Jurnal Coding Sistem Komputer Untan ISSN 2338-493X
Volume 03, No. 3 (2015), hal 67-78

PROTOTIPE PEMROSESAN INFORMASI TERENKRIPSI DENGAN KRIPTOGRAFI VIGENERE MELALUI SINYAL RADIO KOMERSIL

[1]Dhea Novita, [2]Dedi Triyanto, [3]Yulrio Brianorman
[1] [2] [3]Jurusan Sistem Komputer, Fakultas MIPA Universitas Tanjungpura

Jl. Prof. Dr. H. Hadari Nawawi, Kalimantan Barat, 78115
Telp./Fax.: (0561) 577963
e-mail:
[1]dheanovita2112@gmail.com, [2]dedi.triyanto@siskom.untan.ac.id
[3]yulrio.brianorman@siskom.untan.ac.id

ABSTRAK

Radio komersil menggunakan modulasi frekuensi (FM) dalam pengiriman sinyal analog pembawa data suara dalam rentang 88 MHz hingga 108 MHz. Informasi digunakan oleh kepolisian melalui radio komersil rentan terhadap tindak penyadapan. Kriptografi merupakan teknik untuk melindungi dan menjaga kerahasiaan informasi agar terhindar dari orang yang tidak berhak atas informasi tersebut. Oleh karena itu, didapat gagasan penelitian untuk mengirim data karakter (ASCII) yang telah dienkripsi menggunakan metode Kriptografi Vigenere dalam bentuk suara dan dikirim melalui sinyal radio komersil. Penelitian ini menggunakan perangkat keras mikrokontroler Arduino Uno dan sensor suara dengan IC LM393 untuk mendeteksi sinyal bunyi dan memberikan keluaran berupa sinyal digital yang terhubung pada Port A0 Arduino Uno. Hasil dari pengolahan pola bunyi dikirim ke aplikasi antarmuka dengan komunikasi serial melalui Port USB. Aplikasi pengirim dapat bekerja secara manual yaitu dengan menekan tombol kirim manual dan dapat bekerja otomatis saat menit ke-0, 15, 30 dan 45. Keluaran aplikasi pengirim adalah bunyi pendek untuk bit dengan logika 0 dan bunyi panjang untuk bit dengan logika 1. Pada penelitian ini proses pengenalan pola bunyi menggunakan aplikasi penerima dengan keberhasilan sebesar 86% dalam 5 sampel berbeda dengan 10 kali percobaan. Hal ini membuktikan bahwa aplikasi dapat menjaga integritas informasi yang dikirim melalui radio komersil.

Kata Kunci: Arduino Uno, pengolahan bunyi, Kriptografi Vigenere, radio komersil, transmisi radio

1. PENDAHULUAN

Bunyi adalah suatu keadaaan dimana terdapat zat yang bergetar sehingga memiliki frekuensi tertentu. Bunyi dapat dihasilkan dari sinyal digital atau sinyal analog. Bunyi dapat diolah dan dikenali oleh komputer menggunakan metode pengolahan sinyal digital. Sebelumnya telah dilakukan penelitian yaitu "Pengenalan Nada Suling Recorder Menggunakan Fungsi Jarak Chebyshev", sehingga penelitian tersebut membuktikan bunyi dapat dikenali oleh komputer menggunakan metode pengolahan sinyal digital [1].

Pada kehidupan sehari-hari stasiun penyiaran radio komersil menggunakan bunyi dan mengirimkannya dalam bentuk sinyal analog dalam frekuensi radio tertentu misalnya 103,4 *Frequency Modulation* (FM). Radio komersil menggunakan modulasi frekuensi dalam pengiriman sinyal analog pembawa data suara dalam rentang 88 MHz hingga 108 MHz. Stasiun penyiaran menggunakan sinyal radio komersil melakukan aktivitas broadcasting yaitu kegiatan pemancarluasan siaran melalui sarana pemancaran dan sarana transmisi darat, laut dan antariksa menggunakan spektrum frekuensi sinyal radio yang berbentuk gelombang elektromagnetik dan merambat melalui udara, kabel atau media lainnya untuk dapat diterima secara serentak dan bersamaan oleh masyarakat menggunakan perangakat penerima siaran.

Saat ini informasi digunakan oleh kepolisian melalui radio rentan terhadap tindak penyadapan melalui radio komersil. Kriptografi merupakan teknik untuk melindungi dan

menjaga kerahasiaan informasi agar terhindar dari orang yang tidak berhak. Kriptografi adalah kajian ilmu untuk menjaga kerahasiaan informasi dengan cara merubah data ke dalam bentuk yang tidak dapat dimengerti secara langsung.

Kriptografi telah ada dan digunakan sejak berabad-abad yang lalu dikenal dengan istilah kriptografi klasik salah satunya adalah metode Kriptografi Vigenere. Kriptografi tersebut memiliki dua proses, yaitu enkripsi dan dekripsi yang membutuhkan kunci sebagai parameter untuk transformasi. Hasil dari kriptografi adalah sebuah bentuk yang berbeda dari informasi asli dan memiliki pola yang tidak teratur. Perubahan pada hasil tersebut dapat meningkatkan kesulitan pembacaan atau pemrosesan informasi yang tersimpan.

Berdasarkan penelitian yang dilakukan sebelumnya dan prinsip pengiriman bunyi melalui sinyal radio komersil, maka didapat gagasan penelitian untuk mengirim data karakter yang telah dienkripsi menggunakan metode Kriptografi Vigenere dalam bentuk suara untuk dikirim melalui sinyal radio komersil. Data karakter dapat berupa informasi alamat Tempat Kejadian Perkara (TKP) dikirim secara berlanjut dapat dimanfaatkan oleh kepolisian yang memerlukan informasi secara langsung dalam area yang luas. Misalnya terdapat pencurian kendaraan bermotor, maka informasi lokasi dapat disebarkan melalui aplikasi yang dibuat.

Setelah dilakukan penelitian, diharapkan dengan adanya prototipe ini informasi yang dapat secara langsung disebarkan pada jaringan kepolisian melalui radio komersil.

