ELKOMIKA | ISSN (p): 2338-8323 | ISSN (e): 2459-9638 | Vol. 7 | No. 3 | Halaman 427 – 441
DOI : http://dx.doi.org/10.26760/elkomika.v7i3.427 September 2019

Rancang Bangun Sistem Keamanan *RFID Tag* menggunakan Metode *Caesar Cipher* pada Sistem Pembayaran Elektronik

DECY NATALIANA, FEBRIAN HADIATNA, AHMAD FAUZI

Teknik Elektro, Institut Teknologi Nasional Bandung
Email: decyhari@gmail.com

Received 12 Maret 2019 **|** *Revised* 1 April 2019 **|** *Accepted* 24 April 2019

ABSTRAK

Pada penelitian ini mencoba untuk memanfaatkan tag RFID sebagai media untuk menyimpan data berupa nilai nominal uang. Metode enkripsi data Ceasar Cipher akan diterapkan ke dalam sistem yang dirancang sehingga data nominal uang pada tag merupakan data yang terenkripsi. Enkripsi data ini dilakukan untuk memperkuat sistem keamanan yang telah terdapat pada tag, sehingga proses peretasan data akan lebih sulit untuk dilakukan. Perangkat keras yang digunakan untuk merealisasikan sistem terdiri dari unit reader RFID-RC522, tag MIFARE Classic S50 1 kbyte, dan Arduino UNO R3. Dari hasil pengujian diperoleh bahwa tag dapat digunakan untuk menyimpan data berupa nilai nominal uang dan dari sistem yang telah direalisasikan nilai nominal uang tersebut dapat ditambah atau dikurang jumlahnya dari Rp 0 – Rp 4.294.967.295. Penerapan metode Ceasar Cipher berhasil mengubah nilai nominal uang menjadi data yang terenkripsi.

Kata Kunci: *RFID, pembayaran elektronik, sistem keamanan, enkripsi data, ceasar cipher*

ABSTRACT

In this research will try to utilize RFID tag as data storage for a certain value of money. Ceasar cipher as encryption method will be applied to the implemented system so that this certain value of money inside the tag turned into an encrypted data. Ecryption of the data is done to hardened the security sistem that already exists in the tag itself, so any violation behavior like data cracking will be harder to accomplish. The hardware that used on the system consist of a reader unit RFID-RC522, MIFARE Classic tag S50 1kbyte, and Arduino UNO R3. The result of this research proofed that the tag could be utilized to store a certain value of money and with a well built implemented system, the data value could be incremented or decremented ranging from Rp 0 – Rp 4.294.967.295. Implementation of Ceasar Cipher method has succesfully turn that certain value of money inside the tag into an encrypted data.

Keywords: *RFID, Electronic payment, security system, data encryption, ceasar cipher*

1. PENDAHULUAN

Transaksi pembayaran menggunakan sebuah kartu berteknologi RFID merupakan salah satu jenis transaksi non-tunai yang dapat dijadikan alternatif sebagai metode pembayaran. Teknologi RFID *(Radio-Frequency Identification)* digunakan untuk memudahkan identifikasi berbagai macam hal dengan hanya menggunakan sebuah label dan sebuah *reader*. Label/*tag* berfungsi sebagai tanda pengenal yang di dalamnya ditanamkan sebuah antena dan *chip* khusus untuk menyimpan data, sedangkan *reader* berfungsi sebagai pembaca data pada label. Sebuah sistem keamanan data harus diiimplementasikan untuk mencegah penyalahgunaan oleh pihak yang tidak bertanggung jawab. Enkripsi data atau *cipher* adalah sebuah algoritma yang bertujuan untuk mengubah suatu informasi berupa tulisan menjadi informasi lain yang tidak dapat dibaca atau dimengerti **(Sarita, 2017)**. Metode *Ceasar Cipher* merupakan salah satu metode yang cocok digunakan sebagai algoritma enkripsi dan dekripsi data tersebut karena data yang dikirimkan pada label/*tag* RFID adalah data bertipe karakter **(Enas & Farah, 2014)**. Diharapkan dengan melakukan penelitian ini dapat menjadikan *tag* RFID sebagai media untuk menyimpan data berupa nilai nominal uang dan dengan menerapkan metode *Ceasar Cipher* sebagai algoritma enkripsi dapat memperkuat sistem keamanan data pada *tag* RFID.

1.1 RFID (*Radio Frequency Identification)*

Identifikasi frekuensi radio (RFID) adalah sebuah metode identifikasi menggunakan sarana yang disebut transponder (label/*tag)* untuk menyimpan dan mengambil data secara nirkabel yang dihasilkan dari pancaran gelombang radio sebuah unit *reader* **(Christoph, 2013)**. Pada saat sebuah label didekatkan pada unit *reader* yang aktif, maka perubahan medan elektromagnetik akan terjadi di sekitarnya dan akan diterima oleh label sebagai sinyal elektromagetik **(Marcel, 2011)**.

Sebuah label RFID dapat dibaca dengan area jangkauan pembacaan yang berbeda-beda tergantung dari jenis label yang digunakan. Berdasarkan sumber energi, label dibedakan menjadi 3 jenis, yaitu label aktif, label pasif dan label semi-pasif. Berdasarkan frekuensi operasi label dibedakan menjadi 3 jenis yang menentukan tingkat kecepatan transfer data dan jangkauan area pembacaan, yaitu label *low* frekuensi, label *high* frekuensi dan label *ultra-high* frekuensi **(Christoph, 2013)**. Sedangkan berdasarkan kemampuan baca tulis, label RFID dibagi menjadi 5 kelas, yaitu CLASS 0/I (hanya *read only* dan *factory programed*), CLASS II *(write once, read only, factory or user programmed),* CLASS III (memiliki kemampuan *read* dan *write),* CLASS IV *(read, write* dan memiliki *onboard sensor* seperti sensor suhu/gerak)*,* CLASS V *(read, write,* dan mempunyai *integrated transmitter)* sehingga dapat berkomunikasi dengan label atau *device* lain **(Fadhly, 2008)**.

