APLIKASI KEAMANAN EMAIL DENGAN METODE RC4 (RIVEST CODE 4) DAN DES (DATA ENCRYPTION STANDARD) BERBASIS MOBILE ANDROID PADA PT. TIRTA ABADI GEMILANG

Diki Firmansyah[1)], **Rizky Tahara Shita**[2)]
[1]Program Studi Teknik Informatika, Fakultas Teknologi Informasi, Universitas Budi Luhur
[1,2]Jl. Raya Ciledug, Petukangan Utara, Kebayoran Lama, Jakarta Selatan 12260
E-mail : techno.dicky@gmail.com[1)], rizky.tahara@gmail.com[2)]

Abstrak

Pertumbuhan dunia teknologi informasi semakin maju dan semakin pesat setiap waktu berjalan dan membawa perkembangan untuk dunia. PT. Tirta Abadi Gemilang adalah perusahaan yang bergerak dibidang jasa perawatan air (water treatment) dan penjualan produk yang melayani perseorangan dan perusahaan yang terhubung dengan jaringan internet. Pertukaran informasi yang menyangkut hubungan dengan klien dikirim dan diterima melalui email dan data itu bersifat rahasia. Dan seiring pesatnya teknologi, pengiriman email saat ini seringkali dilakukan melalui mobile Android. Maka dengan alasan itu dibutuhkan suatu aplikasi mobile yang dapat menjaga privacy dan keamanan data yang dikirim melalui email, yaitu dengan teknik penyandian data. Penyandian data untuk saat ini biasanya dengan cara kriptografi. Kriptografi ini proses dimana data diubah menjadi sandi-sandi yang tidak dapat di pahami oleh orang biasa dan mengembalikannya ke dalam bentuk awalnya dan itulah yang dinamakan proses Enkripsi dan Dekripsi. Algoritma RC4 sangat dikenal karena kecepatan dan kemudahannya dalam menangani banyak aplikasi. Teknik RC4 adalah teknik yang menginisialisasikan tabel sepanjang 256 byte dengan menggunakan panjang kunci dari 1 sampai 256 byte. Sedangkan Algoritma DES yang dikenal dengan algoritma sistem sandi modern. Teknik DES menggunakan metode penyandian dengan sistem block cipher yang pengacakannya dilakukan dengan blok input dan output per 64 bit. Dengan adanya aplikasi ini, proses pengiriman dan penerimaan email bisa lebih terjamin dan aman untuk dilakukan.

Kata kunci: Email, Mobile, Kriptografi, Enkripsi, Dekripsi.

1. PENDAHULUAN

Kemajuan dunia teknologi dan komunikasi semakin hari semakin pesat, sehingga dapat memudahkan setiap orang dalam melakukan pertukaran informasi dan data dengan orang lain secara cepat. Informasi-informasi yang ingin disampaikan berjalan melalui media komunikasi. Beberapa media komunikasi yang sering digunakan seperti telpon, jaringan internet dan email.

Pada PT. Tirta Abadi Gemilang yang bergerak dibidang jasa perawatan air (water treatment) dan penjualan produk perseorangan serta perusahaan. Seringkali pertukaran informasi yang menyangkut hubungan dengan klien dikirim dan diterima melalui email. Data data yang dikirimkan lewat email itu harus diamankan supaya tidak diketahui pihak yang tidak berkepentingan dan disalah gunakan untuk persaingan bisnis. Maka dari itu dibutuhkan suatu aplikasi pengamanan data pada saat pengiriman email berlangsung.