2. TINJAUAN PUSTAKA

Tinjauan pustaka memuat teori-teori dan kajian keilmuan yang berkaitan dengan penelitian ini dapat dijelaskan sebagai berikut:

2.1. Bunyi

Bunyi merupakan jenis gelombang yang dapat dirasakan oleh indera pendengaran (telinga). Bunyi adalah sesuatu yang dihasilkan dari benda yang bergetar. Benda yang menghasilkan bunyi disebut sumber bunyi. Sumber bunyi yang bergetar akan menggetarkan molekul-molekul udara yang ada disekitarnya. Ada beberapa syarat yang harus dipenuhi agar bunyi dapat terdengar yaitu ada benda yang bergetar (sumber bunyi), ada medium yang merambatkan bunyi dan ada penerima yang berada di dalam jangkauan sumber bunyi dan ada pendengar bunyi

Manusia mendengar bunyi saat terdapat getaran di udara atau medium lain hingga sampai ke gendang telinga manusia. Batas frekuensi bunyi yang dapat didengar oleh telinga manusia berkisar antara 20 Hz sampai 20 KHz pada amplitudo berbagai variasi dalam responnya. Pada penelitian ini, bunyi yang dikirim berupa suara panjang, suara pendek dan tanpa suara.

2.2. ASCII (*American Standard Code of Information Interchange*)

ASCII Adalah standar internasional dalam angka, huruf dan simbol Hex/Unicode, tetapi ASCII memiliki sifat lebih universal, misalnya 95 untuk karakter "_". Kode ASCII digunakan komputer untuk representasi teks. ASCII terdiri dari kode-kode bilangan biner berjumlah 8 bit. Dari bilangan 0000 0000 hingga 1111 1111. Jumlah kombinasi yang dihasilkan sebanyak 256, dimulai dari kode 0 hingga 255 dalam sistem bilangan Desimal.

2.3. Kode Vigenere

Kode Vigenere termasuk kode abjad majemuk (*polyalphabetic substitution cipher*). Dipublikasikan oleh diplomat Perancis, Blaise de Vigenere pada Abad 16, tahun 1586. Kode Vigenere digunakan oleh tentara Konfiderasi pada perang sipil amerika. Kode Vigenere menggunakan angka yaitu menukarkan huruf dengan angka [2].

Kriptografi Vigenere menggunakan *plaintext* pada yang dirubah menjadi bilangan desimal dan merubah kunci menjadi bilangan desimal. Kemudian *plaintext* dan kunci dijumlahkan sehingga data asli terenkripsi menjadi *ciphertext*.

Enkripsi Kode ASCII dengan Kriptografi Vigenere menggunakan rumus sebagai berikut:

$$E(pi) = v(pi, k(i \bmod m) + 1) \quad \text{.....(1)}$$

dengan:
pi = huruf ke-i dalam *plaintext*
kn = huruf ke-n dalam kunci
m = panjang kunci
i = indeks kunci

Setelah melakukan enkripsi, maka dapat dilakukan dekripsi Kode ASCII dengan Kriptografi Vigenere menggunakan rumus sebagai berikut:

$$D(ci) = v(ci, k(i \bmod m) + 1) \quad \text{.....(2)}$$

dengan:
ci = huruf ke-i dalam *ciphertext*
kn = huruf ke-n dalam kunci
m = panjang kunci
i = indeks kunci

2.4. Radio Komersil

Radio memiliki banyak fungsi pada perangkat elektronik, misalnya perangkat *blue-tooth* merupakan perangkat radio jarak terbatas untuk mengirim data. Radio juga digunakan sebagai sarana komersil pada masyarakat yaitu berupa stasiun radio komersil. Fungsi radio adalah sebagai media ekspresi, komunikasi, informasi, pendidikan dan hiburan. Radio juga berperan sebagai media komersil yaitu memenuhi kebutuhan dan kepentingan pen-dengarnya.

Berdasarkan uraian diatas, maka radio dapat digunakan untuk media komunikasi, informasi dan pendidikan oleh masyarakat. Dalam penelitian ini menggunakan perangkat radio *transmitter* untuk mengirimkan data suara secara cepat ke masyarakat.

2.5. Sinyal

Huilbert Kwakernaak menyatakan bahwa "Sinyal adalah sebuah fenomena yang muncul dari suatu lingkungan tertentu dan dapat dinyatakan secara kuantitatif" [3]. Dalam bidang telekomunikasi, sinyal dipergunakan pada perancangan pengirim dan penerima gelombang radio (*Radio Frequency Trans-ceiver*). Selain itu sinyal juga dapat digunakan untuk menganalisis modulasi sinyal, memilih media pengiriman yang tepat dan noise.

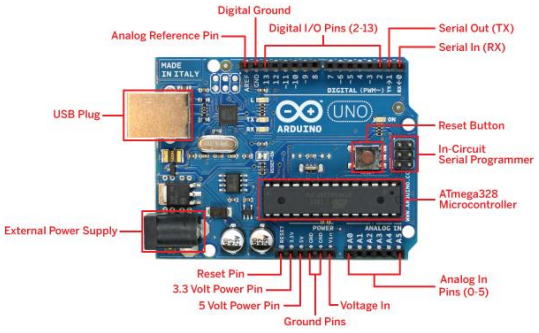
Sinyal dapat digunakan tidak hanya melalui udara, tetapi dapat diterapkan pada medium padat yaitu kabel sehingga pada umumnya menggunakan pemrosesan sinyal digital misal-nya pada komputer. Sinyal digital dapat diklasifikasikan berdasarkan sumbu waktunya yaitu sumbu yang kontinu dan sumbu diskrit.

Sinyal kontinu menggunakan bilangan riil dan sinyal diskrit menggunakan bilangan bulat. Karena menggunakan bilangan riil, maka sinyal kontinu didapatkan dengan kondisi sembarang waktu.

Sinyal diskrit adalah sinyal yang hanya ada pada waktu tertentu, misalnya ditentukan sampling selama 1 menit, maka didapatkan data sinyal diskrit. Sinyal diskrit dapat di-tentukan berdasarkan kondisi sumber waktu-nya yang berarti komponen sinyal harus berupa bilangan bulat sedangkan sinyalnya mungkin saja bernilai bilangan riil. Sinyal waktu diskrit dapat digunakan dalam keluaran sebuah *Port Analog to Digital Converter (ADC)* dari mikrokontroler untuk diproses lebih lanjut menggunakan komputer. Pada penelitian ini menggunakan sinyal diskrit, karena proses pengenalan suara dapat di-lakukan pada waktu tertentu.

2.6. Arduino

Pada penelitian ini, model Arduino Uno digunakan untuk mendapatkan nilai dari sensor suara dalam mendekripsi suara. *Port* yang digunakan adalah *ADC* sehingga sinyal analog berupa radio dapat diubah kedalam sinyal digital. Dalam proses mendekripsi data, nilai dari pembacaan *Port ADC* akan di-repre-sentasikan dengan pola bilangan biner yaitu sepanjang 8-bit. Bagian dan komponen dari Arduino Uno dapat dilihat pada Gambar 1.



