Implementasi Algoritma Kriptografi RC4 pada Sistem Keamanan Jaringan Telepon

Mike Yuliana, Miftahul Huda, Prima Kristalina
Politeknik Elektronika Negeri Surabaya-Institut Teknologi Sepuluh Nopember
Kampus ITS Keputih Sukolilo Surabaya 60111, Indonesia
Tel:+62(31)5947280;Fax:+62(31)5946114
E-mail: mieke@eepis-its.edu

Abstrak

Tujuan dari penelitian ini adalah untuk menghasilkan sebuah produk pengacak sinyal suara yang bisa menjamin keamanan pengiriman informasi melalui jaringan telepon. Sistem yang dihasilkan merupakan integrasi modem dengan DSP TMS320C5402 yang terhubung dengan jaringan telepon serta dilengkapi dengan algoritma kriptografi RC4 untuk mengacak sinyal suara .

Algoritma kriptografi RC4 berhasil diimplementasikan pada DSP TMS320C5402 sebagai algoritma untuk mengacak sinyal suara, hal ini terlihat dari bentuk sinyal terenkripsi yang benar-benar acak. Hasil MOS sebesar 4 menunjukkan bahwa sinyal suara terdekripsi yang telah melewati jalur telepon bisa didengarkan kembali namun tidak begitu jernih. Dari hasil pengujian juga bisa diketahui bahwa untuk komunikasi modem dan DSP TMS320C5402 hanya dapat dilakukan dengan baud rate lebih dari 9600 bps.

Kata kunci: *DSP TMS320C5402, RC4, telepon, modem.*

1. Pendahuluan

Dengan semakin maraknya orang memanfaatkan layanan komunikasi melalui telepon, maka permasalahanpun bermunculan, apalagi ditambah dengan adanya peretas (*hacker*) dan perengkah (*cracker).* Banyak orang kemudian berusaha menyiasati bagaimana cara mengamankan informasi yang dikomunikasikannya, atau menyiasati bagaimana cara mendeteksi keaslian dari informasi yang diterimanya. Oleh karena itulah, dibutuhkan suatu metode enkripsi/dekripsi yang bertujuan untuk menjaga kerahasiaan informasi yang terkandung dalam data sehingga informasi tersebut tidak dapat diketahui oleh pihak yang tidak sah.

DSP TMS320C5402 yang terhubung dengan jaringan telepon serta dilengkapi dengan algoritma RC4 hanya dapat berkomunikasi dengan baik melalui komunikasi berbasis digital(serial), sehingga diperlukan suatu media yang dapat menghubungkan DSP dengan jaringan telepon yang bersifat analog. Pada penelitian ini, algoritma RC4 akan diimplementasikan secara *real time* pada 2 DSP yang terhubung ke jaringan telepon menggunakan sebuah media yaitu modem, dimana komunikasi dari 2 DSP akan dilakukan secara 2 arah(*full duplex).*

Pada bab 2 dijelaskan tentang penelitian terdahulu , pada bab 3 dijelaskan tentang dasar teori, pada bab 4 dijelaskan tentang implementasi dan hasil pengujian, sedangkan bab 5 berisi kesimpulan.

2. Penelitian Terdahulu

Mike Yuliana[5] mendesain dan mengimplementasikan metode scrambler/descrambler berbasis teknik pemfilteran dan modulasi pada DSP TMS320C5402 yang terintegrasi dengan jaringan telepon sebagai metode untuk mengurangi tingkat kejelasan suara. Mike Yuliana[4] mendesain dan mengimplementasikan metode enkripsi/dekripsi RC4 pada 2 DSP TMS320C5402 yang terhubung dengan RS232 kabel silang(*cross cable*).

Penelitian ini merupakan pengembangan dari 2 penelitian sebelumnya, dimana metode enkripsi/dekripsi RC4 diimplementasikan pada 2 DSP TMS320C5402 yang terhubung dengan jaringan telepon dengan menggunakan modem.

.

