artikel 1

by Nuniek Indah

Submission date: 05-Sep-2021 09:05AM (UTC+0700)
Submission ID: 1641499816
File name: 2140-Hasil_penelitian-10334-1-18-20210820.pdf (564.98K)
Word count: 3719
Character count: 22819

Aplikasi Data Pasien Dengan Kriptografi pada HOTSPODT (Hospital Ship for Covid Disaster)

(Patient Data Application with Cryptography on HOTSPODT (Hospital Ship for Covid Disaster))

[1], [2]

***Abstract*— Based on official distribution data via web:covid19.co.id, last update July 6, 2021, positive cases in Indonesia reached 2,345,018. Healed reached 1,958,553, and who died reached 61,868. In addition to patients, victims of COVID-19 are also medical personnel. In this study, Wireless Body Area Network (WBAN) technology can help reduce direct contact interactions between patients and medical personnel with a remote health monitoring system whose application is aboard HOTSPODT (Hospital Ship For Covid Disaster). There is a patient isolation room with a health worker room separated by a bulkhead. In addition, there is a sterilization room between the isolation room and the health worker room that utilizes the development of digital technology, the big problem is the security problem of patient data medical records that can be misused in identity theft or filing false insurance claims by third parties. The methodology uses cryptography encryption decryption with blowfish algorithm for files with extension .doc and .pdf, application programming is implemented using java netbeans. The results of the security of medical records of patient data are sent to the authorized user in the form of ciphertext and given the same key to open the encryption.**

***Intisari*—Berdasarkan data sebaran resmi melalui *web:covid19.co.id update* terakhir 06 Juli 2021 kasus positif di Indonesia mencapai 2.345.018. Sembuh mencapai 1.958.553, dan yang meninggal mencapai 61.868. Selain pasien, korban *covid19* juga para tenaga medis. Pada penelitian ini, teknologi *Wireless Body Area Network* (WBAN) dapat membantu mengurangi kontak interaksi secara langsung antara pasien dan tenaga medis dengan sistem monitoring kesehatan jarak jauh yang penerapannya dikapal HOTSPODT (*Hospital Ship For Covid Disaster*). Terdapat ruang isolasi pasien dengan ruang tenaga kesehatan yang terpisah oleh sekat. Selain itu terdapat ruang sterilisasi antara ruang isolasi dengan ruang tenaga kesehatan yang memanfaatkan perkembangan teknologi *digital*, permasalahan besarnya adalah masalah keamanan rekam medis data pasien yang dapat disalahgunakan dalam memakai identitas secara ilegal atau pemakaian manipulasi syarat asuransi oleh pihak ketiga. Metodologi menggunakan kriptografi enkripsi dekripsi dengan algoritma *blowfish* untuk file ber*extention* *.doc* dan *.pdf*, aplikasi *programming* diimplementasikan menggunakan *java netbeans*. Hasil dari keamanan rekam medis data pasien dikirimkan kepada *user* yang berhak berupa *ciphertext* dan diberikan kunci yang sama untuk membuka enkripsinya.**

***Kata Kunci*— WBAN, Kriptografi, *Blowfish*, HOTSPODT.**

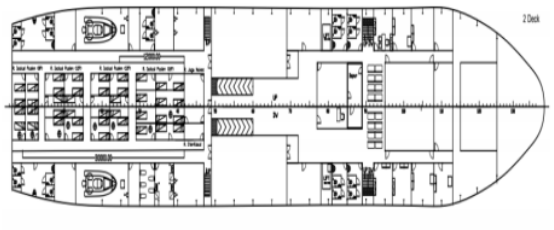
I. PENDAHULUAN

Covid-19 (*Corona Virus Dissease*-2019) adalah penyakit menular yang disebabkan oleh virus. Berdasarkan data sebaran resmi melalui *website* di [1] *update* terakhir 06 Juli 2021 kasus positif di Indonesia mencapai 2.345.018. Sembuh mencapai 1.958.553, dan yang meninggal mencapai 61.868. Petugas dari Ikatan Dokter Indonesia (IDI), Halik Malik pada tanggal 26 April 2020 mengatakan bahwa dari data terlapor IDI terdapat 24 dokter, 6 dokter gigi, dan 17 perawat meninggal dunia akibat tertular dan terinfeksi virus corona. (*BBC News*). Untuk mengurangi tingkat kontak langsung antara pasien dengan tenaga medis guna menurunkan resiko penularan dari pasien ke tenaga medis maka diperlukan solusi yang memanfaatkan perkembangan teknologi *digital*. Digitalisasi menjadi *era* baru yang menghubungkan banyak peralatan *hardware* dimonitoring secara *virtual* menggunakan sensor dengan jaringan komunikasi *nirkabel* berbasis IoT (*internet of things*). Beberapa ujicoba dalam kesehatan menerapkan pengembangan deteksi pemeriksaan tubuh tanpa ada sentuhan fisik berbasis monitoring melalui jaringan komputer, yaitu salah satunya jaringan sensor yang terpasang pada tubuh pasien dinamakan dengan *Body Area Network* (BAN). Jika *Body Area Network* (BAN) ini terpasang secara *wireless*, maka terdapat jaringan tanpa kabel yang terpasang antara perangkat satu dengan lainnya dengan deteksi gelombang elektromagnetik pada tubuh pasien tersebut. Fungsi dari peralatan tersebut merupakan kumpulan rancangan perangkat keras terhubung secara *nirkabel* dengan jaringan sensor berbasis pemancar diperuntukkan untuk monitoring kondisi tubuh manusia, terdiri atas sekelompok modul yang menempel. Yang disampaikan dalam internasional *conference* [2].

