APLIKASI PENGAMANAN *EMAIL* BERBASIS ANDROID DENGAN ALGORITMA KRIPTOGRAFI AES-128DAN RC4 PADAPT TIRTA INVESTAMA

AndrianLesmana[1)], **Rizky Tahara Shinta, M.Kom**[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 : aduls.lesmana@gmail.com[1)], rizky.tahara@gmail.com[2)]

Abstrak

Penggunaan teknologi komputer dan telekomunikasi yang pesat saat ini telah mengubah cara pandang atau perspektif pada masyarakat dalam segi komunikasi. Salah satu perkembangan yang sangat signifikan adalah penggunaan email untuk pertukaran informasi atau pesan melalui jaringan internet.PT. Tirta Investama adalah perusahaan swasta yang bergerak dalam kebutuhan air minum yang ada dalam kemasan. Setiap harinya sering terjadi pertukaran data baik yang bersifat internal maupun eksternal melalui media email. Pengiriman PO (Purchase Order) oleh customer melaui email, bisa saja diretas oleh pihak yang tidak bertanggung jawab seiring persaingan bisnis di bidang air minum dalam kemasan yang semakin sengit. Oleh karena itu, keamanan data pada saat pengiriman email sangat diperlukan. Pengamanan yang di ambil dengan penerapan kriptografi. Kriptografi merupakan ilmu yang digunakan dalam mempelajari cara menjaga data ataupun pesan sehingga akan tetap aman saat dilakukan proses pengiriman dari pengirim untuk penerima. AES merupakan salah satu algoritma kriptografi yang dapat digunakan dalam mengamankan data. Algoritma AES jugamerupakan algoritma blok chiperteks simetrik yang dapat mengenkripsi dan dekripsi data. Sedangkan RC4 termasuk pada salah satu jenis stream chiper, dimana unit dan input data dapat diproses pada satu saat. Dengan cara inipada panjang yang variabel enkripsi ataupun dekripsi dapat dilaksanakan. Algoritma ini juga tidak harus menambahkan byte tambahanuntuk mengenkripatau menunggu sejumlah input data tertentu sebelum diproses. Dengan adanya penggabungan algoritma ini maka diharapkan bisa menghasilkan aplikasi untuk pengamanan email di PT. Tirta Investama.

Kata kunci: Email, Pengamanan Email, Kriptografi, AES-128, RC4

1. PENDAHULUAN

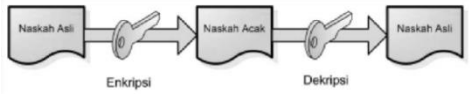
Penggunaan teknologi komputer serta telekomunikasi pada era sekarang itu telah mengubah caramasyarakat dalam melakukan komunikasi. Salah satu perkembangan yang sangat signifikan adalah penggunaan email untuk pertukaran informasi atau pesan melalui jaringan internet. Namun demikian perlu diperhatikan tingkat keamanan informasi tersebut, karena email menggunakan jaringan internet yang merupakan infrastruktur telekomunikasi dengan standar terbuka yang dapat dipergunakan oleh banyak pihak. Penyadapan informasi merupakan hal yang sangat merugikan bagi pengguna jaringan komunikasi saat ini. Dengan adanya kemungkinan penyadapan informasi tersebut, maka keamanan dalam pertukaran informasi menjadi sangat penting. Hal ini akan membuat para pengguna jaringan komunikasi merasa aman dan nyaman.

PT.Tirta Investama adalah perusahaan yang bergerak dalam bidang air minum dalam kemasan. Setiap harinya sering terjadi pertukaran data baik yang bersifat internal maupun eksternal melalui media *email*. Pengiriman PO (*Purchase Order*) oleh *customer* melaui *email*, bisa saja diretas oleh pihak yang tidak bertanggung jawab seiring persaingan bisnis di bidang air minum dalam kemasan yang semakin sengit. Oleh karena itu, keamanan data pada saat pengiriman *email* sangat diperlukan. Pengamanan yang di ambil dengan penerapan kriptografi.