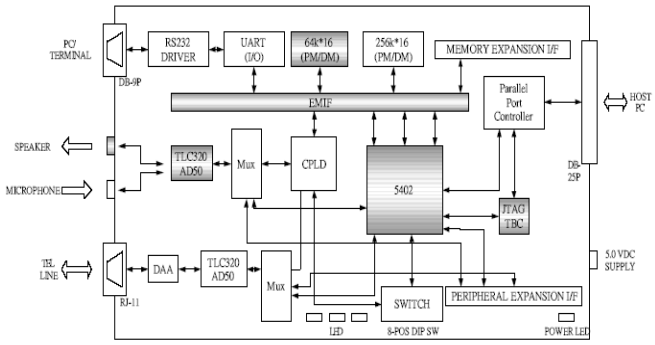
3. Dasar Teori Sistem

3.1 Metode Enkripsi/Dekripsi RC4

RC4 mempunyai sebuah S-Box, S_0, S_1, ….., S_{255}, yang berisi permutasi dari bilangan 0 sampai 255. Menggunakan dua buah indeks yaitu i dan j di dalam algoritmanya. Indeks i digunakan untuk memastikan bahwa suatu elemen berubah, sedangkan indeks j akan memastikan bahwa suatu elemen berubah secara random. Intinya, dalam algoritma enkripsi metode ini akan membangkitkan *pseudorandom byte* dari *key* yang akan dikenakan operasi XOR terhadap *plaintext* untuk menghasilkan *ciphertext*. Dan untuk menghasilkan *plaintext* semula, maka *ciphertext*-nya akan dikenakan operasi XOR terhadap *pseudorandom byte*-nya[1][3].

3.2 DSP TMS320C5402

Pada penelitian ini, metode enkripsi/dekripsi RC4 diimplementasikan pada DSP *Starter Kit* (DSK) C5402. Adapun blok diagram dari DSK C5402 bisa dilihat pada Gambar 1 dibawah ini



Gambar 1. DSP TMS320C5402[6]

DSP C54x memakai modifikasi lanjut dari arsitektur *Harvard* yang meningkatkan kekuatan proses dengan 8 bus (4 program/data dan 4 address)

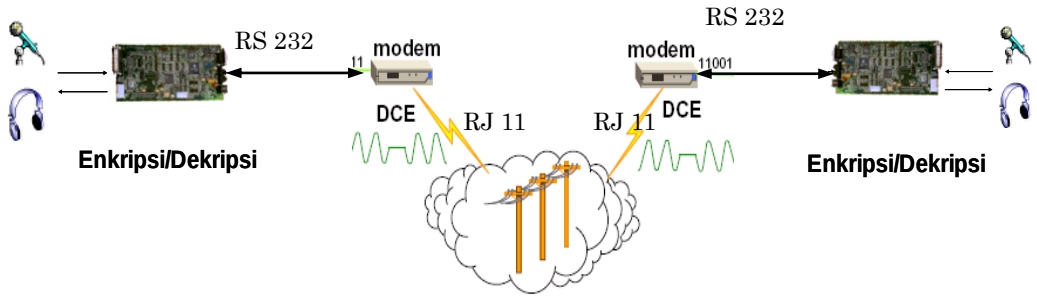
- PB (program bus): membawa *instruction code* dan *immediate operand* dari *program memory*
- Tiga bus data
  - CB(*coefficient bus*): membawa *operand* yang dibaca dari data *memory.*
  - DB(*data bus*): membawa *operand* yang dibaca dari data *memory*.
  - EB(*write bus*): membawa data yang akan ditulis ke *memory*.
- Empat *address bus*: PAB, CAD, DAB, EAB, membawa alamat yang dibutuhkan untuk program *execution*.

Jalur untuk program dan data terpisah membuat akses serentak dari program instruksi dan data, menyediakan mekanisme paralel yang tinggi. Sebagai contoh, tiga proses membaca dan satu proses menulis dapat dilakukan pada satu *cycle*. Instruksi dengan penyimpanan paralel dan instruksi untuk aplikasi khusus sangat memerlukan arsitektur ini. Sebagai tambahan, data dapat ditransfer diantara data dan *program space*. Mekanisme paralel seperti ini mendukung kemampuan untuk aritmatik, logika, operasi manipulasi bit yang semuanya dapat dilakukan pada satu mesin *cycle* saja. Dan juga, C54x mencakup mekanisme kontrol untuk menangani interupsi, operasi pengulangan dan fungsi call. Komponen didalam *Central Processing Unit* (CPU) didukung oleh:

- o 40-bit ALU
- o dua 40-bit *accumulators*
- o 40-bit *Barrel Shifter*
- o 17 x 17 *multiplier*
- o 40-bit *adder*
- o *compare, select, and store unit* (CSSU)
- o *Data address generation unit*
- o *Program address generation unit*

4.Implementasi dan Hasil Pengujian Sistem

Pada tahap ini, metode enkripsi/dekripsi RC4 akan diimplementasikan secara *real time* pada 2 DSP TMS320C5402 yang terhubung dengan jaringan telepon sebagai metode pengacak sinyal suara, dimana komunikasi dari 2 DSP akan dilakukan secara 2 arah (*full duplex*) selain itu sistem yang dibuat dirancang agar dapat bekerja secara *stand alone* sehingga modul dapat bersifat *portable* dan praktis. Blok Diagram sistem yang akan dibuat bisa dilihat pada Gambar 2.



Gambar 2 Blok Diagram Sistem

4.1. Implementasi Sistem

Untuk menyelesaikan sistem pengacak sinyal suara ini, akan dilakukan beberapa tahap yang meliputi:

1. Pembuatan driver modem
2. Pembuatan metode enkripsi/dekripsi RC4
3. Integrasi Sistem enkripsi/dekripsi RC4 pada *board* DSP TMS320C5402 yang terintegrasi dengan jaringan telepon