[1] *Jurusan Teknik Komputer Fakultas Teknik Universitas Muhammadiyah Surabaya, Jl. Raya Sutorejo No.59, Dukuh Sutorejo, Kec. Mulyorejo, Kota SBY, Jawa Timur 60113 (tlp: 031-3811966; fax: 031-3811966; e-mail: xxxxxxxx@ft.um-surabaya.ac.id)*

[2] *Jurusan Teknik Elektro Fakultas Teknik Universitas Muhammadiyah Surabaya, Jl. Raya Sutorejo No.59, Dukuh Sutorejo, Kec. Mulyorejo, Kota SBY, Jawa Timur 60113 (telp: 031-3811966; fax: 031-3811966; e-mail: xxxxxxxx@ft.um-surabaya.ac.id)*

Disisi lain, tempat perawatan juga perlu diperhatikan mengingat saat ini rata-rata UGD (Unit Gawat Darurat) di rumah sakit sudah terisi penuh pasien *Covid-19* bahkan sampai *overload* dari kapasitas normal akibat melonjaknya pasien yang terpapar *Covid19*. Alternatif dapat berupa kapal rumah sakit yang digunakan untuk menampung pasien *Covid19*. Dalam hal ini, Universitas Muhammadiyah Surabaya telah merancang desain kapal rumah sakit HOTSPODT (*Hospital Ship For Covid Disaster*). Kapal Rumah Sakit HOTSPODT (*Hospital Ship For Covid Disaster*) merupakan desain kapal rumah sakit kelas C yang dibuat oleh Universitas Muhammadiyah Surabaya untuk mengikuti kompetisi KKCTBN (Kompetisi Kapal Cepat Tak Berawak Nasional) tahun 2020. Desain kapal terdapat pada gambar.1 dibawah ini yaitu :



Gbr 1. Desain Kapal Rumah Sakit HOTSPODT (*Hospital Ship For Covid Disaster*) [3]

Pada desain tersebut terdapat ruang isolasi pasien dengan ruang tenaga kesehatan yang terpisah oleh sekat. Selain itu terdapat ruang sterilisasi antara ruang isolasi dengan ruang tenaga kesehatan. Ruang isolasi dan ruang tenaga kesehatan berada pada sisi belakang deck 2 dari kapal. Desain berdasarkan [3]. Dengan menerapkan teknologi *Wireless Body Area Network* (WBAN) pada kapal rumah sakit HOTSPODT (*Hospital Ship For Covid Disaster*) maka pertama adalah diharapkan dapat membantu meminimalisir terjadinya kontak langsung antara tenaga medis dengan pasien dan kedua adalah menjadi rujukan tempat penanganan *Covid19*, sehingga dapat membantu menurunkan resiko terjadinya penularan virus *Covid-19*.