2. METODOLOGI PENELITIAN

2.1. Kriptografi

Kriptografi adalah teknik pengamanan informasi yang dilakukan dengan cara menyandikan *plainteks* dengan kunci menggunakan algoritma tertentu sehingga menghasilkan *chiperteks*. Dengan proses dekripsi *cipherteks* dikembalikan menjadi informasi awal (*plainteks*). [1]



Gambar 1. Urutan Proses Kriptografi

Tujuan Kriptografi adalah sebagai berikut : [2]

a. *Confidentiality* (kerahasiaan)

Layanan yang ditujukan untuk menjaga pesan agar terjaga kerahasiaan serta tidak dapat dibaca oleh pihak yang tidak berhak.

b. *Authentication* (Otentikasi)

Penerima infomasi dapat mengetahui keaslian data yang dikirim sedangkan penyerang tidak dapat berpura menjadi pengirim pesan maupun penerima pesan.

c. *Intengrity* (Intengritas)

Penerima harus memeriksa pesan yang diterima karena penyusup tidak dapat mengubah informasi selama data dalam proses pengiriman.

d. Nonrepudiaton

Pengirim dan penerima tidak dapat mengelak bahwa masing-masing terlibat dalam proses pengiriman maupun penerimaan pesan.

2.2. *EMAIL*

Electronic mail (surat elektronik) merupakan sarana pertukaran informasi melalui komunikasi elektronik melalui metode mengirim, menerima, mengubah, dan menyimpan pesan. Format dari pada *e-mail* secara keseluruhan disebut *Multipupose Internet MailExtensions* (MIME). Sebuah pesan *e-mail* terdiri dari dua bagian besar :

a. *Header*

Disusun menjadi beberapa *field*. Penamaan *field* dimulai dengan karakter pertama pada suatu baris, kemudian diikuti oleh tanda ':', nilai non-null, bukan spasi atau bukan tab pada karakter pertamanya. Nama *field* dan nilainya masuk dalam karakter ASCII sebesar 7 bit. Bagian *header* dan bagian *body* dijarakkan dengan satu baris kosong. Pesan paling sedikit memiliki 4 *field*berikut :

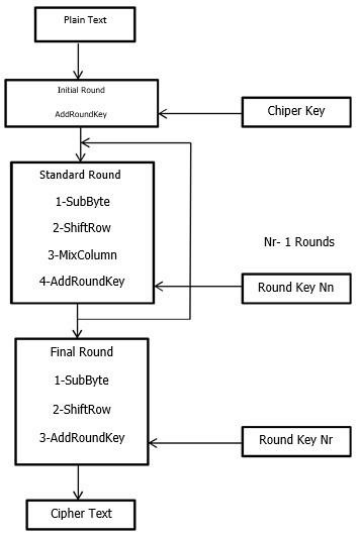
1) *From* : Alamat *e-mail*. Terkadang nama pengirim pesan mengikuti.
2) *To* : Alamat *e-mail*. Terkadang nama penerima pesan mengikuti.
3) *Subject* : Kesimpulan isi pesan.
4) *Date* : Waktu serta tanggal.

b. *Body*

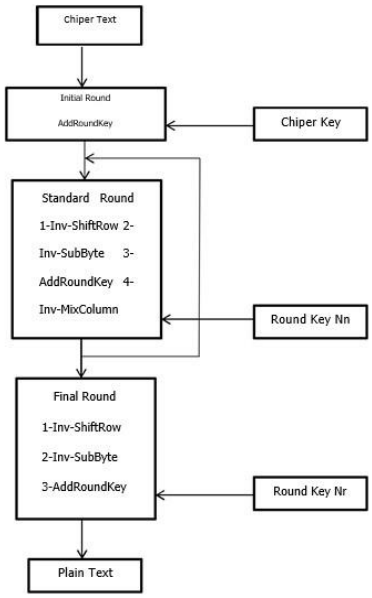
Merupakan pesan diterima yang berisi, teks tanpa struktur dengan seringkali berisi tanda pengenal pada bagian akhir pesa. Adapun *e-mail* pertama kali dikembangkan dengan menggunakan 7-bit ASCII, seiring perkembangan zaman *e-mail* menggunakan 8-bit, namun belum bersifat universal.[3]

