RANCANGAN SISTEM KEAMANAN AERONAUTICAL TELECOMMUNICATION NETWORK MESSAGE HANDLING SYSTEM MENGGUNAKAN ALGORITMA KRIPTOGRAFI BERBASIS RASPBERRY PI

Adiemas Setya Bhakti[1], Yuyun Suprapto[2], Setiyo[3]
[1,2, 3)] Politeknik Penerbangan Surabaya
Jl. Jemur Andayani I/73, Surabaya 60236
Email: setyadimas97@gmail.com

Abstrak

Jaringan *Aeronautical Fixed Telecommunication Network* (AFTN) adalah suatu jaringan yang berperan penting dalam sistem telekomunikasi data penerbangan di dunia penerbangan internasional. Karena jaringan ini menghubungkan antara bandara satu dengan lainnya dan memuat data penerbangan untuk informasi peswat terbang yang sedang beroperasi. Ketika jaringan ini mengalami gangguan non teknis seperti interferensi data, peretasan sistem, penyadapan, dan *hacking*. Maka akan sangat berbahaya bagi pihak yang terkait. Sebab akibatnya bisa menyebabkan pesawat berubah arah atau bandara yang dituju belum siap untuk menyediakan fasilitas yang dibutuhkan pesawat terbang. Tujuan penelitian ini adalah menciptakan rancangan sistem keamanan menggunakan teknologi kriptografi yang berorientasi pada keamanan data penerbangan. Sistem keamanan ini akan megacak bit dari teks pesan yang dikirimkan dan akan dilakukan proses penyandian untuk mendapatkan data rahasia yang acak dan tidak mudah di retas dan pada tujuan akan kembali di terjemahkan dengan teknologi kriptografi yang sama. Sehingga data penerbangan akan tetap utuh dan aman.

Kata Kunci : Sistem Keamanan, Algoritma Kriptografi RC5, Raspberry PI

PENDAHULUAN

Suatu sistem keamanan data sangat diperlukan untuk menjaga keutuhan dan kerahasiaan data penerbangan sehingga data penerbangan dapat dikirm secara aman guna keselamatan penumpang pesawat udara, crew pesawat udara, pihak airline, dan pihak bandara. Metode yang tepat untuk mengamankan data penerbangan adalah Kriptografi. Kriptografi merupakan sistem penyandian dengan merubah teks asli (plaintext) menjadi teks sandi (cipher text) dengan algoritma tertentu sehingga akan menyulitkan pihak – pihak tidak berkepentingan untuk merubah, memodifikasi, dan merusak isi berita yang dikirimkan. Proses enkripsi dan dekripsi akan diperlukan dalam sistem ini. Enkripsi dan dekripsi yang digunakan adalah algoritma *rivest code 5* karena menurut peneliti algoritma ini adalah salah satu jenis lightweight cryptography yang cocok untuk dunia penerbangan karena ringan digunakan pada AFTN dan tidak menimbulkan penumpukan bit pada data atau informasi yang akan disandi

Berdasarkan identifikasi masalah yang telah diuraikan diatas maka dapat dirumuskan permasalahan sebagai berikut:

Bagaimana cara membuat sistem keamanan data pada jaringan penerbangan ?

Bagaimana cara melakukan enkripsi dan dekripsi pada teks berita AFTN menggunakan algoritma kriptografi?

Bagaimana mengaplikasikan algoritma kriptografi berbasis raspberry PI pada jaringan AFTN?