Gambar 1. Model Minimum Sistem Arduino Uno

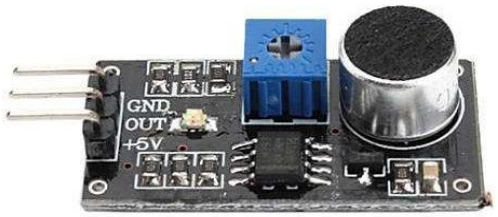
2.7. Sensor Suara

Dalam penelitian ini menggunakan sensor suara yang berfungsi untuk mendeteksi bunyi yang dikirim oleh radio *transmitter*) [4]. Suara yang di deteksi bernilai ada (logika 1) dan tidak ada (logika 0). Sensor mendeteksi lamanya bunyi yang dikirim pada waktu diskrit (n-*second*), kemudian lamanya bunyi tersebut akan dibedakan menjadi jenis suara panjang

dan jenis suara pendek. Sensor suara dapat dilihat pada Gambar 2.

Sensor tersebut bekerja pada *Port ADC* mikrokontroler. Dimensi panjang 32mm x lebar 17mm x tinggi 15mm. Chip utama (IC) LM393, mikrofon elektrik dan tegangan kerja 4 sampai 6 volt DC. Karakteristik dari sensor tersebut adalah sebagai berikut:

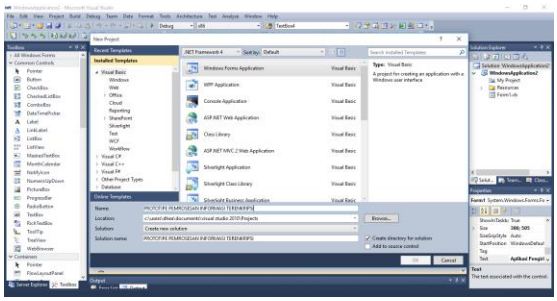
a. Memiliki sensitifitas dengan besaran variabel (potentiometer).
b. Sinyal keluaran yang valid dengan tegangan rendah (active low).
c. Ketika terdapat input suara, maka lampu menyala.
d. Output merupakan sinyal analog.



Gambar 2. Sensor Suara

2.8. Visual Basic

Visual Basic merupakan *Graphical User Inteface (GUI)* dari bahasa pemrograman Basic untuk membuat aplikasi desktop yang berjalan di sistem operasi windows. Pada penelitian ini, Visual Basic digunakan untuk membuat antar-muka aplikasi pengirim *(transmitter)* dan penerima (*receiver).* Tampilan dari Visual Basic dapat dilihat pada Gambar 3.

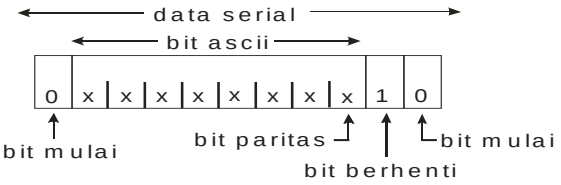


Gambar 3. Tampilan Visual Basic 2010

2.9. Komunikasi Serial

Komunikasi serial adalah komunikasi yang pengiriman datanya setiap bit secara berurutan dan bergantian. Komunikasi ini mempunyai suatu kelebihan yaitu hanya membutuhkan satu jalur dan kabel yang sedikit dibandingkan dengan komunikasi paralel.

Prinsip dari komunikasi serial adalah pengiriman data dilakukan pada setiap bit, sehingga kecepatan pengiriman lebih lambat dibandingkan komunikasi paralel, atau dengan kata lain komunikasi serial merupakan salah satu metode komunikasi data di mana hanya setiap bit data yang dikirimkan melalui seuntai kabel pada suatu waktu tertentu. Pengiriman data dengan komunikasi serial.



Gambar 4. Pengiriman Data Karakter dalam Komunikasi Serial

3. METODE PENELITIAN

Penelitian ini menggunakan metodologi yang mencakup studi pustaka dan studi literatur. Alat yang dibuat mengacu pada referensi yang telah ada untuk kemudian dilakukan pengembangan lebih lanjut. Kemudian dilakukan analisa dari kebutuhan perangkat keras dan perangkat lunak yang dibutuhkan dalam pembuatan sistem.

Perangkat keras yang dibutuhkan yaitu radio pengirim (*transmitter*) yang digunakan untuk mengirimkan suara dalam modulasi frekuensi (FM), radio penerima (*receiver*) digunakan untuk menerima suara yang dikirim oleh radio pengirim, headset dengan ukuran 3,5mm untuk menghubungkan sensor dan radio penerima, sensor suara dengan IC LM393 digunakan sebagai pendeteksi suara yang dihasilkan oleh radio penerima, Arduino Uno merupakan mikrokontroler mengolah data dalam bentuk suara yang berasal dari sensor suara kemudian Perangkat lunak yang dibutuhkan adalah Arduino IDE Versi 1.0.6., *GUI* bahasa pemrograman Basic, yaitu Visual Studio 2010 dan Sistem Operasi Windows 8.1 pada komputer.

Setelah dilakukan penyediaan perangkat keras dan perangkat lunak dalam penelitian ini, kemudian dilakukan perancangan sistem yaitu merancang sistem berdasarkan diagram blok yang sudah dibuat, mulai dari pembuatan alat, pembuatan program untuk menghubungkan Arduino dan komputer, hingga pembuatan aplikasi antarmuka pengirim dan penerima.

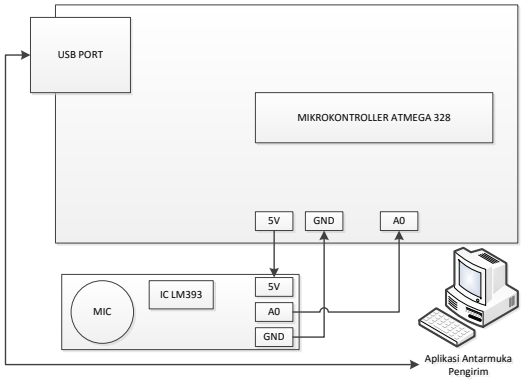
Kemudian dilakukan tahap integrasi dan pengujian terhadap perangkat keras dan perangkat lunak. Tahap yang terakhir adalah analisa hasil pengujian dari sistem, apakah sistem yang dibuat tersebut telah sesuai dengan apa yang diharapkan serta dilakukan analisa terhadap kelebihan dan kekurangan alat, apakah alat sudah sesuai dengan perancangan awal. Setelah dilakukan proses evaluasi dan penyempurnaan maka dilanjutkan ke tahap penerapan.

4. PERANCANGAN SISTEM

Perancangan sistem, melakukan tahap desain atau rancangan yang dibutuhkan dalam pembuatan aplikasi. Perancangan sistem di tinjau dari perangkat keras dan perangkat lunak yang digunakan dalam penelitian.

