Implementasi Algoritma Kriptografi RC4 Pada DSP TMS320C6713 Sebagai Pendukung Sekuritas Jaringan Komunikasi *Voice over Internet Protocol* (VoIP)

Muhammad Fauzan Edy Purnomo, Wahyu Adi Priyono, Sapriesty Nainy Sari, Rusmi Ambarwati dan Asri Wulandari

***Abstrak*–Perkembangan teknologi VoIP yang berbasis IP dapat memberikan efek samping, seperti penyadapan yang tidak menguntungkan bagi pengguna teknologi tersebut. Beberapa kasus penyadapan informasi berupa paket data VoIP, yang mungkin terjadi adalah penyadapan pada jaringan *server* VoIP, maupun pembuatan jalur baru yang paralel dengan jalur yang ditentukan oleh *server* VoIP. Sehingga untuk mengatasi beberapa kasus tersebut diperlukan sebuah sistem pengamanan data (informasi).**

Dalam penelitian ini akan dieksplorasi secara khusus masalah sekuritas jaringan VoIP dengan menggunakan algoritma kriptografi RC4 yang diterapkan pada DSP TMS320C6713, yaitu bagaimana merancang algoritma enkripsi dan menganalisa performansi dari kriptografi RC4 dengan memanfaatkan TMS320C6713 dan jaringan VoIP berbasis SIP *(Session Initiation Protocol).*

Hasil pembahasan yang dilakukan, menunjukkan bahwa sistem perancangan pada penerapan kriptografi RC4 terdiri dari sistem pengacak dan penerjemah. Sistem pengacak dan penerjemah terdiri dari blok sinyal masukan, blok TMS320C6713 yang diprogram algoritma kriptografi RC4 sebagai *interface* untuk memproses sinyal secara digital. Sehingga hasil secara keseluruhan dalam hal sekuritas akan sangat berpengaruh terhadap kualitas layanan komunikasi.

Kata kunci: VoIP, Kriptografi RC4, TMS320C6713, enkripsi.

I. PENDAHULUAN

VOICE *over Internet Protocol* (VoIP) merupakan teknologi komunikasi yang menggunakan jaringan IP dalam proses pengiriman paket data. Teknologi ini akan semakin berkembang dan banyak digunakan karena arah teknologi komunikasi yang menuju ke sistem berbasis IP. Pada komunikasi VoIP, pengguna tidak hanya mampu berkomunikasi melalui *voice* saja melainkan juga mampu melakukan komunikasi berupa video melalui *video call* dan juga teks atau yang lebih dikenal dengan *instant messaging*. Ini adalah salah satu kelebihan komunikasi VoIP dibandingkan dengan komunikasi analog melalui PSTN.

Sistem pengiriman menggunakan VoIP sangat dimungkinkan terjadinya penyadapan informasi. Beberapa kasus penyadapan informasi berupa paket data VoIP, yang mungkin terjadi adalah penyadapan pada jaringan *server* VoIP, maupun pembuatan jalur baru yang paralel dengan jalur yang ditentukan oleh *server* VoIP. Sehingga untuk mengatasi beberapa kasus tersebut diperlukan sebuah sistem pengamanan data (informasi).

Salah satu cara untuk menjaga keamanan dan kerahasiaan suatu data maupun informasi adalah dengan teknik enkripsi dan dekripsi guna membuat pesan, data maupun informasi agar tidak dapat dibaca atau dimengerti oleh sembarang orang, kecuali untuk penerima yang berhak. Teknik pengamanan data menggunakan enkripsi dan dekripsi ini dikenal dengan nama kriptografi, sebagai sebuah ilmu untuk mengamankan pesan atau data dengan cara menyamarkan pesan tersebut sehingga hanya dapat dibaca oleh pengirim dan penerima pesan pada jaringan VoIP. Metode enkripsi dengan algoritma kriptografi RC4 merupakan salah satu metode yang dapat digunakan untuk mengacak dan menerjemahkan sinyal audio.

Sekuritas jaringan VoIP menggunakan algoritma kriptografi RC4 akan diimplementasikan dengan *Digital Signal Processor* (DSP) jenis TMS320C6713. Pada DSP jenis TMS320C6713 digunakan metode transmisi tertentu dimana pengolahan sinyal digital secara *real time* dan terdapat rangkaian ADC (*Analog Digital Converter)*, DSP (*Digital Signal Processor)* dan DAC *(Digital Analog Converter)* yang terintegrasi menjadi satu sistem *embedded*.

