dengan berarti. Hal ini disebabkan pengaruh enkripsi yang tergolong kecil terhadap penggunaan memori dan waktu pemrosesan perangkat lunak.

Penelitian oleh Danang Tri Massandy(2009) mengenai *Algoritma Elgamal dalam Pengamanan Pesan Rahasia.* Penelitian ini menjelaskan tentang pengamanan pesan rahasia dengan menggunakan salah satu algoritma kryptografi, yaitu algoritma ElGamal. Tingkat keamanan

algoritma ini didasarkan atas masalah logaritma diskrit pada grup pergandaan bilangan bulat modulo prima.

Penelitian oleh Agus Hilman Majid(2007) mengenai *Implementasi Algoritma Elgamal sebagai program ADD-IN di Microsoft Word*. Penelitian ini menjelaskan tentang penerapan algoritma ElGamal menjadi *Microsoft Word Add-in.* Penggunaan algoritma ElGamal sebagai sarana pengamanan dokumen, terutama dokumen yang dipertukarkan, bisa menjadi suatu alternatif solusi. Hal ini dikarenakan sifatnya sebagai algoritma kunci publik mempunyai kunci berupa pasangan, yaitu kunci publik (yang bisa disebarkan pada publik) dan kunci rahasia (disimpan oleh pemilik dokumen).

2.2 *Smart Card*

Smart card merupakan kartu yang mempunyai rangkaian terintegrasi di dalamnya dan mampu memproses serta menyimpan data. Pada dasarnya, satu unit *smart card* mampu melayani berbagai aplikasi, tetapi pada kenyataannya, penggunaan *smart card* masih terpisah antara satu aplikasi dengan yang lain. Artinya, satu *smart card* masih digunakan untuk melayani hanya satu aplikasi.

Kartu ini bisa menambah, menghapus, mengubah informasi yang terkandung. Keunggulannya adalah smart card tidak perlu mengakses database di server karena sudah ada sebagian terkandung di kartu.

Sedangkan memory card dipasangi memory silicon tanpa microprocessor.(Mauren, 2011)

Smart card adalah pengembangan dari kartu magnetis, namun berbeda dengan kartu magnetis yang hanya dipakai sebagai tempat penyimpanan data, *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. Hal ini akan mempersulit pemalsuan *smart card*. Selain perbedaan dengan adanya chip, *smart card* memiliki kapasitas memori yang lebih besar dari kartu magnetis.

2.3 Sistem Keamanan

Komunikasi data *elektronis* memerlukan perangkat keamanan yang benar-benar berbeda dengan komunikasi *konvensional*. Keamanan merupakan komponen yang vital dalam komunikasi data *elektronis*. Teknologi kriptografi sangat berperan juga dalam proses komunikasi, yang digunakan untuk melakukan *enkripsi* (pengacakan) data yang ditransaksikan selama perjalanan dari sumber ke tujuan dan juga melakukan *dekripsi* (menyusun kembali) data yang telah teracak tersebut. Berbagai sistem yang telah dikembangkan adalah seperti sistem *private key* dan *public key*. Pada teknologi kriptografi terdapat berbagai macam algoritma kriptografi. Contoh

algoritma kriptografi ini antara lain : DES, IDEA, RC5, RSA, Elgamal, dan ECC (*Elliptic Curve Cryptography*).

2.3 Kriptografi

Kriptografi *(cryptography)* merupakan ilmu dan seni penyimpanan pesan, data, atau informasi secara aman. Kriptografi *(Cryptography)* berasal dari bahasa Yunani yaitu dari kata *Crypto* dan *Graphia* yang berarti penulisan rahasia. Kriptografi adalah suatu ilmu yang mempelajari penulisan secara rahasia. Kriptografi merupakan bagian dari suatu cabang ilmu matematika yang disebut *Cryptology*. Kriptografi bertujuan menjaga kerahasiaan informasi yang terkandung dalam data sehingga informasi tersebut tidak dapat diketahui oleh pihak yang tidak sah.

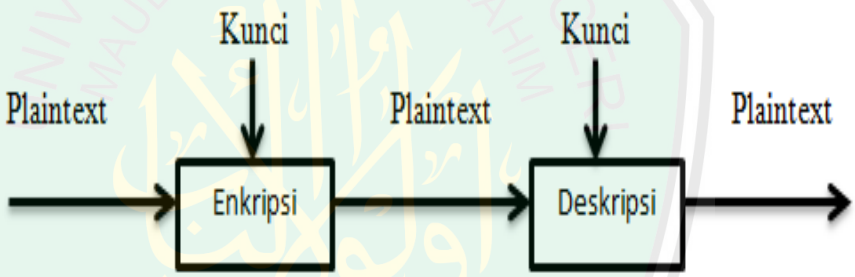
Dalam menjaga kerahasiaan data, kriptografi mentransformasikan data jelas (*plaintext*) ke dalam bentuk data sandi (*ciphertext*) yang tidak dapat dikenali. *Ciphertext* inilah yang kemudian dikirimkan oleh pengirim (*sender*) kepada penerima (*receiver*). Setelah sampai di penerima, *ciphertext* tersebut ditranformasikan kembali ke dalam bentuk *plaintext* agar dapat dikenali.

Proses tranformasi dari *plaintext* menjadi *ciphertext* disebut proses *Encipherment* atau enkripsi (*encryption*), sedangkan proses mentransformasikan kembali *ciphertext* menjadi *plaintext* disebut proses dekripsi (*decryption*).

Untuk mengenkripsi dan mendekripsi data. *Kriptografi* menggunakan suatu algoritma (*cipher*) dan kunci (*key*). *Cipher* adalah fungsi matematika

yang digunakan untuk mengenkripsi dan mendekripsi. Sedangkan kunci merupakan sederetan bit yang diperlukan untuk mengenkripsi dan mendekripsi data.

Suatu pesan yang tidak disandikan disebut sebagai *plaintext* ataupun dapat disebut juga sebagai *cleartext*. Proses yang dilakukan untuk mengubah *plaintext* ke dalam *ciphertext* disebut *encryption* atau e*ncipherment*. Sedangkan proses untuk mengubah *ciphertext* kembali ke *plaintext* disebut *decryption* atau *decipherment*. Secara sederhana istilah-istilah di atas dapat digambarkan sebagai berikut :



Gambar 2.1 Proses Enkripsi dan Dekripsi Sederhana

Dari gambar diatas dapat kita lihat bahwa untuk mengirimkan pesan antara si pengirim dan si penerima menggunakan satu kunci atau kunci yang di gunkan sama. Maksudnya adalah kunci yang digunakan untuk mengenkripsi pesan dan kunci yang digunakan untuk mengdekripsikan pesan sama.

Cryptography adalah suatu ilmu ataupun seni mengamankan pesan, dan dilakukan oleh cryptographer. Sedang, *cryptanalysis* adalah suatu ilmu

dan seni membuka (breaking) ciphertext dan orang yang melakukannya disebut cryptanalyst.

Cryptographic system atau *cryptosystem* adalah suatu fasilitas untuk mengkonversikan *plaintext* ke *ciphertext* dan sebaliknya. Dalam sistem ini, seperangkat parameter yang menentukan transformasi pencipheran tertentu disebut suatu set kunci. Proses *enkripsi* dan *dekripsi* diatur oleh satu atau beberapa kunci *kriptografi*.

Secara umum operasi *enkripsi* dan *dekripsi* dapat diterangkan secara matematis sebagai berikut :

EK (M) = C (*Proses Enkripsi*)

DK (C) = M (*Proses Dekripsi*)

Pada saat proses *enkripsi* dilakukan proses penyandian pesan M dengan suatu kunci K lalu dihasilkan pesan C. Sedangkan pada proses dekripsi, pesan C tersebut diuraikan dengan menggunakan kunci K sehingga dihasilkan pesan M yang sama seperti pesan sebelumnya.

Dengan demikian keamanan suatu pesan tergantung pada kunci ataupun kunci-kunci yang digunakan, dan tidak tergantung pada algoritma yang digunakan. Sehingga algoritma-algoritma yang digunakan tersebut dapat dipublikasikan dan dianalisis.

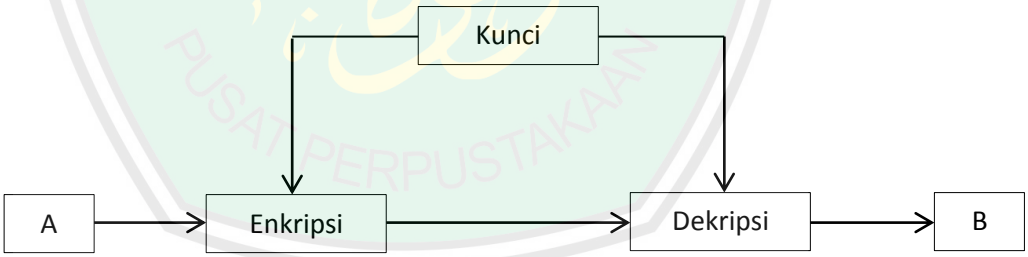
2.5 Algoritma Kriptografi

Algoritma kriptografi atau sering disebut dengan *cipher* adalah suatu fungsi matematis yang digunakan untuk melakukan *enkripsi* dan *dekripsi*.

Ada dua macam algoritma kriptografi, yaitu algoritma simetris (*symmetric algorithms*) dan algoritma asimetris (*asymmetric algorithms*).

2.5.1 Algoritma Simetris

Algoritma simetris adalah algoritma kriptografi yang menggunakan kunci enkripsi yang sama dengan kunci dekripsinya. Algoritma ini mengharuskan pengirim dan penerima menyetujui suatu kunci tertentu sebelum mereka saling berkomunikasi. Keamanan algoritma simetris tergantung pada kunci, membocorkan kunci berarti bahwa orang lain dapat mengenkripsi dan mendekripsi pesan. Agar komunikasi tetap aman, kunci harus tetap dirahasiakan. Algoritma simetris sering juga disebut dengan algoritma kunci rahasia, algoritma kunci tunggal, atau algoritma satu kunci. Secara sederhana ditunjukkan pada Gambar 2.2.



Gambar 2.2 Proses Algoritma Simetris

2.5.2 Algoritma Asimetris

Algoritma asimetris, sering juga disebut dengan algoritma kunci publik, menggunakan dua jenis kunci, yaitu kunci publik (public key) dan

kunci rahasia (secret key). Kunci publik merupakan kunci yang digunakan untuk mengenkripsi pesan. Sedangkan kunci rahasia digunakan untuk mendekripsi pesan. Kunci publik bersifat umum, artinya kunci ini tidak dirahasiakan sehingga dapat dilihat oleh siapa saja. Sedangkan kunci rahasia adalah kunci yang dirahasiakan dan hanya orang-orang tertentu saja yang boleh mengetahuinya. Keuntungan utama dari algoritma ini adalah memberikan jaminan keamanan kepada siapa saja yang melakukan pertukaran informasi meskipun di antara mereka tidak ada kesepakatan mengenai keamanan pesan terlebih dahulu maupun saling tidak mengenal satu sama lainnya. (Widyarto, 2011)

Kunci publik bersifat umum, artinya kunci ini tidak dirahasiakan sehingga dapat dilihat oleh siapa saja. Sedangkan kunci rahasia adalah kunci yang dirahasiakan dan hanya orang-orang tertentu saja yang boleh mengetahuinya. Keuntungan utama dari algoritma ini adalah memberikan jaminan keamanan kepada siapa saja yang melakukan pertukaran informasi meskipun di antara mereka tidak ada kesepakatan mengenai keamanan pesan terlebih dahulu maupun saling tidak mengenal satu sama lainnya. Secara sederhana dapat digambarkan seperti pada Gambar 2.2.

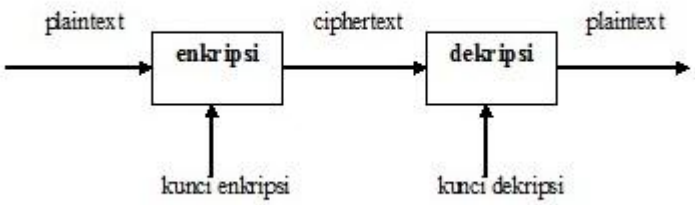
Gambar 2.3 Proses Algoritma Asimetris

2.6 Algoritma Elgamal

Algoritma Elgamal juga adalah algoritma kriptografi kunci-publik. Algoritma ini pada mulanya digunakan untuk *digital signature*, namun kemudian dimodifikasi sehingga juga bisa digunakan untuk enkripsi dan dekripsi.

Algoritma ElGamal merupakan algoritma dalam kriptografi yang termasuk dalam kategori algoritma asimetris. Keamanan algoritma ElGamal terletak pada kesulitan penghitungan logaritma diskret pada bilangan modulo prima yang besar sehingga upaya untuk menyelesaikan masalah logaritma ini menjadi sangat sukar.

Algoritma ElGamal mempunyai kunci publik berupa tiga pasang bilangan dan kunci rahasia berupa satu bilangan. Algoritma ElGamal terdiri dari tiga proses, yaitu proses pembentukan kunci, proses enkripsi dan proses *dekripsi*. Algoritma ini merupakan *cipher* blok, yaitu melakukan proses *enkripsi* pada blok-blok *plainteks* dan menghasilkan blok-blok *cipherteks* yang kemudian dilakukan proses dekripsi dan hasilnya digabungkan. Secara sederhana dijelaskan pada Gambar 2.4.



Gambar 2.4 Proses Algoritma Elgamal

2.6.1 Proses Pembentukan Kunci

Input : Bilangan prima aman p > 255

Output : Kunci publik (p, α, β) dan kunci rahasia a

Proses :

1. Pilih sembarang bilangan prima p>255 (p dapat dipublikasikan).
2. Pilih dua buah bilangan acak, g dan x, dengan syarat g < p dan $0 \leq x \leq p-2$.
3. Hitung $y = g^x \bmod p$.