Berdasarkan permasalahan di atas, perlu dibuat suatu sistem pengamanan data pada saat melakukan pengiriman email. Hal ini dapat dilakukan dengan cara penyandian data yang disebut kriptografi. Kriptografi ini meliputi proses enkripsi dan dekripsi. Enkripsi adalah proses penyandian data dengan memasukan kunci agar data itu menjadi tidak mudah terbaca sedangkan Dekripsi adalah proses pengembalian data yang sudah dienkripsi sehingga datanya menjadi seperti data aslinya dan dapat dibaca kembali. Algoritma enkripsi dekripsi pada saat ini sudah banyak digunakan dan jenisnya juga bermacam-macam. Pada penulisan ini akan diimplementasikan teknik kriptografi menggunakan metode enkripsi dan dekripsi Rivest Code 4 (RC4) dan Data Encryption Standard (DES).

2. METODOLOGI PENELITIAN

2.1. Kriptografi

Kriptografi dulunya dikenal sebagai ilmu yang digunakan dalam mempelajari bagaimana pesan bisa disembunyikan. Namun pada era modern pengertiannya berganti menjadi ilmu dengan menggunakan teknik matematika yang digunakan dalam mengamankan informasi seperti kerahasiaan, data, keutuhan serta entitas otentikasi. Sehingga kriptografi dalam pengertian modern itu tidak saja berurusan dengan teknik menyembunyikan pesan, namun ljuga teknik yang dapat mengamankan informasi [5].

Kriptografi memiliki konsep dasar dengan teknik enkripsi yang dapat mengacak suatu data dengan menggunakan kunci enkripsi sehingga data tersebut tidak mudah dibaca oleh orang yang tidak mempunyai kunci dekripsinya [1]

Pada era teknologi seperti sekarang ini, mekanisme yang digunakan masih tetap sama namun implementasinya berbeda. Beberapa istilah yang sering digunakan ketika membahas kriptografi [6] diantaranya :

1)Plainteks
Plainteks merupakan pesan yang masih asli yang akan dijaga keamanannya dan dikirimkan.
2)Cipherteks
Chipherteks merupakan pesan yang telah diamankan dan diberi penyandian (Enkripsi).
3)Cipher
Cipher adalah algoritma yang digunakan dalam pengubahan plaintext menjadi ciphertext dengan menyandikannya, begitupun sebaliknya.
4)Kunci
Kunci merupakan suatu gabungan angka dan huruf yang bersifat rahasia, digunakan ketika proses Enkripsi dan Dekripsi dijalankan.
5)Enkripsi
Enkripsi merupakan proses yang dilakukan dalam mengubah plainteks menjadi chipherteks
6)Dekripsi
Dekripsi merupakan proses yang dilakukan untuk mengembalikan cipherteks menjadi plainteks
7)Kriptosistem
Kriptosistem adalah sistem yang terdiri dari cipher, plainteks, cipherteks, dan kunci yang digunakan dalam mengamankan informasi.

2.2. Email

Electronic mail (surat elektronik, e-mail) merupakan metode dimana pesan dapat diubah, dikirim, disimpan, dan diterima dengan cara melalui sistem komunikasi elektronik. Istilah e-mail meliputi sistem yan berdasar pada SMTP (Simple Mail Transfer Protocol) yang memungkinkan pengguna satu dapat mengirim pesan kepada pengguna lainnya. Sebuah pesan pada email biasanya terdiri dari 2 bagian besar yaitu Header dan Body.

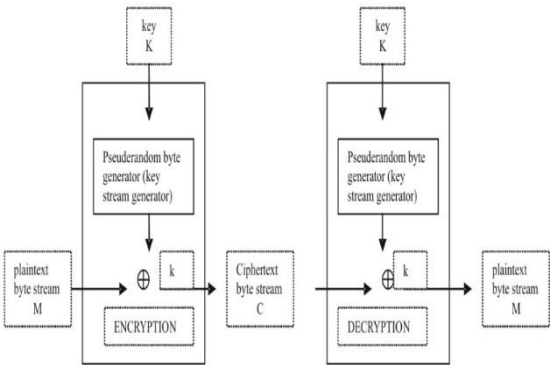
Header umumnya mempunyai nama field yang ada pada karakter pertama di suatu baris, diikuti oleh tanda ':', bukan oleh spasi serta tab pada karakter pertamanya. Nama field masuk dalam karakter ASCII yaitu sebesar 7 bit. Baris kosong ialah yang memisahkan bagian header dengan body. Pada umumnya dalam pesan ada 4 field seperti:
1) From : Alamat e-mail yang biasanya terdapat nama si pengirim pesan
2) To : Alamat e-mail yang biasanya terdapat nama si penerima pesan.
3)Subject : Rangkuman yang terdapat isi dalam pesan.
4)Date : Tanggal dan waktu setempat.