Penelitian ini secara khusus akan mengeksplorasi masalah sekuritas jaringan VoIP dengan menggunakan algoritma kriptografi RC4 yang diterapkan pada DSP TMS320C6713, yaitu bagaimana merancang algoritma

Muhammad Fauzan Edy Purnomo adalah dosen Teknik Elektro Universitas Brawijaya, Malang, Indonesia (Telepon : 0341-554166; email : mfauzanep@ub.ac.id)

Wahyu Adi Priyono adalah dosen Teknik Elektro Universitas Brawijaya, Malang, Indonesia (Telepon : 0341-554166; email : wahjuapie@ub.ac.id)

Sapriesty Nainy Sari adalah dosen Teknik Elektro Universitas Brawijaya, Malang, Indonesia (Telepon : 0341-554166; email : nainy_sari@ub.ac.id)

Rusmi Ambarwati adalah dosen Teknik Elektro Universitas Brawijaya, Malang, Indonesia (Telepon : 0341-554166; email : rusmi@ub.ac.id)

Asri Wulandari adalah dosen Politeknik Negeri Jakarta, Depok, Indonesia (Telepon : 021-7863538; email : asri_fteub@yahoo.co.id)

enkripsi dan menganalisa performansi dari kriptografi RC4 dengan memanfaatkan TMS320C6713 dan jaringan VoIP berbasis SIP.

II. DASAR TEORI

A. *Voice over Internet Protocol (VoIP)*

IP Telephony, Internet Telephony, atau diistilahkan *Voice Over Internet Protocol* (VoIP) merupakan teknologi yang memanfaatkan *Internet Protocol* (IP) untuk menyediakan komunikasi suara secara *real-time*. VoIP adalah teknologi yang mampu melewatkan trafik suara, yang berbentuk paket melalui jaringan IP. Jaringan IP sendiri merupakan jaringan komunikasi data yang berbasis *packet-switch*. Sinyal suara sebelum dipaketkan mengalami *voice coding* atau pengubahan format suara kedalam bentuk digital agar dapat dilewatkan melalui jaringan IP.

Dalam perancangan jaringan VoIP, kelemahan dari sistem VoIP adalah keamanan panggilan VoIP yang bisa dilakukan penyadapan dari sumber (pengirim) ke tujuan (penerima) sehingga komunikasi suara dapat terekam dan privasi tidak terjamin. Konfigurasi jaringan VoIP secara umum ditunjukkan pada Gambar 1.

B. *Session Initiation Protocol (SIP)*

Session Initiation Protocol (SIP) adalah standar *Internet Engineering Task Force (*IETF*)* yaitu protocol pensinyalan pada layer aplikasi yang berfungsi untuk memulai, membangun, dan mengakhiri suatu sesi multimedia yang melibatkan satu atau beberapa pengguna. Sesi multimedia adalah pertukaran data antara pengguna yang meliputi suara, video, dan teks.

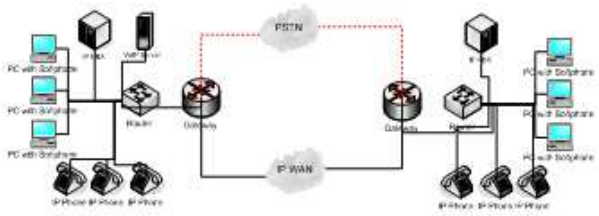
C. *Digital Signal Processor Starter Kit (DSK) TMS320C6713*

Digital Signal Processor (DSP) seri TMS320C6x adalah mikroprosesor berkecepatan tinggi dengan tipe arsitektur yang cocok digunakan untuk mengolah sinyal. Notasi C6x merupakan kode dari produk DSP keluaran Texas Instruments TMS320C6000. Dengan menggunakan arsitektur *Very Long Instruction Word* (VLIW), DSP C6x menjadi prosesor tercepat keluaran Texas Instruments. Gambar 2. menunjukkan diagram DSK TMS320C6713. Arsitektur VLIW pada DSP C6x sangat cocok untuk proses perhitungan yang intensif [1].