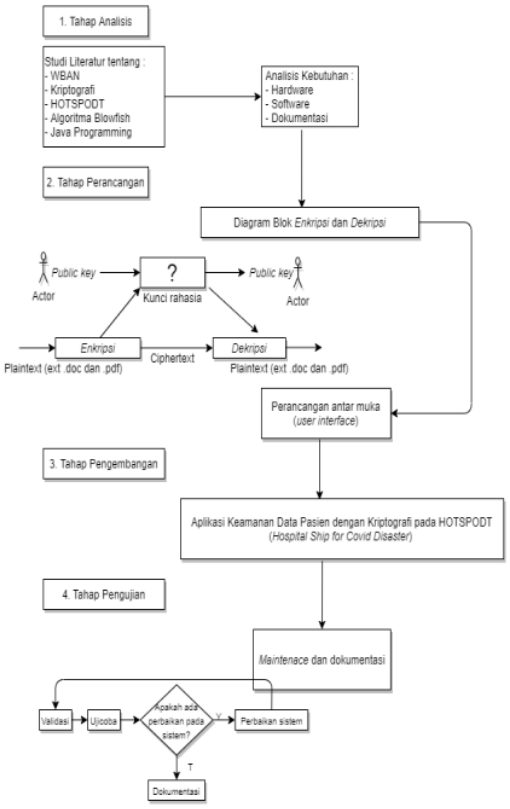
Terkait digitalisasi akan muncul permasalahan yang berkaitan dengan masalah adanya lubang keamanan komunikasi jaringan didalam sebuah sistem informasi. Rumah sakit sangat sensitif terhadap peretasan *Cyber* pada lubang keamanan komunikasi jaringan dimana data rekam medis pasien menjadi tujuan peretasan. Pada artikel jurnal [4] rekam medis data pasien itu dapat disalahgunakan dalam memakai identitas secara ilegal atau pemakaian manipulasi syarat asuransi oleh pihak ketiga. File rekam medis pasien menjadi bagian penting didalam *database* rumah sakit. Secara obyektif terdapat banyak petugas di rumah sakit, baik petugas pendukung atau pihak yang berwenang atas file pemberkasan diruang pemeriksaan pasien. Ini menjadi indikator bahwa berkas-berkas fisik rekam medis pasien bisa saja terbaca oleh pihak yang tidak berhak atas berkas tersebut. Artikel jurnal di [5] bahwa menjadi point kepentingan mencegah adanya ilegal *user* yang dapat menembus data dengan tujuan untuk mengambil, merusak, dan atau menghilangkan berkas serta mengoperasikan alur *software* yang menimbulkan sistem *eror*. Data-data bisa diolah menjadi sebuah pesan. Yang dimaksutkan adalah data dalam bentuk *file* yang biasa dipakai dalam program komputer, yang tidak dapat dibaca seperti : pesan berupa teks, pesan berupa gambar, pesan suara dan pesan video. Dan pada artikel jurnal [6] terdapat berbagai cara atau metode bisa digunakan untuk menutup lubang keamanan jaringan informasi dari ilegal *user* sehingga terhindar dari tindak kejahatan *cyber*. Kembali pada pembahasan sebelumnya, dalam pemberkasan file rekam medis data pasien yang disimpan biasanya *berextension .doc* dan *.pdf*. dari hal diatas, masih cukup efektif apabila teknik kriptografi digunakan dalam proses pengelolaan pesan (data) yang tidak dapat dibaca. Kriptografi adalah bagian dari seni sebuah keamanan informasi di jaringan komunikasi melalui *internet*. Konsep pengamanan data rekam medis pasien disesuaikan dengan posisi *user* terhadap kepentingan data-data itu. Baik petugas medis yang berwenang, keluarga pasien dan pasien itu sendiri. Sehingga diharapkan penerapan pengubahan file yang diberikan kepada yang berwenang berupa pengkodean data, dapat mencegah sesuatu yang bisa disalahgunakan. Akses merupakan salah satu lubang keamanan yang perlu dicermati dan dijaga sistem keamanannya.

Artikel jurnal [6] penjelasan mengenai Kriptografi (*cryptography*) adalah alur penyelamatan pesan (data file) supaya terhindar dari ilegal *user*. *Cryptography adalah seni dalam ilmu keamanan pesan rahasia*. "*Crypto*" berarti kerahasiaan dan "*graphy*" adalah media. Asal usul kriptografi dipahami sebagai ilmu seni menyembunyikan pesan. Orang yang menggunakan kriptografi disebut *cryptographers*. Hasil proses perubahan struktur logika dari pesan yang dirahasiakan yaitu berupa sandi. Pada implementasinya memiliki karakteristik teknik enkrip dengan dekrip dan sebaliknya teknik dekrip dengan enkrip. Untuk proses pengkodean data file *berextension .doc* dan *.pdf* pada penelitian ini menerapkan *Blowfish Algorithm*. Algoritma tersebut dikembangkan untuk memenuhi parameter metode capaian 26 siklus jam per *byte* nya diterapkan dalam penyimpanan *hardware* tidak lebih dari 5 *KiloByte*, menerapkan logika aritmatika *addition*, gerbang XOR dan pencarian baris dan kolom pada *operand* 32 bit, panjang kode untuk kunci *Blowfish Algorithm* bisa bermacam sampai 448 bit (56 *byte*).