4.1. Diagram Blok Perangkat keras

Diagram blok perancangan sistem ditunjukkan pada Gambar 5.



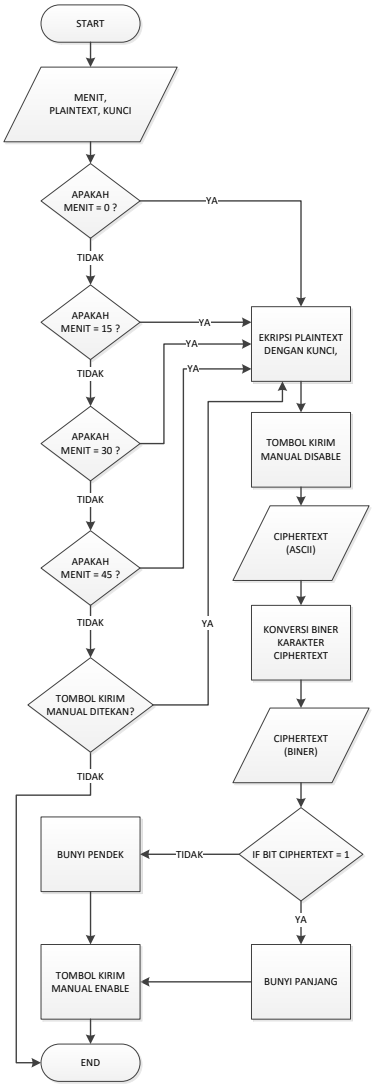
Gambar 5. Diagram Blok Perangkat keras

Penjelasan dari diagram blok perangkat keras adalah sebagai berikut:

a. Mikrokontroler ATMEGA 328 digunakan untuk memproses data yang masuk melalui *Port* analog "A0" dan mengeluarkan data komunikasi serial melalui *Port USB*.
b. Sensor suara dengan IC LM393 menggunakan tegangan sebesar 5V untuk memproses sinyal analog menjadi nilai digital yang berasal dari MIC, sehingga didapatlah keluaran sensor yang dihubungkan melalui *Port* A0.
c. Aplikasi antarmuka pengirim digunakan untuk menampilkan data yang diproses oleh sensor melalui Arduino. Aplikasi antarmuka pada komputer terhubung dengan Arduino melalui *Port USB*.

4.2. Diagram Alir Antarmuka Enkripsi dengan Kriptografi Vigenere

Diagram alir aplikasi antarmuka dimulai dengan menyediakan data waktu berupa menit, *plaintext* yang akan di enkripsi dan kunci untuk enkripsi dengan dapat dilihat pada Gambar 6.



Gambar 6. Diagram Alir Antarmuka Enkripsi dengan Kriptografi Vigenere

Enkripsi Kriptografi Vigenere tersebut dapat dijabarkan sebagai berikut:

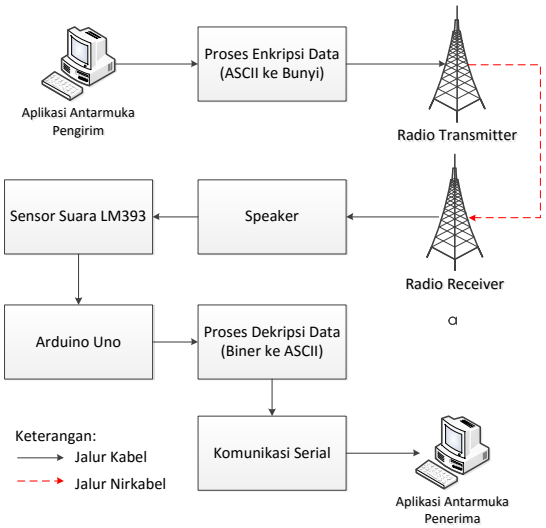
a. Pada saat program dimulai maka dilakukan inisiasi variabel waktu berupa menit, variabel *plaintext* dan variabel kunci.

b. Jika waktu komputer sama dengan menit ke 0, 15, 30 dan 45 maka akan dilakukan proses enkripsi kemudian tombol kirim manual akan tidak aktif sehingga aplikasi
c. Pengguna dapat melakukan enkripsi dan pengiriman secara manual dengan menekan tombol kirim.
d. Ketika aplikasi melakukan enkripsidenan Kriptografi Vigenere maka akan menghasilkan *ciphertext* dalam bentuk kode ASCII. Kemudian dilakukan konversi kode ASCII ke bilangan biner. Sehingga *ciphertext* menjadi bentuk 1 dan 0 dalam bilangan biner.
e. Aplikasi mengeluarkan bunyi panjang ketika bit setiap *ciphertext* adalah 1 dan bunyi pendek ketika bit setiap *ciphertext* adalah 0.
f. Ketika aplikasi bekerja secara otomatis maka tombol kirim akan tidak aktif dan kondisi tombol akan kembali aktif apabila pengiriman selesai.

4.3. Diagram Blok Pengiriman dan Penerimaan Informasi Melalui Radio

Diagram blok pengiriman dan penerimaan informasi pada Gambar 7, dapat dijelaskan sebagai berikut:

a. Pengguna memasukan *plaintext* dan kunci kedalam *textbox* pada aplikasi antarmuka.
b. Antarmuka melakukan enkripsi dengan Kriptografi Vigenere dan menghasilkan bunyi panjang untuk logika 1 dan bunyi pendek untuk logika 0.
c. Radio *transmitter* akan mengirimkan bunyi yang dihasilkan aplikasi antarmuka melalui sinyal radio komersil dengan frekuensi 97,3 FM.
d. Penerima akan menangkap sinyal radio komersil dengan menggunakan perangkat radio *receiver* dengan frekuensi yang sama yaitu 97,3 FM.
e. Setelah pengirim dan penerima terhubung, maka penerima akan mendapatkan bunyi berupa panjang dan pendek menggunakan speaker.
f. Sensor suara akan mendeteksi bunyi yang diterima melalui speaker radio *receiver*. Bunyi sebagai keluaran (output) dan sensor suara mendeteksi suara sebagai masukan (input) pada Mikrokontroler Arduino Uno dan selanjutnya dilakukan proses dekripsi dengan menggunakan Kriptografi Vigenere.
g. Hasil dari proses dekripsi menggunakan kunci yang sama dengan pengirim akan ditampilkan pada aplikasi antarmuka sebagai *ciphertext* yang tidak dapat dimengerti atau diproses pengguna secara langsung.
h. Komputer terhubung dengan perangkat keras melalui komunikasi serial kemudian data *ciphertext* akan dikirim ke komputer penerima.
i. Aplikasi antarmuka akan menampilkan data yang dikirim oleh Arduino Uno dan kemudian memasukan kunci yang sama dengan pengirim sehingga menghasilkan *plaintext* yang dapat dimengerti oleh pengguna.