Metode pengiriman data untuk label RFID pasif dibagi menjadi 2, yaitu *inductive coupling* dan *propagation coupling.* Pada metode *inductive coupling* lilitan tembaga dari unit *reader* berfungsi sebagai pembangkit medan elektromagnetik. Setiap label RFID yang berada pada jangkauan medan elektromagnetik ini akan terinduksi oleh medan ini. Hasil induksi inilah yang akan menjadi sumber energi bagi label untuk mengirimkan data kembali pada unit *reader* dengan jarak yang relatif dekat (dalam cm)*.* Sedangkan pada metode *propagation coupling,* unit *reader* berfungsi untuk memancarkan energi elektromagnetik (gelombang radio), kemudian label RFID akan mengumpulkan energi gelombang radio tersebut sebagai sumber daya untuk memantulkan sinyal balikan yang karakteristiknya sudah diubah sesuai dengan data pada label **(Heri, 2011)**.

1.2 Kriptografi

Kriptografi atau *Cryptography* adalah gabungan sebuah seni dan ilmu pengetahuan untuk membuat sebuah komunikasi yang tidak dapat dimengerti oleh semua pihak kecuali pihak tertentu yang diinginkan **(Enas & Farah, 2014).** *Cipher* merupakan persamaan matematik dalam proses enkripsi dan dekripsi untuk mengodekan suatu informasi menjadi informasi lain. Proses enkripsi bertujuan untuk menyembunyikan informasi asli *(plaintext)* menjadi informasi terenkripsi *(ciphertext)*, sedangkan proses dekripsi bertujuan untuk menerjemahkan kembali *ciphertext* menjadi *plaintext* **(Jati, 2005)**. Berdasarkan perkembangannya, kriptografi diklasifikasikan menjadi dua jenis, yaitu kriptografi klasik dan kriptografi modern **(Mohammad, 2014)**.

Kriptografi klasik merupakan sebuah metode kriptografi berbasis karakter yang memanfaatkan proses substitusi (mengganti nilai karakter) atau proses transposisi (menggeser nilai karakter). Kriptografi klasik dapat digunakan sebagai sarana untuk memahami konsep dasar dari kriptografi modern. Beberapa contoh metode kriptografi klasik antara lain *reverse cipher, zig-zag cipher,* dan *Ceasar Cipher.*

Kriptografi modern merupakan sebuah metode kriptografi berbasis bit data. Proses substitusi dan proses transposisi diterapkan terhadap setiap bit (nilai biner) dari setiap data yang akan diproses. Algoritma dari kriptografi modern sangat kompleks sehingga waktu eksekusi dari setiap data yang akan diproses relative lebih lama dan pengetahuan khusus terhadap ilmu matematika diperlukan untuk dapat memahami kriptografi modern. Beberapa contoh metode kriptografi modern antara lain AES dan DES.

1.3 *Ceasar Cipher* (Kriptografi Klasik)

Ceasar Cipher adalah sebuah metode enkripsi paling pertama ditemukan dan digunakan oleh Julius Ceasar dan tentaranya pada saat terjadi perang Gaul tahun 50 SM. Cara kerja dari algoritma ini ialah dengan memanfaatkan proses substitusi ke dalam sebuah surat, kalimat atau kumpulan kata-kata sehingga terbentuk sebuah kumpulan huruf yang tidak dapat dimengerti oleh siapapun **(Yusuf, Ferina, Donny, Lia, & Septiawan, 2014)**.

Ceasar Cipher merupakan sebuah tipe *cipher* dimana setiap huruf dari *plaintext* diubah dengan huruf alphabet lain yang sebelumnya sudah dipetakan dengan urutan angka dimulai dari memetakan huruf A dengan angka nol (A=0), kemudian huruf B=1, C=2, D=3 hingga Z=25. Proses pengkodean *(ciphering)* dari metode *Ceasar Cipher* dibentuk oleh dua persamaan, yaitu:

a. Persamaan Enkripsi

$$(Cx) = (Px) + (k)\ mod\ 26 \quad (1)$$

b. Persamaan Dekripsi

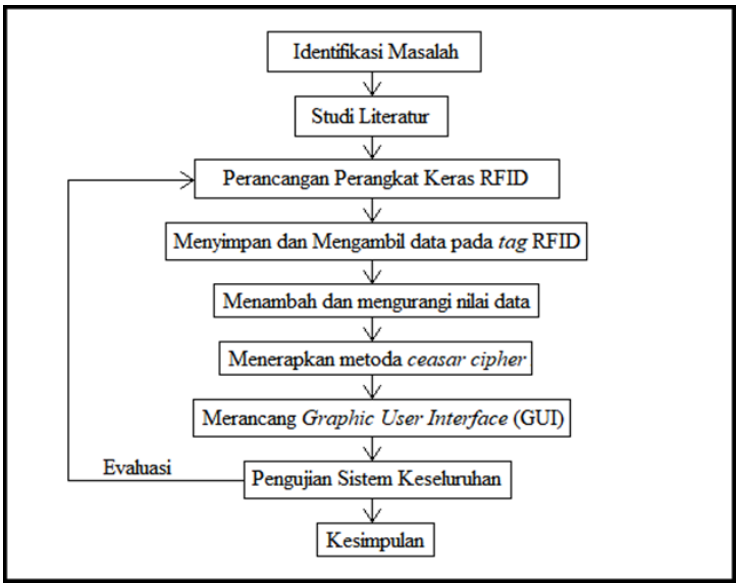
$$(Px) = (Cx) - (k)\ mod\ 26 \quad (2)$$