II. METODOLOGI

Dibawah ini adalah langkah-langkah untuk proses pemberkasan file rekam medis data pasien yang disimpan *berextension .doc* dan *.pdf*. mulai dari studi literatur, susunan desain sistem, penerapan terhadap *software* aplikasi, dan tahapan ujicoba. Algoritma yang digunakan adalah *Blowfish*, diimplementasikan pada *java programming*. Penerapan dengan teknologi *Wireless Body Area Network* (WBAN) pada kapal rumah sakit HOTSPODT (*Hospital Ship For Covid Disaster*). Langkah-langkah metodologi menjadi proses awal dimulainya penelitian ini. Sebagai acuan tahapan yang

dilakukan. Dimasing-masing tahapan tersebut terdapat proses implementasi. Berikut adalah langkah-langkah tersebut, yaitu :



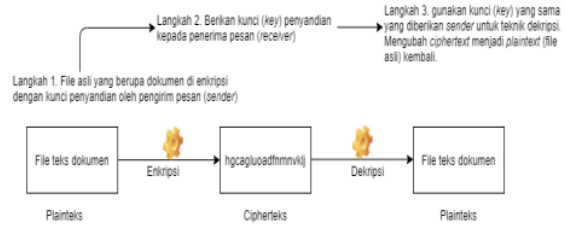
Gbr 2. Alur sistem keamanan data pasien Kapal Rumah Sakit HOTSPODT (*Hospital Ship For Covid Disaster*)

Berikut adalah uraian dari mekanisme pengkodean data untuk proses keamanan rekam medis data pasien, yaitu :

1. Menggunakan *publickey* untuk membuka hasil pengkodean data dari *sender* ke *receiver*.
2. Masing-masing *sender* dan *receiver* menerapkan aplikasi yang sama di perangkat komputer mereka.
3. membuat *Public Key* yang hanya diketahui oleh *sender* dan *receiver* yang berwenang
4. Penerapan struktur logika dalam pengkodean data menggunakan dua kode untuk kunci, kode 1 untuk pengkodean kode 2 untuk membuka pesan yang dikodekan. *Sender* dan *receiver* menggunakan masing-masing kode untuk kunci yang sama.

A. Enkripsi dan Dekripsi

Buku pada [7] Enkripsi dan dekripsi adalah struktur logika sandi yang tersembunyi atau Kriptografi yang diartikan secara umum adalah ilmu dan seni untuk menjaga kerahasiaan pesan. Hanbook pada [8] terdapat pula pengertian ilmu yang mempelajari logika matematika yang berhubungan dengan aspek keamanan informasi seperti kerahasiaan data, legalitas data, integritas data, serta keaslian data. Dibawah ini tahapan dari proses enkripsi dan dekripsi pada keamanan data rekam medis data pasien di Kapal Rumah Sakit HOTSPODT (*Hospital Ship For Covid Disaster*) :



Gbr 3. Proses Enkripsi dan Dekripsi

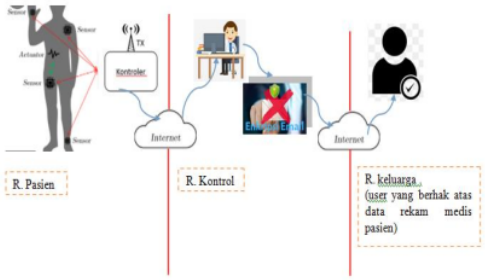
B. Implementasi

Kebutuhan terhadap pembuatan program dengan *blowfish algorithm* pada *java programming* adalah perangkat kerasnya : komputer *merk* **Hewlett Packard** Inc dengan kriteria : *Procesor Intel Core™ i3-6006U (Cache 3M,2,00GHz) RAM 4 GB, 64-bit OS. Software*: *Ms. Office, Ms. Excel, Microsoft Windows 10, JavaNetbean IDE 8.0.2*. dibawah ini adalah tabel keterangan *extension* file dokumen yang digunakan untuk ujicoba implementasi yaitu ada dua file yang *berextension .doc* dan .pdf. berikut adalah tabelnya :

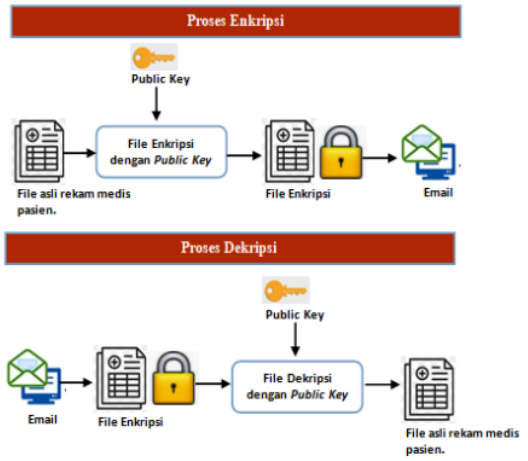
TABEL 1
JENIS FILE

No	Format Dokumen	Keterangan
1.	*.DOC	Kepanjangannya adalah *document* yang disingkat doc. Digunakan dalam program pengolah kata. Dengan berbagi fitur diantaranya yang terdapat pada *title bar*, *tab menu, ribbon tool, scroll bar, windows menu*, seperti yang umum digunakan pada Ms.Word.
2.	PORTABLE DOCUMENT FORMAT (*.PDF)	Merupakan hasil transformasi dua dimensi dari *document* dengan *fitur : page view, read aloud, draw, higligh, erase, zoom in/out, print, save as, rotate, fit to windth*.