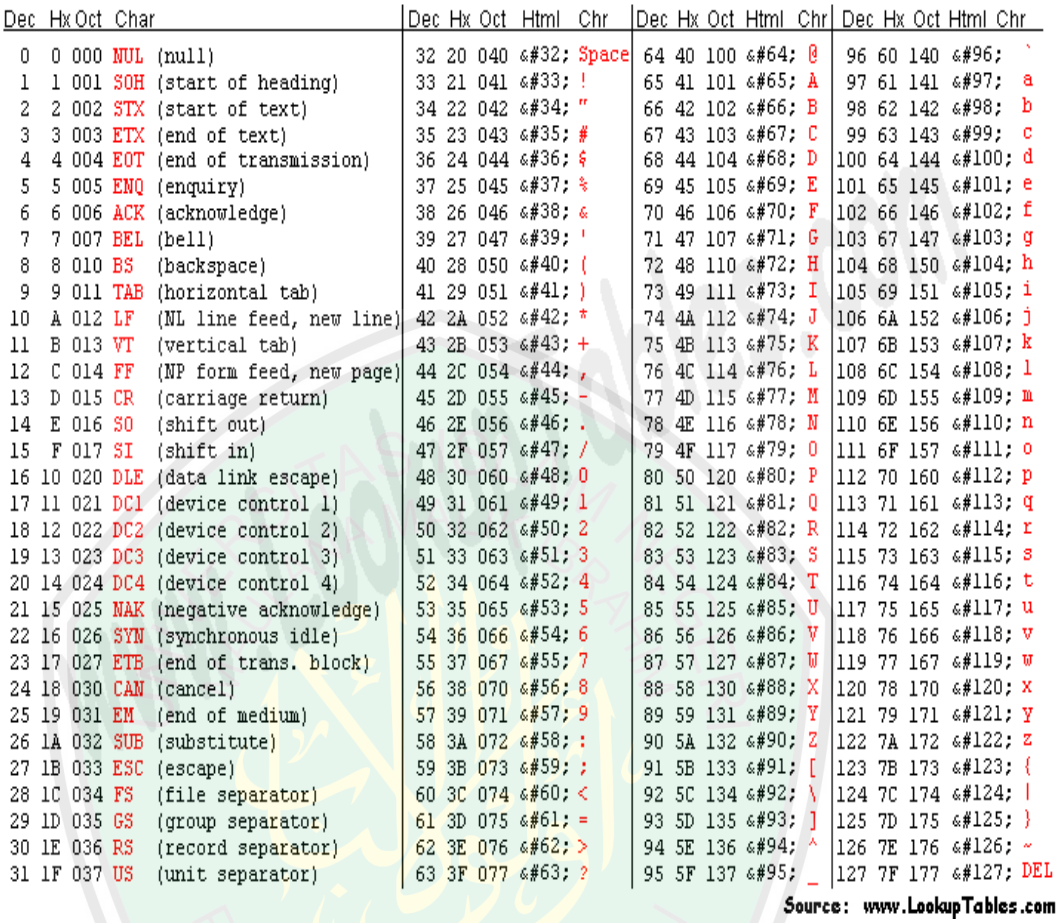
   y adalah bagian dari kunci publik, sehingga kunci publik algoritma ElGamal berupa pasangan 3 bilangan, yaitu (y,g,p). Sedangkan kunci rahasianya adalah bilangan x tersebut.

Proses pembangkitan kunci dilakukan di sisi penerima pesan, lalu setelah kunci publik dibangkitkan, kunci publik dikirimkan kepada pengirim pesan untuk selanjutnya dilakukan proses enkripsi.

2.6.2 Proses Enkripsi

Pada proses ini pesan dienkripsi menggunakan kunci publik (y,g,p) dan sembarang bilangan acak rahasia k anggota {0,1,…, p - 2}. Misalkan m adalah pesan yang akan dikirim. Selanjutnya, m diubah ke dalam blok-blok karakter dan setiap karakter dikonversikan ke dalam kode ASCII, sehingga diperoleh *plaintext* $m_1, m_2, \ldots, m_n$ dengan m_i anggota {1, 2,…, p - 1} , i =1, 2,…, n .

Berikut ini merupakan tabel ASCII yang dijelaskan pada Gambar 2.5.



Dec	Hx	Oct	Char	Dec	Hx	Oct	Html	Chr	Dec	Hx	Oct	Html	Chr	Dec	Hx	Oct	Html	Chr
0	0	000	NUL (null)	32	20	040		Space	64	40	100	@	@	96	60	140	`	`
1	1	001	SOH (start of heading)	33	21	041	!	!	65	41	101	A	A	97	61	141	a	a
2	2	002	STX (start of text)	34	22	042	"	"	66	42	102	B	B	98	62	142	b	b
3	3	003	ETX (end of text)	35	23	043	#	#	67	43	103	C	C	99	63	143	c	c
4	4	004	EOT (end of transmission)	36	24	044	$	$	68	44	104	D	D	100	64	144	d	d
5	5	005	ENQ (enquiry)	37	25	045	%	%	69	45	105	E	E	101	65	145	e	e
6	6	006	ACK (acknowledge)	38	26	046	&	&	70	46	106	F	F	102	66	146	f	f
7	7	007	BEL (bell)	39	27	047	'	'	71	47	107	G	G	103	67	147	g	g
8	8	010	BS (backspace)	40	28	050	(	(	72	48	110	H	H	104	68	150	h	h
9	9	011	TAB (horizontal tab)	41	29	051	)	)	73	49	111	I	I	105	69	151	i	i
10	A	012	LF (NL line feed, new line)	42	2A	052	*	*	74	4A	112	J	J	106	6A	152	j	j
11	B	013	VT (vertical tab)	43	2B	053	+	+	75	4B	113	K	K	107	6B	153	k	k
12	C	014	FF (NP form feed, new page)	44	2C	054	,	,	76	4C	114	L	L	108	6C	154	l	l
13	D	015	CR (carriage return)	45	2D	055	-	-	77	4D	115	M	M	109	6D	155	m	m
14	E	016	SO (shift out)	46	2E	056	.	.	78	4E	116	N	N	110	6E	156	n	n
15	F	017	SI (shift in)	47	2F	057	/	/	79	4F	117	O	O	111	6F	157	o	o
16	10	020	DLE (data link escape)	48	30	060	0	0	80	50	120	P	P	112	70	160	p	p
17	11	021	DC1 (device control 1)	49	31	061	1	1	81	51	121	Q	Q	113	71	161	q	q
18	12	022	DC2 (device control 2)	50	32	062	2	2	82	52	122	R	R	114	72	162	r	r
19	13	023	DC3 (device control 3)	51	33	063	3	3	83	53	123	S	S	115	73	163	s	s
20	14	024	DC4 (device control 4)	52	34	064	4	4	84	54	124	T	T	116	74	164	t	t
21	15	025	NAK (negative acknowledge)	53	35	065	5	5	85	55	125	U	U	117	75	165	u	u
22	16	026	SYN (synchronous idle)	54	36	066	6	6	86	56	126	V	V	118	76	166	v	v
23	17	027	ETB (end of trans. block)	55	37	067	7	7	87	57	127	W	W	119	77	167	w	w
24	18	030	CAN (cancel)	56	38	070	8	8	88	58	130	X	X	120	78	170	x	x
25	19	031	EM (end of medium)	57	39	071	9	9	89	59	131	Y	Y	121	79	171	y	y
26	1A	032	SUB (substitute)	58	3A	072	:	:	90	5A	132	Z	Z	122	7A	172	z	z
27	1B	033	ESC (escape)	59	3B	073	;	;	91	5B	133	[	[	123	7B	173	{	{
28	1C	034	FS (file separator)	60	3C	074	<	<	92	5C	134	\	\	124	7C	174			|
29	1D	035	GS (group separator)	61	3D	075	=	=	93	5D	135	]	]	125	7D	175	}	}
30	1E	036	RS (record separator)	62	3E	076	>	>	94	5E	136	^	^	126	7E	176	~	~
31	1F	037	US (unit separator)	63	3F	077	?	?	95	5F	137	_	_	127	7F	177	&#127;	DEL

Source: www.LookupTables.com

Gambar 2.5 Standart ASCII

Input : Data string (id pelanggan , saldo pelanggan) yang akan dienkripsi dan kunci publik (p, α, β).

Output : *Ciphertext* (a_i,b_i), i = 1, 2, …, n.

Proses :

1. Susun *plaintext* menjadi blok-blok m_1, m_2, ...m_n dengan setiap blok adalah satu karakter pesan.

2. Kovnersikan masing-masing karakter ke dalam kode ASCII maka diperoleh plainteks sebanyak n bilangan, yaitu m_1, m_2, ...m_n
3. Untuk i dari 1 sampai n kerjakan :
    - Pilih sembarang bilangan acak rahasia $k_i \in \{0,1, ..., p-2\}$
    - Hitung $a_i = g^{ki} \bmod p$
    - Hitung $b_i = y^{ki} m_i \bmod p$
4. Hasil *chiphertext* yaitu (a_i, b_i) , i=1, 2,... ,n. Jadi ukuran *ciphertext* dua kali ukuran plainteksna.

Skenario selanjutnya adalah pengirim mengirimkan pesan kepada penerima.

2.6.2 Proses Dekripsi

Setelah menerima *ciphertext* (a,b) , proses selanjutnya adalah mendekripsi *ciphertext* menggunakan kunci publik p dan kunci rahasia x. Dapat ditunjukkan bahwa *plaintext* m dapat diperoleh dari *ciphertext* menggunakan kunci rahasia x.

Input : *Chipertext* (a_i,b_i), i = 1, 2,…, n kunci publik p dan kunci rahasia a.

Output : Data asli

Proses :

1. *Ciphertext* (a_i,b_i), i =1, 2, ..., n, kunci publik p dan kunci rahasia x.

2. Untuk *i* dari 1 sampai *n* hitung $m = b_i.a_i^{p-1-x} \bmod p$
3. Nilai m_i yang didapat dalam bentuk ASCII kemudian diubah menjadi *plaintext*.
4. Susun *plaintex*t dengan urutan $m_1, m_2, m_3, \ldots, m_n$.

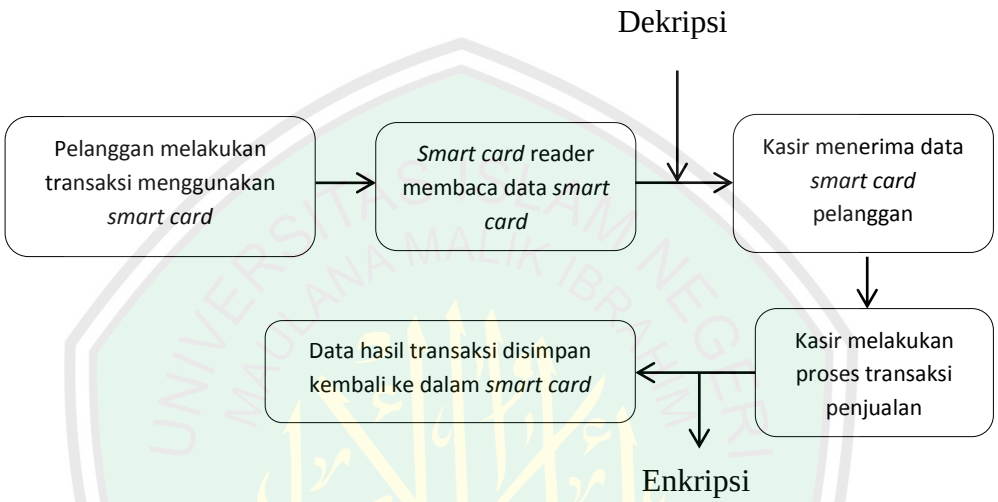
Hasil yang didapat dari proses dekripsi berupa pesan asli (*plaintext*).

BAB III

METODE DAN PERANCANGAN SISTEM

3.1 Blog Diagram

Blog diagram tentang proses transaksi jual beli yang dilakukan oleh pelanggan dijelaskan pada gambar 3.1.



Gambar 3.1 Blog Diagram

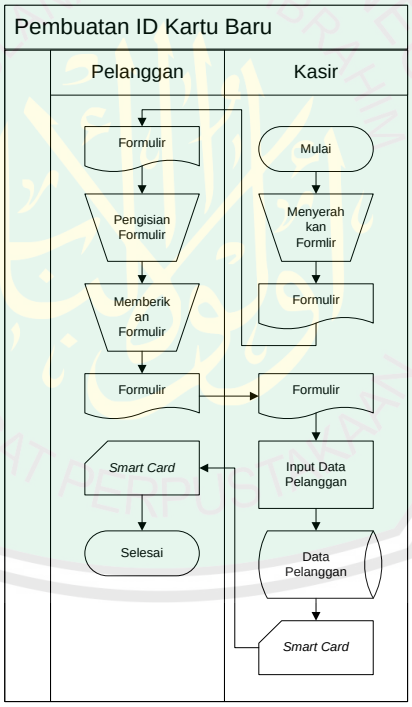
Pada Gambar 3.1 dijelaskan bahwa pelanggan melakukan pembayaran menggunakan *smart card*. Data dari *smart card* tersebut dibaca oleh aplikasi dengan melakukan proses dekripsi data *smart card*. Setelah data didekripsi kemudian dilakukan proses transaksi jual beli. Hasil transaksi dimasukkan kembali ke dalam *smart card* dengan melakukan proses enkripsi.

3.2 Diagram Alir Sistem

Diagram alir adalah diagram yang menggambarkan bagaimana jalankan program mulai dari awal hingga akhir. Pada tahap ini dijelaskan tentang proses dari jual beli menggunakan aplikasi *smart card.*

3.2.1 Diagram Alir Pembuatan ID Pelanggan Baru

Id pelanggan merupakan id yang digunakan di dalam proses identifikasi *smart card*. Pada tahap proses pembuatan id pelanggan baru, petugas memberikan formulir pendaftaran kepada pelanggan selanjutnya pelanggan mengisi formulir dan diberikan kepada petugas. Petugas memasukkan data formulir ke dalam *database* dan *memory smart card*. Kemudian *smart card* diberikan kepada pelanggan. Pada tahap pembuatan id pelanggan baru ditunjukkan pada Gambar 3.2.

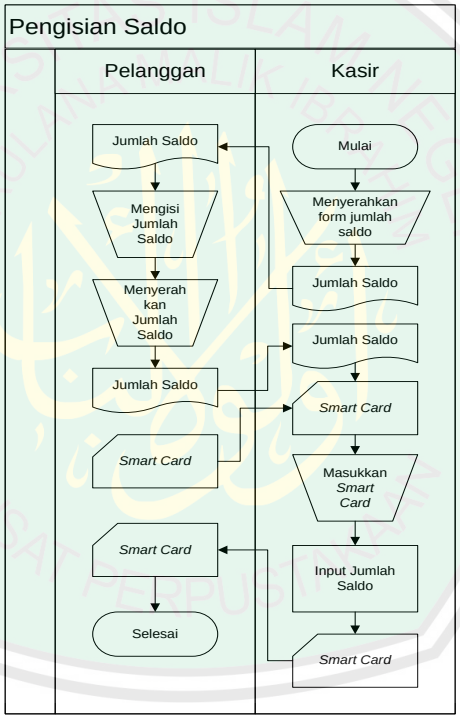


Gambar 3.2 Diagram Alir Pembuatan ID Pelanggan Baru

3.2.2 Diagram Alir Pengisian Saldo

Saldo merupakan jumlah nominal yang harus dimilik oleh pelanggan di dalam *memory smart card*. Saldo berfungsi sebagai pengganti uang dalam

proses transaksi jual beli. Pada proses pengisian saldo pada *smart card* petugas memberikan form pengisian saldo kepada pelanggan selanjutnya pelanggan mengisi jumlah saldo yang ingin diisi kemudian form tersebut diberikan kembali bersamaan dengan memberikan *smart card* kepada petugas. Petugas memasukkan julah pulsa ke dalam *smart card.* Saldo *smart card* telah terisi kemudian *smart card* dikembalikan kepada pelanggan. Pada tahap proses pengisian saldo ditunjukkan pada Gambar 3.3.