Dengan (Cx) adalah nilai desimal karakter *ciphertext* (data terenkripsi) ke-i, (Px) adalah nilai desimal karakter *plaintext* (data asli) ke-i, (k) adalah nilai desimal karakter *key* (kunci) ke-i dan *mod 26* adalah modulus dari jumlah karakter alfabet yaitu 26 **(Galih & Entik, 2016).**

2. METODOLOGI DAN PERANCANGAN SISTEM

2.1 Metodologi Penelitian

Proses pelaksanaan penelitian ini dilakukan dengan tahapan-tahapan yang digambarkan dalam diagram alir *(Flowchart)* pada Gambar 1.



Gambar 1. Diagram Alir Metodologi Penelitian

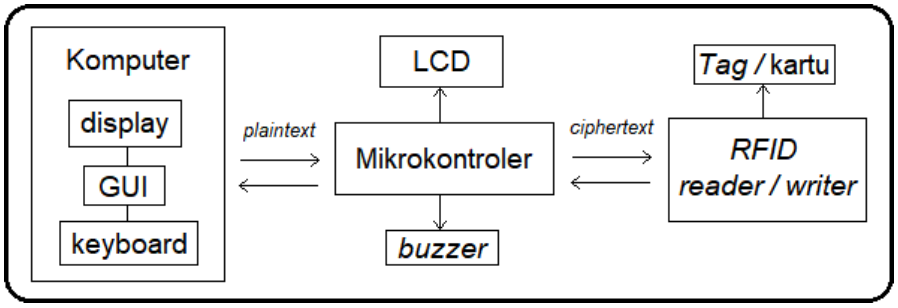
Identifikasi masalah dilakukan untuk mengetahui berbagai masalah yang mungkin muncul saat melakukan penelitian, seperti bagaimana cara menambah nilai data pada *tag* RFID, dll. Studi literatur dilakukan dari jurnal-jurnal terkait mengenai pemanfaatan teknologi RFID dan jurnal mengenai sistem keamanan data. Metode *Ceasar Cipher* dipilih sebagai algoritma enkripsi data dikarenakan oleh kecepatan proses data yang hampir instan jika dibandingkan dengan algoritma enkripsi modern (seperti AES/MARS) yang memerlukan waktu pemrosesan data hingga beberapa detik dan dapat memperpanjang durasi/waktu *tapping* kartu.

2.2 Penjelasan Umum Sistem

Autentifikasi setiap *tag* RFID harus dilakukan supaya *tag* tersebut dapat dikenali oleh sistem. Pengisian nilai nominal uang dapat dilakukan dengan bantuan GUI *(Graphic User Interface)* pada peranti komputer setelah *tag* berhasil diautentifikasi. Proses enkripsi data dilakukan untuk mengubah nilai nominal uang yang akan disimpan pada *tag* menjadi data terenkripsi. Proses dekripsi data dilakukan untuk mengubah data terenkripsi menjadi nilai nominal uang kembali. Jika nilai nominal uang yang tersimpan pada *tag* RFID mencukupi untuk proses transaksi, maka akan dilakukan pemotongan saldo sebesar nilai nominal yang diinputkan pada GUI. Pengisian saldo *(Top up)* dapat dilakukan kembali untuk menambah nilai nominal pada *tag*.

2.3 Perancangan Perangkat Keras

Sistem keamanan dengan metode *Ceasar Cipher* akan diimplementasikan pada sistem pembayaran elektronik yang dirancang dengan blok diagram sistem seperti yang terlihat pada Gambar 2.

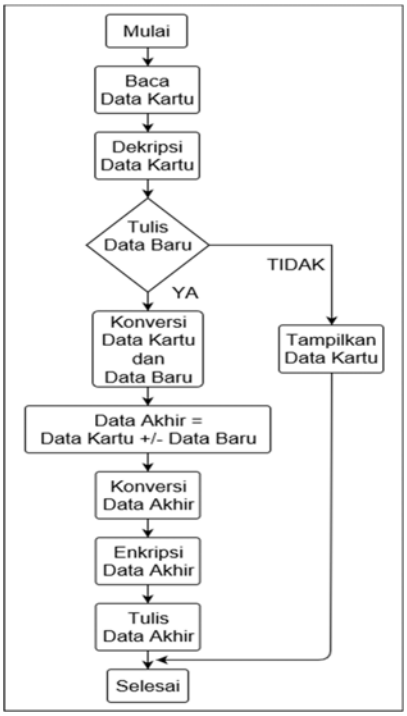


Gambar 2. Blok Diagram Perangkat Keras Sistem

Berdasarkan Gambar 2, sistem diintegrasikan dengan peranti komputer yang berfungsi sebagai *display* dan antarmuka melalui GUI *(Graphic User Interface)* yang akan diprogram dengan menggunakan *software* Visual Basic 2008 Express. Fungsi keseluruhan dari GUI yaitu untuk mempermudah pengiriman perintah untuk proses baca/tulis data pada kartu RFID. Pada proses penulisan, data berupa *plaintext* (data asli) akan dienkripsi terlebih dahulu pada mikrokontroler untuk menghasilkan *ciphertext* (data terenkripsi) kemudian data tersebut akan dikirim ke unit RFID untuk dituliskan pada *tag*. Pada proses pembacaan, data berupa *ciphertext* akan didekripsi pada mikrokontroler untuk menghasilkan *plaintext* kembali sebelum pada akhirnya dikirim ke peranti komputer untuk ditampilkan pada *display*. LCD dan *Buzzer* digunakan sebagai perangkat untuk menampilkan informasi transaksi berupa informasi *Audio* dan *Visual.*

2.4 Perancangan Perangkat Lunak

Gambar 3 merupakan diagram alir dari perangkat lunak sistem yang dirancang.