METODE

Perangkat CIP-98 ini adalah perangkat yang dapat digunakan untuk melakukan enkripsi dan dekripsi data dengan menggunakan private key dan public key. Perangkat CIP-98 menggunakan Raspberry PI sebagai modul sandi (crypto machine) yang diimplementasikan menggunakan algoritma kriptografi *Rivest Code 5* pada mikrontrollernya. Perangkat modul sandi ini digunakan untuk keperluan mempertahankan keutuhan data dan mengantisipasi apabila terjadi interferensi berupa penyadapan dari pihak yang tidak berkepentingan. Pada Raspberry PI yang digunakan, perangkat ini memilik fitur algoritma sandi pada micro SD dan memiliki Ghost Protocol pada gatewaynya. Berbasis ilmu kriptologi dan intelijen sinyal maka perangkat ini disebut CIP-98 oleh perancang modul. CIP-98 adalah singkatan dari Crypto Intelligent Protocol dan 98 adalah kode khusus dari pembuat alat.. Penggunaan CIP-98 ini harus melewati 3 tahap yaitu :

Proses Instalasi

Pada tahap ini, pengguna harus melakukan pemasangan perangkat CIP-98 pada PC pengguna dengan cara menghubungkan kabel UTP *crossover* melalui *port Ethernet* pada CIP-98 dan PC. Pengguna juga harus menghubungkan kabel *micro* USB melalui *port power* pada CIP-98 dengan *port* USB pada PC. Prosedur yang dilakukan harus berurutan, yaitu menghubungkan kabel UTP dahulu setelah itu menghubungkan kabel *micro* USB sebagai sumber daya listrik pada perangkat CIP-98. Hal ini dimaksudkan agar ketika perangkat CIP-98 ini menyala, layar LCD 20x4 dapat langsung menampilkan alamat IP pada *interface* eth0 yang diperlukan untuk mengoneksikan PC dengan perangkat melalui SSH.

Proses Konfigurasi

Setelah memastikan bahwa instalasi selesai, maka pengguna melakukan konfigurasi PC dengan perangkat CIP-98. Konfigurasi dilakukan dengan cara mengatur alamat PC tujuan menggunakan IP config. Setelah itu melakukan ping data dari PC pengirim ke PC penerima. Beberapa hal yang harus diperhatikan dalam konfigurasi adalah :

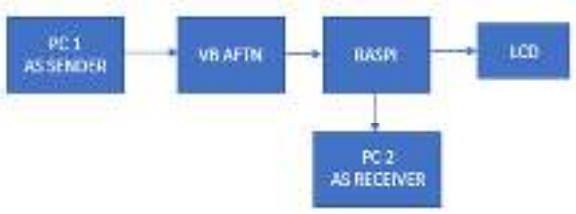
1. setting aplikasi pengirim data penerbangan di PC pengirim
2. setting inputan format AFTN sesuai dengan prioritas
3. IP atau alamat tujuan adalah valid
4. Monitoring pada Raspberry PI di perangkat CIP-98 yang bertindak sebagai central kontrol

Proses Aktivasi

Proses aktivasi dilakukan jika semua perangkat CIP-98 telah terpasang dengan baik maka akan dilakukan proses pengiriman data dari PC pengirim ke PC tujuan. Pada PC pengirim, pengguna akan memasukkan format Aeronautical Fixed Telecommunication Network (AFTN) dan teks berita yang akan dikirimkan. Setelah teks berita di ketik dan dikirimkan, maka data tersebut akan di monitoring pada PC Entitas dan akan masuk ke CIP-98 kemudian akan dilakukan proses enkripsi. Data akan di enkrip sesuai dengan key yang dimasukkan. Setelah di enkrip akan masuk ke PC penerima dengan key yang telah di otentifikasi di PC pengirim dan perangkat CIP-98. Maka Modul Sandi CIP-98 siap digunakan.

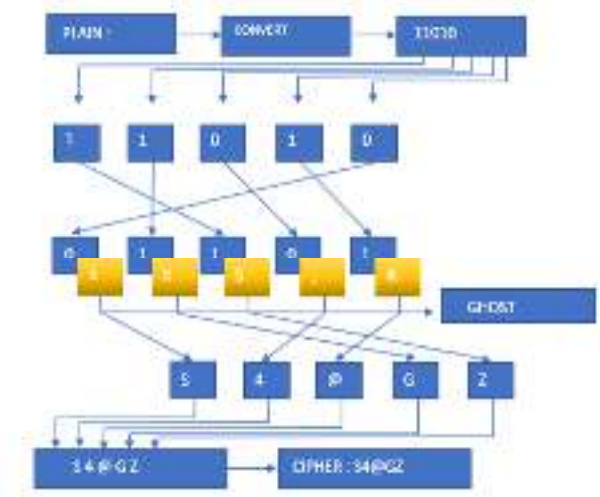
Konsep Blok Diagram

Berikut adalah gambaran singkat secara keseluruhan dan sistem ini adalah:

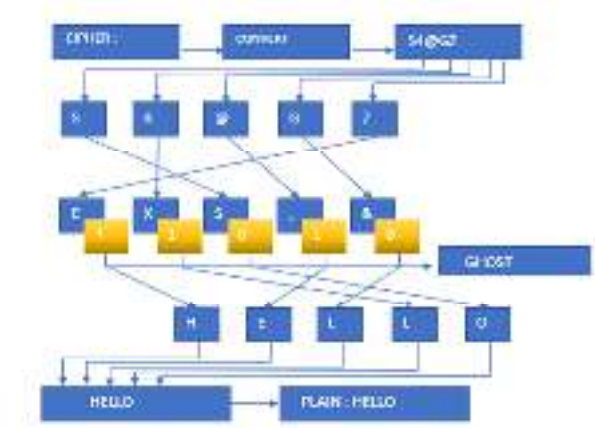


Blok diagram di atas menjelaskan bahwa PC1 sebagai pengirim berita dan diumpamakan sebagai Telex 1 yang mengirim data penerbangan melalui AFTN. Kemudian terdapat software menggunakan visual basic 6.0 yang berfungsi sebagai *checker* format AFTN. Jika tidak sesuai maka akan kembali ke PC1 jika sesuai akan dilanjutkan ke Raspberry PI dan terjadi proses penyandian dengan algoritma kriptografi *Rivest Code 5*. Sehingga Raspberry PI disebut modul sandi yang diberi nama CIP-98. Pemberitahuan PC pangirim dan penerima akan terlihat pada LCD yang tersambung pada modul sandi. Hasil enkripsi akan masuk pada PC2 sebagai penerima atau diumpamakan sebagai Telex 2. PC2 akan mendapatkan informasi teks berita yang telah di enkripsi menjadi teks sandi

Proses Enkripsi :



Proses Dekripsi :



Identifikasi Kebutuhan Perangkat Lunak dan Perangkat Keras

Berdasarkan perancangan yang telah dibahas, maka modul sandi CIP-98 ini membutuhkan beberapa perangkat lunak dan perangkat keras sebagai penunjang agar CIP-98 dapat bekerja secara optimal. Baik perangkat lunak atau perangkat keras untuk mengoperasikan CIP-98 ini memili spesifikasi khusus. Yaitu harus memenuhi kualifikasi sebagai peralatan rancang bangun peralatan sandi atau disebut rancang bangun palsan dan peralatan intelijen sinyal (L.B Moerdani,2000). Komponen yang digunakan untuk merancang CIP-98 ini adalah

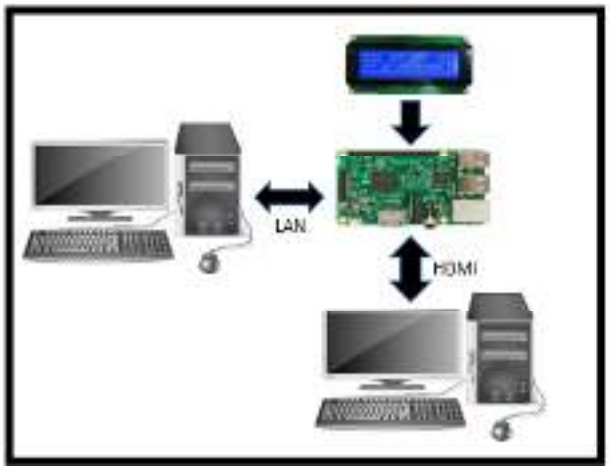
Perangkat Keras

Perancangan penelitian ini menggunakan SBC Raspberry PI sebagai perangkat keras CIP-98. Daftar komponen perangkat keras untuk membangun dan merancang modul sandi CIP-98 adalah sebagai berikut