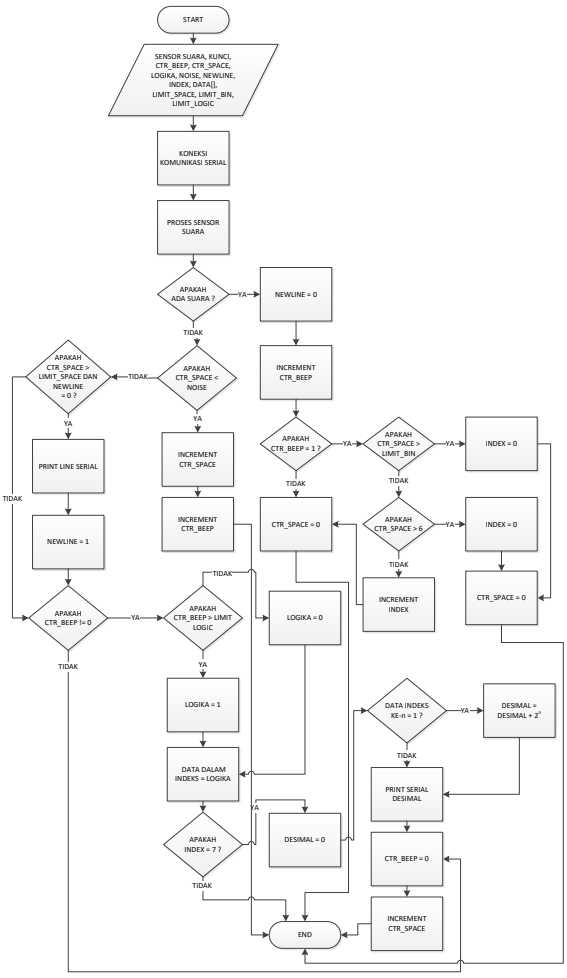
Gambar 7. Diagram Blok Transmisi

4.4. Diagram Alir Proses Dekripsi dengan Kriptografi Vigenere

Proses dekripsi menggunakan perangkat keras Arduino dengan Sensor Suara LM393 sebagai pendeteksi bunyi yang telah di enkripsi dapat dilihat pada Gambar 8. Deskripsi dengan algoritma pengenalan bunyi perangkat keras pada diagram alir dapat dijelaskan sebagai berikut:

a. Ketika perangkat keras dihidupkan maka dilakukan inisiasi variabel yaitu sensor suara, kunci, ctr_beep, ctr_space, logika, noise, newline, index, data[], limit_space, limit_bin, limit_logic.
b. Kemudian dilakukan komunikasi serial antara perangkat keras dan komputer.

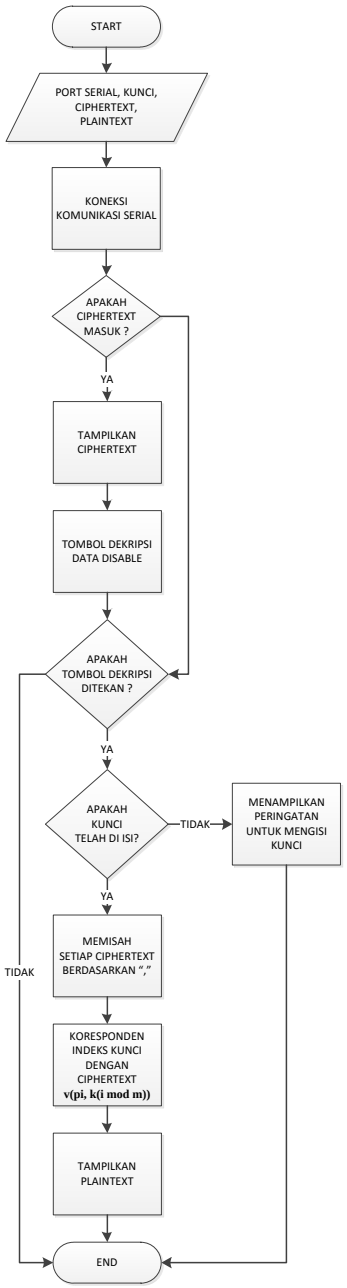
c. Sensor suara mendeteksi suara yang berasal oleh radio penerima.
d. Jika terdapat suara, maka variabel newline adalah 0, hal ini berfungsi untuk menjadi pertimbangan saat terdapat kalimat baru.
e. Kemudian dilakukan proses penambahan (increment) variabel ctr_beep, jika kondisi ctr_beep pada saat mulai adalah 0, maka seteleh proses increment akan menghasilkan 1 dan selanjutnya.
f. Setelah dilakukan proses increment pada variabel ctr_beep, maka akan ditentukan apakah nilai ctr_beep adalah 1, jika ya maka akan dilakukan pertimbangan lagi yaitu apakah ctr_space lebih besar dari limit_biner. Hal ini akan menentukan pergantian pengenalan urutan bit selanjutnya yang dipengaruhi oleh variabel index karena limit_biner akan menjadi batas setelah pengiriman dalam waktu singkat sebelum pengiriman bit selanjutnya.
g. Variabel ctr_beep akan terus di increment ketika terdapat suara dan ctr_space akan bernilai 0 jika terdapat suara.
h. Jika tidak terdapat suara, maka ctr_space akan dilakukan proses increment dan ctr_beep akan berhenti di increment untuk dilakukan pertimbangan pengenalan bunyi panjang dan pendek.
i. Pada program terdapat pengabaian sinyal noise yang berasal dari sensor itu sendiri sehingga nilai pembacaan dapat konstan, yaitu jika setelah ctr_beep di increment (ada suara) terdapat tidak ada suara (increment ctr-beep), variabel noise ditentukan sebanyak 5 kali ctr_space. Sehingga jika terdapat ctr_space sebanyak 5 kali setelah ctr_beep maka ctr_space diabaikan dan nilai pembacaan ctr_beep akan konstan.
j. Setelah pengiriman pada menit ke 0, 15, 30 dan 45 maka perangkat keras akan menentukan pola bunyi panjang dan pendek, maka terdapat jeda yang sangat panjang sehingga ctr_space akan menjadi sangat banyak. Variabel limit_space akan berfungsi untuk menghitung pola setelah pengiriman yaitu sebanyak 1000. Jika tidak terdapat suara maka ctr_space telah lebih dari limit space yaitu 1000 seingga akan dilakukan perintah print line serial. Print line berfungsi untuk memuat data baru pada aplikasi antarmuka.
k. Variabel ctr_beep akan digunakan untuk keputusan pengenalan pola bunyi panjang atau pendek pada saat tidak terdapat suara dan varabel index adalah 7, variabel index akan digunakan untuk menentukan indeks array dari urutan bit yang akan membentuk bilangan biner 8 bit.
l. Variabel ctr_beep akan mengenali bunyi panjang jika ctr_beep bernilai lebih dari nilai variabel limit_logic sehingga menghasilkan bit 1.
m. Variabel ctr_beep akan mengenali bunyi pendek jika ctr_beep bernilai kurang dari nilai variabel limit_logic sehingga menghasilkan bit 0.