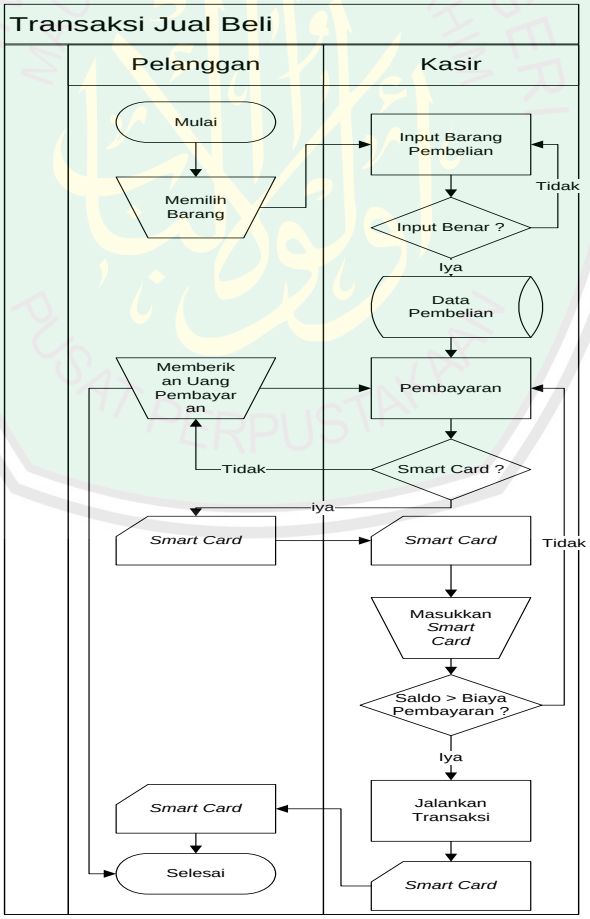


Gambar 3.3 Diagram Alir Proses Pengisian Saldo

3.2.3 Diagram Alir Transaksi Jual Beli

Pada proses transaksi jual beli, pelanggan memilih barang yang akan dibeli kemudian barang tersebut dibawa ke petugas kasir. Pada proses transaksi jual beli, pelanggan memilih barang yang akan dibeli kemudian

barang tersebut dibawa ke petugas kasir. Pelanggan memilih cara pembayaran *cash* atau menggunakan *smart card.* Untuk cara pembayaran menggunakan *smart card* pelanggan harus menyerahkan *smart card* kepada petugas kasir kemudian di cek saldo yang terdapat di dalam *smart card*. jika saldo melebihi dari jumlah biaya yang harus dibayar maka proses pembayaran akan berlanjut dengan cara mengurangi sisa jumlah saldo dengan biaya pembayaran. Jika tidak memenuhi maka akan dilakukan biaya pembayaran secara manual. Selanjutnya *smart card* dikembalikan kepada pelanggan. Pada tahap proses transaksi jual beli ditunjukkan pada Gambar 3.4.



Gambar 3.4 Diagram Alir Proses Transaksi Jual Beli

3.3 Analisis *Input*

Pada aplikasi *smart card* tipe data yang digunakan untuk proses *input* berupa tipe data string yang dimasukkan ke dalam *smart card* dengan bantuan *card reader and writer* ACR38. Sebelum data dimasukkan ke dalam *smart card*, data akan dienkripsi sehingga data yang masuk ke dalam *smart card* berupa data *ciphertext*. Selanjutnya untuk proses membaca, data *ciphertext* didekripsi, sehingga data tersebut dapat terbaca kembali (*plaintext*).

3.4 Analisis *Output*

Output merupakan hasil pengolahan data-data yang telah dimasukkan, sehingga menghasilkan keluaran yang sesuai dengan apa yang direncanakan. *Output* yang dihasilkan oleh sistem aplikasi ini terbagi menjadi dua *output* , merupakan *output* yang dihasilkan saat memasukkan data pada *smart card* dan saat membaca data pada *smart card*. *Output* yang dihasilkan pada proses *input* data berupa teks yang telah terenkripsi (*ciphertext*) yang merupakan hasil proses membaca data pada *smart card* berupa data *plaintext*.

3.5 Perancangan Data

Perancangan data dilakukan untuk mendesain dan merencanakan data apa saja yang akan digunakan dalam proses enkripsi dan dekripsi pada *smart card* dengan masing-masing tipe data yang digunakan.

3.5.1 Perancangan Data *Input*

Data *input* merupakan data-data yang dimasukkan untuk diproses. Pada tabel 3.1 merupakan perancangan data *input* yang nantinya akan digunakan di dalam proses enkripsi pada aplikasi *smart card* ini.

Tabel 3.1 Tabel Perncangan Data *Input*

No	Nama Data	Type Data	Keterangan
1.	Isi Data kartu (id pelanggan dan saldo)	String	Data yang dimasukkan ke dalam kartu dan dilakukan proses enkripsi
2.	Text Kunci	String	Kunci rahasia yang dimasukkan dan digunakan untuk perhitungan enkripsi dan dekripsi.
3.	Data Kartu (*ciphertext*)	String	Data kartu yang telah dienkripsi (*ciphertext*) dilakukan proses dekripsi sehingga data kartu dapat dibaca kembali .

3.5.2 Perancangan Data *Output*

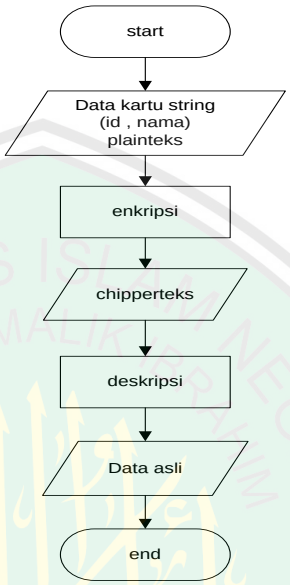
Data *output* merupakan data jadi yang telah selesai mengalami proses pengolahan yakni proses enkripsi. Pada tabel 3.2 ini merupakan perancangan data *output* yang telah dienkripsi.

Tabel 3.2 tabel Perancangan Data *Output*

No	Nama Data	Type Data	Keterangan
1.	Data kartu terenkripsi (*ciphertext*)	String	Pesan yang telah dimasukkan ke dalam kartu dan dilakukan proses enkripsi sehingga menghasilkan data yang telah terenkripsi.
2.	Pembacaan data kartu (*plaintext*)	String	Data yang telah dienkripsi dilakukan proses dekripsi sehingga dapat membaca isi dari data *smart card*.

3.6 Flowchart Sistem

Pada flowchart sistem ini menjelaskan tentang proses pada aplikasi *smart card* dapat dilihat pada Gambar 3.5.



Gambar 3.5 Flowchart sistem

Pada aplikasi *smart card* terdapat beberapa proses, pertama pengguna harus memiliki *smart card* sehingga *smart card* dapat diisi data. Sebelum mengisi data, *user* telebih dahulu harus melakukan koneksi dengan *smart card reader writer*, digunakan alat ACR38 untuk melakukan proses menulis dan membaca *smart card*. Kemudian *user* melakukan *input* data (*plaintext*), sebelum data *plaintext* masuk ke dalam *smart card* terlebih dahulu data *plaintext* akan dienkripsi, sehingga dihasilkan data *ciphertext* yang nantinya akan dimasukkan ke dalam *smart card*. Setelah data *ciphertext* masuk ke dalam *smart card* dilakukan proses membaca kartu. Ketika proses membaca data *ciphertext*, dilakukan proses dekripsi pada data di dalam *smart card*

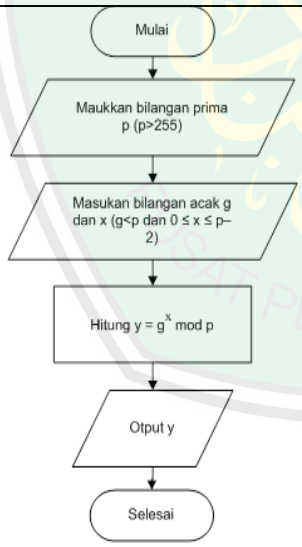
sehingga *user* dapat membaca kembali data asli (*plaintext*) yang telah dimasukkan ke dalam kartu.

3.6 Flowchart Algoritma

Untuk mempermudah proses perancangan sistem implementasi algoritma ElGamal, perlu didefinisikan langkah-langkah yang dibuat ke dalam flowchart. Ada beberapa tahapan dalam proses algoritma elgamal ini :

3.6.1 Proses Pembentukan Kunci

Pada proses pembentukan kunci algoritma elgamal terdapat beberapa tahap yang harus dilakukan. Proses pembentukan kunci ini dapat dijelaskan pada Gambar 3.6.

Flowchart	Contoh Manual
	Memulai proses
	P = 257
	g = 11 | x = 13
	$y = 11^{13} \bmod 257$
	22
	Pembentukan kunci y selesai

Gambar 3.6 Flowchart Pembentukan Kunci

Dimisalkan dilakukan pengacakan terhadap nilai kunci p, g dan x sehingga menghasilkan nilai p = 257 , g = 11 dan x = 13. Selanjutnya akan diproses perhitungan pada nilai kunci y dengan menggunakan rumus :

$y = g^x \bmod p$

$y = 11^{13} \bmod 257$

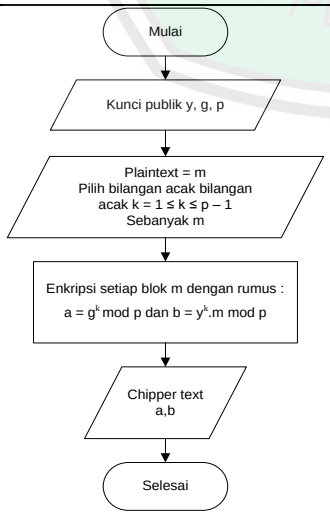
Sehingga diketahui y = 22

Dari perhitungan diatas dihasilkan kunci y = 22 . Dari kunci p, g, x dan y akan dikelompokkan menjadi dua kelompok kunci yaitu kelompok kuci *public* dan kunci *private* dimana kunci *public* terdiri dari y, g dan p sedangkan kunci *private* terdiri dari x dan p. Sehingga dihasilkan :

Public (y = 22, g = 11 dan p = 257).
Private (x = 13 dan p = 257).

3.6.2 Proses Enkripsi

Pada proses enkripsi algoritma elgamal terdapat beberapa tahap yang harus dilakukan. Proses enkripsi ini dapat dijelaskan pada Gambar 3.7.

Flowchart	Contoh Manual
	Menentukan kunci yang akan digunakan
	Y = 22 | P = 257 | g = 11
	M=2 | ASCII = 50 | k = 27
	$a = 11^{27} \bmod 257 = 184$ $b = 22^{27}.50 \bmod 257 = 140$
	184,140
	Proses enkripsi seslesai

Gambar 3.7 Flowchart Proses Enkripsi

Setelah dilakukan proses perhitungan untuk membentuk kunci y dengan menggunakan kunci p, g dan x selanjutnya dilakukan proses enkripsi. Sebelum dilakukan proses enkripsi terlebih dahulu dilakukan proses penentuan nilai k dari masing-masing *plaintext* yang dimasukan. Sebelum menentukan nilai k dari *plainteks*, data *plainteks* diubah ke dalam kode ASCII. Nilai k ditentukan dengan syarat $0 < k < p - 1$. Misalkan terdapat data yang akan dimasukkan ke dalam *smart card* m = 1234. Proses selanjutnya yaitu menentukan nilai k :

Tabel 3.3 Proses Pembentukan Kunci k

Char	**ASCII**	**Kunci k**
1	49	54
2	50	55
3	51	56
4	52	57

Kemudian dihitung nilai dari a_1 dan b_1 , dengan menggunakan kunci publik yang telah ditentukan sebelumnya dengan rumus :

$a = g^k \bmod p$ dan

$b = y^k.m \bmod p$

$a_1 = g^x \bmod p$
$= 11^{58} \bmod 257$
$= 30$

$b_1 = y^k.m \bmod p$
$= 22^{58}.49 \bmod 257$
$= 31$

$a_2 = 11^{27} \bmod 257$ $\quad$ $b_2 = 22^{27}.50 \bmod 257$

$= 184$ $\quad$ $= 159$

$a_3 = 11^{46} \bmod 257$ $\quad$ $b_3 = 22^{46}.51 \bmod 257$

$= 15$ $\quad$ $= 127$

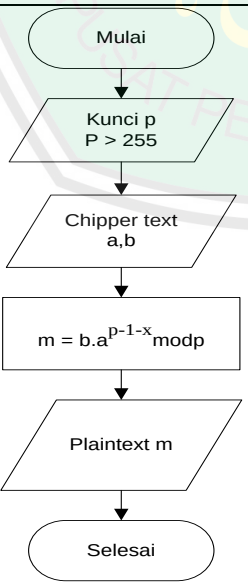
$a_4 = 11^{57} \bmod 257$ $\quad$ $b_4 = 22^{57}.52 \bmod 257$

$= 213$ $\quad$ $= 207$

Setelah melakukan perhitungan di atas dihasilkan nilai *ciphertext* (a,b) dari perhitungan *plaintext* yang dimasukkan yaitu m_1 = 30,31 m_2 = 184,159 m_3 = 15,257 m_4 = 213,207. Nilai *ciphertext* inilah yang akan dimasukkan ke dalam *smart card*.

3.6.2 Proses Dekripsi

Pada proses dekripsi algoritma elgamal terdapat beberapa tahap yang harus dilakukan. Proses dekripsi ini dapat dijelaskan pada Gambar 3.8.

Flowhart	Contoh Manual
	Memulai Proses dekripsi
	P = 257 | x = 13
	184,159
	M = $159.184^{257-1-13}$
	M = 2
	Proses dekripsi selesai

Gambar 3.8 Flowchart Dekripsi

Dalam proses dekripsi diambil data *chipertext* kartu yang telah dimasukkan pada proses enkripsi. Data *ciphertext* (a,b) tersebut dihitung kembali di dalam proses dekripsi dan dihasilkan data awal (*plaintext*). Sehingga *user* dapat membaca kembali data yang telah masuk (*plaintext*) diawal proses enkripsi.