Sedangkan arsitektur keamanan rekam medis data pasien pada Kapal Rumah Sakit HOTSPODT (*Hospital Ship For Covid Disaster*) yang telah menggunakan teknologi *Wireless Body Area Network* (WBAN) dan juga proses kriptografi rekam medis data pasien, digambarkan sebagai berikut :



Gbr 4. Arsitektur keamanan rekam medis data pasien Kapal Rumah Sakit HOTSPODT (*Hospital Ship For Covid Disaster*)



Gbr 5. Proses kriptografi keamanan rekam medis pasien Kapal Rumah Sakit HOTSPODT (*Hospital Ship For Covid Disaster*)

Pada gambar 4. merupakan arsitektur dari proses pemeriksaan pasien dengan menempatkan *Body Area Network* (BAN) berbasis kontroler pada tubuh pasien yang selanjutnya dimonitor oleh petugas kesehatan. Sensor mendeteksi nilai suhu badan, *heart rate*, pernapasan per menit pada objek di setiap ruang pasien. Mengirim data pada Kontroler. Data ditransmisikan secara nirkabel (*internet*) ke penerima di ruang kontrol tenaga medis. Data yang ditampilkan dalam bentuk tabel maupun grafik dapat diunduh oleh tenaga medis dalam bentuk berkas dengan format *pdf* dan *doc* sebagai data laporan kondisi pasien. Selanjutnya petugas kesehatan yang bertanggung jawab atas pasien juga melakukan proses enkripsi terhadap rekam medis data pasien yang ada di Kapal Rumah Sakit HOTSPODT (*Hospital Ship For Covid Disaster*) dan hasilnya dikirim kepada keluarga atau *user* yang berhak terkait data pasien tersebut melalui *email*. *User* akan melakukan proses dekripsi atas data rekam medis pasien yang sudah diterima dengan memasukkan kunci *public key*, yaitu kunci yang sama pada saat petugas kesehatan melakukan enkripsi sebelumnya. Petugas kesehatan dan *user* sama-sama menggunakan aplikasi kriptografi yang sudah terinstal di perangkat *desktop* masing-masing. Apabila tidak memiliki atau tidak diberikan kode akses kunci *public key* maka tidak dapat membuka file yang telah terenkripsi. Terdapat 2 ruang yang terpisah antara ruang pasien dengan ruang kontrol dalam interaksi pemeriksaan pasien sehingga bisa mengurangi resiko penularan *Covid19* terhadap tenaga kesehatan (medis) karena kontrol berbasis teknologi *Wireless Body Area Network* (WBAN) Sedangkan di gambar 5. Memperlihatkan proses kriptografi terhadap *file* rekam medis data pasien yang merupakan data rahasia yang tersandikan agar data tersebut tidak disalah gunakan peruntukannya. Dari *file* asli sebagai plainteks di enkripsi dengan kunci *public key* sehingga berubah dengan file enkripsi disebut *cipherteks* dikirim *via email*. Dari *email* yang berupa file enkripsi dibuka kembali dengan kunci *public key* sehingga *autentikasi* file dapat dilihat, proses ini dinamakan proses kebalikan pada struktur kriptografi.

C. Aplikasi Dengan Java Netbeans

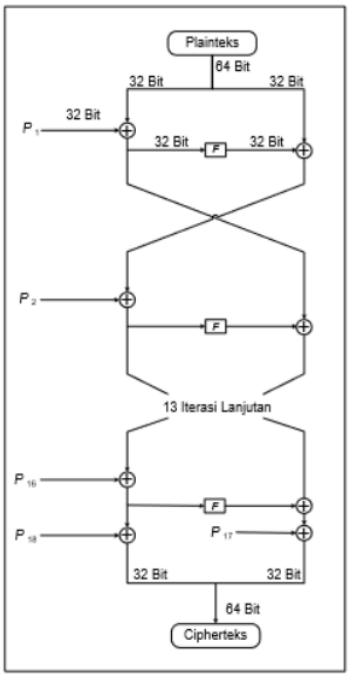
Berikut adalah tampilan *user interface* dari aplikasi kriptografi keamanan rekam medis data pasien dengan *algoritma Blowfish* Kapal Rumah Sakit HOTSPODT (*Hospital Ship For Covid Disaster*), pada gambar 6 dibawah ini :