Body merupakan Pesan teks yang diterima tanpa struktur, terkadang pada bagian akhir. mengandung tanda pengenal. Pada awalnya yang digunakan adalah ASCII 7 bit, namun sekarang sudah menggunakan 8-bit, walaupun belum universal. [2]

2.3. Algoritma RC4

RC4 stream cipher yang dapat menginput data dan memproses unit dengan satu saat. Byte merupakan hal umum pada unit ataupun data. Maka pada panjang variabel proses enkripsi dan dekripsi dapat dilaksanakan. Sebelum diproses algoritma ini tidak mesti menunggu jumlah input data tertentu atau menambahkan byte untuk mengenkrip.

RC4 sendiri merupakan standar yang telah ditetapkan untuk komunikasi antara Web browser dan server dimana didalamnya digunakan SSL/TLS (Secure Socket Layer/Transport Layer Security). Selain digunkan pada protocol Wired Equivalent Privacy (WEP), RC4 juga digunakan pada protokol WiFi Protected Access (WPA) yang merupakan bagian dari standar Wireless LAN IEEE 802.11. RC4 merupakan algoritma yang cukup mudah dan sangat sederhana dalam mengimplementasikannya. Sebuah variabel kunci yang panjangnya 1 sampai dengan 256 byte (8 sampai dengan 2.048 bit) digunakan dalam menginisialisasi 256 byte larik S, dengan elemen S[0], S[1], ..., S[255]. Setiap larik S berisi permutasi dari semua angka 8-bit mulai dari 0 sampai 255. Dalam proses enkripsi dan dekripsi, sebuah byte k dihasilkan dari larik S secara sistematis dengan memilih salah 1 byte dari 255 byte. Karena setiap nilai larik S yang dipermutasi maka akan menghasilkan nilai K [7].



Gambar 1. Algoritma RC4

a. Inisialisasi S

Untuk memulai inisialisasi larik S, maka ditetapkan nilai larik S sama dengan nilai dari 0 hingga 255 dalam urutan menaik yaitu; S[0]=0, S[1]=1, ..., S[255]=255. Kemudian diciptakan sebuah larik T sebagai larik sementara. Jika 256 byte adalah satuan panjang kunci K, maka elemen K ditransfer ke elemen T. Jika tidak, tergantung dengan panjang kunci, maka elemen pertama dari T disalin dari elemen K dan kemudian diulangi sebanyak yang diperlukan untuk mengisi elemen T. Operasi tersebut dapat diringkas sebagai berikut:

```
/* Inisialisasi*/
for i = 0 to 255 do
S[i] = i;
T[i] = K[i mod keylen];
```

Dalam menghasilkan permutasi awal larik s maka digunakanlah elemen larik T dalam melakukan permutasi larik. Ini melibatkan mulai dari S[0]

hingga S[255] dan untuk setiap larik S[i] menukar S[i] dengan byte lainnya menurut skema larik S yang ditentukan oleh T[i] seperti ringkasan dibawah ini:

```
/* Inisialisasi permutasi dari S*/
j = 0;
for i = 0 to 255 do
j = (j + S[i] + T[i]) mod 256;
Swap (S[i], S[j]);
```

Agar nilai dari larik S tetap angka 0 sampai 255 maka perlu ditukar letak atau permutasi, seperti proses diatas.