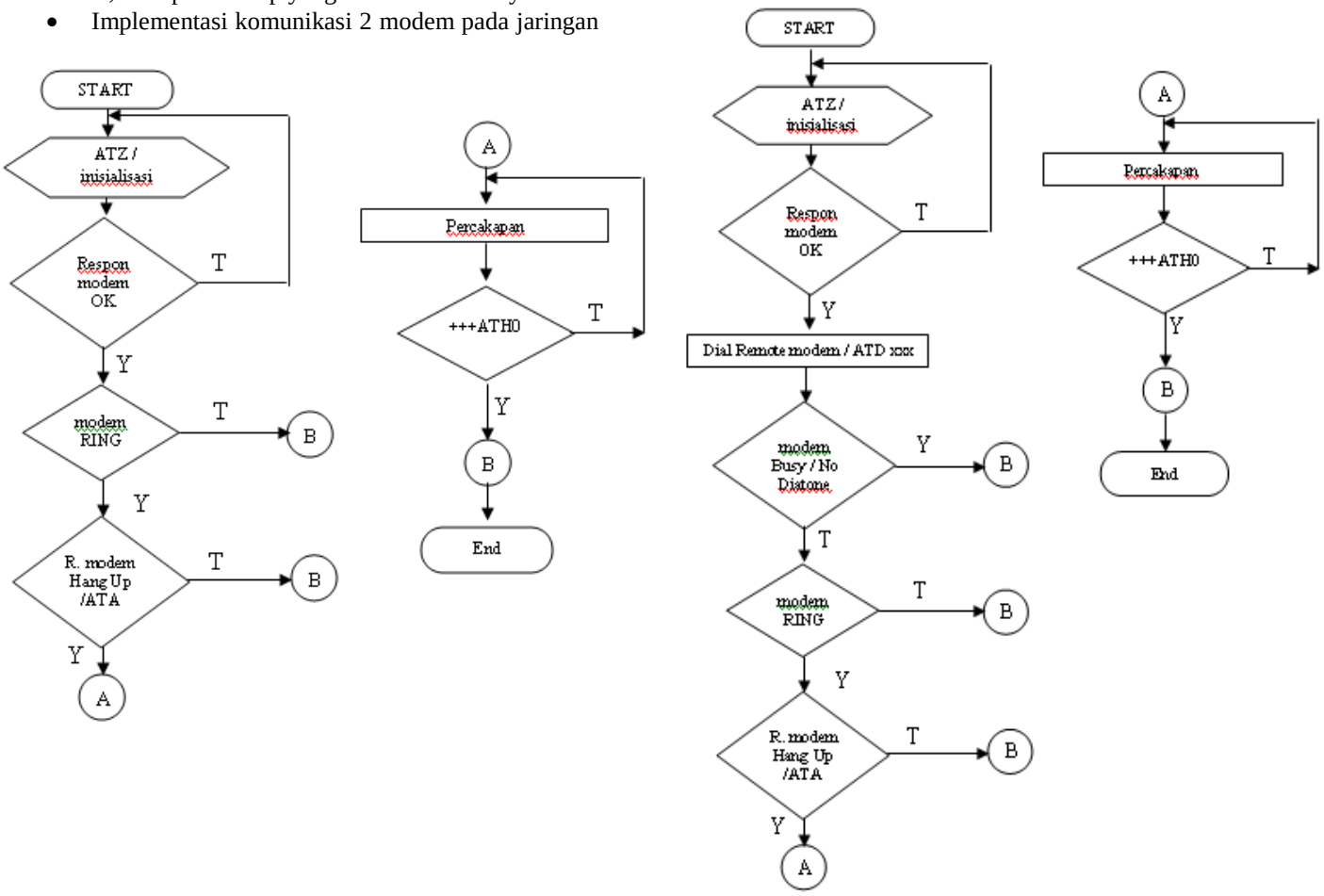
4.1.1 Pembuatan Driver Modem

Modem berfungsi sebagai modulator dan demodulator agar sinyal digital yang ditransmisikan dapat dilewatkan pada jaringan analog seperti jaringan telepon. Modem merupakan peralatan yang berbasis *software driver*, sehingga memerlukan sebuah *driver* yang berupa AT-command yang akan dikenali oleh modem. Command ini akan mengaktifkan dan mengoperasikan modem berdasarkan jenis *command*-nya. Pada pembuatan driver modem ini, terdapat 2 tahap yang harus dilakukan yaitu:

- Implementasi komunikasi 2 modem pada jaringan telepon menggunakan PC
- Integrasi board DSP dengan PABX yang dihubungkan dengan menggunakan modem sebagai media yang memodulasi data digital dari UART DSP menjadi data analog kemudian ditransmisikan melalui jalur analog.

a. Implementasi Komunikasi 2 modem pada jaringan telepon menggunakan PC

Untuk membuat driver modem ini, perlu diketahui command-command yang dibutuhkan agar sebuah modem dapat membangun sesi komunikasi yang dapat menghubungkan terminal yang terkoneksi dengannnya. Pada gambar 3 bisa dilihat proses pembentukan komunikasi modem yang berupa pengiriman AT-command ke modem sehingga modem dapat mengerjakan instruksi AT-Command yang diberikan oleh PC.

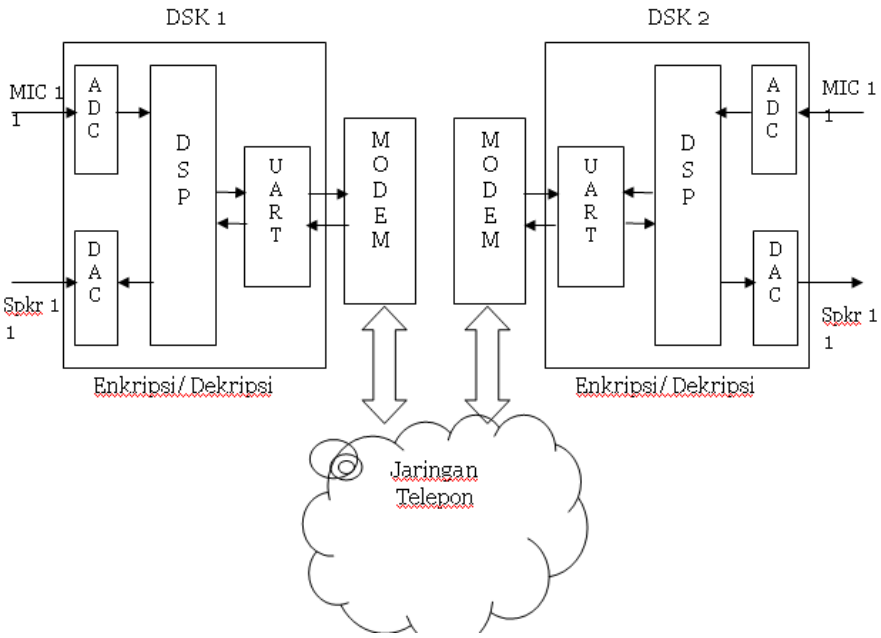


(a) (b)

Gambar 3. Proses Pembentukan Komunikasi 2 Modem (a) Penerima (b) Pemanggil

b. Integrasi board DSP dengan PABX yang dihubungkan dengan menggunakan modem.