Gbr 6. Tampilan *User Interface* aplikasi kriptografi keamanan rekam medis data pasien Kapal Rumah Sakit HOTSPODT (*Hospital Ship For Covid Disaster*)

D. Algoritma Blowfish

Implementasi dari program aplikasi keamanan data rekam medis pasien menerapkan fungsi pengkodean data di kriptografi menggunakan *algoritma Blowfish*, struktur logika ini dirancang oleh seorang penganalisa kriptografi bernama Bruce Scheneir, menjabat Presiden sebuah perusahaan *Counterpane Internet Security*, Inc (Perusahaan konsultan tentang kriptografi dan keamanan komputer) dan diinformasikan ke publik tahun 1994. Dengan pola algoritma simetri merupakan bagian dari metode *block cipher*. Algoritma simetris terdiri dari tahapan mendasar *block cipher* dan *stream cipher*. Jika *block cipher* memproses *block byte* (biasanya 64 atau 128 bit) pada satu waktu. Sedang sebuah *stream cipher* memproses satu *byte* atau bahkan satu bit pada suatu waktu. Struktur logika *Blowfish* menggunakan teknik

pengkodean serupa DES (*data encryption stadart*) diperuntukkan pada mikroprosesor tergolong banyak (lebih dari 32 bit dan *cache* data banyak juga). *Blowfish Algorithm* dibangun dengan desain dengan ketentuan sebagai berikut : mencapai proses maksimal sampai 26 *clock cycle* per *byte*, proses di memori setidaknya kurang dari 5KB, menerapkan logika aritmatika *addition*, gerbang XOR dan pencarian baris dan kolom pada *operand* 32 bit, memudah analisis terhadap kesalahan implementasi, *key Blowfish* nya memiliki karakter variasi setidaknya sampai 448 bit (56 *byte*). Terdapat *End Of File* (EOF) merupakan bagian dari tahapan *security* pada *steganografi*. Tahapan ini berfungsi menyisipkan pesan pada akhir file. Selanjutnya didesain sesuai tahapan *feistel network* terdiri 16 iterasi. Masukan pada nilai 64 bit, X. Gambar untuk *feistel network*, yaitu :



Gambar 7. Bentuk *Feistel Network* [5]

Pada buku [9] *Blowfish Algorithm* mempunyai dua bentuk proses, yaitu perluasan kode kunci dan pengkodean pesan. Struktur perluasan kode kunci merubah kunci terkecil menjadi *array* bagian kode kunci sebanyak 4168 *byte* berikut langkah-langkahnya :

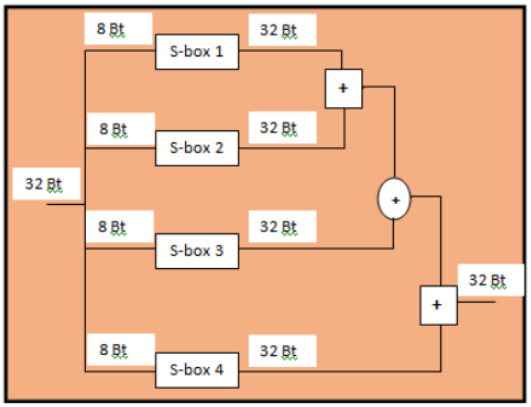
1. mencatat P-*array* kesatu dan keempat pada S-box, secara berututan, bersama *string* yang telah pasti. *String* tersebut adalah angka *heksadesimal* dari *phi*, selain angka tiga di awal. Contoh : P1= 0x243f6a88 P2= 0x85a308d3 P3= 0x13198a2e P4= 0x03707344 seterusnya sampai P18.
2. Lakukan XOR pada P1 = 32-bit awal kode kunci, lakukan XOR pada P2 = 32-bit berikutnya dari kode kunci, dan seterusnya untuk semua bit kode kunci. Jika panjang kode kunci tidak lebih dari sama dengan jumlah Pbox, maka pertukaran perhitungan akan diiterasi sampai semua P dilakukan XOR.
3. Kodekan *string* yang semuanya nol (*allzero string*) dengan strutur logika *Blowfish*, menggunakan bagian kunci yang telah diuraikan tahapan ke-1, tahapan ke-2.
4. hilangkan P1 dan P2 dari luaran langkah ke-3
5. Kodekan luaran langkah ke-3 menggunakan struktur logika *Blowfish* bersama bagian kunci yang telah dirubah sebagian.
6. hilangkan P3 dan P4 dari luaran langkah ke-5.
7. Lanjutkan tahapan ke 1-6, hilangkan seluruh unsur P-array dan selanjutnya keempat S-box secara berurutan, sehingga hasil luaran struktur logika *Blowfish* menjadi tidak pasti.