Dari data *ciphertext* , kita akan menggunakan rumus :

$$m = b.a^{p-1-x} \bmod p$$

$m_1 = 31.30^{257-1-13} \bmod p$

$= 49$

$m_2 = 159.184^{257-1-13} \bmod p$

$= 50$

$m_3 = 257.15^{257-1-13} \bmod p$

$= 51$

$m_4 = 207.213^{257-1-13} \bmod p$

$= 52$

ASCII

Tabel 3.4 Proses Pengembalian ASCII to Char

Dec	**Char**
49	1
50	2
51	3
52	4

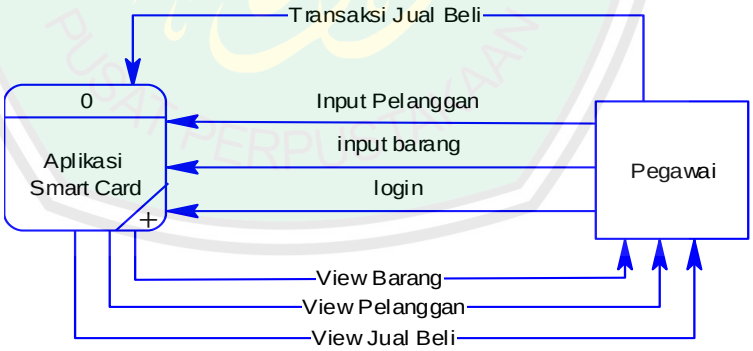
Sesuai perhitungan di atas maka dihasilkan data awal (*plaintext*) dari hasil *ciphertext* kartu m = 1234, sehingga *user* dapat membaca kembali data yang telah dimasukkan ke dalam *smart card*.

3.7 Data Flow Diagram

Data Flow Diagram (DFD) merupakan representasi grafik dari sebuah sistem. DFD menggambarkan komponen-komponen sebuah sistem, aliran-aliran data dimana komponen-komponen tersebut, asal, tujuan, dan penyimpanan dari data tersebut. Secara garis besar DFD menggambarkan alur sistem dan memecahkan menjadi beberapa bagian yang lebih terperinci. DFD dapat digambarkan dengan *Context Diagram* dan *level* n, dimana *level* n berasal dari *compose Context Diagram*. Pada sistem ini terdapat beberapa level dari DFD, seperti yang dijelaskan berikut ini.

3.7.1. Context Diagram

Pada proses *context diagram* ditunjukkan pada Gambar 3.9 ini dijelaskan bahwa satu aplikasi yang diakses oleh pegawai.

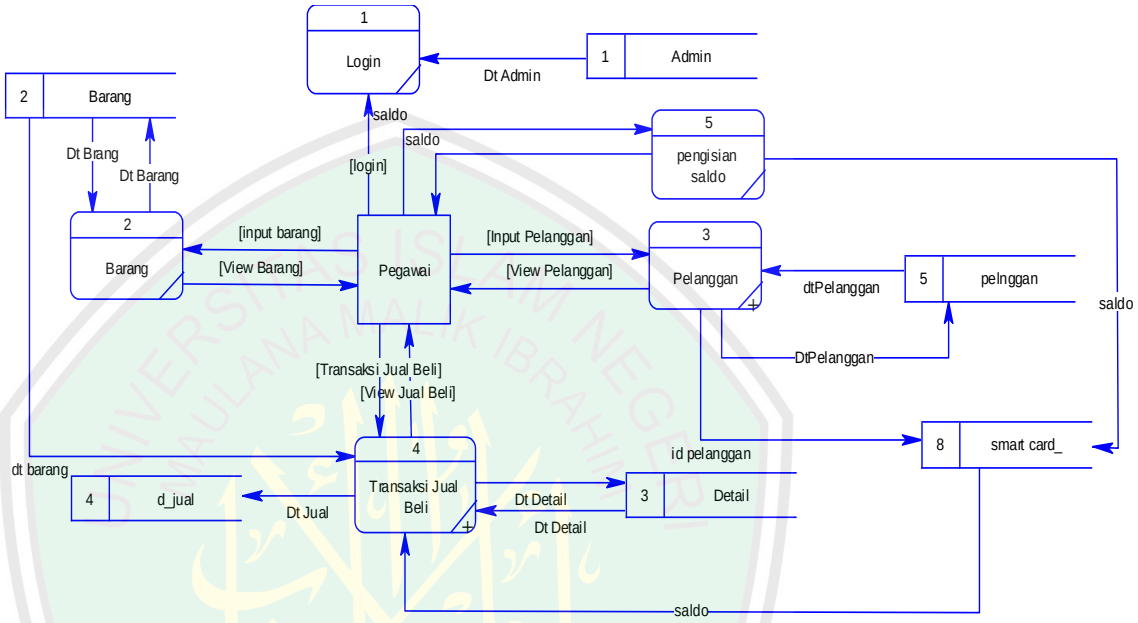


Gambar 3.9 Context Diagran

Pegawai dapat melakukan beberapa proses kegiatan, yakni proses *input* barang, *input* pelanggan, transaksi jual beli, *input* saldo, laporan barang, laporan jual beli dan terahir laporan pelanggan.

3.7.2. DFD level 1

Pada proses dfd level 1 dapat dilihat pada Gambar 3.10 terdapat beberapa proses diantarnya proses *input*, *view* dan transaksi jual beli.

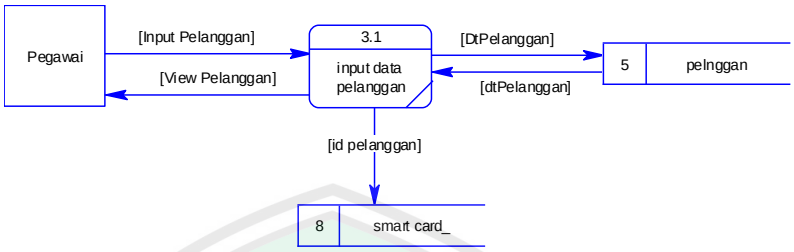


Gambar 3.10 Dfd Level 1

Pada proses dfd level 1 Dalam proses *input* ada beberapa tabel yang akan menampung data yang dimasukkan. Yang pertama untuk menampung data barang telah disediakan tabel barang dan dari tabel ini juga dilakukan proses *view* barang. Yang kedua untuk menampung data pelanggan telah disediakan tabel pelanggan dan dari tabel ini juga dilakukan proses *view* pelanggan. Yang ketiga yaitu tabel detail dan d_jual yang berguna untuk menampung data penjualan dan juga dapat dilaksanakan proses *view* dan laporan penjualan.

3.7.3. DFD Level 2 *Input* Data Pelanggan

Pada proses DFD Level 2 dapat dilihat pada Gambar 3.11 terjadi proses *input* data pelanggan.

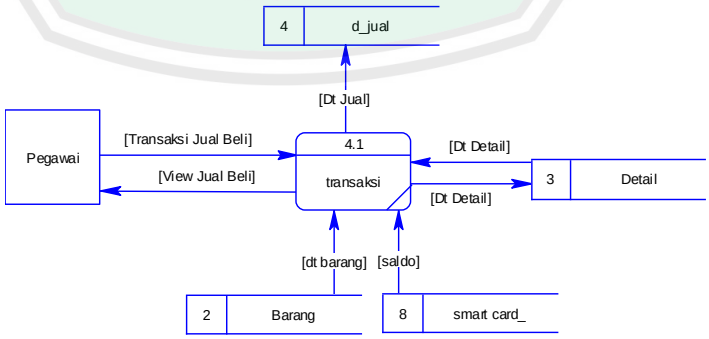


Gambar 3.11 DFD Level 2 *input* data pelanggan

Data pelanggan dimasukkan ke dalam *database* pelanggan yang terdiri dari data nama, id pelanggan, alamat dan nomor telpon. Dari data pelanggan diambil satu data yaitu data id pelanggan dan dimasukkan ke dalam *smart card.*

3.7.4. DFD Level 2 Transaksi Jual Beli

Pada proses dfd level 2 dapat dilihat pada Gambar 3.12 terjadi proses transaksi jual beli



Gambar 3.12 DFD Level 2 transaksi jual beli

Pada transaksi ini terjadi bergai macam proses *input* maupun *output*. Pada proses *input* terjadi di dalam tabel d_jual dan detail. Sedangkan dalam

proses *output* terjadi pada tabel barang, detail dan *smart card.* Pada *smart card* data yang diambil adalah data id pelanggan dan saldo pelanggan.

3.8 Desain Interface

Tampilan merupakan salah satu hal yang terpenting dalam pembuatan aplikasi. Dalam mendesain sebuah tampilan haruslah dibuat secara rapi dan jelas, hal tersebut dimaksudkan agar setiap pengguna dapat menggunakan aplikasi tersebut secara mudah tanpa harus mempelajarinya secara terperinci. Oleh sebab itu, pada aplikasi *Smart card* ini, peneliti merancang beberapa *form* yang dimaksudkan dapat mempermudah pengguna dalam menjalankan aplikasi tersebut. Berikut rancangan beberapa *form* yang nantinya akan diterapkan dalam pembuatan aplikasi.

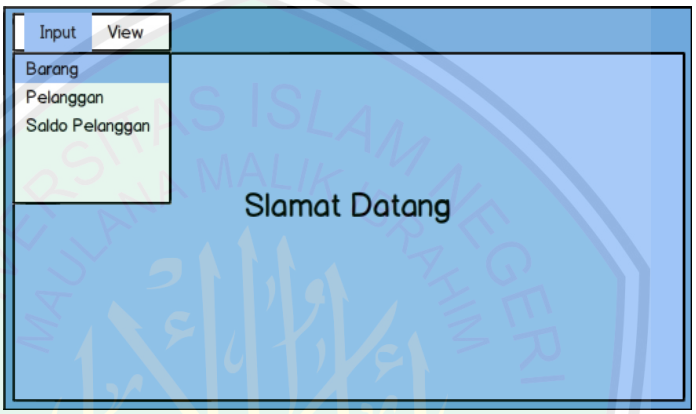
1. Form Utama

2. Form utama, dijelaskan *user* melakukan proses *login*. *User* disini berperan sebagai kasir dan dilanjutkan dengan proses tansaksi jual beli. Dapat dilihat pada Gambar 3.13.

Gambar 3.13 Form *login*

3. Form *Home*

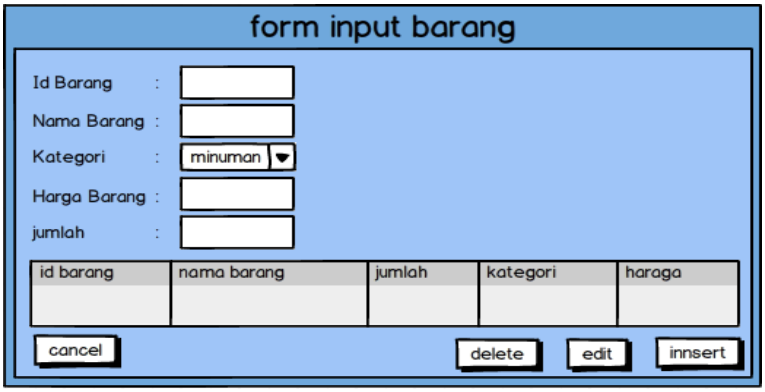
   Pada form home *user* dapat mengakses beberapa form, diantaranya form *input* yang terdiri dari *input* barang, *input* pelanggan dan *input* saldo pelanggan. Selain form *input* juga ada form *view* dan laporan. Form tersebut terdiri dari form laporan barang, laporan pelanggan dan laporan penjualan. Dapat dilihat pada Gambar 3.14.



Gambar 3.14 Form *home*

4. Form *Input* Barang

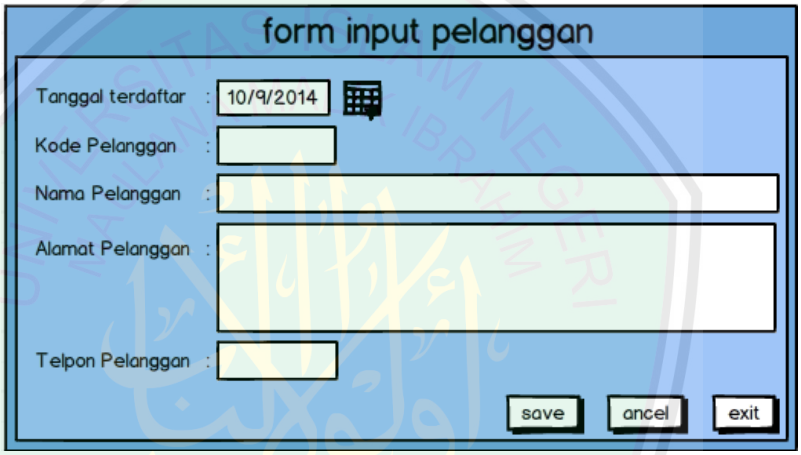
   Dalam form *input* barang *user* dapat *melakukan* pengisian *database* barang sesuai yang hendak dimasukkan ke dalam *database*, baik dari jumah, kategori, harga, jenis barang dll. Dapat dilihat pada Gambar 3.15



Gambar 3.15 Form *Input* Barang

5. Form *Input* Pelanggan

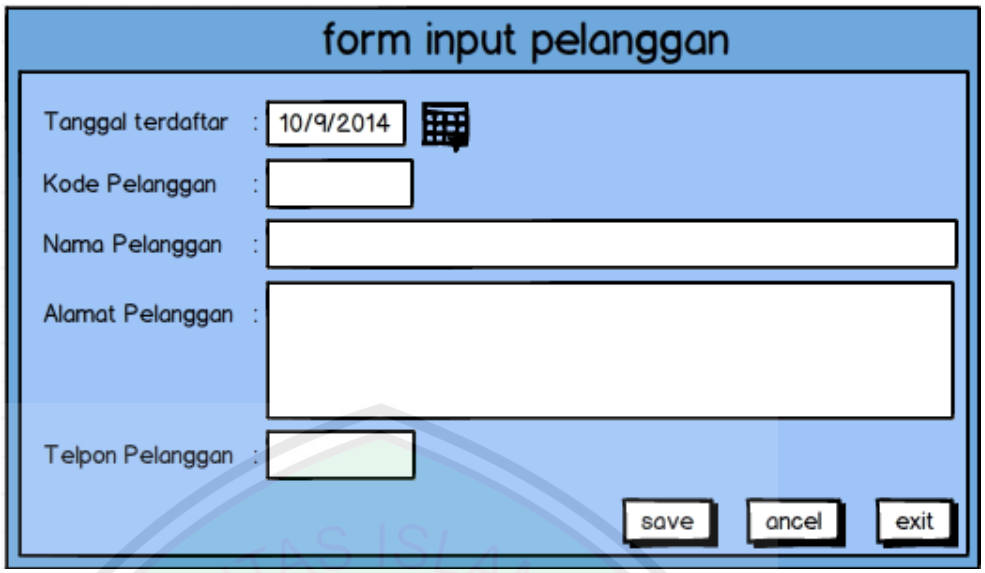
   Pada form *input* pelanggan *user* dapat melakukan proses *input* data pelanggan, data ini terdiri dari nama, alamat, id pelanggan, no telpon dll. Dari form ini dilakukan proses *input* data id pelanggan ke dalam *smart card*. Data id pelanggan terlebih dahulu dienkripsi sehingga data yang masuk ke dalam adalah data yang sudah terenkrip (*ciphertext*). Dapat dilihat pada Gambar 3.16.