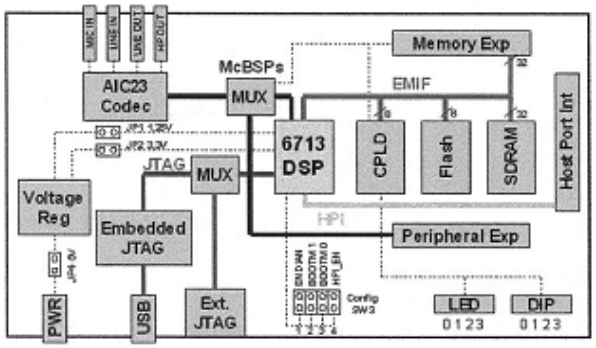
DSP dapat diaplikasikan sebagai pengontrol suara, pengolah gambar dan pengolah sinyal lainnya. DSP dapat ditemukan pada telepon seluler, *harddisk*, radio, printer, MP3 players, HDTV, kamera digital dan alat elektronik lainnya. DSP dapat melakukan banyak proses karena DSP dapat diprogram untuk aplikasi yang berbeda-beda. Selain itu, DSP sangat sedikit terpengaruh oleh perubahan kondisi lingkungan sekitar seperti suhu.

D. *Code Composer Studio (CCS) v3.1*

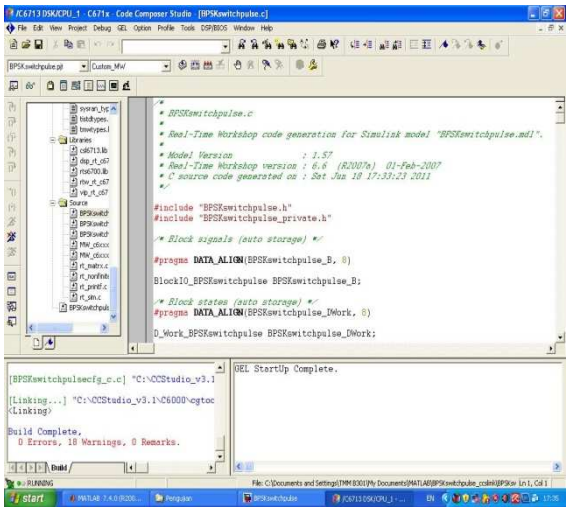
Code Composer Studio (CCS) merupakan perangkat lunak yang digunakan untuk menghasilkan kode seperti *C compiler*, *assembler* dan *linker* untuk DSK keluaran Texas Instruments. CCS memiliki kemampuan *real-time debugging*. *C compiler* mengkompilasi sebuah program dalam bahasa C dengan ekstensi **.c,* sedangkan untuk menghasilkan file *assembly* menggunakan ekstensi **.asm*. *Assembler* memproses file **.asm* untuk dihasilkan file bahasa mesin dengan ekstensi **.obj*. Kemudian *linker* menggabungkan file – file tersebut menjadi *executable file* dengan ekstensi **.out*. File ini dapat dimasukkan ke dalam prosesor C6713. DSK harus dihubungkan ke PC melalui port USB agar bisa diprogram dengan bantuan CCS [1].



Gambar 1. Jaringan VoIP.



Gambar 2. Diagram Blok DSK TMS320C6713 [1].



Gambar 3. Tampilan Code Composer Studio v3.1.

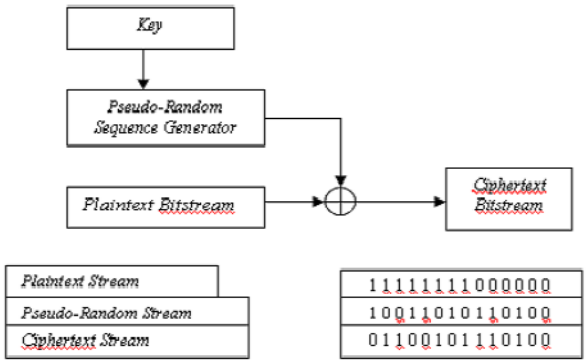
CCS juga mendukung kegiatan *debugging* antara lain: setting *Breakpoint*, secara otomatis meng-*update* jendela saat *breakpoint*, mengamati nilai variabel, melihat dan mengamati memori dan register, menggunakan *probe point* untuk menggalirkan data dari dan ke target untuk mengumpulkan *snapshot memory*, menggambarkan sinyal yang ada pada target,

melakukan *profiling* terhadap statistik eksekusi, memeriksa instruksi C dan instruksi yang di-*disassembly* pada target. Gambar 3. menunjukkan tampilan dari CCS v3.1.