Sedang pada tahap pengkodean di algoritma *Blowfish* adalah pengkodean pesan diproses dalam 16 kali iterasi dengan masukannya adalah pesan tidak dikenali terdiri dari 64 bit, setiap putaran menerapkan operasi XOR. Pertama lakukan XOR sisi kiri dengan bagian kunci untuk *round*/putaran itu adalah langkah-langkahnya yaitu :

1. File masukan dirubah menjadi *binary*. Proses pengkodean dan kebalikan pengkodean *Blowfish* dipecah menjadi file per 64 bit. Diinisialkan sebagai "Z".
2. Inputan pesan "Z" 64 bit ini dipisah menjadi dua sisi yaitu XR (X *Right*) dan XL (X *Left*) masing-masing 32 bit.
3. Proses pengkodean dan kebalikan pengkodean dijalankan 16 kali putaran.
4. Rumus dari pengkodeannya : XL = XL XOR p[i] XR = F(XL) XOR XR Tukar XL dan XR Dimana rumus F adalah F(XL) = ((S[1,a] + S2[2,b] *mod* 232) XOR S[3,c]) + S[4,d] 4. Setelah iterasi ke-16, tukar XL dan XR jika melakukan pembatalan penukaran terakhir.
5. Dari tahapan diatas, tahapan akhirnya menggabungkan XR dan XL untuk mendapatkan sandi pesan, adalah data dari pesan yang tidak dapat dibaca. Jika ingin merubah menjadi teks aslinya maka dikodekan kembali menggunakan kode kunci yang sama dalam satu proses aplikasi.

Blowfish Algorithm adalah blok sandi, bisa diartikan bahwa dalam proses pengkodean dan kebalikan pengkodean, akan membagi pesan menjadi blok-blok dengan ukuran yang sama panjang. Panjang blok nya adalah 64-bit. Jika ada pesan yang bukan kelipatan delapan *byte* maka akan ada bit tambahan (*padding*) sehingga ukuran untuk tiap blok sama. Lebih jelasnya lihat gambar *feistel network* pada Gambar 7.

Untuk Proses kebalikan pengkodean, langkah sesuai dengan tahapan pengkodean, hanya barisan Pbox digunakan dengan barisan terbalik. Langkah diatas pada *feistel network* tentang fungsi F. Dimana Bagi X_l menjadi empat bagian 8-bit : a,b,c,d. $F(X_l) = ((S1,a+S2,b \bmod 2^{32}) \text{ XOR } S3,c)+S4,d \bmod 232$. Untuk dapat memahami Fungsi F perhatikan gambar dibawah ini :



Gambar 8. Fungsi F

E. Penelitian Sebelumnya

Pada penelitian sebelumnya di artikel jurnal [10], beberapa penelitian melakukan analisis betapa pentingnya manajemen arsip medis sebagai usaha menjaga kerahasiaan medis. Rahasia medik adalah sesuatu hal yang menjadi hak pasien tentang kondisi tubuh secara medis oleh dokter dan pasien, disampiakan secara langsung oleh pasien dengan subyektifitas yang ada maupun secara obyektif diketahui oleh petugas kesehatan ketika melakukan pemeriksaan tubuh dan analisis sesuai parameter medis. Rahasia medis menjadi bagian penting pasien yang harus dilindungi dan dijaga kerahasiaannya oleh setiap badan pelayanan kesehatan. Pada penelitian lainnya di artikel jurnal [11], menyebutkan : Pengelolaan dan penyelenggaraan layanan kesehatan rekam medis di beberapa rumah sakit ada yang belum melaksanakan sesuai standart. Pemberkasan *database* pemeriksaan kesehatan pada tempat *filing* masih ada permasalahan khususnya tentang keamanan dan kerahasiaan dokumen pemeriksaan kesehatan di tempat *filing*. Adanya interaksi secara langsung antar petugas medis keluar masuk di tempat *filing* bertujuan membaca informasi, melengkapi berkas pemeriksaan kesehatan, meminjam atau mengembalikan berkas pemeriksaan kesehatan sehingga dapat mengakibatkan munculnya pengungkapan informasi pribadi individu pasien tertentu kepada sesama petugas medis, terkadang masih ada petugas makan dan minum di ruang *filing* yang dapat merusak isi dokumen rekam medis, karena disatu sisi adanya tuntutan pekerjaan yang tidak bisa ditinggalkan. tempat pengembalian dokumen rekam medis bersifat manual sehingga akses bagi orang yang tidak berhak akan terbuka dengan mudah.