Gambar 3.16 Form *input* pelanggan

6. Form *Input* Saldo

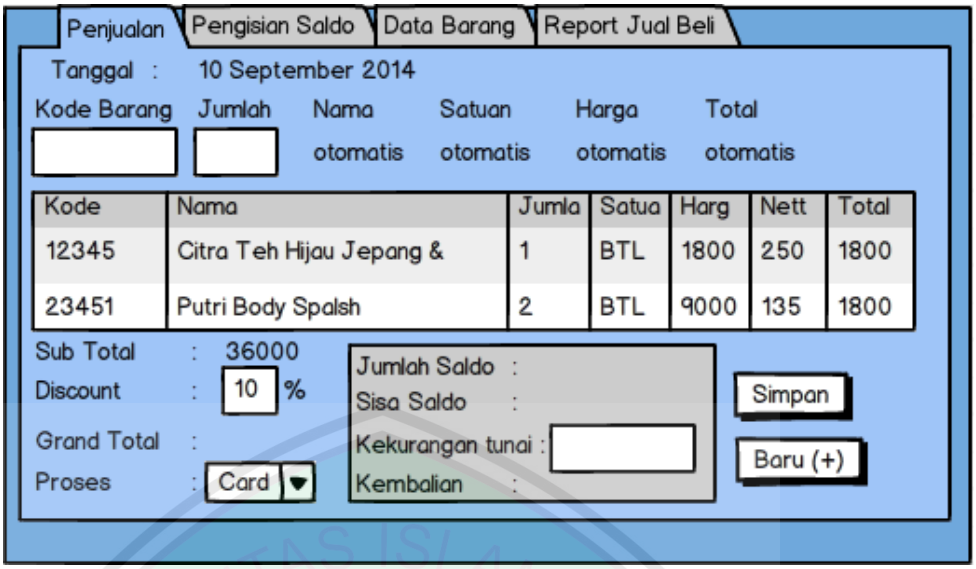
   Pada form ini *user* melakukan pengisian saldo terhadap *smart card*. Data jumlah saldo yang dimasukkan sebelumnya akan dilakukan proses enkripsi. Dalam form ini juga dilakukan proses untuk membaca kartu yang diambil dari data id pelanggan dan sisa dari saldo kartu. Selanjutnya dilakukan proses dekripsi data yang ada pada *smart card* (*ciphertext*) dan sehingga data pada kartu dapat dibaca kembali oleh *user*. Dapat dilihat pada Gambar 3.17.



Gambar 3.17 Form *input* saldo

7. Form Penjualan

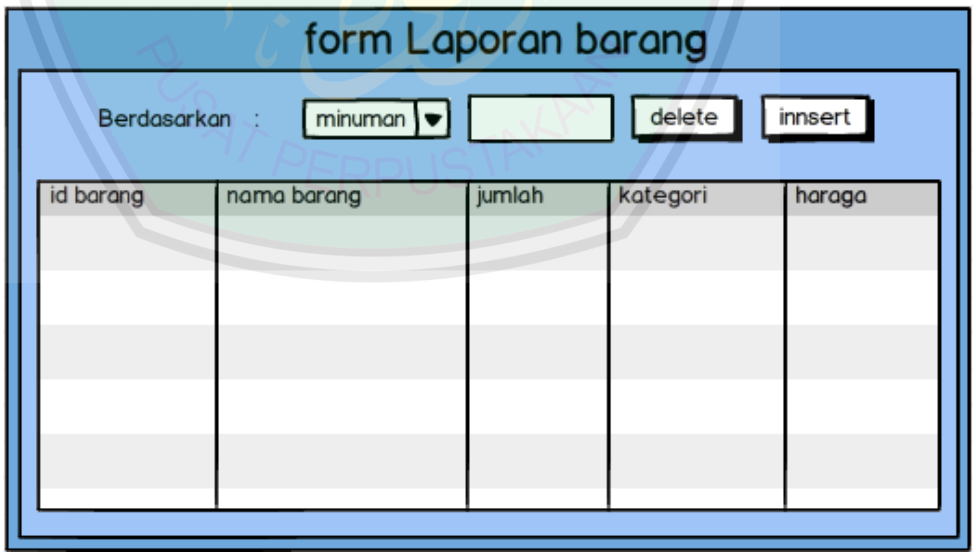
   Pada form ini *user* melakukan proses transaksi penjualan dan pembayaran. Pada proses pembayaran dapat dilakukan dengan dua cara yakni dengan menggunakan kartu dan tidak menggunakan kartu. Pada proses pembayaran dengan menggunakan kartu dilakukan proses dekripsi untuk mengambil data id pelanggan dan saldo pelanggan. Dalam proses ini juga dilakukan proses enkripsi. Proses ini terjadi pada saat melakukan pengurangan saldo sesuai dengan jumlah biaya yang harus dibayar oleh pelanggan kemudian sisa saldo setelah melakukan transaksi pembayaran dimasukkan kembali ke dalam kartu. Sebelumnya data dari sisa saldo tersebut dienkripsi terlebih dahulu dan kemudian dimasukkan kembali ke dalam *smart card*. dapat dilihat pada Gambar 3.18.



Gambar 3.18 Form penjualan

8. Form Laporan Barang

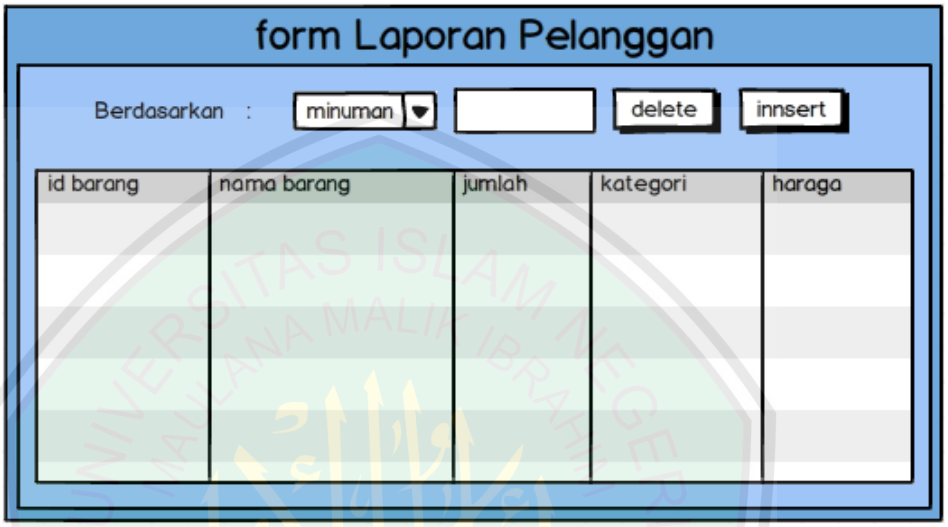
Pada form laporan ini *user* dapat melaporkan data barang yang telah dimasukkan sesuai dengan tanggal masuk, kategori maupun yang lainnya. Dapat dilihat pada Gambar 3.19.



Gambar 3.19 Form laporan barang

9. Form Laporan Pelanggan

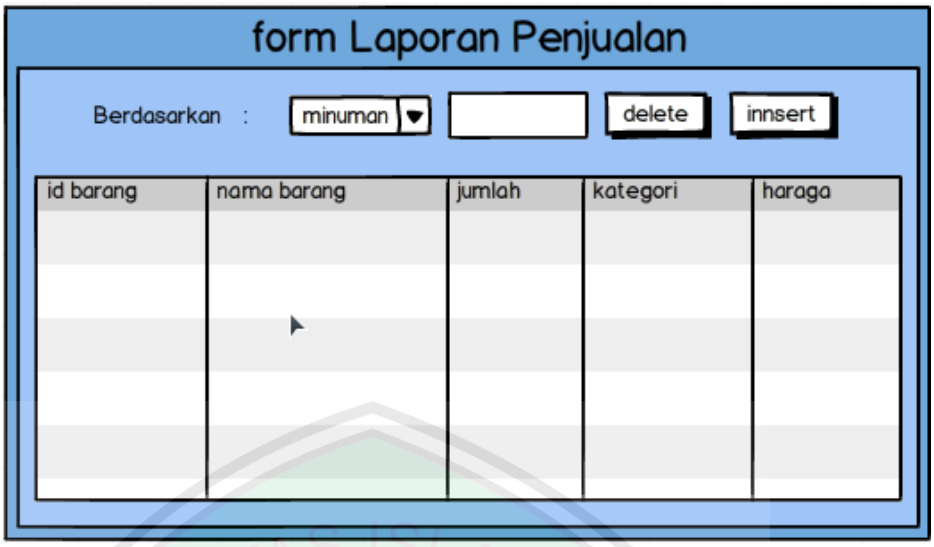
   Pada form laporan pelangan *user* dapat melaporkan atau melihat data dari pelanggan yang telah terdaftar. *User* juga dapat memilih laporan sesuai tanggal, bulan dll. Dapat dilihat ada Gambar 3.20.



Gambar 3.20 Form laporan pelanggan

10. Form Laporan Penjualan

    Pada form laporan penjualan ini memang sangat penting untuk dilakukan karena dalam proses jual beli memang sangat dibutuhkan laporan jual beli baik itu dilakukan per hari, minggu ataupun perbulan. U*ser* dapat memilih melaporkannya dalam kurun waktu harian, mingguan atapun bulanan. *User* juga dapat melakukan *view* dari id pelanggan untuk melihat pembelian apa saja yang telah dilakukan, sehingga pelanggan juga dapat meminta laporan pembelian. Dapat dilihat pada Gambar 3.21.



Gambar 3.21 Form laporan penjualan

3.9 Kebutuhan Sistem

Pada bagian spesifikasi kebutuhan sistem ini, memaparkan tentang kebutuhan sistem perangkat keras (hardware) maupun perangkat lunak (software) yang mendukung dalam pembuatan maupun saat pengoperasian program aplikasi *Smart Card* ini.

Kebutuhan perangkat keras yang digunakan untuk mendukung proses pembuatan dan pengembangan aplikasi ini adalah :

1. Komputer

   Dalam hal ini komputer digunakan untuk membangun aplikasi *smart card.*

2. *Smart Card*

   Smart card merupakan kartu yang mempunyai rangkaian terintegrasi di dalamnya dan mampu memproses serta menyimpan data. Pada aplikasi

ini , *smart card* yang digunakan yaitu *smart card* dengan tipe SLE4428. SLE4428 ini merupakn tipe *smart card* dengan ruang penyimpanan 1Kbyte dengan memiliki ukuran kartu sekitar 86 x 54 x 0,76 mm.

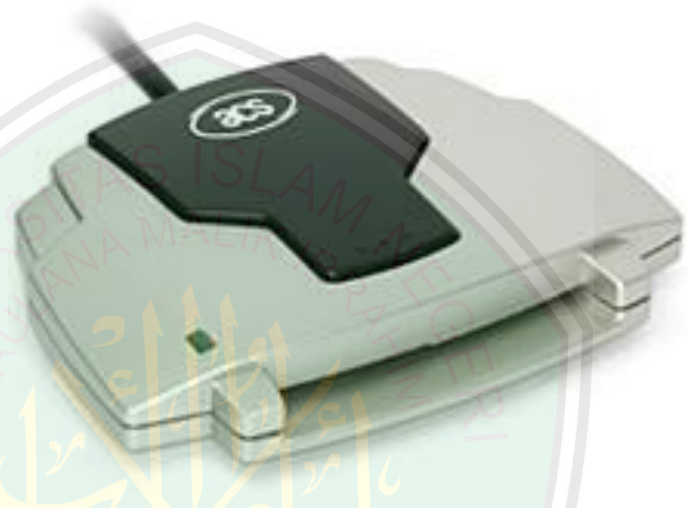
Gambar 3.22 Kartu SLE4428

3. *Card Reader Writer* ACR38

   ACR38 USB *Smart Card Reader Writer* ini merupakan sarana pembangunan aplikasi *smart card* berbasis *reader writer* .ACR38 USB *Smart Card Reader and Writer* ini memiliki spesifikasi sebagai berikut :

   - Kecepatan Antarmuka Penuh Ke PC Dengan Struktur Perintah Sederhana.
   - Membaca Dan Menulis Semua Kartu Mikroprosesor Dengan T = 0, T = 1 Protokol.
   - Mendukung *memory card* dengan protokol I2C (dengan kapasitas 1K - 1024K bit).

- Mendukung *memory card* dengan *fungsi write protect* (SLE4432/ 4442 dan SLE4418/ 4428) , dan juga *secure memory* card (AT88SC153 & AT88SC1608).
- Proteksi hubungan singkat.
- Mendukung sistem operasi Windows 98, ME, NT, 2000 dan XP.



Gambar 3.23 *Smart Card Rider Writer* ACR38

Perangkat lunak (*software*) yang dibutuhkan untuk membuat *smart card* menggnakan algoritma elgamal ini adalah:

1. *Windows XP*

   Sistem Operasi yang digunakan adalah *Microsoft Windows* XP . Sistem operasi *windows* XP ini merupakan sistem operasi yang mudah digunakan oleh siapapun (*user friendly*).

2. *Visual Basic* 6

   Dalam pembuatan aplikasi *smart card* ini kami menggunakan bahasa pemrograman *Visual Basic* 6. *Visual Basic* 6 ini merupakan sebuah bahasa pemrograman yang menawarkan *Integrated Development*

Environment (IDE) visual untuk membuat program perangkat lunak berbasis sistem operasi *Microsoft Windows* dengan menggunakan model pemrograman (COM).

3. SDK ACR38
4. *Microsoft Acces* 2010

   Pada pembuatan *database* aplikasi *smart card* ini kami menggunakan *microsoft acces*. *Microsoft Access* merupakan suatu program aplikasi basis data komputer relasional yang digunakan untuk merancang, membuat dan mengolah berbagai jenis data dengan kapasitas yang besar.