E. Algoritma Kriptografi RC4

Algoritma kriptografi *Rivest Code* 4 (RC4) merupakan salah satu algoritma kunci simetris yang dibuat oleh RSA *Data Security Inc* (RSADSI) yang berbentuk *stream chipper*. Algoritma ini ditemukan pada tahun 1987 oleh Ronald Rivest dan menjadi simbol keamanan RSA (merupakan singkatan dari tiga nama penemu: Rivest Shamir Adleman). RC4 menggunakan panjang kunci dari 1 sampai 256 byte yang digunakan untuk menginisialisasikan tabel sepanjang 256 byte. Tabel ini digunakan untuk generasi yang berikut dari *pseudo random* yang menggunakan XOR dengan *plaintext* untuk menghasilkan *ciphertext*. Masing – masing elemen dalam tabel saling ditukarkan minimal sekali.

Untuk menunjukkan cara kerja dari algoritma RC4 dapat dilihat dalam blok diagram pada Gambar 4. RC4 menggunakan dua buah kotak substitusi (S-Box) array 256 byte yang berisi permutasi dari bilangan 0 sampai 255 dan S-Box kedua yang berisi permutasi fungsi dari kunci dengan panjang yang variabel. Cara kerja algoritma RC4 yaitu inisialisasi Sbox pertama, S[0],S[1],...,S[255], dengan bilangan 0 sampai 255. Pertama isi secara berurutan S[0] = 0, S[1] = 1,…, S[255] = 255. Kemudian inisialisasi array lain (S-Box lain), misal array K dengan panjang 256. Isi array K dengan kunci yang diulangi sampai seluruh array K[0], K[1],...,K[255] terisi seluruhnya.



Gambar 4. Blok Diagram Algoritma RC4 Secara Umum.

- Proses inisialisasi S-Box (Array S)
  For r = 0 to 255
  S[r] = r
- Proses inisialisasi S-Box(Array K)
  Array Kunci // panjang kunci"length".
  for i = 0 to 255
  K[i] = Kunci[i mod length]
- Kemudian dilakukan pengacakan S-Box dengan langkah sebagai berikut :
  j = 0
  For i = 0 to 255
  j = (j + S[i] + K[i]) mod 256
  isi S[i] dan isi S[j] ditukar

Dengan demikian berakhirlah proses persiapan kunci RC4. Untuk membangkitkan kunci enkripsi, dilakukan proses sebagai berikut:

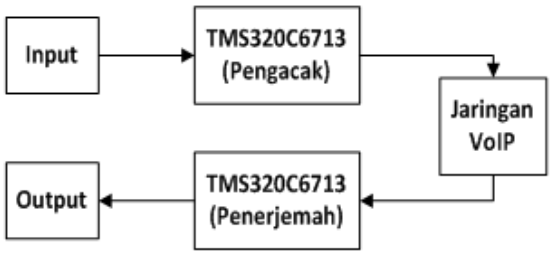
i = j = 0
i = (i + 1) mod 256
j = (j + S[i]) mod 256
isi S[i] dan S[j] ditukar
k = S [S[i] + S[j]] mod 256

Perhatikan bahwa k kecil merupakan kunci yang langsung beroperasi terhadap plainteks, sedangkan K besar adalah kunci utama atau kunci induk.

III. METODE PENELITIAN

Data yang diambil dalam penelitian ini meliputi data primer dan data sekunder. Data primer berupa pengukuran secara langsung terhadap perancangan sistem, sistem yang dimaksud adalah kriptografi RC4 sebagai pendukung sekuritas pada VoIP *(Voice over Internet Protocol)* berbasis *SIP (Session Initiation Protocol)* dengan memanfaatkan TMS320C6713 yang terdiri dari perangkat keras dan perangkat lunak, yang akan dirancang sesuai dengan teori yang berkaitan dengan kriptografi RC4, VoIP *(Voice over Internet Protocol)* berbasis *SIP (Session Initiation Protocol)* dan TMS320C6713. Data sekunder berupa studi literatur diambil dari buku teks, jurnal, internet, standart, maupun data dari sumber lain yang berhubungan penerapan kriptografi RC4 sebagai pendukung sekuritas pada VoIP *(Voice over Internet Protocol)* berbasis *SIP (Session Initiation Protocol)* dengan memanfaatkan TMS320C6713.