b. Stream Generation

Kunci K tidak digunakan lagi.setelah larik S diinisialisasi, dalam mencakup perputaran semua elemen S[i] maka dilakukan stream generation. Untuk setiap elemen S[i], menukar S[i] dengan byte larik S lainnya berdasarkan skema yang telah ditentukan. Setelah S[255] tercapai, proses berlanjut dan dimulai lagi dari S[0]:

```
/*Stream Generation*/
i, j = 0;
while (true)
i = (i + 1) mod 256;
j = (j + S[i]) mod 256;
Swap (S[i], S[j]);
t = (S[i] + S[j]) mod 256;
k = S[t];
```

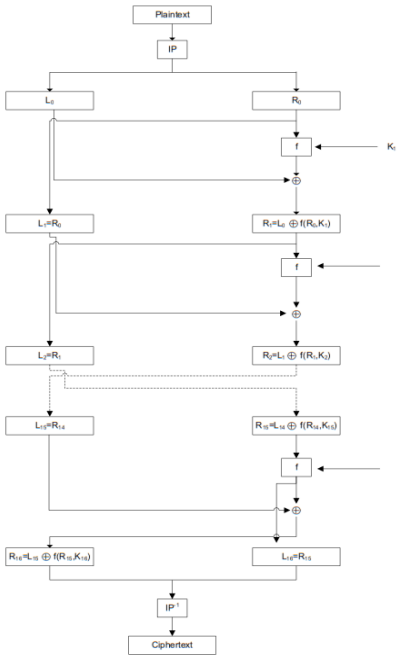
2.4. Algoritma DES

Algoritma DES merupakan algoritma enkripsi yang diadopsi oleh NIST (National Institue of Standards and Technology) ada tajim 1977 sebagai FIPS 46 (Federal Information Processing Standard) dan yang paling banyak digunakan di dunia [4]. Data plainteks dienkrip dalam blok-blok 64 bit menjadi 64 bit data chiperteks menggunakan kunci 56 bit kunci internal (Internal key). DES mentrasnformasikan input 64 bit dalam beberapa tahap enkripsi ke dalam output 64 bit. Dengan demikian, DES termasuk block cipher. Dengan tahapan dan kunci yang sama, DES digunakan untuk membalik enkripsi. Kunci internal pada algoritma DES dibangkitkan dari kunci eksternal(external key) 64 bit [3].

a) Enkripsi Algoritma DES

Setelah permutasi awal maka proses enkripsi pada blok plainteks dapat dilakukan. Putaran enkripsi sebanyak 16 kali dialami oleh setiap blok plainteks. Dan secara matematis setiap putaran enkripsi DES dapat dinyatakan sebagai berikut :

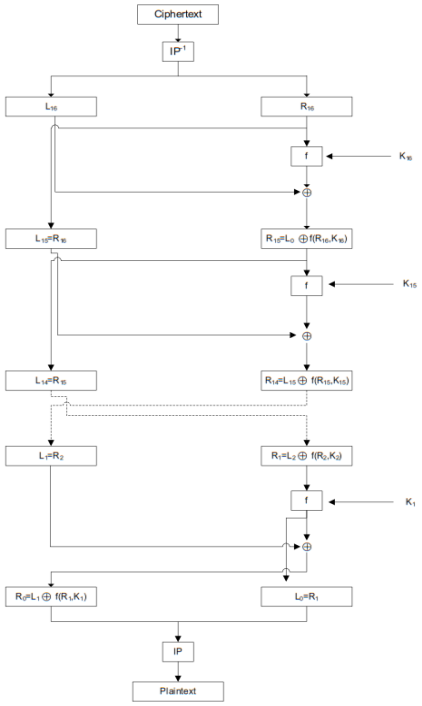
$$Li = Ri - 1$$
$$Ri = Li - 1 \oplus f(Ri - 1, K i)$$