1		
2		
3		
4		
5		-
6		-

Interface jaringan yang ada di SBC Raspberry PI adalah interface ethernet oleh karena itu peneliti menggunakan kabel UTP sebagai penghubung PC (personal computer) terhadap modul sandi CIP-98. SBC Raspberry PI akan ditambahkan dengan LCD 20x4 sebagai monitor agar user dapat mengetahui IP atau alamat PC pengirim. LCD 20x4 ini dihubungkan oleh kabel jumper female to female dengan perangkat SBC Raspberry PI sebagai interfaci modul sandi (crypto machine) CIP-98. Kabel power USB to Micro USB digunakan sebagai power input SBC Raspberry PI karena input power hanya dapat

menggunakan kabel Micro USB sedangkan USB port digunakan pada adaptor dan terhubung dengan source PLN 220 V. Perangkat keras selanjutnya adalah Acrylic Case yang berfungsi sebagai case pada SBC Raspberry PI agar meningkatkan keamanan modul sandi CIP-98 secara fisik. Rancangan secara perangkat keras (hardware) adalah sebagai berikut

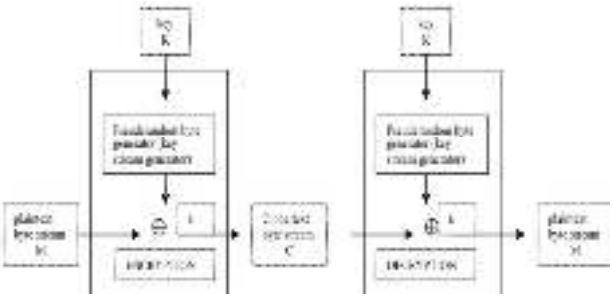


Perangkat Lunak

Pada penelitian penelitian ini dibutuhkan perangkat lunak yang secara umum dikembangkan dengan bahasa pemrograman C. Perangkat lunak yang dirancang adalah Lightweight Cryptography dengan algoritma kriptografi *Rivest Code 5* yang beroperasi pada perangkat CIP-98. Lightweight Cryptography dengan algoritma kriptografi *Rivest Code 5* merupakan modifikasi dari Algoritma RC 4. Perbedaan antara algoritma kriptografi *Rivest Code 5* dengan Algoritma RC 4 adalah ditambahkannya algoritma pengunci sebagai algoritma dasar kriptografi yang dikembangkan menjadi Lightweight Cryptography. *Lightweight Cryptography* tersebut diimplementasikan pada *library crypto* yang ada di dalam jaringan AFTN (Aeronautical Fixed Telecommunication Network) sebagai penyuplai algoritma kriptografi pada modul sandi CIP-98. Untuk melakukan implementasi pada jaringan AFTN (Aeronautical Fixed Telecommunication Network) tersebut, perlu dirancang algoritma kriptografi (Ciphersuites) baru. *Ciphersuites* tersebut merupakan kombinasi antar beberapa algoritma kriptografi RC5 dengan algoritma dasar enkripsi sebagai algoritma penyandian data (*bulk encryption algorithm*). Kombinasi algoritma yang kemudian menjadi *ciphersuites* terdiri dari algoritma otentikasi *server*, algoritma pertukaran kunci, algoritma penyandian data, dan algoritma *hash* atau protokol. Daftar komponen perangkat lunak untuk membangun dan merancang modul sandi CIP-98 adalah sebagai berikut.

HASIL DAN PEMBAHASAN

Pengujian enkripsi merupakan pengujian performa penyandian data dengan menggunakan algoritma *Rivest Code 5* (RC5) dan algoritma pesan digital berupa *Message Digest 5* (MD5) untuk pesan yang dikirimkan melalui AMSC pada jaringan AFTN. Sistem enkripsi ini dibuat berdasarkan sistem AMSC baik menggunakan analog atau *IP Base*. Sistem enkripsi telah dibuat dengan software *NetBeans IDE 8.2* dan *Raspbian Jessie* pada perangkat Raspberry PI 3.