Setelah komunikasi 2 modem pada jaringan telepon menggunakan PC berhasil, maka tahap selanjutnya yang dilakukan adalah implementasi penggunaan modem pada DSP TMS320C5402 yang terintegrasi dengan jaringan telepon. Gambar 4 menunjukkan Blok Diagram Integrasi Board DSP dan modem yang terintegrasi dengan jaringan telepon..



Gambar 4. Integrasi Board DSP dan Modem yang Terintegrasi dengan Jaringan Telepon

Terdapat 2 tahap yang harus dilewati pada implementasi penggunaan modem pada DSP TMS320C5402, dimana tahapan tersebut meliputi:

Proses Incoming

- Inisialisasi Modem menggunakan init string.
- Poll ring menunggu deteksi ring
- Setelah mendeteksi ring, poll ring menunggu ring untuk finish;
- Menunggu DSP untuk merespon dengan mengirimkan AT-COMMAND.
- Autonegosiasi kecepatan modem dan Uart DSP.
- *Modem off hook* supaya bisa terjadi *conversation.*
- Untuk mengakhiri panggilan, DSP megirimkan lagi AT-COMMAND

Proses Outgoing

- Inisialisasi Modem menggunakan init string.
- DSP mngirimkan AT-COMMAND unurk melakukan panggilan..
- Men*dial* nomor telepon yang dituju.
- Autonegosiasi kecepatan modem dan Uart DSP.
- *Modem off hook* supaya bisa terjadi *conversation.* Untuk mengakhiri panggilan, DSP megirimkan lagi AT-COMMAND

4.1.2 Pembuatan Metode Enkripsi/Dekripsi RC4

Secara garis besar algoritma dari metode RC4 ini terbagi menjadi dua bagian, yaitu : Setup Kunci dan proses enkripsi/dekripsi.

a. Setup Kunci

Pada bagian ini, terdapat tiga tahapan proses yaitu :

1. Inisialisasi S-Box

   Pada tahapan ini, S-Box akan diisi dengan nilai sesuai indeksnya untuk mendapatkan S-Box awal. Inisialisasi S-Box adalah sebagai berikut :

```
for i = 0 to 255
S[i] = i
```

2. Menyimpan *key* dalam *Key Byte Array*

   Pada tahapan ini, kunci yang akan kita gunakan untuk mengenkripsi atau mendekripsi akan dimasukkan ke dalam *array* berukuran 256 *byte* secara berulang sampai seluruh array terisi.

4. Permutasi pada S-Box
   Pada tahapan ini, akan dibangkitkan sebuah nilai yang akan dijadikan aturan untuk permutasi pada S-Box dengan operasi sebagai berikut :

```
j = 0
for i = 0  to 255
j = (j + S[i] + K[i] ) mod 256
pertukarkan isi S[i] dan isi S[j]
```

b. Proses Enkripsi dan dekripsi

Pada tahapan ini akan dihasilkan nilai *pseudorandom byte* dari *key* yang akan dikenakan operasi XOR untuk menghasilkan *ciphertext* ataupun sebaliknya untuk menghasilkan *plaintext* . Untuk membangkitkan kunci enkripsi/dekripsi dilakukan proses sebagai berikut :

```
x= y = 0
x = (x+1) mod 256
y = (y + S[x]) mod 256
pertukarkan isi S[i] & S[j]
k = S[(S[x] +S[y]) mod 256]
```

k merupakan kunci yang langsung beroperasi terhadap *plaintext(P)* ataupun *ciphertext(C)*, sedangkan *K* adalah kunci utama atau kunci induk.

$$C = P \oplus k$$
$$P = k \oplus C$$

4.2 Hasil Pengujian Sistem

Pengujian merupakan salah satu langkah penting yang harus dilakukan untuk mengetahui apakah sistem yang dibuat telah sesuai dengan apa yang direncanakan. Pada bagian ini akan dilakukan pengujian dan analisa sistem yang meliputi:

- Pengujian dan Analisa Kualitas Komunikasi pada 2 board DSP yang terintegrasi dengan jaringan telepon
- Pengujian dan Analisa Kehandalan Metode Enkripsi/Dekripsi RC4 pada 2 board DSP yang terintegrasi dengan jaringan telepon.