2.3. Algoritma AES

Advanced Encryption Standard (AES) merupakan algoritma *cryptographic* yang dapat digunkan untuk mengamakan data. Algoritma AES adalah blok*chipertext* simetrik yang dapat mengenkripsi (*encipher*) dan dekripsi (*decipher*) infoermasi. Enkripsi merubah data yang tidak dapat lagi dibaca disebut ciphertext; sebaliknya dekripsi adalah merubah ciphertext data menjadi bentuk semula yang kita kenal sebagai *plaintext*. Algoritma AES is mengunkan kunci kriptografi 128, 192, dan 256 bits untuk mengenkrip dan dekrip data pada blok 128 bits. [4]



Gambar 2. Diagram Enkripsi AES



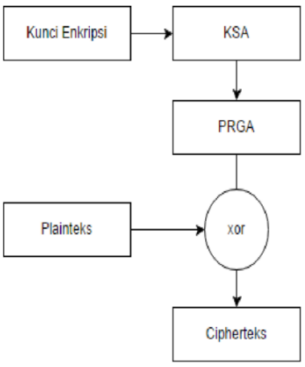
Gambar 3. Diagram Dekripsi AES

2.4. Algoritma RC4

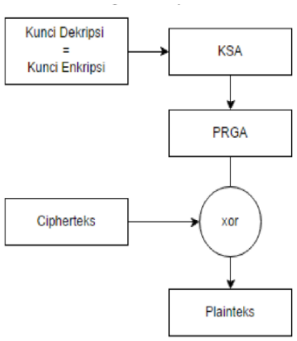
RC4 adalah algoritma kriptografi simetris. Disebut algoritma kriptografi simetris karena menggunakan kunci yang sama untuk mengenkripsi atau mendekripsi suatu pesan, data, ataupun informasi.RC4 telah menjadi bagian dari protocol enkripsi yang standard dan sering digunakan. Faktor utama yang menjadi kesuksesan dari RC4 adalah kecepatannya dan kesederhanaannya dalam menangani banyakaplikasi, sehingga mudah untuk mengembangkan implementasi yang effisien ke *software* dan *hardware*.

RC4 menggunakan panjang variabel kunci 1 s.d. 256 *byte* untk menginisialisasi *state* tabel.*State* tabel digunakan untuk pengurutan menghasilkan *byte pseudo random* yang kemudian menjadi *stream pseudo-random*. Setelah di-XOR dengan plainteks sehingga didapatkan chiperteks. Tiap elemen pada *state* tabel di *swap* sedikitnya sekali. Kunci RC4 sering dibatasi sampai 40 bit, tetapi dimungkinkan

untuk menggunakan kunci 128 bit. RC4 memiliki kemampuan penggunaan kunci antara 1 sampai 2048 bit.Panjang kunci merupakan factor utama dalam sekuritas data.RC4 dapat memiliki kunci sampai dengan 128 bit.[5]



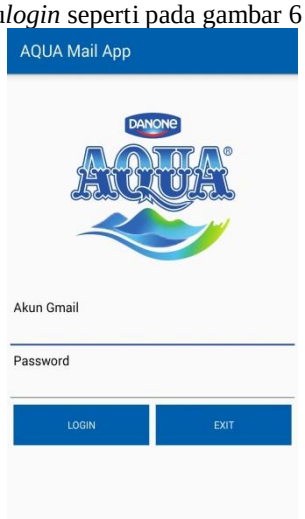
Gambar 4. Arsitektur Enkripsi RC4



Gambar 5. Arsitektur Dekripsi RC4

3. HASIL DAN PEMBAHASAN

Berikut adalah tahapan proses penggunaan aplikasi email berbasis android yang mengimplementasikan algoritma AES-128 dan RC4. Pada saat program pertama dijalankan maka akan munculmenu*login* seperti pada gambar 6 ini:

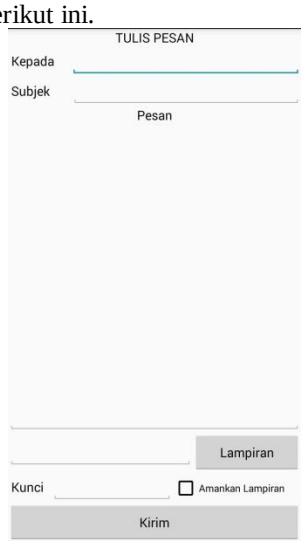


Gambar 6. Tampilan Menu Login

Ketika *user* telah berhasil melakukan *login*, maka tampilan layar *form* menu akan tampil. Pada *form* menu ini terdapat 4 menu yaitu, menu tulis pesan, menu pesan masuk, menu pesan terkirim,dan form buka *file*, serta terdapat tombol *logout* untuk keluar dari aplikasi ini. Terilihat pada gambar 7 berikut.

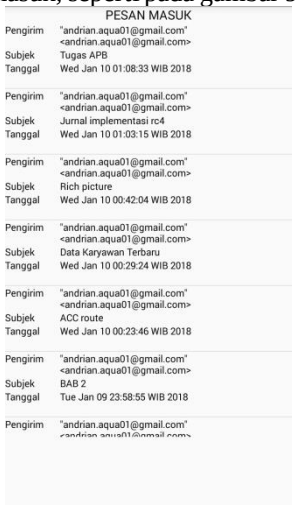
Gambar 7.Tampilan Layar Form Menu

Ketika *user* akan menulis pesan *email*, maka *user* dapat memilih menu tulis pesan seperti pada gambar 8 berikut ini.



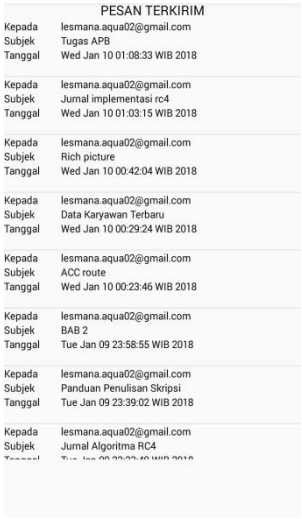
Gambar 8.Tampilan Menu Tulis Pesan

Dalam menu pesan masuk ini, *user*dapat melihat pesan*email*masuk, seperti pada gambar 9 dibawah ini.



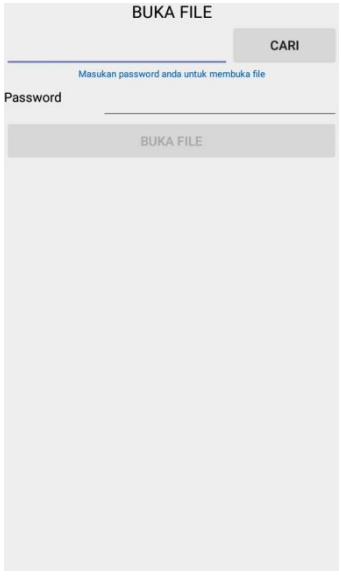
Gambar 9. Tampilan Menu Pesan Masuk

User bisa melihat daftar dari pesan yang telah terkirimpada menu pesan terkirim seperti pada gambar 10 berikut ini.



Gambar 10.Tampilan Menu Pesan Terkirim

Untuk membuka *file* yang telah terenkrip yang diterima oleh *user*, maka digunakan menu buka *file* seperti gambar 11 berikut ini.



