

PEMANFAATAN METODE KRIPTOGRAFI GOST DAN AES-128 UNTUK APLIKASI PENGAMANAN EMAIL BERBASIS WEB PADA CV. GADING SWADAYA PERKASA

Hanithio Juwono¹⁾, Pipin Farida Ariyani²⁾

Teknik Informatika, Fakultas Teknologi Informasi, Universitas Budi Luhur
Jl. Raya Ciledug, Petungkang Utara, Kebayoran Lama, Jakarta Selatan 12260
Telp. (021) 5853753, Fax. (021) 5866369
E-mail : hanithiojuwono@gmail.com¹⁾, pipin.faridaariyani@budiluhur.ac.id²⁾

ABSTRAK

CV. GADING SWADAYA PERKASA merupakan perusahaan yang bergerak dibidang pengolahan air baik itu air bersih, air limbah serta air industri untuk boiler/ ketel uap serta beberapa alat penukar panas lainnya. Dalam melakukan proses bisnisnya, CV. GADING SWADAYA PERKASA sering kali menggunakan surat elektronik atau (e-mail) untuk mengirim berbagai macam pesan dan dokumen yang diperlukan dalam bertransaksi dengan perusahaan lain. Dokumen tersebut adalah dokumen yang rahasia karena berisi data perusahaan, nominal transaksi dan dokumen lain yang bersifat rahasia sehingga diperlukan pengamanan dokumen dan pesan yang dikirimkan melalui e-mail. Pengamanan informasi atau pesan tersebut bertujuan agar tidak jatuh ke orang – orang yang salah. Cara yang dapat digunakan untuk megamankan dokumen rahasia pada surat elektronik (e-mail) adalah menggunakan teknik kriptografi. Tujuan dari penelitian ini untuk menghasilkan aplikasi yang mampu menjaga kerahasiaan informasi atau pesan yang bersifat rahasia dan mengamankan file dan proses komunikasi melalui surel (email) yang tidak dapat diketahui oleh orang lain yang tidak berhak, serta menghasilkan aplikasi enkripsi surat elektronik (e-mail) yang mudah dimengerti dan digunakan oleh pengguna. Teknik kriptografi yang penulis gunakan adalah Algoritma AES (Advanced Encryption Standard) 128 dan GOST (Government Standard). Aplikasi ini dibangun menggunakan bahasa pemrograman Php berbasis web (Internet), Dari hasil pengujian aplikasi ini berhasil melakukan proses enkripsi dan dekripsi pada body email dan file attachment. Dengan adanya proses pengamanan ini dapat memecahkan masalah pada CV. GADING SWADAYA PERKASA.

Kata Kunci : Kriptografi, E-mail, Aes 128, GOST

1. PENDAHULUAN

CV GADING SWADAYA PERKASA adalah perusahaan yg bergerak dibidang pengolahan air baik itu air bersih, air limbah serta air industri untuk boiler/ ketel uap serta beberapa alat penukar panas lainnya. Selain itu juga melayani proses pembersihan dengan menggunakan bahan kimia untuk mesin-mesin seperti Boiler (Ketel uap), Cooling tower , Condenser, Heat Exchanger, Coil cooler PHE, Air Fin Cooler/Air Exchanger dan lain-lain, pesan-pesan penting pemesanan yang melalui email, dalam melakukan transaksi ada file penawaran antar perusahaan yang dikirim melalui email yang sangatlah bersifat rahasia. Tentu hal seperti itu tidak boleh diketahui oleh pihak lain.

Layanan *email* konvensional sudah memiliki pengamanan karena memiliki *password* namun jika *password user* di *hack* maka *hacker* bisa masuk ke *email*. Hal tersebut sudah tentu membuat kekhawatiran jika akan bertukar informasi melalui media *email*. Untuk ini diperlukan aplikasi pengamanan data di *email*.

Berdasarkan uraian di atas penulis bermaksud untuk membuat suatu aplikasi penyandian informasi atau pesan yang akan dikirimkan memanfaatkan

media *email* dengan mengimplementasikan algoritma kriptografi GOST dan AES 128 berbasis Web yang ditunjukan untuk membantu mengatasi masalah keamanan data atau informasi. Di pilihnya algoritma GOST (*Government Standard*) dan AES (*Advanced Encryption Standard*) 128 Kedua algoritma ini adalah algoritma kunci simetris yang melakukan proses enkripsi dan dekripsi lebih cepat daripada algoritma dengan kunci asimetris [1].