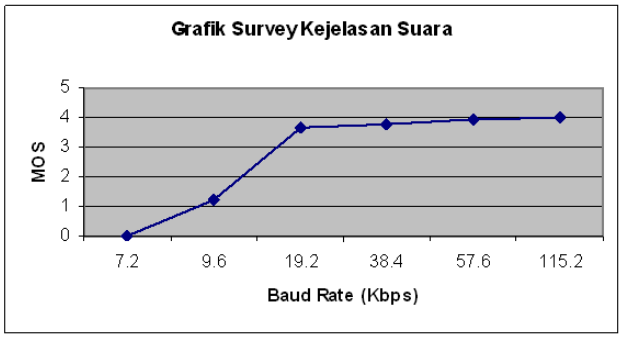
4.2.1 Pengujian dan Analisa Kualitas Komunikasi pada 2 board DSP yang Terintegrasi pada Jaringan Telepon

Pengujian ini dilakukan dengan mengambil sampel audio secara *real time* untuk tiap-tiap variasi *baud rate*, kemudian dilakukan metode ACR untuk menentukan sampel yang terbaik. Pengujian dilakukan dengan cara survey kepada 20 pendengar dari mahasiswa PENS terdiri dari 12 laki-laki dan 8 perempuan. Sampel suara berupa sinyal wicara yang direkam dengan menggunakan frekuensi sampling 16 KHz setelah melalui jaringan telepon. Hasil pengujian diperlihatkan pada tabel 1.

Tabel 1. Hasil Survei Pengujian Sinyal Wicara untuk Tiap-tiap Baud Rate

Baud Rate	Bad (1)	Poor (2)	Fair (3)	Good (4)	Excellent (5)
115200 Hz	-	-	5	10	5
57600 Hz	-	-	4	13	3
38400 Hz	-	-	8	7	5
19200 Hz	-	1	8	8	3
9600 Hz	16	3	1	-	-
< 9600 Hz	Tidak berhasil , modem gagal mendial				

Pada baud rate < 9600 tidak bisa terjadi koneksi antara modem pada jaringan telepon , karena respon yang diberikan modem sangat lambat sehingga baud rate tersebut tidak dapat digunakan pada sistem ini. Adapun hasil perhitungan MOS dari Tabel 1 bisa ditampilkan secara grafis pada Gambar 5.