Gambar 2. Skema Proses Enkripsi DES

b) Dekripsi Algoritma DES

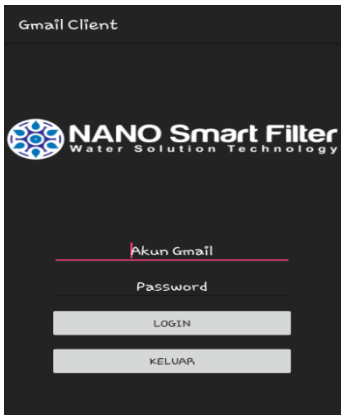
Proses dekripsi pada algoritma DES ialah menggunakan kunci yang sama dengan kunci yang digunakan saat proses enkripsi. Proses dekripsi pada cipherteks merupakan proses kebalikan dari proses enkripsi. Jika pada proses enkripsi urutan kunci yang digunakan adalah K1, K2, ...K16, maka untuk proses dekripsi urutan kunci yang digunakan adalah K16, K15, ..., K1. Masukkan awalnya adalah R16 dan L16 untuk deciphering. Blok R16 dan L16 diperoleh dengan mempermutasikan cipherteks dengan matriks permutasi IP-1.



Gambar 2. Skema Proses Dekripsi DES

3. HASIL DAN PEMBAHASAN

Berikut adalah tampilan aplikasi dan ujicoba. Dalam aplikasi ini terdapat beberapa menu yang memiliki fungsi berbeda namun saling berhubungan antara menu satu dan lainnya. Ketika program baru dibuka maka akan terlihat tampilan menu login, dan tampilannya seperti gambar 3 :

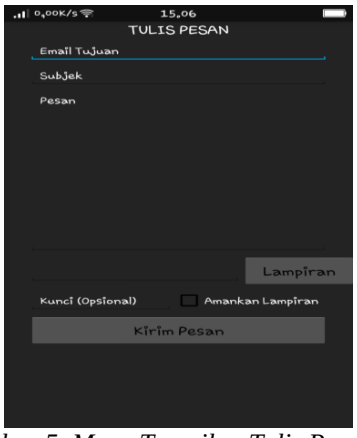


Gambar 3. Tampilan Menu Login

Setelah Login berhasil, user masuk ke dalam Menu Home yang didalamnya ada menu tulis pesan, pesan masuk, pesan keluar dan buka file serta menu logout. Seperti pada gambar 4 :

Gambar 4. Tampilan Menu Home

Ketika user akan menulis pesan baru maka user akan pilih menu tulis pesan seperti gambar 5 ini.



Gambar 5. Menu Tampilan Tulis Pesan

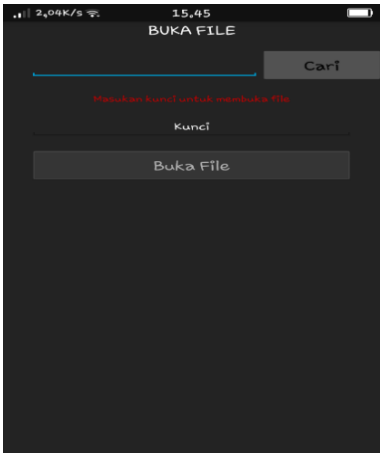
Ketika user ingin melihat pesan masuk pada aplikasi ini maka user dapat memilih menu pesan masuk seperti pada gambar 6

Gambar 6. Tampilan Pesan Masuk

Ketika user ingin melihat pesan yang sudah terkirim pada aplikasi ini maka user dapat memilih menu pesan keluar seperti pada gambar 7