BAB IV

HASIL DAN PEMBAHASAN

Bab ini menjelaskan tentang pengujian metode algoritma yang digunakan dan analisanya dalam membangun aplikasi yang telah dibuat serta implementasi metode tersebut pada sistem aplikasi *smart card* yang telah dibuat. Uji coba ini bertujuan untuk mengetahui apakah aplikasi tersebut telah berjalan sesuai dengan yang diharapkan sesuai dengan rancangan sistem pada BAB III. Pada bab ini juga akan dibahas mengenai fitur dan interface yang terdapat dalam sistem aplikasi.

4.1 Implementasi Sistem

Pada tahap implementasi ini, rancang sistem yang telah di desain pada BAB III diterapkan dengan membangun komponen-komponen yang telah direncanakan. Server memanfaatkan *database miscrosoft acces* 2010 pada progam *smart card* menggunakan bahasa *Visual Basic* 6. *Microsoft acces* 2010 berperan sebagai basis data dan *Visual Basic* 6 berperan sebagai bahasa pemrograman. Selain menggunakan *microsoft acces* 2010 dan *Visual Basic* 6 sebagai media pembuatan program, adapun alat yang berfungsi sebagai penghubung antara program dengan *smart card* yakni *smart card reader writer* ACS ACR38. Alat ini berfungsi untuk melakukan proses membaca dan menulis data ke dalam *smart card*.

4.2 Implementasi Algoritma Elgamal

Pada proses implementasi algoritma elgamal pada aplikasi smart card. Terdapat beberapa tahapan :

4.2.1 Tahapan Pembentukan Kunci

Pada tahap ini sebelum melakukan proses enkripsi maupun dekripsi terhadap data yang ada dalam *smart card* terlebih dahulu kita akan memasukkan kunci p, g dan x. Dari kunci p, g dan x dihasilkan kunci y.

Listing program proses pembentukan kunci :

```
Private Sub kunci
Dim p As Double, g As Double, x As Double, y As Double
p = 257
g = 11
x = 13
SetValueDec (g & "^" & x & "\" & p)
y = digits(1).Text
End Sub
```

4.2.2 Tahapan Proses Enkripsi

Pada proses ini sebelum data asli (*plaintext*) dimasukkan ke dalam *smart card* terlebih dahulu akan dilakukan proses enkripsi sehingga data yang akan masuk ke dalam *smart card* berupa data yang terenkripsi (*ciphertext*). Untuk melakukan proses ini kita akan menggunakan kunci yang telah ditentukan.

Listing program proses enkripsi :

```
Private Sub enkrip()
Call kunci
SetValueDec (g & "^" & x & "\" & p)
y = digits(1).Text
'MsgBox y
Dim hh As String
Dim i As Integer, m As Integer, b As Integer, c As
Integer, gt As Integer
hh = ""
For i = 1 To Len(id_pel.Caption)
k = Mid(id_pel, i, 1)
c = Asc(k)
gt = c + 5
SetValueDec (g & "^" & gt & "\" & p)
a = digits(1)
SetValueDec (y & "^" & gt & "*" & c & "\" & p)
b = digits(1)
hh = hh & " " & a & "-" & b
Next
'MsgBox hh
Text1.Text = hh
End Sub
```

4.2.3 Tahapan Proses Dekripsi

Pada proses dekripsi ini data yang telah didapat oleh sistem dari *smart card* berupa data yang terenkripsi (*ciphertext*) kemudian data tersebut

didekripsi sehingga user dapat membaca kembali data yang telah dimasukkan (*plaintext*) ke dalam *smart card*.

Listing program proses dekripsi :

```
Private Sub deskrip()
Call kunci
Dim gg As String, qq() As String, ww() As String, v As
String
Dim w As Integer, i As Integer, j As Integer, a As
Integer, b As Integer
gg = ""
j = 0
For i = 1 To Len(Text5.Text)
    If Mid(Text5.Text, i, 1) = " " Then
        j = j + 1
    End If
'    MsgBox i & " " & Mid(Text3.Text, i, i)
Next
qq = Split(Text5.Text, " ")
For i = 0 To j
 '   MsgBox hh(i) & " " & j
 If qq(i) = "" Then
 Else
ww = Split(qq(i), "-")
a = ww(0)
b = ww(1)
SetValueDec (b & "*" & a & "^" & "(" & p & "-" & s & "-
" & x & ")" & "\" & p)
'MsgBox (b & "*" & a & "^" & "(" & p & "-" & s & "-" &
```

```
x & ")" & "\" & p)
v = digits(1)
gg = gg & "" & Chr(v)
End If
Next
'MsgBox gg
Text2.Text = gg
End Sub
```

4.3Implementasi *Interface* danFungsinya

Berikut tampilan *interface* dari Aplikasi *Smart Card* :

1. Tampilan Menu *Login*

   Pada tampilan menu *login* terdapat proses *login* yang dilakukan oleh *user* sebagai jalan akses untuk menuju tampilan selanjutnya. Pada tampilan menu ini user berperan sebagai pegawai (kasir) dalam proses jual beli. Pada tampilan menu utama dapat dilihat pada Gambar 4.1.

Gambar 4.1 Form Menu *Login*

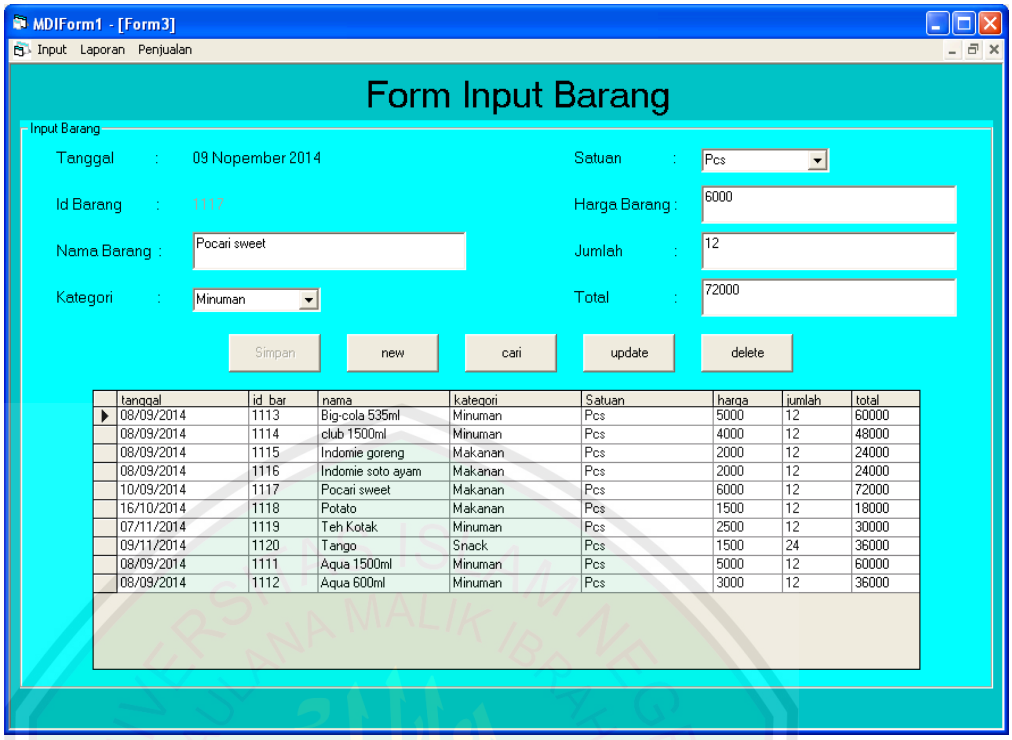
2. Tampilan Menu *Home*

Pada halaman menu *home* user (pegawai) dapat memilih melakukan proses apa selanjutnya. Dalam tampilan menu ini ada beberapa pilihan menu, pilihan menu *input* dan menu laporan. Pada menu *input* terdapat sub menu yaitu *input* barang, *input* pelanggan dan *input* saldo. Selanjutnya ada pilihan menu laporan. Pada pilihan ini terdapat laporan barang, laporan pelanggan dan laporan jual beli. Dalam tampilan menu ini selain ada pilihan menu *input* dan laporan ada juga pilihan menu transaksi jual beli. *User* (pegawai) dapat melakukan proses transaksi jual beli dengan pelanggan.

Gambar 4.2 Form Menu *Home*

3. Tampilan Menu *Input* Barang

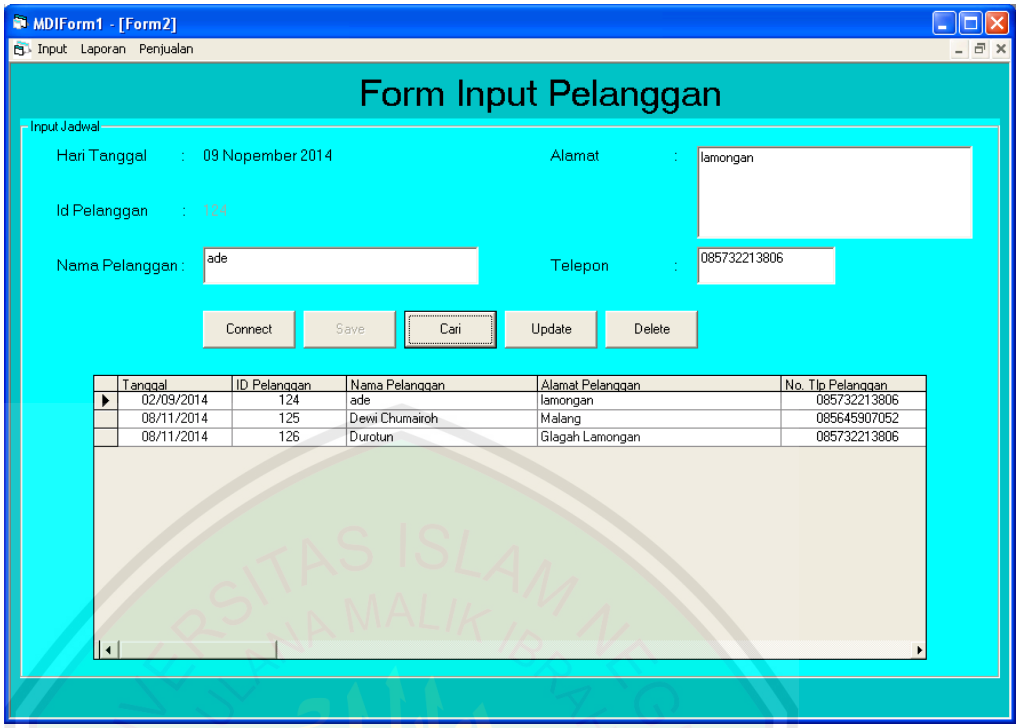
Pada form menu input barang ini user (pegawai) melakukan proses input ataupun update barang ke dalam database yang telah tersedia.



Gambar 4.3 Form Menu *Input* Barang

4. Tampilan Menu *Input* Pelanggan

   Pada form ini *user* (pegawai) melakukan proses *input* data pelanggan yang terdiri dari data id pelanggan, nama, alamat dll. Data tersebut disimpan di dalam *database* yang telah disediakan. Pada proses ini juga dilakukan proses *input* data pada *smart card*. Dalam proses *input* data pada *smart card*, sebelum data dimasukkan ke dalam *smart card* terlebih dahulu data dienkripsi sehingga data yang masuk ke dalam *smart card* sudah berbentuk data *ciphertext* dari data asli. Di sini data yang akan dimasukkan ke dalam *smart card* hanya data id pelanggan.

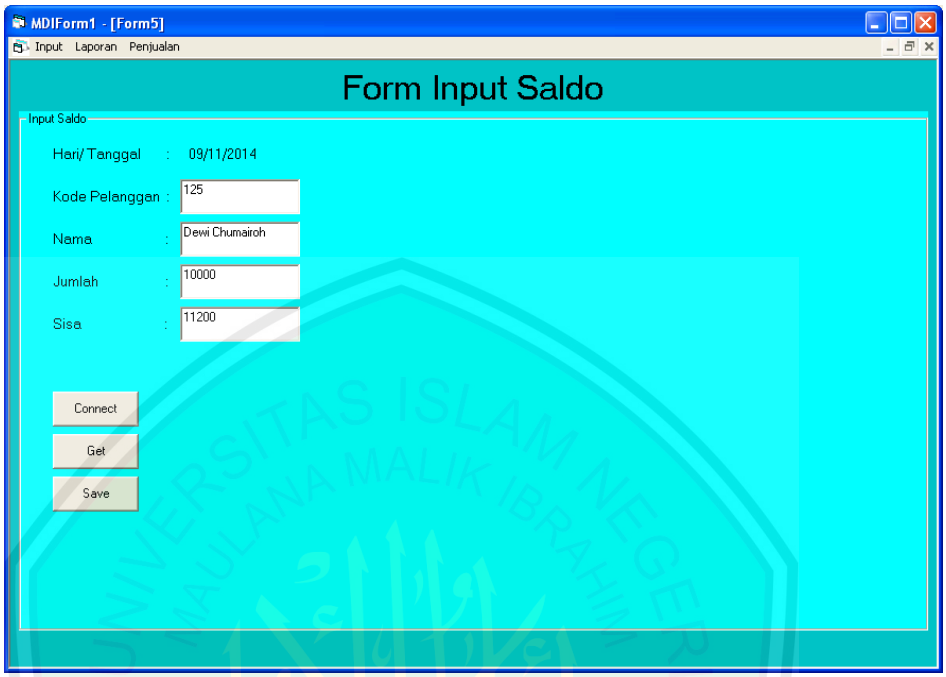


Gambar 4.4 Form Menu *Input* Pelanggan

5. Tampilan Menu *Input* Saldo

Pada form ini *user* akan melakukan proses *input* saldo. Di dalam proses ini dilakukan proses algoritma yakni proses enkripsi dan dekripsi. Pada proses enkripsi dilakukan pada saat *user* hendak menambah saldo pada *smart card*. Penambahan tersebut dimasukkan ke dalam *smart card*. Sebelum dilakukan *input* saldo ke dalam kartu terlebih dahulu data penambahan jumlah saldo tersebut dienkripsi, sehingga data yang masuk ke dalam kartu juga berupa data *ciphertext.* Selanjutnya melakukan proses dekripsi, dalam proses ini data yang ada di dalam kartu (*ciphertext*) akan diambil dan dilakukan proses dekripsi, sehingga data yang ada di dalam kartu dapat dibaca kembali oleh *user* sebagaimana data awal yang dimasukkan ke

dalam kartu. Pada tampilan menu *input* saldo dapat dilihat pada Gambar 4.5.