Gambar 3. Diagram Alir Perancangan Perangkat Lunak

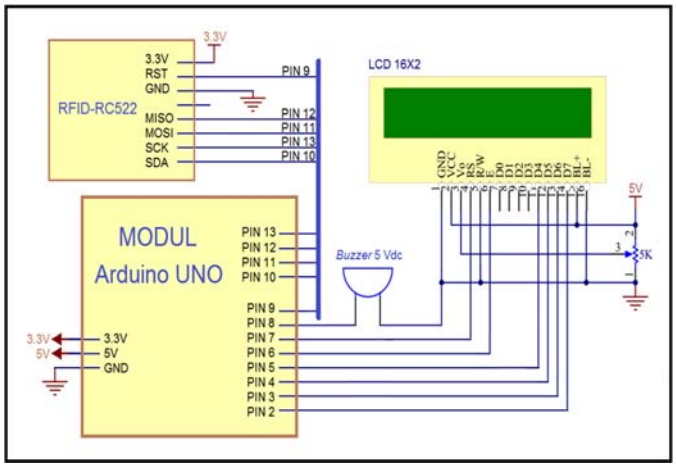
Berdasarkan Gambar 3, alur kerja sistem terdiri dari beberapa tahap yang dimulai dari melakukan pembacaan nilai Data_Kartu dilanjutkan dengan melakukan dekripsi pada nilai Data_Kartu kemudian menampilkan nilai hasil dekripsi pada *display*. Jika terjadi proses penulisan terhadap Data_Baru maka hasil dekripsi dari nilai Data_Kartu tidak akan ditampilkan pada *display*, namun akan dilakukan konversi tipe data dari tipe karakter menjadi tipe *integer* (konversi tipe data dilakukan untuk nilai Data_Kartu dan Data_Baru). Operasi penjumlahan (proses tambah saldo) atau pengurangan (proses bayar tagihan) dilakukan terhadap nilai Data_Kartu dan Data_Baru untuk menghasilkan nilai Data_Akhir. Nilai Data_Akhir yang masih bertipe *integer* dikonversi menjadi tipe karakter kembali, kemudian dilakukan proses enkripsi terhadap nilai Data_Akhir dan melakukan proses penulisan data ke dalam *tag*.

2.5 Realisasi Perangkat Keras

Berdasarkan perancangan pada Gambar 2, digunakan beberapa perangkat yang diuraikan pada Tabel 1. Diagram skematik dari perangkat keras yang direalisasikan dapat dilihat pada Gambar 4.

Tabel 1. Perangkat Keras yang Digunakan

No	Jenis Komponen	Fungsi
1	RFID-RC522	Unit pembaca /penulis *tag* RFID
2	MIFARE Classic Tag S50 1kbyte	*Tag* (media penyimpan data)
3	Arduino UNO	Pengolah data
4	LCD 16x2	Tampilan Visual
5	Buzzer	Tampilan Suara

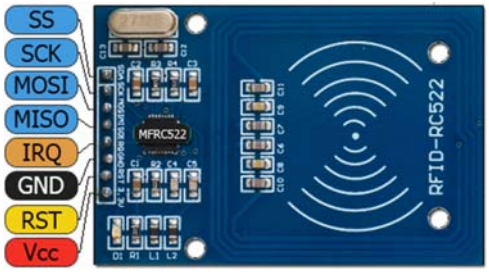


Gambar 4. Diagram Skematik Perangkat Keras

2.5.1 RFID-RC522

RFID-RC522 merupakan sebuah *reader/writer* terintegrasi untuk melakukan komunikasi nirkabel dan bekerja pada frekuensi 13.56 Mhz. Modul RFID-RC522 menggunakan *chipset* MFRC522 *Contacless Reader/Writer IC* dan jarak deteksi sekitar 5 cm. Kecepatan transfer data dari modul RFID ini adalah 848 kbps dan kebutuhan *power supply* minimal 2.5 – 3.3

volt. Modul RFID ini memiliki fitur antarmuka SPI *(Serial Peripheral Interface)* pada kecepatan 10 Mbit/s. Konfigurasi pin dari modul RFID-RC522 dapat dilihat pada Gambar 5.



Gambar 5. Konfigurasi Pin RFID-RC522

2.5.2 Tag MIFARE Classic S50 1kbyte

MIFARE *Classic* merupakan sebuah *device* memori penyimpanan *(Memory Storage Device)* yang dibagi menjadi beberapa sektor dan mempunyai mekanisme keamanan untuk akses kontrol. Label MIFARE *Classic* pada umumnya digunakan untuk dompet elektronik, tiket transportasi, kartu ID atau sebagai kunci akses kontrol. Spesifikasi dari kartu MIFARE *Classic* 1k ialah memiliki frekuensi operasi 13,56 Mhz, EEPROM 1 kbyte yang dibagi menjadi 16 Sektor, ketahanan data dapat mencapai sekitar 10 tahun, ketahanan *re-Write* data sekitar 200 ribu kali. Gambar 6 menunjukkan contoh kartu MIFARE *Classic* 1 kbyte.