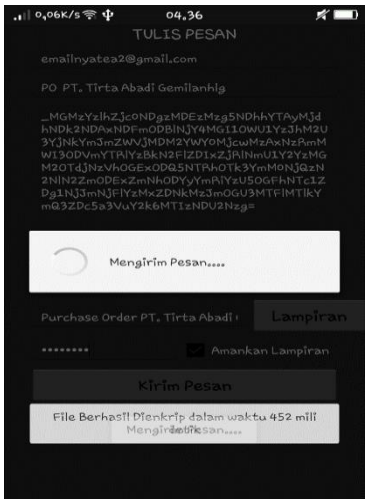
Gambar 7. Tampilan Pesan Terkirim

Dan apabila user ingin mendekrip file atau dapat memilih menu buka file seperti pada gambar 9



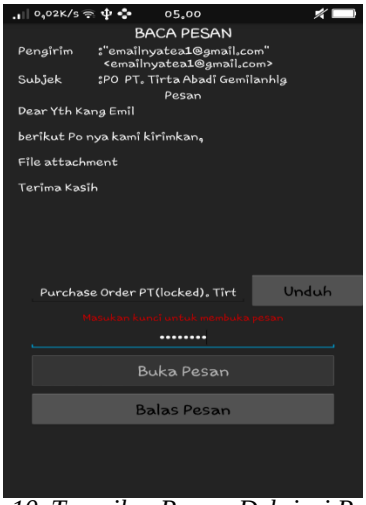
Gambar 8. Tampilan Buka File

Lalu apabila user sedang mengenkripsi pesan dan attachment maka tampilannya akan seperti gambar 9 ini



Gambar 9.. Tampilan Proses Enkripsi Pesan

Dan apabila user sedang melakukan proses dekripsi pesan maka prosesnya akan seperti gambar 10 ini :



Gambar 10. Tampilan Proses Dekripsi Pesan

Berikut ini adalah tabel hasil pengujian proses enkripsi dan dekripsi pada isi pesan dan file.

Tabel 1. Hasil Pengujian Enkripsi Isi Pesan

Isi Pesan Asli	Isi Pesan Enkripsi	Kunci Pengamanan
Selamat Berjuang	_OGU2ODE2ZDhmYjlhOTM4ZGM1MjNiYTBhYjNhNWU3NTlrdW5jaTpyYWhhc2lhMTIz	Rahasia123
	_NjEOZDQYjUoNWZIMGQ5ZTY20DY3ODQ3ZTcwNmRhYzUwZTYyOGQ4MDNIMjMyNDMxNTdiMjQyMzhhYjJmYjk3M2t1bmNpOnJhaGFzaWExMjM=	Rahasia123
File ini jangan sampai hilang	DQ3ZTcwNmRhYzUwZTYyOGQ4MDNIMjMyNDMxNTdiMjQyMzhhYjJmYjk3M2t1bmNpOnJhaGFzaWExMjM=	
Segerakan Pembayaran	_MWMyZTk1Y2VjYTNjYzUzZGM2NzNiODMwOGVhNTk50Tk5ZQMDc5ntq2nZFmNDBmY2I1MmRjMjM4NTQ3Y2Y1Nmt1bmNpOnJhaGzaWExMjM=	Rahasia123

Tabel 2. Hasil Pengujian Dekripsi Isi Pesan

Isi Pesan Enkripsi	Isi Pesan Asli	Kunci Pengamanan
_OGU2ODE2ZDhmYjlhOTM4ZGM1MjNiYTBhYjNhNWU3NTlrdW5jaTpyYWhhc2lhMTIz	Selamat Berjuang	Rahasia123
_NjEOZDQYjUoNWZIMGQ5ZTY20DY3ODQ3ZTcwNmRhYzUwZTYyOGQ4MDNIMjMyNDMxNTdiMjQyMzhhYjJmYjk3M2t1bmNpOnJhaGFzaWExMjM=	File ini jangan sampai hilang	Rahasia123
_MWMyZTk1Y2VjYTNjYzUzZGM2NzNiODMwOGVhNTk50Tk5ZQMDc5ntq2nZFmNDBmY2I1MmRjMjM4NTQ3Y2Y1Nmt1bmNpOnJhaGzaWExMjM=	Segerakan Pembayaran	Rahasia123