Perancangan blok diagram ini digunakan sebagai acuan untuk menerapkan metode kriptografi RC4 sebagai pendukung sekuritas pada VoIP *(Voice over Internet Protoco)* berbasis SIP *(Session Initiation Protocol)* dengan memanfaatkan TMS320C6713. Blok diagram yang disusun terdiri dari sinyal masukan, TMS320C6713, komputer, jaringan VoIP dan sinyal keluaran seperti pada Gambar 5.



Gambar 5. Blok Diagram Penerapan Metode Kriptografi RC4 pada VoIP.

IV. HASIL DAN PEMBAHASAN

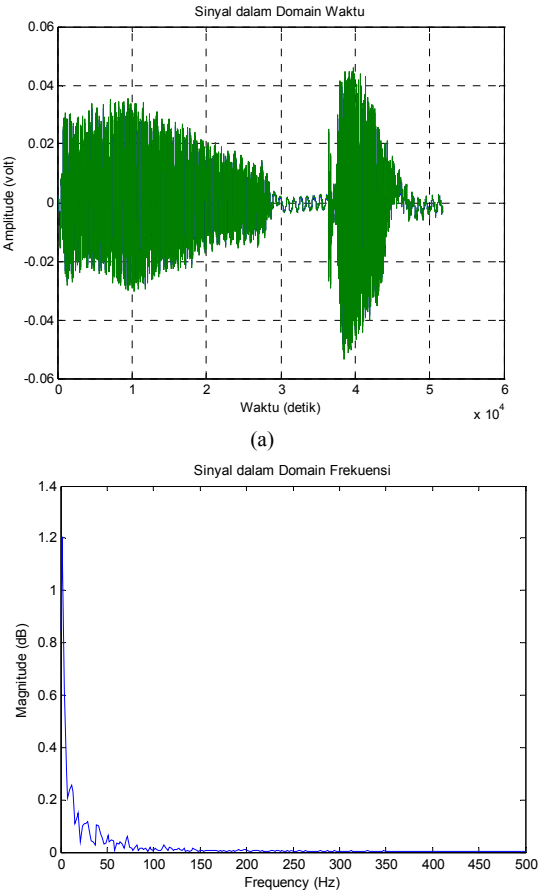
A. Pengujian Kanal Masukan TMS320C6713

Sebelum suara diamankan dengan cara diacak menggunakan algoritma kriptografi RC4 yang dioperasikan oleh TMS320C6713, maka dilakukan

pengujian untuk memastikan bahwa data yang akan diamankan sudah benar.

Pengujian ini bertujuan untuk mengetahui sinyal suara masukan pada *line input* TMS320C6713 sebagai sinyal informasi asli sebelum diacak. Variabel yang diamati pada pengujian ini adalah kekonsistensian sinyal masukan dari segi amplitude dan frekuensi.

Data hasil pengujian kanal masukan adalah sinyal suara dalam domain waktu dan frekuensi. Berikut ini merupakan hasil pengujian kanal masukan ditampilkan dalam Gambar 6. hasil pengujian pertama dan Gambar 7. hasil pengujian kedua.



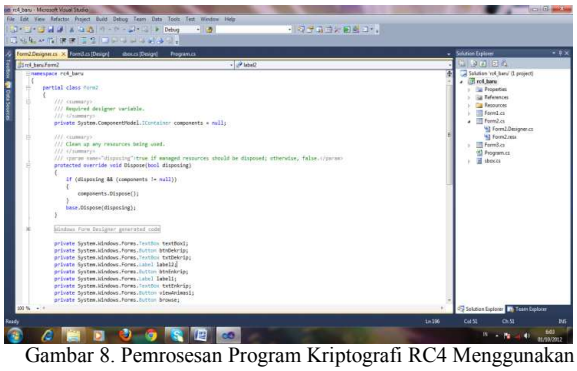
Gambar 6. Hasil Pengujian Kanal Masukan Berupa Suara Manusia Pengujian Pertama dalam (a) Domain Waktu dan (b) Domain Frekuensi.