Gambar 6. Kartu MIFARE Classic 1 kbyte

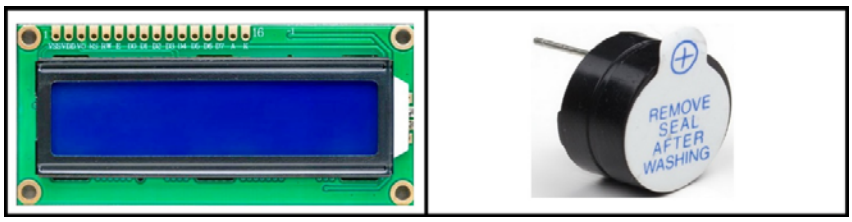
2.5.3 Arduino UNO

Arduino merupakan perangkat elektronik pengganti sistem minimum mikrokontroler secara keseluruhan. Pemrograman dilakukan dengan menggunakan bahasa C/C++ dan kode program dapat langsung diunggah melalui port-USB. Selain dapat digunakan sebagai port untuk melakukan komunikasi serial, port-USB dapat difungsikan sebagai catu daya. Arduino UNO menggunakan mikrokontroler AVR seri ATMega328, dengan jumlah pin I/O sebanyak 20, yaitu 6 pin untuk *input* analog dan 14 pin untuk *input/output* digital. Perangkat *(board)* Arduino UNO ditunjukkan pada Gambar 7.

Gambar 7. Arduino UNO

2.5.4 LCD dan *Buzzer*

LCD 16x2 digunakan untuk menampilkan informasi dari hasil Cek Saldo, Tambah Saldo, Bayar Tagihan dan Pendaftaran Kartu. *Buzzer* berfungsi sebagai pemberi informasi suara ketika transaksi yang dilakukan berhasil atau gagal. Gambar 8 merupakan bentuk fisik dari LCD dan *Buzzer* yang digunakan.



(a) **(b)**

Gambar 8. (a) LCD 16x2 dan (b) Buzzer

2.6 Realisasi Perangkat Lunak

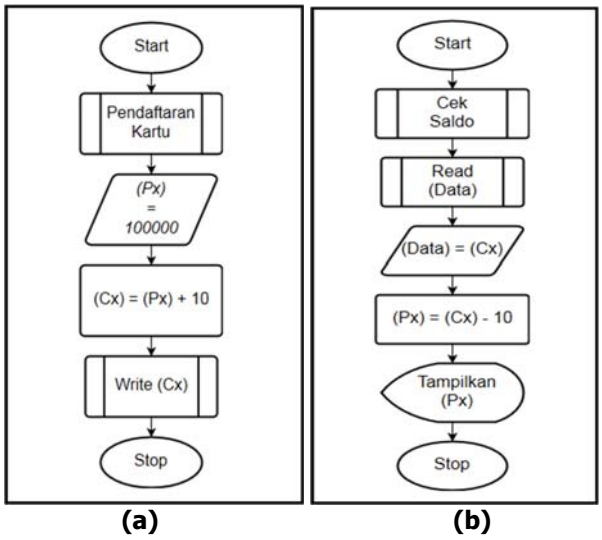
Enkripsi data dilakukan untuk mengubah *plaintext* (nilai nominal uang) menjadi *ciphertext* (data terenkripsi). Karakter-karakter dari tabel ASCII digunakan sebagai patokan untuk memetakan nilai dari setiap karakter *Ceasar Cipher*. Jumlah keseluruhan karakter di dalam tabel ASCII berjumlah 256 karakter, namun yang akan digunakan dalam penelitian ini hanya berjumlah 20 karakter yang dapat dilihat pada Tabel 2.

Tabel 2. Pemetaan Nilai Setiap Karakter dari Tabel ASCII

Karakter	Nilai Desimal	Nilai Heksadesimal	Karakter	Nilai Desimal	Nilai Heksadesimal
0	48	0x30	:	58	0x3A
1	49	0x31	;	59	0x3B
2	50	0x32	<	60	0x3C
3	51	0x33	=	61	0x3D
4	52	0x34	>	62	0x3E
5	53	0x35	?	63	0x3F
6	54	0x36	@	64	0x40
7	55	0x37	A	65	0x41
8	56	0x38	B	66	0x42
9	57	0x39	C	67	0x43

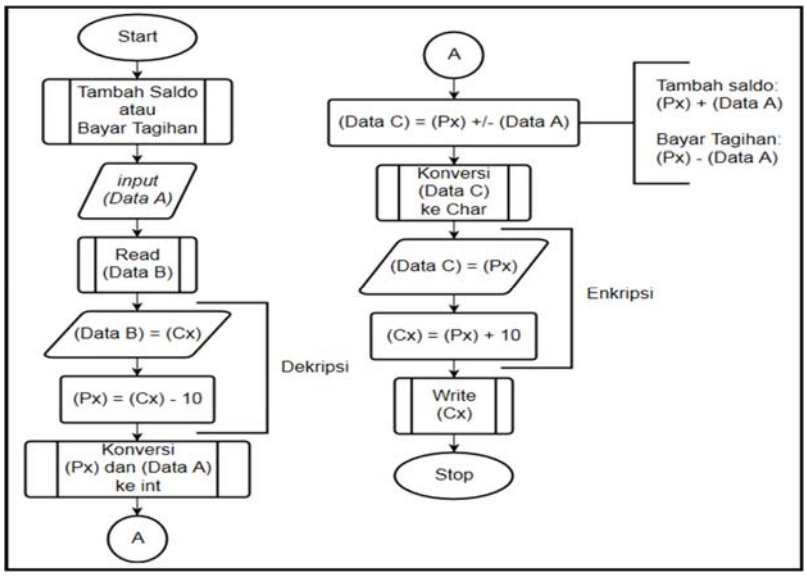
Terdapat 4 proses utama dari sistem secara keseluruhan yaitu, proses pendaftaran kartu, cek saldo, tambah saldo dan bayar tagihan. Enkripsi data dilakukan pertama kali saat proses pendaftaran kartu. Data berupa *plaintext* dienkripsi menjadi *ciphertext* kemudian langsung dituliskan ke dalam *tag*. Proses dekripsi tidak dilakukan pada tahap ini sehingga diagram alir enkripsi data saat proses pendaftaran kartu seperti yang terlihat pada Gambar 9.