Gambar 8. Diagram Alir Proses Dekripsi

4.5. Diagram Alir Antarmuka Dekripsi

Diagram alir dekripsi menggunakan antarmuka ditunjukkan pada Gambar 9.



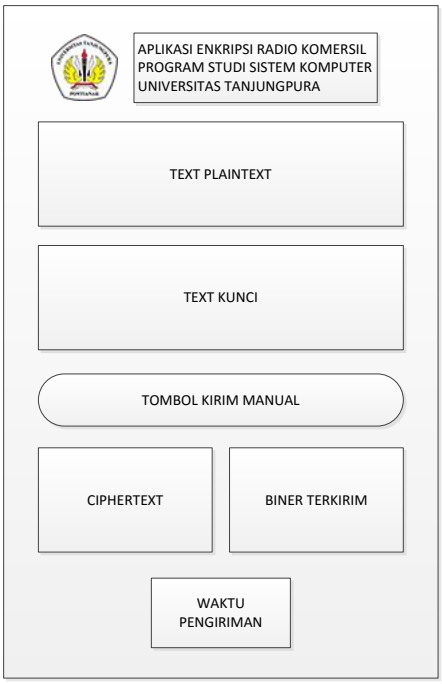
Gambar 9. Diagram Alir Proses Dekripsi

Deskripsi diagram alir proses dekripsi dapat dijelaskan sebagai berikut:

a. Program dimulai dengan inisiasi variabel port serial, kunci, *ciphertext* dan *plaintext*.
b. Kemudian dilakukan koneksi komunikasi serial dengan memilih port yang terhubung oleh Arduino Uno pada komputer.
c. *Ciphertext* akan diterima dan ditampilkan pada *form ciphertext* dan pengguna memasukan kunci yang sama pada saat pengiriman.
d. Proses dekripsi dimulai ketika tombol dekripsi ditekan, jika kunci belum diisi maka akan terdapat peringatan bahwa kunci harus diisi. Jika kunci dan *ciphertext* sudah tampil pada aplikasi antarmuka, maka setiap *ciphertext* akan dilakukan pemisahan berdasarkan koma.
e. Kriptografi Vigenere dilakukan dengan korespondensi dari indeks kunci yang digunakan dan *ciphertext*. Kemudian akan dilakukan operasi pengurangan dari nilai desimal *ciphertext* dengan nilai desimal dari kunci. Sehingga akan ditampilkan pada aplikasi antarmuka yaitu *plaintext* yang merupakan hasil dari pengiriman informasi terenkripsi melalui radio.

4.6. Rancangan Tampilan Antarmuka Aplikasi Enkripsi

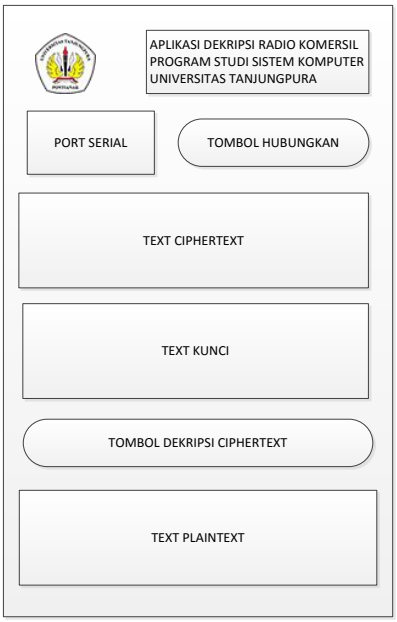
Antarmuka aplikasi enkripsi digunakan oleh pengguna untuk melakukan proses enkripsi informasi dan mengirim bunyi. Antarmuka aplikasi enkripsi berisi masukan kunci dan *plaintext* dapat dilihat pada Gambar 10.



Gambar 10. Tampilan Antarmuka Enkripsi

4.7. Rancangan Tampilan Antarmuka Aplikasi Dekripsi

Antarmuka aplikasi dekripsi digunakan oleh pengguna untuk melakukan proses dekripsi informasi dan pola bunyi. Antarmuka aplikasi dekripsi berisi masukan kunci dan *ciphertext* dapat dilihat pada Gambar 11.



Gambar 11. Tampilan Antarmuka Dekripsi

4.8. Implementasi Proses Enkripsi Kriptografi Vigenere

Proses enkripsi dilakukan dengan menggunakan Visual Basic 2010 yaitu dengan korespondensi setiap karakter *plaintext* dengan setiap karakter *ciphertext*. Karakter informasi direpresentasi menjadi kode ASCII desimal dan dilakukan penambahan karakter *plaintext* dengan kunci hingga menghasilkan *ciphertext* pada setiap karakter. Kode Program 1 digunakan untuk menambahkan kode ASCII *plaintext* dengan kode ASCII kunci.

Kode Program 1. Proses Enkripsi dengan Visual Basic

```
Public Shared Function Encrypt(ByVal plaintext As String,
ByVal key As String)
    Dim ciphertext As String = ""
    For i As Integer = 1 To plaintext.Length
     Dim temp As Integer = AscW(GetChar(plaintext, i)) +
AscW(GetChar(key, i Mod key.Length + 1)) //enkripsi
     ciphertext = ciphertext & temp & "," //menggabungkan string
ciphertext kedalam textbox
    Next
    Return ciphertext
End Function
```

4.9. Implementasi Proses Dekripsi Kriptografi Vigenere

Setelah data dikenali oleh mikrokontroler maka akan menghasilkan karakter ASCII *ciphertext* dalam bentuk bilangan desimal akan dikurangi dengan nilai desimal dari karakter ASCII kunci. Kode Program 2 merupakan proses dekripsi *ciphertext* dengan kunci sehingga menghasilkan *plaintext*.