B. *Pengujian Jaringan VoIP*

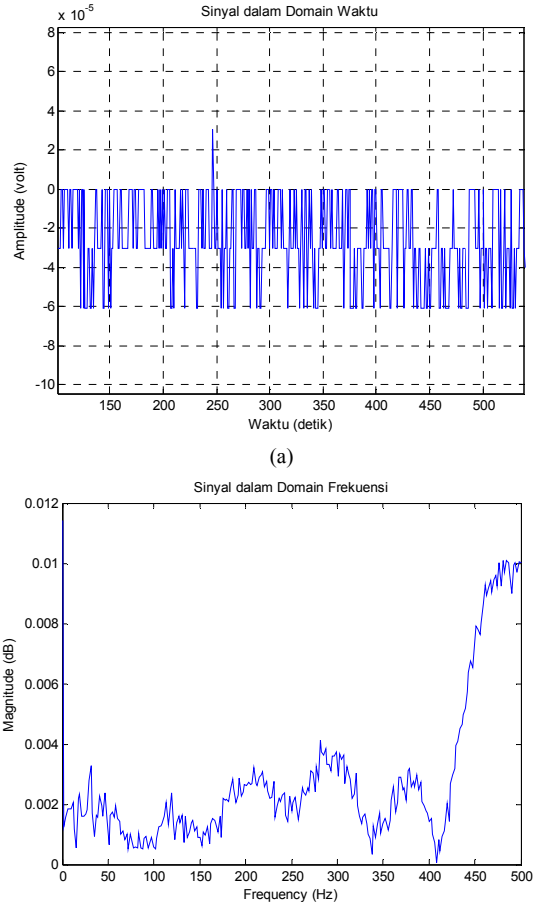
Setelah melakukan pengujian kanal pada TMS320C6713, selanjutnya pengujian koneksi jaringan VoIP yaitu antara *server* dengan *client* dan antara *client* dengan *client.* Adapun data hasil pengujian berupa respon waktu pengiriman paket data uji pada saat perintah dituliskan sampai perintah dikirimkan kembali oleh *server* atau *client* yang dituju.

Pengujian *client* bertujuan untuk mengetahui VoIP *client* sudah terdaftar (register) pada *server* VoIP dengan benar sehingga dapat melakukan panggilan ke semua *client* yang sudah terdaftar pada *server.* Data hasil pengujian *client* berupa respon-repon dari aliran pensinyalan menggunakan *SIP* serta proses terjadinya panggilan meliputi pembentukan panggilan, sesi bicara antar *client* serta mengakhiri panggilan.

Pengujian *server* bertujuan untuk mengetahui PC *server* dapat bekerja dengan baik dalam melayani registrasi dari VoIP *client*. Data hasil pengujian *server* berupa respon – respon dari aliran pensinyalan menggunakan SIP serta proses registrasi *client.*



Gambar 8. Pemrosesan Program Kriptografi RC4 Menggunakan *Microsoft Visual Studio 2010.*



Gambar 7. Hasil Pengujian Kanal Masukan Berupa Suara Manusia Pengujian Kedua dalam (a) Domain Waktu dan (b) Domain Frekuensi.

C. *Pengujian Algoritma Kriptografi RC4*

Kriptografi RC4 merupakan algoritma yang akan diunduh ke dalam perangkat TMS320C6713 melalui program *Code Composer Studio v3.1* (CCS v3.1) dengan bahasa pemrograman C++. Kriptografi RC4

diimplementasikan secara *real time* dengan menggunakan prosesor DSP yang terintegrasi pada suatu *starter kit,* yakni DSP *Starter Kit* TMS320C6713. Tahap pertama dalam perancangan sistem ini adalah melakukan simulasi terhadap algoritma kriptografi RC4 dengan menggunakan program *Microsoft Visual Studio 2010* untuk melihat performansi dari algoritma kriptografi RC4 sebagai sekuritas jaringan (Gambar 8).