Berdasarkan Gambar 9 (a), setiap kartu yang didaftarkan akan diberi saldo awal *(plaintext*) sebesar Rp 100.000. Kunci (*k*) yang digunakan untuk menggeser nilai karakter dari *plaintext* adalah 10, maka *ciphertext* (Cx) sebagai data yang akan dituliskan ke dalam *tag* RFID adalah (Cx) = (Px) + 10 = ;::::: yaitu susunan karakter sesuai dengan pemetaan nilai dari tabel ASCII. Berdasarkan Gambar 9 (b), proses cek saldo dimulai dari pembacaan data pada *tag* yang masih berupa *ciphertext* (Cx), kemudian data tersebut diolah dengan persamaan didekripsi data (Px) = (Cx) – 10 untuk menghasilkan *plaintext* (Px) yang akan ditampilkan pada *display.*



Gambar 9. (a) Diagram Alir Enkripsi Data saat Proses Pendaftaran Kartu (b) Diagram Alir Dekripsi Data saat Proses Cek Saldo

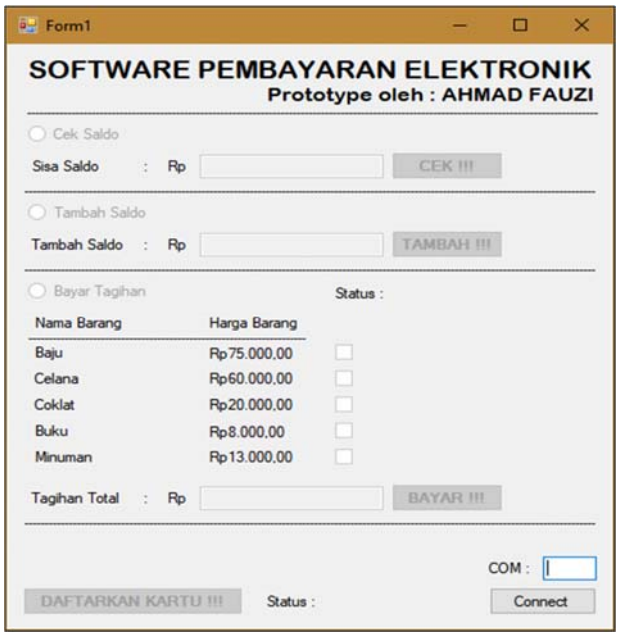
Berdasarkan Gambar 10, diagram alir proses tambah saldo dan/atau bayar tagihan dimulai dengan memasukan *input* nilai nominal dengan *keyboard* (Data A) sebagai data untuk menambah/mengurangi nilai saldo pada *tag*. *Read tag* dilakukan untuk mengambil nilai pada *tag* (Data B) yang berupa *ciphertext*, kemudian didekripsi untuk menghasilkan *plaintext* (Px) dengan persamaan (Px) = (Cx) – 10.



Gambar 10. Diagram Alir Proses Tambah Saldo dan Bayar Tagihan

Tahap selanjutnya adalah melakukan konversi tipe data (Px) dan (Data A) ke dalam tipe *integer*, kemudian dilakukan proses penjumlahan atau pengurangan (untuk proses tambah saldo atau bayar tagihan) untuk menghasilkan (Data C). (Data C) sebagai *plaintext* (Px) dikonversi kembali ke dalam tipe karakter (Char) dan dienkripsi menjadi *ciphertext* (Cx) dengan persamaan (Cx) = (Px) + 10. Proses penulisan data ke dalam *tag* dilakukan terhadap (Data C) yang telah terenkripsi. Tampilan GUI sistem pembayaran elektronik secara

keseluruhan yang dirancang dengan menggunakan bantuan *software* Microsoft Visual Basic 2008 Express dapat dilihat pada Gambar 11.



Gambar 11. Tampilan GUI yang direalisasikan

3. PENGUJIAN DAN ANALISIS

Beberapa tahap pengujian dilakukan untuk mengetahui apakah sistem pembayaran elektronik yang telah direalisasikan dapat bekerja sesuai dengan harapan. Pengujian tersebut meliputi pengujian sistem pembayaran elektronik secara keseluruhan yang dimulai dari proses pendaftaran kartu/*tag,* cek saldo, tambah saldo, bayar tagihan serta melakukan pengujian metode *Ceasar Cipher* (enkripsi data) yang telah diimplementasikan.