III. KESIMPULAN DAN SARAN

Berdasarkan perancangan, desain dan pembuatan aplikasi keamanan rekam medis data pasien yang telah dilakukan, dapat disimpulkan bahwa terdapat ruang berbeda untuk desain Kapal Rumah Sakit HOTSPODT (*Hospital Ship For Covid Disaster*) dalam penanganan pasien *Covid19* antara ruang pasien dan ruang kontrol. Deteksi dan pemeriksaan pasien menggunakan teknologi *Wireless Body Area Network* (WBAN) berbasis kontroler dengan sensor. Dan untuk data kerahasiaan medis guna menunjang tata kelola dokumen rekam medis yang merupakan hak pasien yang harus dilindungi digunakan aplikasi kriptografi dengan algoritma *Blowfish* pada *java netbeans*.

Untuk pengembangan selanjutnya teknologi elektronika berbasis frekuensi bisa dilakukan mengingat tempat untuk penelitian adalah di armada kapal. Dan untuk sistem keamanan data dapat menggunakan algoritma kriptografi lainnya sesuai dengan kebutuhan sistem.

UCAPAN TERIMA KASIH

Bpk. Dedy Wahyudi, S.T.,M.T selaku kaprodi Teknik Perkapalan Universitas Muhammadiyah Surabaya periode 2017-2021 yang telah memberikan data berupa desain Kapal Rumah Sakit HOTSPODT (*Hospital Ship For Covid Disaster*).

REFERENSI

[1] *web:covid19.co.id*, tanggal akses: 06-Juli-2021.

[2] Barakah, D.M. dan Ammad-uddin, M., 2012. Third International Conference on Intelligent Systems Modelling and Simulation A Survey of Challenges and Applications of Wireless Body Area Network (WBAN) and Role of A Virtual Doctor Server in Existing Architecture. hal.214 – 219.

[3] Taufik, Ary. 2020. HOTSPODT (Hospital Ship For Covid Disaster). Kementrian Pendidikan dan Kebudayaan, Pusat Prestasi Nasional. Kontes Kapal Cepat Tak Berawak Nasional (KKCTBN) Tahun 2020

[4] T.I prasasti dan D.B Santoso. "keamanan dan Kerahasiaan Berkas Rekam Medis di RSUD Dr. Soehadi Prijonegoro Sragen". Jkesvo (Jurnal Kesehatan Vokasional) Vol. 2 No 1, hal 135-139, Mei 2017.

[5] N. Fahriani dan Harunur . "Implementasi teknik enkripsi dan dekripsi di file video menggunakan algoritma *Blowfish*". JTIIK Vol.6 hal. 697-702. Desember 2019.

[6] INDRIYONO, B.V. Implementasi Sistem Keamanan File dengan Metode Steganografi EOF dan Enkripsi Caesar Cipher. Jurnal Sisfo, 06(01), pp.1–16. 2016.

[7] Schneier, Bruce. 2017. Applied Cryptography 20th Anniversary Eddition.Protocols, Algorithm, and Source Code in C. John Wiley & Sons.

[8] A. Menezes, P. van Oorschot and S. Vanstone - Handbook of Applied Cryptography. 1996

[9] Schneier, Bruce. 1996. Applied Cryptography 2nd. John Wiley & Sons

[10] Judi. 2017. Tata Kelola Dokumen Rekam Medis sebagai Upaya Menjaga Rahasia Medis di Pelayanan Kesehatan. Jurnal Manajemen Informasi Kesehatan Indonesia. Vol 5 nomer 1 Maret 2017

[11] Gamasiano Alfiansyah, Rossalina Adi Wijayanti, Selvia Juwita Swari, Novita Nuraini , dan Siti Wafiroh. DETERMINAN KEAMANAN DAN KERAHASIAAN DOKUMEN REKAM MEDIS DI RUANG FILING RS X. J-REMI : Jurnal Rekam Medik Dan Informasi Kesehatan. Vol. 1 No. 2 Maret 2020.

artikel 1

ORIGINALITY REPORT

3% EN	%	2%	3%
SIMILARITY INDEX	INTERNET SOURCES	PUBLICATIONS	STUDENT PAPERS

PRIMARY SOURCES

1	Submitted to Universitas Brawijaya Student Paper	2%
2	Peng Zhang, Chengqing Ye, Xin Li, Yanhua Cheng, Xueying Ma. "Constant-round contributory group key agreement for ad hoc networks", Proceedings. 2005 International Conference on Wireless Communications, Networking and Mobile Computing, 2005., 2005 Publication	<1%
3	Submitted to Higher Education Commission Pakistan Student Paper	<1%
4	Jeyamala Chandrasekaran, B. Subramanyan, Raman Selvanayagam. "Chapter 52 A Chaos Based Approach for Improving Non Linearity in S Box Design of Symmetric Key Cryptosystems", Springer Science and Business Media LLC, 2011 Publication	<1%

Exclude quotes	Off	Exclude matches	Off
Exclude bibliography	Off		