Kode Program 2. Dekripsi Kriptografi Vigenere pada Visual Basic

```
  For Each c In cip //untuk setiap ciphertext yang dipecah akan
diproses dekripsi
     If (c <> "") Then //jika data tidak kosong maka akan
diproses dekripsi
        Dim var_int As Integer
       If Integer.TryParse(c, var_int) Then jika bilangan bulaa
          ' childAge successfully parsed as Integer
         Dim temp As Integer = c - AscW(GetChar(key, i Mod
key.Length + 1)) //dekripsi
          decryptedText = decryptedText & Chr(temp) //
menggabungkan hasil string dekripsi
        Else
          ' childAge is not an Integer
        End If
        i = i + 1 // increment indeks
     End If
  Next c
```

5. IMPLEMENTASI DAN PENGUJIAN SISTEM

Setelah dilakukan proses perancangan sistem pada perangkat lunak dan perangkat keras yaitu melalui diagram alir, diagram blok dan penulisan kode program, maka dilanjutkan dengan tahap implementasi.

5.1. Implementasi Perancangan Perangkat Keras

Aplikasi pengirim terhubung dengan radio *transmitter* untuk mengirimkan suara yang dihasilkan setelah proses enkripsi dilakukan ditunjukkan pada Gambar 12.

Gambar 12. Penggunaan FM *Transmitter* dengan Aplikasi Pengirim

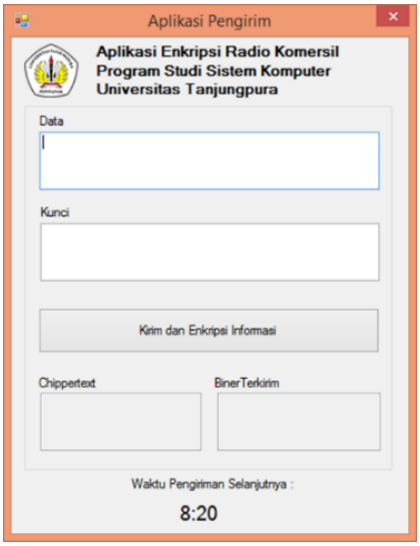
Pada Gambar 13 merupakan perangkat radio penerima, sensor suara, Arduino Uno yang terhubung dengan aplikasi penerima. Data biner yang dihasilkan oleh Arduino Uno dikirim ke Aplikasi melalui komunikasi serial

dan di ubah kedalam karakter ASCII sehingga menghasilkan *ciphertext* kemudian dilakukan proses dekripsi.

Gambar 13. Penggunaan FM *Transmitter* dengan Aplikasi Pengirim.

5.2. Tampilan Antarmuka Aplikasi Enkripsi

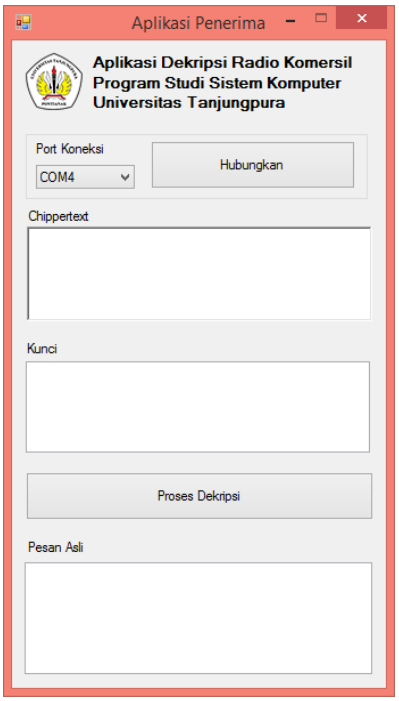
Tampilan antarmuka aplikasi pengirim dapat dilihat pada Gambar 14. Aplikasi berisi *form* data, kunci, *ciphertext* dan biner terkirim. Pada *form* data akan berisi informasi yang akan di enkripsi oleh aplikasi menggunakan *form* kunci dengan metode Kriptografi Vigenere.



Gambar 14. Antarmuka Aplikasi Pengirim

5.3. Tampilan Antarmuka Aplikasi Dekripsi

Tampilan antarmuka aplikasi penerima dapat dilihat pada Gambar 15. Aplikasi tersebut berisi *form* kunci, *ciphertext* dan pesan asli. Aplikasi antarmuka penerima menggunakan komunikasi serial yang terhubung dengan Arduino.



Gambar 15. Antarmuka Aplikasi Penerima

5.4. Pengujian Proses Enkripsi Kriptografi Vigenere

Pengujian dilakukan dengan menghitung secara manual *ciphertext* dengan kriptografi Vigenere. Pada penelitian digunakan sampel *plaintext* dan kunci yang digunakan adalah sebagai berikut:

Plaintext : Alamat Jl.A.Yani No.21
Kunci : s1sk0m

Proses enkripsi *plaintext* menggunakan rumus yaitu:

$$E(pi)=v(pi,k(i \mod m)+1)$$

Setelah ditentukan *plaintext* dan kunci maka dilakukan proses enkripsi *plaintext* dengan memasangkan indeks kunci. Sebagai sampel *plaintext* "A" dirubah terlebih dahulu menjadi desimal, kemudian kunci indeks dimulai dari "1" dan dirubah menjadi desimal. Selanjutnya dijumlahkan *plaintext* dan kunci sehingga menghasilkan *ciphertext* dengan menggunakan variabel i dan m yaitu:

i = 1
m = 6

Sehingga rumus enkripsi Kriptografi Vigenere menjadi:

E(pi)=v(pi,k(i mod m)+1)
E(pi)=v(p(1),k(1 mod 6)+1)
E(pi)=v(p(1),k(1)+1))
E(pi)=v(p(1),k(2))

Berdasarkan penggunaan rumus tersebut, maka akan dilakukan korespondensi p(1) yaitu *plaintext* ke-1 adalah "A" dan k(2) yaitu *ciphertext* ke-2 adalah "1":

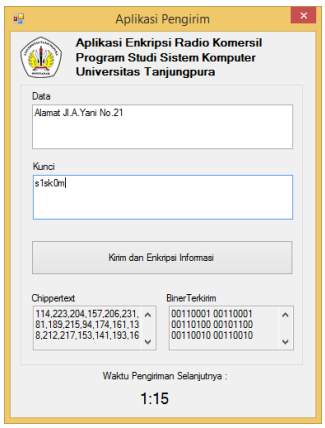
E(pi)=v(A,1)

Kemudian dilakukan perubahan kode ASCII menjadi bilangan desimal dan dilakukan proses fungsi enkripsi kriptografi vigenere yaitu menjumlahkan nilai *plaintext* dan kunci:

E(pi)=v(65,49)
E(pi)=(65+49)
E(pi) = 114

5.5. Pengiriman dengan Aplikasi Pengirim

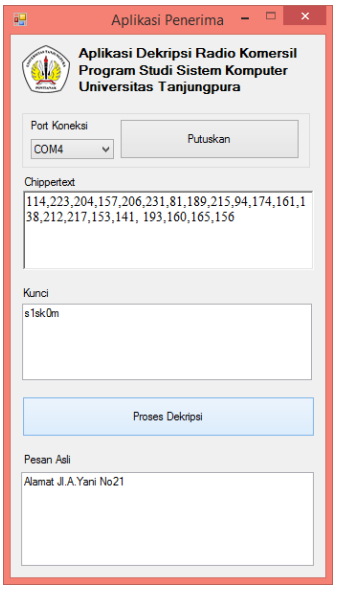
Implementasi aplikasi pengirim dilakukan dengan memasukan sampel *plaintext* ke dalam aplikasi antarmuka dan dilakukan pengiriman suara melalui radio komersil. Hasil dari proses enkripsi menggunakan aplikasi pengirim menghasilkan *ciphertext* pada Gambar 16.