3.1 Pengujian Sistem Pembayaran Elektronik

Autentikasi atau pendaftaran kartu harus dilakukan terlebih dahulu sebelum melakukan proses yang lain seperti cek saldo atau tambah saldo. Jika kartu belum terdaftar maka setiap transaksi yang dilakukan akan ditolak, saldo awal sebesar Rp 100.000 diberikan kepada setiap kartu yang melakukan proses pendaftaran. Gambar 12 merupakan tampilan ketika dilakukan pengecekan saldo terhadap kartu yang telah terdaftar.

(a) **(b)**

Gambar 12. Tampilan Pengujian Cek Saldo
(a) Tampilan GUI (b) Tampilan LCD

Pengujian proses tambah saldo sebesar Rp 35.000 berhasil dilakukan, hal ini dapat dikonfirmasi melalui pengecekan saldo kembali seperti yang terlihat pada Gambar 13.

(a) **(b)**

Gambar 13. Tampilan Pengujian Tambah Saldo
(a) Tambah saldo (b) Cek Saldo

Pengujian proses pembayaran dapat dillihat pada Gambar 14 dengan tagihan Rp 116.000.

(a) **(b)**

Gambar 14. Tampilan Proses Pembayaran Berhasil
(a) Tampilan GUI (b) Tampilan LCD

Setelah melakukan transaksi pembayaran sebesar Rp 116.000 maka jumlah saldo yang terdapat pada kartu menjadi Rp 19.000. Proses bayar tagihan dilakukan kembali dengan tagihan total sebesar Rp 20.000. Sisa saldo pada *tag* tidak mencukupi untuk melakukan transaksi pembayaran. Gambar 15 memperlihatkan tampilan ketika saldo pada kartu tidak mencukupi untuk melakukan pembayaran.

(a) **(b)**

Gambar 15. Tampilan Proses Pembayaran Gagal
(a) Tampilan GUI (b) Tampilan LCD

Pengujian batas maksimum nilai saldo dilakukan dengan cara melakukan penambahan nominal sebesar Rp 4.294.967.295 dan jika penambahan saldo masih tetap dilakukan maka saldo berubah menjadi Rp 0 (nol) kembali seperti yang terlihat pada Gambar 16.

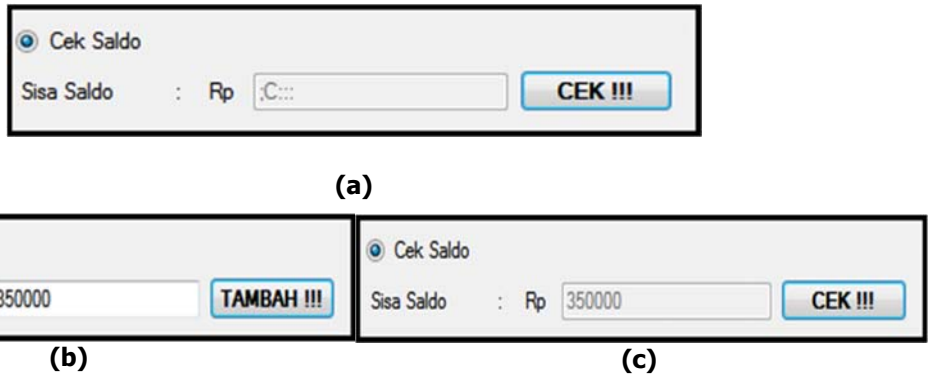
(a) **(b)**

Gambar 16. Batas Maksimum Penambahan Saldo
(a) Batas Maksimum (b) Batas Minimum

Hal ini menunjukan bahwa tipe data yang digunakan dalam pemrograman dapat mempengaruhi jumlah maksimum penambahan saldo. Rentang nilai batas minimum dan batas maksimum dari tipe data yang digunakan *(unsigned long integer)* adalah dari 2^0-1 hingga 2^{32}-1, sehingga batas maksimum penambahan saldo dari sistem yang telah direalisasikan adalah Rp 4.294.967.295. Pada pengembangan penelitian lebih lanjut, sebaiknya penambahan nilai saldo dibatasi hanya sampai 1 juta, hal ini dilakukan untuk mencegah berubahnya nilai saldo menjadi Rp 0 (nol) kembali dan untuk memperkecil resiko kerugian jika seandainya kartu hilang.

3.2 Pengujian Metode *Ceasar Cipher* (Enkripsi Data)

Pengujian dilakukan dengan menggunakan unit RFID *reader* lain yang diprogram untuk melakukan proses baca/tulis kartu *(read/write)*. Proses pengujian ini dilakukan dengan menggunakan GUI yang sama dan bertujuan untuk mengetahui apakah metode *Ceasar Cipher* dapat bekerja sesuai dengan harapan. Gambar 17 menunjukkan hasil yang diperoleh ketika proses cek saldo *(read)* dan tambah saldo *(write)* dilakukan oleh unit RFID lain.



(a)

(b) **(c)**

Gambar 17. Pengujian Enkripsi Data dengan Unit RFID Lain
(a) Tampilan Cek Saldo 1 (b) Tampilan Tambah Saldo
(c) Tampilan Cek Saldo 2

Berdasarkan Gambar 17, sisa saldo dari kartu yang digunakan pada pengujian sebelumnya sebesar Rp 19.000 berubah menjadi data terenkripsi yaitu simbol ;C::: (Gambar 17a), jika dibandingkan terhadap tabel ASCII maka dengan persamaan dekripsi data dan kunci (k) = 10, diperoleh:

Persamaan Dekripsi Data :

(Px) = (Cx) – k (1)

(Cx) = ;C::: dan (k) = 10, maka:
(Px) = (;C:::) – 10

→ konversi (Cx) ke dalam desimal, maka:

(Px) = (59-10), (67-10), (58-10), (58-10), (58-10)
(Px) = (49), (57), (48), (48), (48)

→ jika dikonversi ke dalam karakter kembali, maka:

(Px) = 19000

Kemudian proses penulisan data sebesar Rp 350.000 berhasil dilakukan (Gambar 17b), hal ini dapat dikonfirmasi melalui pengecekan saldo kembali (Gambar 17c), namun ketika transaksi pembayaran sebesar Rp 176.000 dilakukan kembali dengan unit RFID asli, setiap proses/transaksi pembayaran akan selalu ditolak, hal ini menunjukan bahwa sistem yang direalisasikan telah bekerja sesuai dengan harapan (Gambar 18).