Berdasarkan blok diagram sistem enkripsi diatas dapat dilihat bahwa *plaintext byte stream* adalah teks berita yang akan dikirimkan oleh AMSC yang dibuat dengan *IP Base*. Salah satu bandara yang sudah menggunakan AMSC yang berbasis *IP Base* adalah Bandara Internasional Soekarno-Hatta Tangerang. AMSC yang berbasis IP adalah *Automatic Message Handling System* (AMHS) yang dirawat dan dioperasikan oleh teknisi Otomasi di Airnav Cabang Utama Jakarta Air Traffic Services Center (JATSC). *Pseuderandom byte generator* menciptakan kombinasi *byte* yang digabung dengan *key algorithm* oleh *Rivest Code 5* dan *Message Digest 5* sehingga menjadi *Ciphertext byte Stream* yang disebut teks enkripsi.

Source code tersebut dibuat untuk melakukan enkripsi dan dekripsi dengan menggunakan algoritma penyandian yang ditentukan. Bahasa pemrograman yang digunakan adalah Java. Setelah *script* dibuat dan dapat di *compile* dengan baik tanpa *error* maka langsung masuk ke dalam sistem mini AMHS pada bagian *Message Security Protocol* yang telah dibuat. User harus memasukan *username* dan *password* untuk bisa mengakses sistem dan melakukan pengiriman berita.

Hasil pengujian merupakan hasil akhir yang diperoleh dari pengujian enkripsi pada Modul CIP-98 dengan menggunakan algortima *Rivest Code 5* (RC5) dan algoritma pesan digital *Message Digest 5* (Md5) pada pesan berita yang dikirim dengan menggunakan AMHS dan AFTN atau ATN sebagai jaringannya.

Sebuah pesan disebut terkirim sempurna apabila dapat diterima oleh tujuan dalam keadaan utuh dan tidak ada perbedaan sedikitpun. Oleh karena itu dibutuhkan pengamanan data di era digital seperti ini untuk memastikan bahwa data terkirim sempurna.

Dari gambar diatas dapat dilihat bahwa pesan yang semula terbaca dapat diacak sedemikian rupa sehingga mejadi karakter yang tidak bisa dibaca karena masing – masing bit dalam pesan berita akan dipecah dan diolah dengan

algortima untuk menjadi karakter yang berbeda. Nilai Hash yang dihasilkan oleh algoritma *Message Digest* (Md5) akan membuat pesan tersebut menjadi bahasa unik yang didalamnya terkandung susunan yang sulit di pecahkan. Algoritma *Message Digest 5* (Md5) memeiliki cara kerja sebagai berikut :

Penambahan bit-bit pengganjal (*padding bits*).

a. Pesan ditambah dengan sejumlah bit pengganjal sedemikian sehingga panjang pesan (dalam satuan bit) kongruen dengan 448 modulo 512.
b. Jika panjang pesan 448 bit, maka pesan tersebut ditambah dengan 512 bit menjadi 960 bit. Jadi, panjang bit-bit pengganjal adalah antara 1 sampai 512.
c. Bit-bit pengganjal terdiri dari sebuah bit 1 diikuti dengan sisanya bit 0.

Penambahan nilai panjang pesan semula

a. Pesan yang telah diberi bit-bit pengganjal selanjutnya ditambah lagi dengan 64 bit yang menyatakan panjang pesan semula.
b. Jika panjang pesan > 264 maka yang diambil adalah panjangnya dalam modulo 264. Dengan kata lain, jika panjang pesan semula adalah *K* bit, maka 64 bit yang ditambahkan menyatakan *K* modulo 264.
c. Setelah ditambah dengan 64 bit, panjang pesan sekarang menjadi kelipatan 512 bit.