Gambar 11.Tampilan Menu Buka File

Dibawah ini adalah table hasil pengujian enkripsi dan dekripsi isi pesan dan lampiran *email.*

Tabel1. Hasil Pengujian Enkripsi

Email	***Plaintext***	***Ciphertext***	**Waktu**
Isi pesan	Materi Enkripsi dan Dekripsi	_ZDU1Y2Y3YWNlNTY4MGRlYjM4NzlmNThkZjZjYzA1NDgxZDU4ZjFiZjc0MDI4MzM1Y2Q0ZmVkYzEzNzhiNTI5OWt1bmNpOjEyMzQ1Njc4	0.0396 detik
Jumlah Karakter	28 karakter	105 karakter	
Lampiran	03 Enkripsi-dan-dekripsi.pdf	03 Enkripsi-dan-dekripsi(locked).pdf	
Ukuran Lampiran	289 KB	770 KB	
Isi pesan	Jurnal Algoritma AES	_OWI4NmE4ZmNhMDc2MTMwNTRlNzgxM2JiMzNhYjMwNDgzMzliY2MxMDc4ODM0MGUwMjZjMmQwYmMxY2UyNGI1YWt1bmNpOjEyMzQ1Njc4	0.1137 detik
Jumlah Karakter	20 karakter	105 karakter	
Lampiran	383-1152-1-PB.pdf	383-1152-1-PB(locked).pdf	
Ukuran Lampiran	1.49 MB	3.98 MB	
Isi pesan	Jurnal Algoritma RC4	_ZTg1YzhlZjJiYzQ3NGZhNmVmYmMxMDNlMjczNjVlOWZlMjA2OWE5ZTllNzJmZDdkZGI5ZTc0OWI0ZjRlNWU3Nmt1bmNpOjEyMzQ1Njc4	0.0347 detik
Jumlah Karakter	20 karakter	105 karakter	
Lampiran	hpO91 Jurnal Nurcahyo.pdf	hpO91 Jurnal Nurcahyo(locked).pdf	
Ukuran Lampiran	467 KB	1.22 MB	
Isi pesan	Panduan Penulisan Skripsi	_YmQ0NjU3MWUyNGI2YWRmNmVkMGQxM2E1OGE0ZGVkNmZmOTY2ZTA4YzQ3Yzc1OTgwMWVkNjJkNzRiOGNjMTNhNWt1b	0.0710 detik

		mNpOjEyMzQ1Njc4	
Jumlah Karakter	25 karakter	105 karakter	
Lampiran	PANDUAN-PENULISAN-SKRIPSI-Gasal-2017-2018.pdf	PANDUAN-PENULISAN-SKRIPSI-Gasal-2017-2018(locked).pdf	
Ukuran Lampiran	0.94 MB	2.51 MB	
Isi pesan	Paper skripsi bab 2	_OGY5ODExYTU2YzRlNjYyNGU3ZTgyMDlmZDEyM2MwNDUxNTI2YjI0YzhkZjgwMjI3Y2VlMDgwY2ZmNDAzNmYxN2t1bmNpOjEyMzQ1Njc4	0.1418 detik
Jumlah Karakter	19 karakter	105 karakter	
Lampiran	BAB II andrian.docx	BAB II andrian(locked).docx	
Ukuran Lampiran	1.97 MB	5.26 MB	