Gambar 16. Proses Enkripsi dengan Kriptografi Vigenere

5.6. Penerimaan dengan Aplikasi Penerima

Setelah dilakukan pengiriman dengan menggunakan aplikasi pengirim, informasi akan dikirim melalui radio komersil dan ditangkap oleh radio penerima dengan frekuensi yang sama dengan pengirim.



Gambar 17. Proses Dekripsi dengan Kriptografi Vigenere

5.7. Pengujian Proses Dekripsi Kriptografi Vigenere

Pengujian dilakukan dengan menghitung secara manual *plaintext* dengan kriptografi Vigenere. Proses dekripsi *plaintext* menggunakan rumus (2) yaitu:

D(ci) = v(ci, k(i mod m)+1)

Setelah ditentukan *plaintext* dan kunci maka dilakukan proses enkripsi *ciphertext* dengan memasangkan indeks kunci. Sebagai sampel *ciphertext* "114" merupakan bilangan desimal, kemudian kunci indeks dimulai dari "1" dan dirubah menjadi desimal. Selanjutnya dijumlahkan *plaintext* dan kunci sehingga menghasilkan *ciphertext* dengan menggunakan rumus:

i = 1
m = 6

Sehingga rumus dekripsi Kriptografi Vigenere menjadi:

D(ci) = v(ci,k(i mod m)+1)
D(ci) = v(c(1),k(1 mod 6)+1)
D(ci) = v(c(1),k(1)+1)
D(ci) = v(c(1),k(2))

Berdasarkan penggunaan rumus tersebut, maka akan dilakukan korespondensi c(1) yaitu

ciphertext ke-1 adalah "114" dan k(2) yaitu *ciphertext* ke-2 adalah "1":

D(ci) =v(114,1)

Kemudian dilakukan perubahan kunci menjadi bilangan desimal, sedangkan *ciphertext* sudah dalam bentuk desimal dan dilakukan proses fungsi dekripsi kriptografi vigenere yaitu mengurangkan nilai *ciphertext* dan kunci:

D(ci) = v(114,49)
D(ci) = (114-49)
D(ci) = 65
D(ci) = A

6. KESIMPULAN

Setelah dilakukan proses perancangan perangkat dan dilakukan proses implementasi pengiriman dan penerimaan informasi terenkripsi dengan Kriptografi Vigenere melalui radio komersil maka diperoleh kesimpulan antara lain:

a. Enkripsi informasi berupa karakter dengan metode Kriptografi Vigenere menjadi bunyi. Informasi di enkripsi menjadi *ciphertext* oleh aplikasi Visual Basic dengan merubah setiap data dalam bilangan desimal dan dijumlahkan dengan bilangan desimal dari indeks kunci. Setelah dilakukan enkripsi maka *ciphertext* dirubah dalam bentuk biner dan diakukan pengiriman setiap bit dari *ciphertext*, Setelah informasi dikirim maka akan menghasilkan tanpa bunyi yang terus dideteksi sebagai informasi baru jika terdapat bunyi setelah tanpa bunyi.
b. Bunyi dikirim dengan menggunakan radio pengirim (*transmitter*) dengan frekuensi 97,3 FM dan diterima oleh radio penerima *(receiver)* kemudian dikenali pola dengan sensor suara. Hasil dari pengenalan pola adalah karakter ASCII dalam bentuk desimal dan dipisahkan oleh koma pada setiap karakter.
c. Dekripsi informasi dengan Kriptografi Vigenere. *Ciphertext* yang diterima oleh aplikasi penerima yang dibuat dengan Visual Basic akan di dekripsi menjadi *plaintext* ketika pengguna memasukan kunci yang sama dengan pengirim. Data dari *ciphertext* akan secara otomatis berganti ketika terdapat informasi baru yang dikirim oleh aplikasi pengirim.

7. SARAN

Berdasarkan penelitian yang telah dilakukan pada pengiriman dan penerimaan informasi terenkripsi dengan kriptografi Vigenere melalui sinyal radio komersil maka diperoleh saran untuk penelitian lebih lanjut yaitu:

a. Pada penelitian akurasi ditentukan oleh sensor analog yang mudah terpengaruh oleh lingkungan sekitar sehingga diharapkan untuk melakukan pengenalan pola suara langsung menggunakan sinyal digital sehingga menigkatkan akurasi dan menghindari terjadinya *noise* jika menggunakan sinyal analog.
b. Meningkatkan kecepatan prose pengiriman dengan mempersingkat waktu dari suara panjang dan suara pendek.
c. Menerapkan penelitian pada transmisi radio komersil sebenarnya, sehingga didapat pengujian dengan jarak pengiriman yang jauh.

DAFTAR PUSTAKA

[1] Wijaya, M. H. (2012). Pengenalan Nada Suling Rekorder Menggunakan Fungsi Jarak Chebyshev. *Program Studi Teknik Elektro Fakultas Sains dan Teknologi Universtas Sanata Dharma*. Prosiding Seminar Nasional Aplikasi Sains & Teknologi (SNAST) Periode III. ISSN: 1979-911X, Hal B-82 s.d. B-89.

[2] Arius, D. (2008). *Pengantar Ilmu Kriptografi.* Yogyakarta: Andi.

[3] Ferdianto, H. (2010). *Dasar-dasar Sinyal dan Sistem.* Yokyakarta: Andi.

[4] Instrument, T. (2014, Desember). *Datasheet LM393*. Retrieved from Texas Instrument Datasheet:

[5] Iswanto. (2011). *Belajar Mikrokontroller AT89S51 dengan Bahasa C.* Yokyakarta: Andi.

[6] Suhata. (2005). *Aplikasi Mikrokontroler Sebagai Pengendali Peralatan Elektronik Via Line Telepon.* Jakarta: PT. Gramedia.