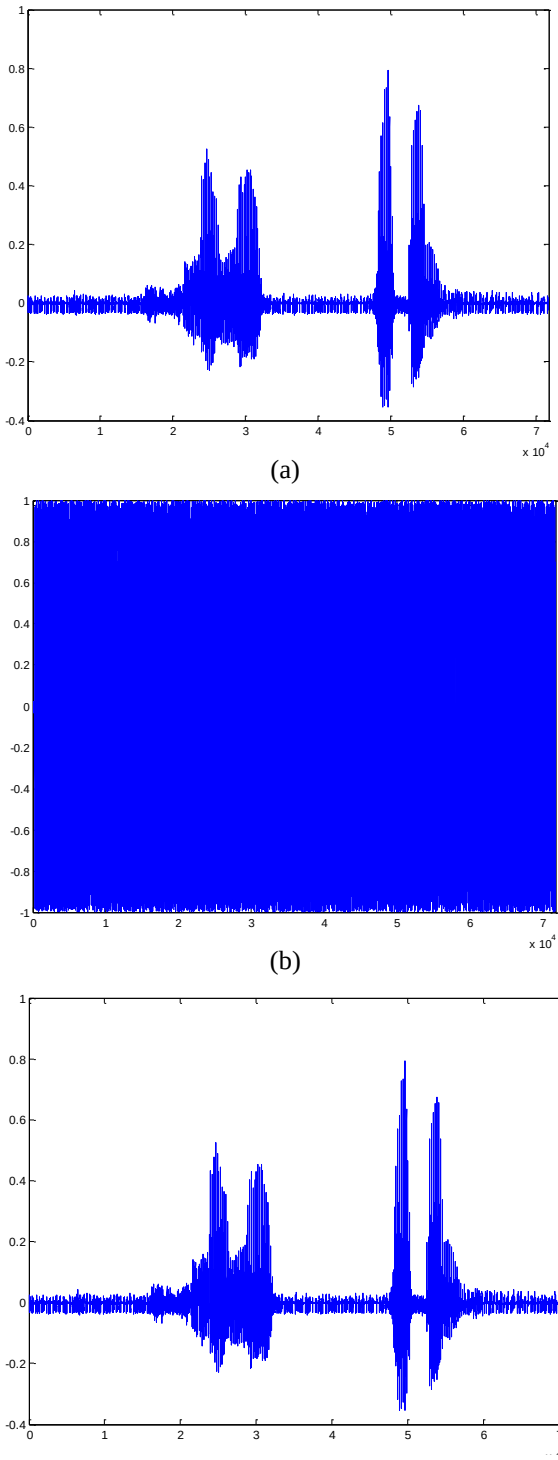


Gambar 5. Grafik Hasil Perhitungan MOS

Gambar 5 menunjukkan hubungan antara *baud rate* dan kualitas suara dari sistem. Pada baud rate yang tinggi dihasilkan kualitas suara yang baik, hal ini dikarenakan pada *baud rate* yang tinggi kecepatan transmisi data lebih cepat sehingga bit-bit data yang dikirim lebih *real time.*

4.2.2 Pengujian dan Analisa Kehandalan Metode Enkripsi/Dekripsi RC4 pada 2 board DSP yang terintegrasi dengan jaringan telepon

Pada tahap ini, pengujian dilakukan secara *off line* , sample suara yang yang memiliki kualitas paling baik pada pengujian sebelumnya dalam bentuk file wav akan dienkripsi oleh DSK kemudian dikirimkan melalui modem pada jaringan telepon.



(a)

(b)

(c)

Gambar 6. Enkripsi/Dekripsi RC4 pada Sinyal Wicara Pengucapan Kata "/Selamat Datang/" yang Berformat ".wav" pada DSP TMS320C5402 (a) Sebelum Enkripsi (b) Sesudah Enkripsi(c) Sesudah Dekripsi

Dari hasil pengujian pada Gambar 6 terlihat bahwa sinyal hasil enkripsi berbeda dengan sinyal input, sedangkan sinyal hasil dekripsi sama dengan sinyal suara aslinya. Dan apabila didengarkan ternyata suara hasil dekripsi sama dengan suara aslinya, hal ini menunjukkan keberhasilan board DSP 1 dan DSP 2 sebagai enkriptor/dekriptor suara yang tehubung dengan jaringan telepon.

5. Kesimpulan

1. DSK TMS320C5402 tidak dapat terkoneksi dengan modem pada baud rate kurang dari 9600 bps, sehingga sistem ini hanya dapat digunakan pada *baud rate* 115.2 kbps, 57.6 kbps, 33.8 kbps, 19.2 kbps, dan 9600 bps saja.
2. Berdasarkan hasil MOS (*Mean Opinion Score)* maka kualitas suara yang terbaik didapat pada baud rate 115.2 kbps dengan nilai MOS sebesar 4 (*good)*.
3. Algoritma Kriptografi RC4 berhasil diimplementasikan pada DSP TMS320C5402 sebagai pengacak suara pada Sistem Keamanan Jaringan Telepon.

6. Referensi

[1] A. J. Menezes, P.C.V. Oorschot and S.A. Vanstone , "*Handbook of Applied Cryptography*", CRC Press, 1996.

[2] Berkeley, "Choosing a DSP Processor. California: Berkeley Design Technology, Inc., http://www.BDTI.com

[3] B. Schneier, "*Applied Cryptography: Protocols, Algorithms and Source Code in C* ", 2nd edition, John Wiley & Sons, Inc., USA, 2001

[4] H. Oktavianto, M. Yuliana, "Implementasi Real Time Enkripsi/Dekripsi Sinyal Wicara pada 2 DSP TMS320C5402 Berbasis RC4", Proceeding of IES 2007, Surabaya, November 2007

[5] M. Yuliana, M.Huda, P.Kristalina," Implementasi Real Time Scrambler/Descrambler pada DSK TMS320C5402 yang Terintegrasi dengan Jaringan Telepon", Proceeding of IES 2008, Surabaya, Oktober 2007.

[6] Texas Instruments (2000). SPRS079D : TMS320 VC5402 Fixed-Point Digital Signal Processor datasheet. USA: Texas Instruments.