Table 2. Hasil Pengujian Dekripsi

Email	***Ciphertext***	***Plaintext***	**Waktu**
Isi pesan	_ZDU1Y2Y3YWNlNTY4MGRlYjM4NzlmNThkZjZjYzA1NDgxZDU4ZjFiZjc0MDI4MzM1Y2Q0ZmVkYzEzNzhiNTI5OWt1bmNpOjEyMzQ1Njc4	Materi Enkripsi dan Dekripsi	0.0429 detik
Jumlah Karakter	105 karakter	28 karakter	
Lampiran	03 Enkripsi-dan-dekripsi(locked).pdf	03 Enkripsi-dan-dekripsi(unlocked).pdf	
Ukuran	770 KB	289 KB	
Lampiran			
Isi pesan	_OWI4NmE4ZmNhMDc2MTMwNTRlNzgxM2JiMzNhYjMwNDgzMzliY2MxMDc4ODM0MGUwMjZjMmQwYmMxY2UyNGI1YWt1bmNpOjEyMzQ1Njc4	Jurnal Algoritma AES	0.1662 detik
Jumlah Karakter	105 karakter	20 karakter	
Lampiran	383-1152-1-PB(locked).pdf	383-1152-1-PB(unlocked).pdf	
Ukuran Lampiran	3.98 MB	1.49 MB	
Isi pesan	_ZTg1YzhlZjJiYzQ3NGZhNmVmYmMxMDNlMjczNjVlOWZlMjA2OWE5ZTllNzJmZDdkZGI5ZTc0OWI0ZjRlNWU3Nmt1bmNpOjEyMzQ1Njc4	Jurnal Algoritma RC4	0.0624 detik
Jumlah Karakter	105 karakter	20 karakter	
Lampiran	hpO91 Jurnal Nurcahyo(locked).pdf	hpO91 Jurnal Nurcahyo(unlocked).pdf	
Ukuran Lampiran	1.22 MB	467 KB	
Isi pesan	_YmQ0NjU3MWUyNGI2YWRmNmVkMGQxM2E1OGE0ZGVkNmZmOTY2ZTA4YzQ3YzC1OTgwMWVkNjJkN	Panduan Penulisan Skripsi	0.0989 detik

	zRiOGNjMTNhNWt1bmNpOjEyMzQ1Njc4		
Jumlah Karakter	105 karakter	25 Karakter	
Lampiran	PANDUAN-PENULISAN-SKRIPSI-Gasal-2017-2018(locked).pdf	PANDUAN-PENULISAN-SKRIPSI-Gasal-2017-2018(unlocked).pdf	
Ukuran Lampiran	2.51 MB	0.94 MB	
Isi pesan	_OGY5ODExYTU2YzRlNjYyNGU3ZTgyMDlmZDEyM2MwNDUxNTI2YjI0YzhkZjgwMjI3Y2VlMDgwY2ZmNDAzNmYxN2t1bmNpOjEyMzQ1Njc4	Paper skripsi bab 2	0.2212 detik
Jumlah Karakter	105 karakter	19 Karakter	
Lampiran	BAB II andrian(locked).docx	BAB II andrian(unlocked).docx	
Ukuran Lampiran	5.26 MB	1.97 MB	

4. KESIMPULAN

Dari hasil pengujian aplikasi terhadap aplikasi yang dibangun dapat ditarik beberapa kesimpulan, antara lain:

a. Data yang dikirimkan melalui email yang dianggap penting dapat terjaga kerahasiannya dari pihak yang tidak bertanggung jawab dan tidak berkepentingan.
b. Dengan menggunakan algoritma *Advanced Encryption Standard* - 128 (AES-128) dan *Rivest Code 4* (RC4), *email* yang sudah dienkripsi dapat dikembalikan menjadi pesan *email* dan lampiranasli tanpa ada perubahan.
c. Dengan adanya aplikasi enkripsi dan dekripsi *email* yang telah dibuat ini, proses pertukaran data atau *file* di PT. Tirta Investama yang dikirimkan melalui *email* menjadi lebih aman.

5. DAFTAR PUSTAKA

[1]Sadikin, R, 2012, *Kriptografi untuk keamanan jaringan*, Yogyakarta, Andi.

[2]Bodic, G., 2003, *Mobile Messaging Technologies and Services*, John Wiley & Sons Ltd, West Sussex, England.

[3]Budi, Nurcahyo Nugroho, dkk, 2016, *Aplikasi Keamanan Email Menggunakan Algoritma RC4*, Medan, Jurnal SAINTIKOM Vol.15, No. 3, September 2016 (ISSN : 1978-6603).

[4]DocSlide, 2012, *Langkah-Langkah Algoritma AES*, Retrieved from http://documents.tips/documents/langkah-langkah-algoritma-aes.html. [Diakses April 24, 2017].

[5]Hanriyawan, A, 2004,*Enkripsi Data Menggunakan Algoritma RC4*, Padang, Teknik Elektro Politeknik Negeri Padang.