Inisialisasi penyangga *Message Digest/Hash*

a. *MD5* membutuhkan 4 buah penyangga (*buffer*) yang masing-masing panjangnya 32 bit. Total panjangpenyangga adalah 4 ´ 32 = 128 bit.
b. Keempat penyangga ini menampung hasil antara dan hasil akhir.Keempat penyangga ini diberi nama *A*, *B*, *C*, dan D. Setiap penyangga diinisialisasi dengan nilai-nilai (dalam notasi HEX) sebagai berikut :
   A = 01234567
   B = 89ABCDEF
   C = FEDCBA98
   D = 76543210

Pengolahan pesan dalam blok berukuran 512 bit

a. Pesan dibagi menjadi *L* buah blok yang masing-masing panjangnya 512 bit (*Y*0 sampai *YL* – 1).
b. Setiap blok 512-bit diproses bersama dengan penyangga *MD* menjadi keluaran 128-bit, dan ini disebut proses *H*MD5.

Pesan dapat terenkripsi karena di dalam modul sandi CIP-98 yang menggunakan *Raspberry PI 3* sebagai Hardware telah diberikan algoritma sandi untuk melindungi data dari berbagai serangan digital karena data yang dikirim menggunakan bit yang dapat di transformasikan ke dalam bentuk biner dengan menggunakan tabel ASCII per karakternya sehingga data dapat dengan mudah di interferensi apabila tidak diberikan perlindungan. Selain dengan perlindungan data modul CIP-98 ini juga dilengkapi dengan perlindungan protokol khusus dengan menggunakan SSH karena jika tidak menggunakan *Raspberry PI 3* ini maka tidak akan bisa melakukan enkripsi data. Bukan hanya dari sektor data namun juga dari sektor jaringan.

Pembuatan AMHS ini merupakan *upgrade* dari AMSC yang telah berbasis IP yang sudah digunakan oleh Bandara Udara Internasional Soekarno-Hatta Jakarta tepatnya AMHS ini berada di Perum LPPNI Cabang Utama Jakarta Air Traffic Services Center (JATSC) yang sudah berbasis IP dan peneliti membuat replika kecil sistem yang ada pada AMHS dengan tambahan Protokol perlindungan data.

PENUTUP

Simpulan

Berdasarkan perancangan, pembuatan, pengujian dan analisa rancangan keamanan rancangan sistem keamanan jaringan aeronautical fixed telecommunication network menggunakan algoritma kriptografi RC5 berbasis raspberry pi, maka dapat diambil kesimpulan bahwa Algoritma kriptografi hanya

diterapkan melalui Raspberry PI saja sebagai modul sandi untuk melakukan proses enkripsi dan dekripsi. Hanya pada bagaian teks berita yang dilakukan enkripsi dan dekripsi karena format berita AFTN baik menggunakan AMSC atau AMHS sudah ditetapkan oleh ICAO pada ANNEX 10 volume 2

Saran

Saran yang dapat diberikan peneliti guna mempermudah untuk mengembangakan renacangan ini mengikuti perkembangan teknologi di masa depan adalah Penggunakan algoritma penyandian lain yang lebih kuat dan lebih aman sesuai dengan perkembangan zaman untuk mengembangkan teknologi agar dapat berguna pada dunia penerbangan

DAFTAR PUSTAKA

Sumarkidjo. 2007. *Jelajah Kriptologi*. Jakarta : Lemsaneg RI

Wiley. 2007. *Computer Security and Cryptography*. Amerika : Bicentennial

Menezes, Alfred. 1996. *Handbook of Applied Cryptography*. Massachusetts : Massachusetts Institute of Technology

Poltekbang. 2017. *Modul Telekomunikasi III Automatic Message Switching Center*. Surabaya : Politeknik Penerbangan Surabaya Prodi Teknik Telekomunikasi dan Navigasi Udara

Poltekbang. 2017. *Modul Telekomunikasi II Telekomunikasi Penerbangan*. Surabaya : Politeknik Penerbangan Surabaya Prodi Teknik Telekomunikasi dan Navigasi Udara

Jubliee. 2017. *Otodidak Pemrograman Python*. Jakarta : PT Elex Media Komputindo