Tabel 3. Hasil Pengujian Enkripsi File

Nama File Enkripsi	Kunci Pengamanan	Ukuran Asli	Ukuran Hasil Enkripsi
Purchase Order PT Tirta Abadi Gemilang (locked).pdf	Rahasia123	218 Kb	580 Kb
Purchase Order ke Supplier SAMSUNG (locked).docx	Rahasia123	53 Kb	141Kb

Tabel 4. Hasil Pengujian Dekripsi File

Nama File Dekripsi	Kunci Pengamanan	Ukuran Hasil Enkripsi	Ukuran Hasil Dekripsi
Purchase Order PT Tirta Abadi Gemilang (unlocked).pdf	Rahasia123	580 Kb	218 Kb
Purchase Order ke Supplier SAMSUNG (unlocked).docx	Rahasia123	141 Kb	53 Kb

4. KESIMPULAN

Berdasarkan hasil dan pembahasan aplikasi mobile ini, maka dapat disimpulkan :

a.Aplikasi ini hanya dapat digunakan oleh pengguna yang memiliki akun gmail.

b.Pada aplikasi ini pengguna dapat membuat pesan email baru dan membalas pesan email yang diterima.

c.Pada aplikasi ini pengguna dapat melihat pesan email masuk dan pesan email yang terkirim.

d.Pesan email yang dikirimkan dapat berupa body pesan dan attachment file yang telah diamankan terlebih dahulu sebelum pengiriman.

e.Dengan adanya aplikasi pengamanan pesan email menggunakan metode RC4 dan DES ini, maka pengiriman pesan email, yang ada ada PT. Tirta Abadi Gemilang dapat menjaga kerahasiaan dari sembarang orang.

f.Aplikasi kriptografi ini dapat mengamankan jenis file .doc, .docx, .ppt, .pptx, .pdf, .xls, .xlsx dan isi pesan email.

Dan setelah menarik kesimpulan maka saran yang dapat dikembangkan antara lain :

a.Tampilan yang sederhana diharapkan dapat ditambahkan beberapa fitur seperti, draft, forward pesan email dan lain sebagainya.

b.Tampilan bisa lebih responsif, bisa mode landscape.

c.Karena pada penulisan ini akun yang dapat digunakan hanya gmail, maka untuk pengembangannya penulis berharap bisa dikembangkan dengan baik agar pengguna akun selain gmail juga bisa melakukan pengamanan file-file mereka pada saat pengiriman dan penerimaan pesan.

5. DAFTAR PUSTAKA

[1]Kromodimoeljo, S., 2010. Teori dan Aplikasi Kriptografi, SPK IT Consulting.

[2] Nugroho, Nurcahyo Budi., Zulfian Azmi dan Saiful Nur Arif., 2016. APLIKASI KEAMANAN EMAIL MENGGUNAKAN ALGORITMA RC4. Jurnal ISSN : 1978-6603.

[3] Primartha, R., 2011. Penerapan Enkripsi dan Dekripsi File Menggunakan Algoritma Data Encryption Standard (DES). Jurnal Sistem Informasi (JSI), 3(2), pp.371-387.

[4] Rohmanu, Ajar., 2017. Implementasi Kriptografi dan Steganografi Dengan Metode Algoritma DES dan Metode End Of File. Jurnal ISSN 2541-3244.

[5] Stal Sadikin, Rifki., 2012. Kriptografi Untuk Keamanan Jaringan, Yogyakarta: ANDI.lings, W., 2005. The RC4 Stream Encryption Algorithm.

[6] Stal Sadikin, Rifki., 2012. Kriptografi Untuk Keamanan Jaringan, Yogyakarta: ANDI.lings, W., 2005. The RC4 Stream Encryption Algorithm.

[7] Stallings, W., 2005. The RC4 Stream Encryption Algorithm.