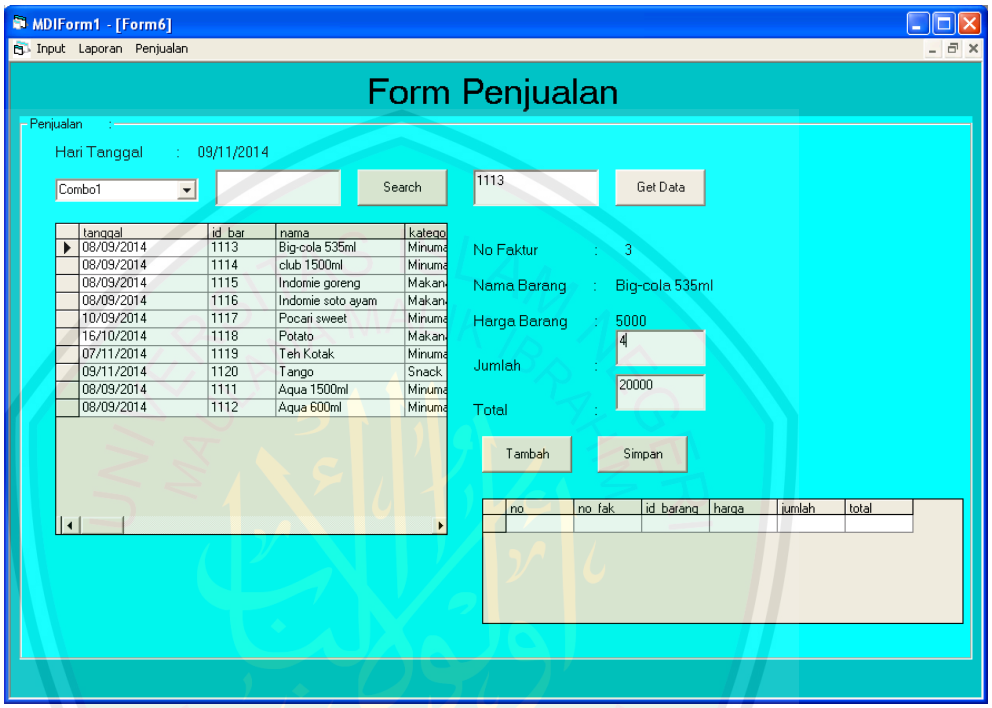


Gambar 4.5 Form Menu *Input* Saldo

6. Tampilan Menu Transaksi Jual Beli

Pada form menu transaksi jual beli *user* (pegawai) melakukan proses pendataan barang yang terjual. Dalam proses jual beli ini pelanggan dapat melakukan pembayaran dengan dua cara. Cara pertama dengan memberikan uang tunai, sedangkan untuk cara yang kedua pembayaran dilakukan menggunakan *smart card* sehingga dalam form ini juga terjadi proses enkripsi dan dekripsi, dimana proses dekripsi terjadi pada saat program mengambil data dari *smart card*. Data yg terdapat di dalam *smart card* berupa data *ciphertext*. Perlu dilakukan proses dekripsi agar pengguna dapat membaca kembali data tersebut. Data yang akan diambil

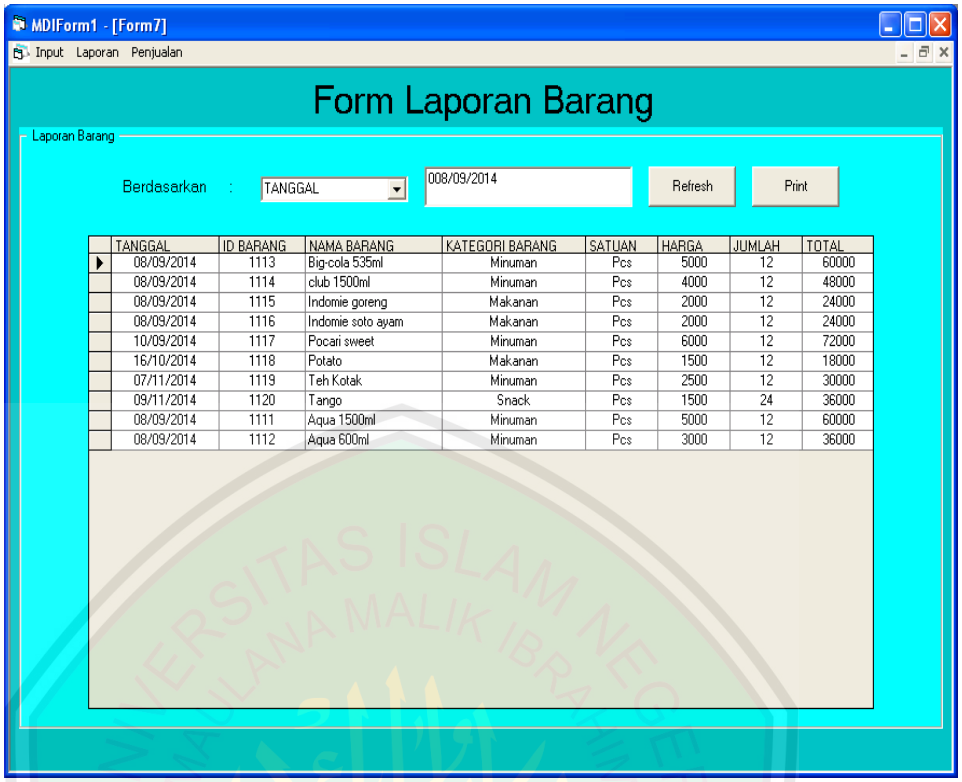
yakni data id pelanggan dan saldo pelanggan. Untuk proses enkripsi sendiri dilakukan pada saat proses pembayaran. Saldo akan berkurang sehingga diperlukan adanya update dari data yang ada di dalam *smart card*. tampilan menu transaksi jual beli dapat dilihat pada Gambar 4.6.



Gambar 4.6 Form Menu Transaksi Jual Beli

7. Tampilan Menu Laporan Barang

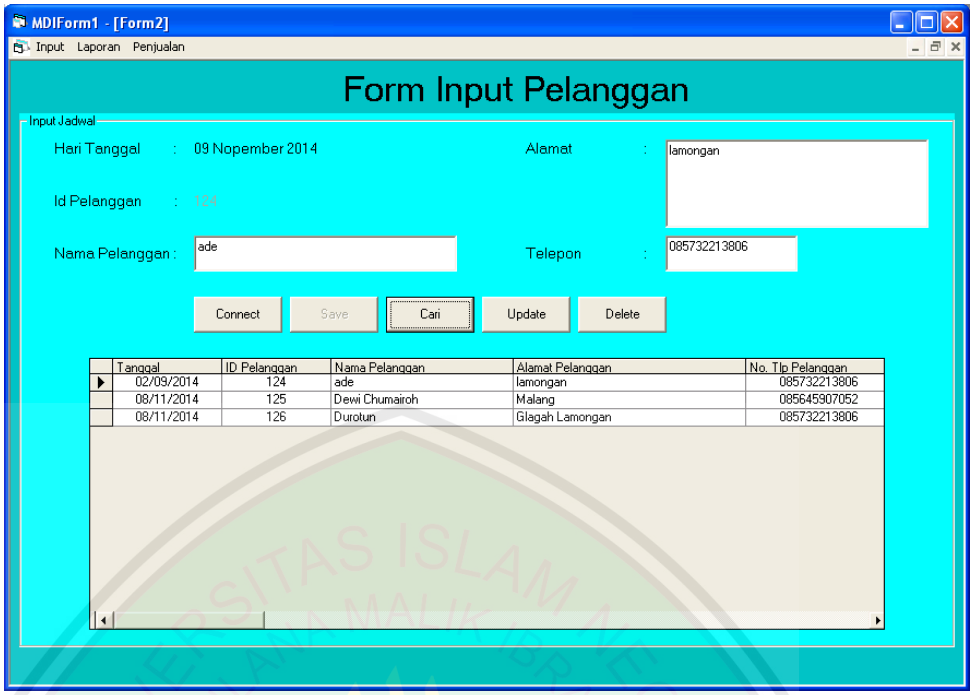
Pada form menu laporan barang *user* (pegawai) dapat melihat laporan ataupun menyerahkan laporan dalam bentuk *print out*. *User* (pegawai) dapat memilih kurun waktu dalam melakukan proses melaporkan barang. Tampilan menu laporan barang dapat dilihat pada Gambar 4.7.



Gambar 4.7 Form Menu Laporan Barang

8. Tampilan Menu Laporan Pelanggan

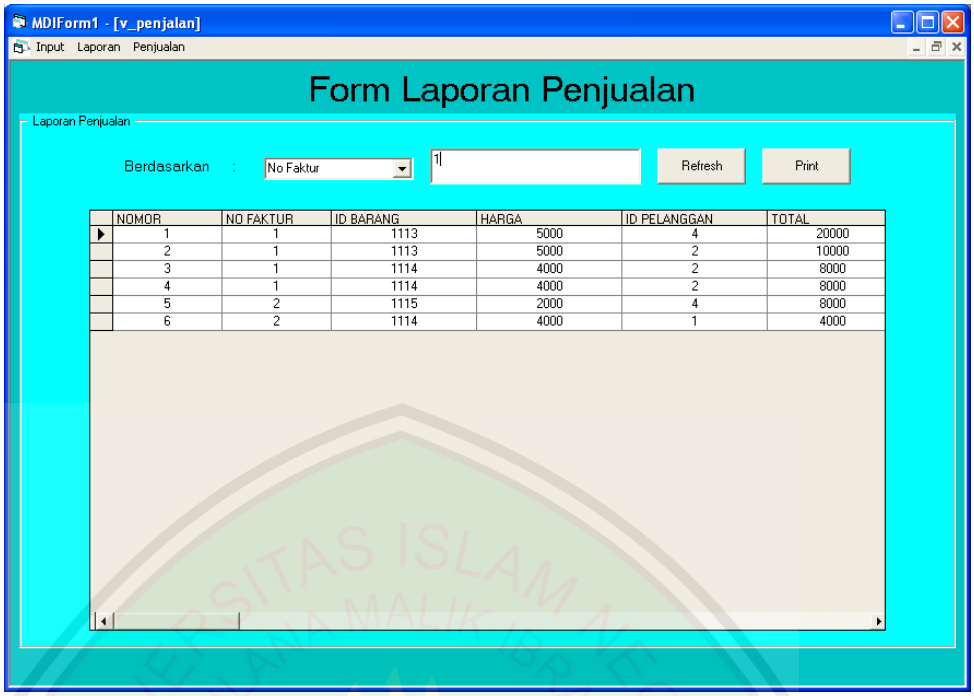
   Pada menu laporan pelanggan ini *user* (pegawai) juga dapat melihat laporan ataupun menyerahkan laporan dalam bentuk *print out*. Proses ini *user* (pegawai) juga dapat melakukan pemilihan kurun waktu dalam proses melaporkan pelanggan.



Gambar 4.8 Form Menu Laporan Pelanggan

9. Tampilan Menu Laporan Jual Beli

Pada proses menu laporan penjualan ini sama seperti halnya pada proses laporan lainnya, *user* (pegawai) dapat melihat laporan penjualan dan menyerahkan *print out* laporan penjualan. Pada proses laporan penjualan *user* (pegawai) dapat memilih kategori dari proses laporan, baik menurut kurun waktu maupun melihat sesuai dengan id pelanggan, nomor faktur dll sehingga dalam form ini pelanggan juga dapat melihat transaksi jual beli apa saja yang telah pelanggan lakukan selama kurun waktu pandaftaran anggota pelanggan *smart card*. tampilan menu laporan jual beli dapat dilihat pada Gambar 4.9.



Gambar 4.9 Form Menu Laporan Penjualan

4.4 Evaluasi dan Analisis Hasil Pengujian

Pengujian yang dilakukan menitikberatkan pada hasil *output* dari kendali *input*. Pada kendali *input*, pengujian dikatakan berhasil apabila *output* sesuai dengan kendali input.

Berdasarkan rencana pengujian aplikasi sistem keamanan ini telah disusun, maka dapat dilakukan pengujian sebagai berikut.

4.4.1 Pengujian Proses Enkripsi

Untuk pengujian pada proses enkripsi ini, kita akan memasukkan data id pelanggan dan saldo. Pada pengujian kali ini akan dilakukan proses perhitungan secara manual dari data yang akan dimasukkan kedalam *smart card.*

1. Proses input id pelanggan

   Id pelanggan = 251052

   p = 257

   g = 11

   x = 13

   $y = 11^{13} \bmod 257$

   = 22

Public (y = 22, g = 11 dan p = 257).