Secara garis besar algoritma dari metode RC4 ini terbagi menjadi dua bagian, yaitu:

- Setup Kunci

  Pada bagian ini, terdapat tiga tahapan proses yaitu :

  - 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
  - Menyimpan *key* dalam *Key Byte Array*

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

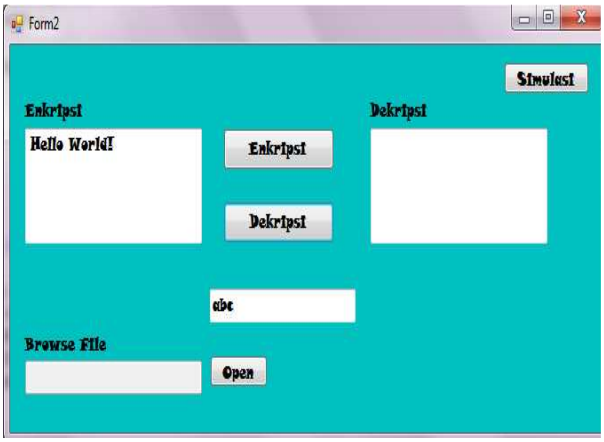
- Proses Enkripsi dan Dekripsi

  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 :

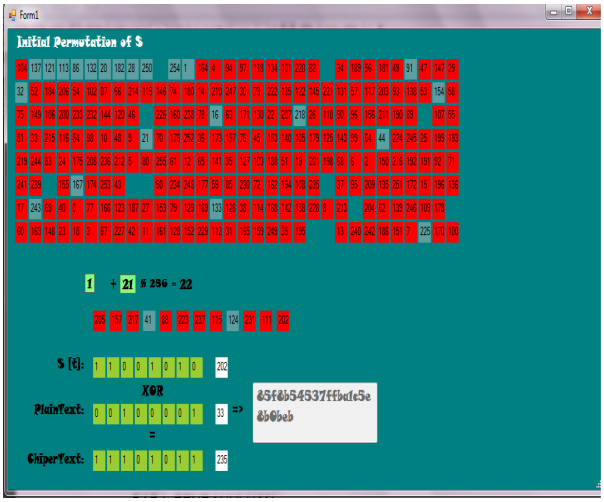
  x= y = 0
  x = (x+1) mod 256
  y = (y + S[x]) mod 256
  pertukarkan isi S[i] & S[j]
  k = S[(S[x] +S[y]) mod 256]

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

Pengujian algoritma kriptografi RC4 yang telah dibuat pada proses enkripsi data dilakukan dengan memasukkan data asli berupa pesan 'Hello World!' dengan kata kunci 'abc' seperti yang ditampilkan dalam Gambar 9.



Gambar 9. Proses Enkripsi dengan Algoritma RC4.



Gambar 10. Proses Pengacakan dengan Metode RC4.

Selanjutnya data masukan akan diacak dengan proses pengacakan yang telah dijelaskan pada bab sebelumnya. Adapun hasil proses pengacakan pesan dengan metode RC4 dapat dilihat pada Gambar 10. Hasil proses enkripsi kata 'Hello World!' adalah '85f8b54537ffba1c5e8b0beb'.

V. KESIMPULAN

Sistem perancangan pada penerapan kriptografi RC4 sebagai pendukung sekuritas pada VoIP *(Voice over Internet Protocol)* berbasis SIP *(Session Initiation Protocol)* dengan memanfaatkan TMS320C6713 terdiri dari sistem pengacak dan penerjemah.

Perangkat keras yang terdiri dari TMS320C6713, komputer, *sound card*, *microphone*, *speaker*, konektor audio, konektor USB, Kabel UTP, serta HUB yang dirancang sesuai dengan fungsinya untuk membangun sistem perancangan. Perangkat lunak yang dirancang adalah perangkat lunak kriptografi RC4.

Penerapan kriptografi RC4 dengan memanfaatkan TMS320C6713 dapat menjadi salah satu sistem sekuritas yang dilakukan dengan cara mengacak sinyal informasi sebelum ditransmisikan sehingga jika terjadi

penyadapan dengan cara yang sama, maka yang didapatkan adalah sinyal teracak.

REFERENCES

[1] [1] R. Chassaing, "Digital Signal Processing and Application with the C6713 and C6416 DSK", Wiley-Interscience, United State of America, Ch. 1, 2005.

[2] [2] B. Schneier, "Applied Cryptography: Protocols, Algorithms and Source Code in C", 2nd edition, John Wiley & Sons, Inc., USA, 1996.

[3] [3] http:// www.newport-networks.com/VoIP-Bandwidth.pdf

[4] [4] http://www.cisco.com/en/US/tech/tk652/tk698

[5] [5] Spectrum Digital (2003). TMS320C6713 DSK Technical Reference. Stafford: Spectrum Digital Inc.

[6] [6] Texas Instruments (2001). TMS320C6713 Floating-Point Digital Signal Processor. USA: Texas Instruments.