Gambar 18. Penolakan Transaksi Pembayaran Dengan Unit RFID Asli

Ketika penulisan nilai nominal uang dengan RFID lain sebesar Rp 350.000 berhasil dilakukan, maka proses dekripsi data yang dilakukan oleh RFID asli ialah:

(Px) = (Cx) – k

(Cx) = 350000 dan (k) = 10
(Px) = (350000) – 10

→ konversi ke dalam desimal, maka:

(Px) = (51-10), (53-10), (48-10), (48-10), (48-10), (48-10)
(Px) = (41), (43), (38), (38), (38), (38)

→ jika dikonversi ke dalam karakter , maka:

(Px) =)+&&&&

Dari hasil dekripsi data terlihat bahwa nilai (Px) berubah menjadi)+&&&& , sehingga nilai (Px) tidak dapat dikonversi menjadi nilai bilangan atau tipe *integer*. Hal ini menunjukan bahwa sistem telah bekerja sesuai dengan harapan, karena dengan berubahnya nilai (Px) menjadi karakter)+&&&& mengakibatkan data yang akan diproses menjadi tidak sesuai dan algoritma pemrograman yang direalisasikan akan langsung menghentikan transaksi ketika *input* data yang diperoleh tidak dapat dikonversi ke dalam tipe *integer*.

4. KESIMPULAN

Berdasarkan dari hasil pengujian dan analisis, dapat diambil kesimpulan sebagai berikut:

1. Sistem yang telah dirancang mampu menambah dan mengurangi nilai nominal yang terdapat di dalam kartu RFID dari Rp 0 - Rp 4.294.967.295.
2. Batas maksimum penambahan nilai bilangan (penambahan saldo) ditentukan oleh tipe data yang digunakan dalam pemrograman.
3. Metode *Ceasar Cipher* dapat digunakan sebagai algoritma untuk proses enkripsi dan dekripsi dengan pemetaan nilai setiap karakter melalui tabel ASCII.
4. Setiap transaksi akan ditolak secara permanen, jika nilai data yang terdapat di dalam *tag* dimodifikasi menggunakan unit RFID lain.

DAFTAR RUJUKAN

Christoph, J. (2013, Juli 25). *A Survey Paper on Radio Frequency Identification (RFID) Trends*. Retrieved Juli 25, 2017 at 03.04 pm, from http://www.cse.wustl.edu/~jain/cse574-06/ftp/rfid/index.html

Enas, I. I., & Farah, A. (2014). Enhancement Ceasar Cipher for Better Security. *IOSR Journal of Computer Engineering, 16*(3), 01-05.

Fadhly, H. (2008). *Sistem Absensi Menggunakan Teknologi RFID.* Depok: Departemen Teknik Elektro Fakultas Teknik Universitas Indonesia.

Galih, F. R., & Entik, I. (2016, May). *Implementasi algoritma chiper caesar untuk enkripsi dan dekripsi pada tabel ascii menggunkan bahasa java*. Retrieved april 15, 2018 at 03.17 pm, from https://www.researchgate.net/publication/303382290_implementasi_algoritma_chiper_caesar_untuk_enkripsi_dan_dekripsi_pada_tabel_ascii_menggunkan_bahasa_java

Heri, R. (2011). *Perancangan dan Implementasi untuk salah satu Aplikasi Biling Subsidi BBM menggunakan RFID dan Visual Basic 6.0.* Bandung: Jurusan Teknik Elektro Fakultas Teknologi Industri Institut Teknologi Nasional.

Jati, S. (2005). Pengamanan Data Informasi menggunakan Kriptograpfi Klasik. *Jurnal Teknologi Informasi DINAMIK, 10*(3), 160-167.

Marcel, F. (2011). *RFID techniques for indoor warehouse location sensing.* Amsterdam: Vrije Universiteit Artificial Intelligence Department.

Mohammad, I. D. (2014, Desember 25). *Perbandingan Kriptographi Klasik (Ceasar Cipher) dan Kriptographi Modern (MD5)*. Retrieved Desember 25, 2017 at 02.45 pm, from https://www.researchgate.net/publication/303382769_Perbandingan_Kriptograpfi_Klasik_Ceasar_Cipher_dan_Kriptografi_Modern_MD5

Sarita, K. (2017). A Research Paper on Criptography Encryption and Compression Techniques. *International Journal of Engineering And Computer Science, 6*(4), 20915-20919.

Yusuf, T., Ferina, F., Donny, A. B., Lia, A., & Septiawan. (2014). Implementasi Algoritma Ceasar, Cipher Disk, dan Scytale pada Aplikasi Enkripsi dan Dekripsi Pesan Singkat, LumaSMS. *Prosiding Seminar Ilmiah Nasional Komputer dan Sistem Intelijen (KOMMIT 2014). 8*, pp. 467-472. Depok: Universitas Gunadarma.