Private (x = 13 dan p = 257)

Id pelanggan = 251052 , menentukan nilai k :

Tabel 4.1 Tabel pembentukan kunci k pada data id pelanggan

Char	ASCII	Kunci k
2	50	55
5	53	58
1	49	54
0	48	53
5	53	58
2	50	55

Menghitung nilai a_i , b_i

$a_1 = 11^{55} \bmod 257 = 23$ $b_1 = 22^{55}.50 \bmod 257 = 196$

$a_2 = 11^{56} \bmod 257 = 30$ $b_2 = 22^{56}.53 \bmod 257 = 65$

$a_3 = 11^{54} \bmod 257 = 189$ $b_3 = 22^{54}.49 \bmod 257 = 62$

$a_4 = 11^{53} \bmod 257 = 134$ $b_4 = 22^{53}.48 \bmod 257 = 224$

$a_5 = 11^{56} \bmod 257 = 30$ $b_2 = 22^{56}.53 \bmod 257 = 65$

$a_6 = 11^{55} \bmod 257 = 23$ $b_5 = 22^{55}.50 \bmod 257 = 196$

Hasil enkripsi dari data id pelanggan (23,196 | 30,65 | 189,62 | 134,224 | 30,65 | 23,196)

2. Proses Input Saldo

Sisa saldo = 11200

Tabel 4. 2 proses pembentukan kunci k pada data saldo pelanggan

Char	ASCII	Kunci k
1	49	54
1	49	54
2	50	55
0	48	53
0	48	53

Menghitung nilai a_i , b_i

$a_1 = 11^{49} \bmod 257 = 189$ $b_1 = 22^{154}.49 \bmod 257 = 62$

$a_2 = 11^{49} \bmod 257 = 189$ $b_2 = 22^{54}.49 \bmod 257 = 62$

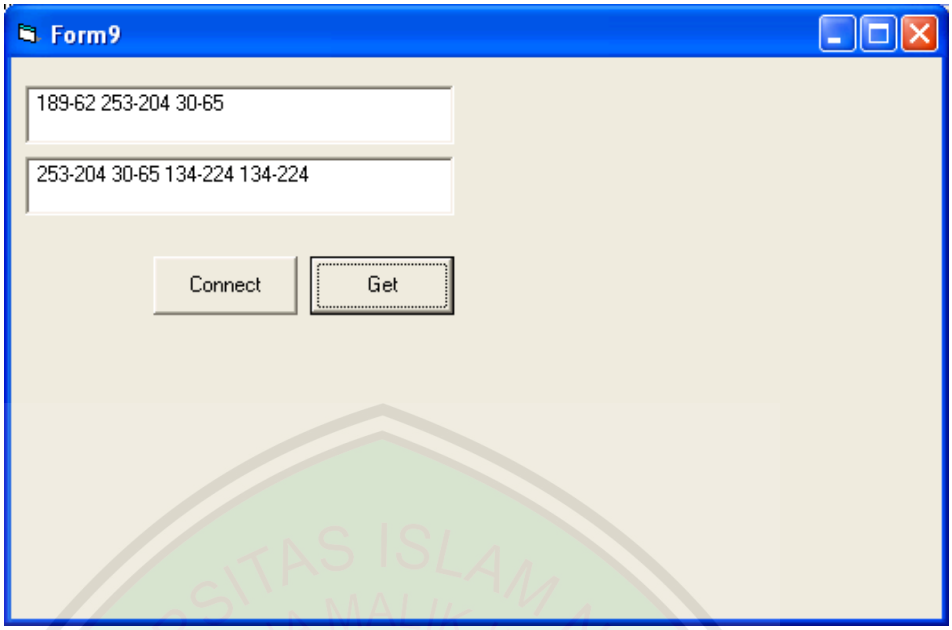
$a_3 = 11^{50} \bmod 257 = 23$ $b_3 = 22^{55}.50 \bmod 257 = 196$

$a_4 = 11^{48} \bmod 257 = 134$ $b_4 = 22^{48}.48 \bmod 257 = 224$

$a_5 = 11^{48} \bmod 257 = 134$ $b_5 = 22^{48}.48 \bmod 257 = 224$

Hasil enkripsi dari saldo (189,62 | 189,62 | 23,196 | 134,224 | 134,224)

Hasil enkripsi tersebut selanjutnya akan dimasukkan ke dalam *smart card* sehingga data yang masuk ke dalam *smart card* berupa data *ciphertext.* Dapat dilihat pada Gambar 4.10.



Gambar 4.10 Membaca Data Kartu

Dari gambar 4.10 menunjukkan bahwa data yang dimasukkan ke dalam *smart card* sudah berupa data yang telah dienkripsi (*ciphertext*) sehingga ketika ada pihak yang tidak berwenang ingin membaca kartu maka data yang akan terbaca adalah berupa data yang telah terenkripsi (*ciphertext*).

Tabel 4.3 Tabel hasil pengujian proses enkripsi

No.	Isi Data	P. kar	Hasil Enkripsi	Keterangan
1.	251052	6	23,196 | 30,65 | 189,62 | 134,224 | 30,65 | 23,196	Data yang telah masuk kedalam *smart card* berupa data hasil enkripsi sesuai dengan hasil perhitungan [√]
2.	11200	5	189,62 | 189,62 | 23,196 | 134,224 | 134,224	Data yang telah masuk kedalam *smart card* berupa data hasil enkripsi sesuai dengan hasil perhitungan [√]

4.4.2 Pengujian Proses Dekripsi

Pada proses pengujian dekripsi iniakan dilakukan perhitungan secara manual kemudian akan dibandingkan dengan hasil yang terbaca oleh progam aplikasi *smart card* . Data yang akan didekripsi adalah data *ciphertext* dari id pelangan dan data *ciphertext* dari saldo pelanggan.

Ciphertext id pelanggan 23,196 | 30,65 | 189,62 | 134,224 | 30,65 | 23,196

$m_1 = 196.23^{257-1-13} \bmod$

$= 50$

$m_2 = 65.30^{257-1-13} \bmod p$

$= 53$

$m_3 = 62.189^{257-1-13} \bmod p$

$= 49$

$m_4 = 224.134^{257-1-13} \bmod p$

$= 48$

$m_5 = 65.\ 30^{257-1-13} \bmod p$

$= 53$

$m_6 = 196.23^{257-1-13} \bmod$

$= 50$

ASCII

Tabel 4.4 hasil dekripsi id pelanggan

Dec	Char
50	2
53	5
49	1
48	0
53	5
50	2

Hasil dekripsi dari data *ciphertext* id pelanggan(251052)

Ciphertext saldo pelanggan 189,62 | 189,62 | 23,196 | 134,224 | 134,224

$m_1 = 62.189^{257-1-13} \bmod$

$= 49$

$m_2 = 62.189^{257-1-13} \bmod$

$= 49$

$m_3 = 196.23^{257-1-13} \bmod p$

$= 50$

$m_4 = 224.134^{257-1-13} \bmod$

$= 48$

$m_5 = 224.134^{257-1-13} \bmod p$

$= 48$

ASCII

Tabel 4.5 hasil dekripsi saldo pelanggan

Dec	Char
49	1
49	1
50	2
48	0
48	0

Hasil dekripsi dari data *ciphertext* saldo pelanggan (11200)

Dari hasil tabel diatas menunjukkan bahwa aplikasi telah berhasil untuk mendekripsikan data *ciphertext* dari *smartcard* menjadi data *plaintext*, sehingga *user* dapat membaca kembali data asli dari *smartcard*.

Tabel 4.6 Tabel Hasil Pengujian Proses Dekripsi

No.	**Isi Data Pada *SmartCard***	**Hasil Dekripsi**	**Keterangan**
1.	189,62 | 23,196 | 30,65	125	Data yang terbaca oleh aplikasi berupa data *plaintext* sesuai dengan hasil perhitungan (data awal) [√]
2.	189,62 | 189,62 | 23,196 | 134,224 | 134,224	11200	Data yang terbaca oleh aplikasi berupa data *plaintext* sesuai dengan hasil perhitungan (data awal) [√]

4.4.3 Pengujian Autentifikasi pada *SmartCard*

Hasil pengujian saat melakukan autentifikasi menggunakan *smartcard* antara lain sebagai berikut :

Tabel 4.7 Tabel hasil autentifikasi aplikasi *smart card*

Butir Uji	**Hasil yang diharapkan**	**Hasil yang diamati**	**Kesimpulan**
Masukkan kartu	Sistem mampu mendeteksi keberadaan kartu.	Sistem dapat mendeteksi keberadaan kartu.	Berhasil [√] Gagal [ ]
Input data ke *smartcard*	Menginputkan data kedalam *smartcard*	Data berhasil diinputkan kedalam *smartcard*	Berhasil [√] Gagal [ ]
Baca data *smartcard*	Membaca data *smartcard*	Data berhasil terbaca oleh sistem	Berhasil [√] Gagal [ ]

4.5 Hasil Pengujian Algoritma Elgamal

Hasil pengujian saat menerapkan algoritma elgamal adalah sebagai berikut :

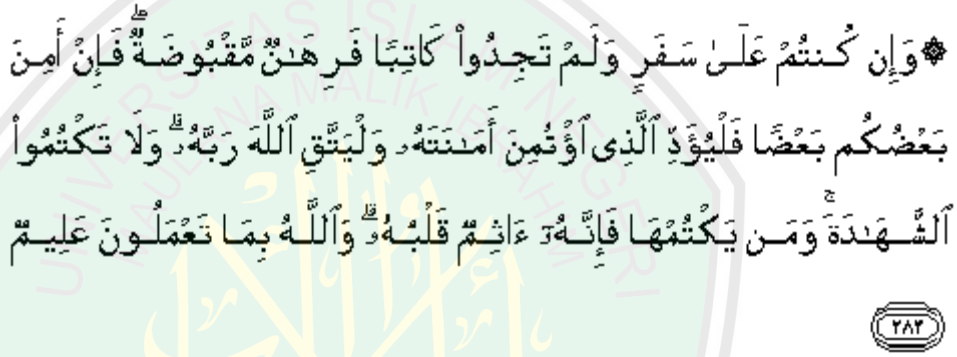
Tabel 4.8 Tabel hasil penerapan algoritma elgamal

Butir Uji	**Hasil yang diharapkan**	**Hasil yang diamati**	**Kesimpulan**
Proses enkripsi	Data yang dimasukkan kedalam *smartcard* berupa data terenkripsi (*ciphertext*)	Data yang masuk ke dalam *smartcard* berupa data *ciphertext*	Berhasil [√] Gagal [ ]
Proses dekripsi	Data *smartcard* yang dibaca oleh aplikasi berupa data *plaintext* (asli)	Data *output* (terbaca) oleh aplikasi*smartcard*adalah data *plaintext*	Berhasil [√] Gagal [ ]

4.6 Integrasi Kriptografi menurut Kajian dalam Al-qur'an

Kriptografi (cryptography) merupakan ilmu dan seni penyimpanan pesan, data, atau informasi secara aman.*Kriptografi* bertujuan menjaga kerahasiaan informasi yang terkandung dalam data sehingga informasi tersebut tidak dapat diketahui oleh pihak yang tidak sah.

Sesuai dengan ayat 283 surat Al-Baqarah yang berbunyi :



"Jika kamu dalam perjalanan (dan bermu'amalah tidak secara tunai) sedang kamu tidak mendapatkan seorang penulis, maka hendaklah ada barang jaminan yang dipegang[1] (oleh yang berpiutang)[2]. Tetapi, jika sebagian kamu mempercayai sebagian yang lain[3], maka hendaklah yang dipercayai itu menunaikan amanatnya (hutangnya) dan hendaklah ia bertakwa kepada Allah Tuhannya[4]. Dan janganlah kamu (para saksi) menyembunyikan kesaksian[5], karena barang siapa menyembunyikannya, maka sesungguhnya ia adalah orang yang berdosa hatinya; dan Allah Maha mengetahui apa yang kamu kerjakan"

Pada ayat tersebut telah dijelaskan bahwa amanah merupakan kepercayaan yang diberikan orang lain terhadapnya sehingga menimbulkan ketenangan jiwa. Pada penelitian kali ini kita akan melakukan proses kriptografi dengan tujuan untuk mengamankan data yang akan didigunakan sehingga orang tersebut dapat menjaga amanah dengan tenang.

Pada proses kriptografi ini tahapan yang akan dilakukan setelah sebuah informasi atau data dikirim ke pihak tertentu, data tersebut sebelumnya akan dikunci sehingga untuk membaca data pihak yang dituju harus membuka kunci tersebut. Hasil data yang dikunci tersebut berupa data chipertext (kode) sehingga untuk membaca kode tersebut harus ada kesepakatan kunci yang harus diketahui oleh pihak pengirim dan pihak penerima. Sehingga data yang terkirim akan menjadi aman dan apabila ada pihak lain yang tidak berhak menerima pesan menginginkan data pesan tersebut maka yang akan didapatkan adalah hanya data berbentuk chipertext (kode) yang tidak bisa dibaca oleh pihak tersebut sehingga data pesan bisa dikatakan aman.

BAB V

KESIMPULAN DAN SARAN

5.1 Kesimpulan

Adapun kesimpulan yang diambil dari implementasi algoritma ElGamal dalam aplikasi *smart card* yaitu :

1. Algoritma Elgamal dapat diterapkan pada *smart card* untuk mengamankan data yang ada di dalam *smart card*.
2. *Smart Card* sebagai alat pembayaran Jual beli memberikan kemudahan dan waktu yang lebih efisien bagi pelanggan juga memberikan kemudahan dalam proses penghitungan .
3. Dengan sistem enkripsi yang diterapkan pada aplikasi *smart card* tersebut, akan dirasa sulit apabila ada pihak yang tidak berhak ingin mengambil data dari kartu (*smart card*) karena data yang ditangkap berupa data *ciphertext.*

5.2 Saran

Saran untuk penelitian dan pengembangan aplikasi selanjutnya adalah dapat dilakkan penelitian dengan menerapkan aplikasi *smart card* berbasis *online* atau untuk pengembangan keamanan maka juga dapat diterapkan berbagai macam metode algoritma.

Daftar Pustaka

Ari Wibowo, Wihartantyo. 2004. *Advanced Encryption Standard Algoritma Rijndael.* Departemen Teknik Elektro Institut Teknologi Bandung

Zulhazmi, Dimas . 2012. *Analisis Algoritma Enkripsi Elgamal, Grain V1, dan AES dengan Studi Kasus Aplikasi Resep Makanan.* Jurusan Teknik Informatika, Fakultas Teknologi Informasi Institut Teknologi Sepuluh Nopember.

Gilang Kautsar, Mohammad. 2009. *Implementasi Sistem Enkripsi Pengirim Pesan Instan Java dengan Algoritma Blowfish.* Departemen Teknik Informatika Institut Teknologi Bandung.

Aribowo, Eko. 2008. *Aplikasi Pengaman Dokumen Office dengan Algoritma Kriptografi Kunci Asimetris Elgamal.* Program Studi Teknik Informatika, Fakultas teknologi Industri Universitas Ahmad Dahlan Yogyakarrta.

Daniel, Ahmad. 2008. *Mengatasi Serangan Buffer Overflow Keamanan Data Berbasis Smart Card.* Jurusan Teknik Informatika, Fakultas Ilmu Komputer Universitas Sriwijaya.

Widyartono, Agustinus. 2011. *Algoritma Elgamal untuk Enkripsi Data Menggunakan GPUNG.* STIMK PalComTech Palembang.

Monica, Marta. 2012. *Pemanfaatan Algoritma Kriptografi dalam Pembuatan Smart Card.* Departemen Teknik Informatika, Sekolah Teknik Elektro dan Informatika Institud Teknologi Bandung.

Risky Firmansyah, Eka. 2012. *Algoritma Kriptografi dan Contohnya.* Teknik Informatika 5B, Fakultas Sains dan Teknologi Universitas Islam Negri Syarif Hidayatullah Jakarta.

Ariyus, Dony. 2006. *Kriptografi Keamanan Data dan Komunikasi. Yogyakarta: Graha Ilmu.*

Linda Caroline, Maureen. 2011. *Perbandingan Algoritma Kriptografi Kunci Public RSA, Rabin dan Elgamal.* Program Studi Tekni Informatika, Sekolah Teknik Elektro dan Informatika Institut Teknologi Bandung.

Agung Satria, Adhitya. *Kajian Perkembangan Teknologi Smart Card dari Segi Keamanan dan Implementasinya di Kehidupan Sehari-hari.* Departemen Teknik Informatika, Institut Teknologi Bandung.

Tri Massandy, Danang. 2009. *Algoritma Elgamal dalam Pengamanan Pesan Rahasia.* Program Studi Teknik Informatika, Sekolah Teknik Elektro dan Informatika Institut Teknologi Bandung.