Dalam pembuatan aplikasi tersebut, diberi batasan yang bertujuan untuk memfokuskan penelitian, yaitu:

- Email* yang digunakan adalah *email* dari *Google*.
- Bagian *email* yang di enkripsi dan dekripsi adalah *body*.
- Isi *attachment* yang bisa di enkripsi dan dekripsi adalah *file* berformat *.doc*, *.ppt*, *.pdf* dan *.xls*
- Mengirim *file* dan pesan *email* dengan menerapkan algoritma enkripsi GOST dan AES 128 .
- Membaca file dan pesan email menggunakan algoritma dekripsi GOST dan AES.

- f. Ukuran attachment pada email dibatasi kurang dari 3 MB dan jika ukuran lebih kecil akan mempercepat proses pengiriman

2. METODE

2.1 Proses Pengembangan Aplikasi

Pada Penelitian ini penulis melakukan pencarian untuk menentukan metode pengembangan yang digunakan dalam penelitian ini. Adapun metode yang digunakan sebagai berikut :

- Survey lapangan, adalah proses turun langsung pada lokasi penelitian.
- Wawancara, adalah proses tanya jawab langsung kepada orang yang mengetahui tentang permasalahan yang sedang diamati, dalam proses ini yang diwawancarai adalah pemilik perusahaan.
- Studi Literatur, Adalah penelitian yang dilakukan dengan mengumpulkan data dengan membaca buku-buku referensi serta mencari jurnal dan penelitian menggunakan internet yang dapat menunjang penyusunan penelitian ini.
- Metode pengembangan aplikasi yang digunakan dalam mengembangkan aplikasi ini adalah *Waterfall*[2]. Tahap-tahap yang harus di selesaikan secara berurut, yaitu :
 - Requirement Analysis* : Menyusun kebutuhan yang akan dianalisa dan menghasilkan kebutuhan yang harus dipenuhi oleh software.
 - Design* : terdiri dari dua proses yaitu pemodelan system yang menggunakan *flowchart* sebagai penggambaran alur dan desain antarmuka yang menggunakan rancangan layar
 - Implementation* : tahapan dimana rancangann system yang di buat di konversi menjadi suatu aplikasi yang sesuai dengan fungsinya, penulis menggunakan bahasa pemrograman PHP.
 - Testing / Verification* : merupakan pengujian terhadap fungsional aplikasi dapat beroperasi secara tepat.

2.2 Proses Enkripsi Algoritma GOST

Di dalam melakukan proses enkripsi dengan menggunakan algoritma Gost terdiri dari 32 iterasi. Untuk lebih jelasnya mengenai langkah-langkah di dalam melakukan enkripsi data, di mana di dalam flowchart tersebut terdapat dua komponen rahasia yaitu 256 bit kunci kriptografi dan S-boxes (S1,...,S8) .

Metode enkripsi blok cipher yang digunakan pada algoritma GOST adalah[3] sebagai berikut :

- Plaintext 64 bit dipecah menjadi dua bagian yaitu 32 bit bagian kiri (xL) dan 32 bit bagian kanan (xR).
- Berikutnya lakukan proses dengan rumus $xLi = xRi-1$ dan $xRi = xLi-1 \text{ Xor } f(xRi-1, Ki)$
- Selanjutnya pada fungsi f yang pertama yaitu pada iterasi kurang dari 24 bagian kanan data ditambah dengan subkunci ke-i modulus 232, Untuk lebih jelasnya dapat dilihat pada rumus di bawah ini:

$$F = xL + Ko \pmod{232}$$

- Hasilnya dipecah menjadi delapan bagian, dimana setiap bagiannya terdiri dari 4 bit dan setiap bagian menjadi input s-box yang berbeda, di dalam GOST itu sendiri terdapat 8 buah s-box.
- s-box pertama didapat dari 4 bit pertama, s-box kedua didapat dari bit kedua, dan seterusnya.
- Output dari 8 s-box kemudian dikombinasikan menjadi bilangan 32 bit kemudian bilangan ini dirotasi 11 bit ke kiri.
- Akhirnya hasil proses di atas akan di-XOR dengan data bagian kiri yang kemudian menjadi bagian kanan dan bagian kanan menjadi bagian kiri (swap).
- Ini merupakan akhir dari iterasi yang pertama, iterasi selanjutnya dilakukan dengan menggunakan langkah-langkah yang sama dengan iterasi pertama.
- Iterasi ke 3, 4, 5, 6, 7, 8 menggunakan kunci parsial secara terurut (K2 s/d K7)
- Dari iterasi ke 9 sampai 16 dan dari iterasi ke 17 sampai 24 menggunakan kunci parsial yang sama.
- Untuk iterasi ke 25 sampai 32 menggunakan kunci parsial yang terbalik, jadi iterasi yang ke 25 menggunakan kunci K7, iterasi ke 26 menggunakan kunci K6, maka untuk iterasi yang terakhir menggunakan kunci Ko.
- Untuk lebih jelasnya mengenai penggunaan kunci parsial di dalam 32 iterasi tersebut adalah sebagai berikut: K0,..., K7 K0,..., K7 K0,..., K7 K7,..., K0
- Setelah melakukan 32 iterasi maka output dari yang di dalamnya terdapat xL dan xR dengan menyimpan nilai yang sebelumnya.
- Index dari xL dan xR di dalam 64-bit ciphertext akan menghasilkan 64-bit plaintext.

2.3 Proses Dekripsi Algoritma GOST

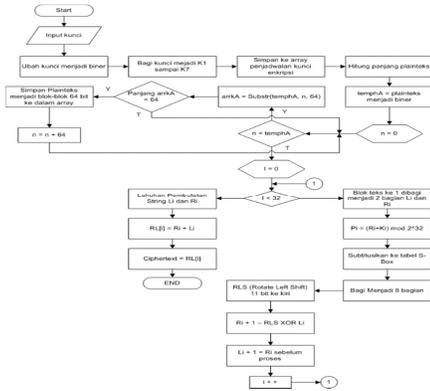
Proses dekripsi sama dengan proses enkripsi dengan urutan k, dibalik, yaitu pada tahap ke 3, 9, 10, 11, 12 dari proses enkripsi maka pada proses dekripsi adalah sebagai berikut:[3]

- Pada fungsi f yang pertama yaitu pada iterasi kurang dari 24 bagian kanan data ditambah dengan subkunci ke-i modulus 232, Untuk lebih jelasnya dapat dilihat pada rumus di bawah ini: $L + K7 \pmod{232}$

- pemrograman PHP menggunakan Atom 1.23.3 dan xampp sebagai *localhost*-nya.
- g. Melakukan *testing* pada aplikasi untuk melihat apakah aplikasi telah berjalan sesuai *design*.
 - h. Merumuskan hasil penelitian dan pembahasan
 - i. Menyusun laporan.

3.2 Flowchart Enkripsi Algoritma GOST

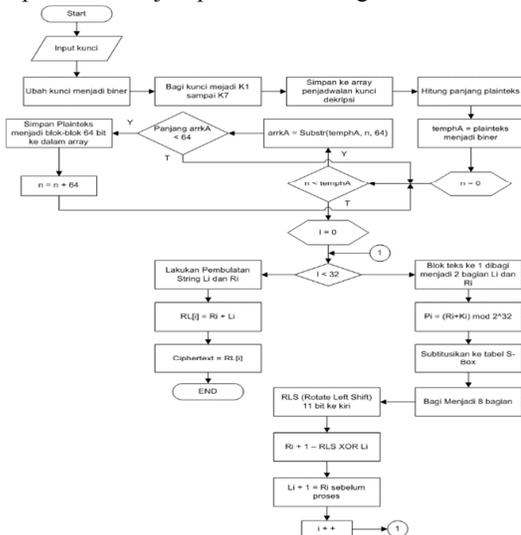
Flowchart ini menjelaskan perubahan dari *plaintext* menjadi *ciphertext* dari algoritma Gost.



Gambar 3: Flowchart Enkripsi GOST

3.3 Flowchart Deskripsi Algoritma GOST

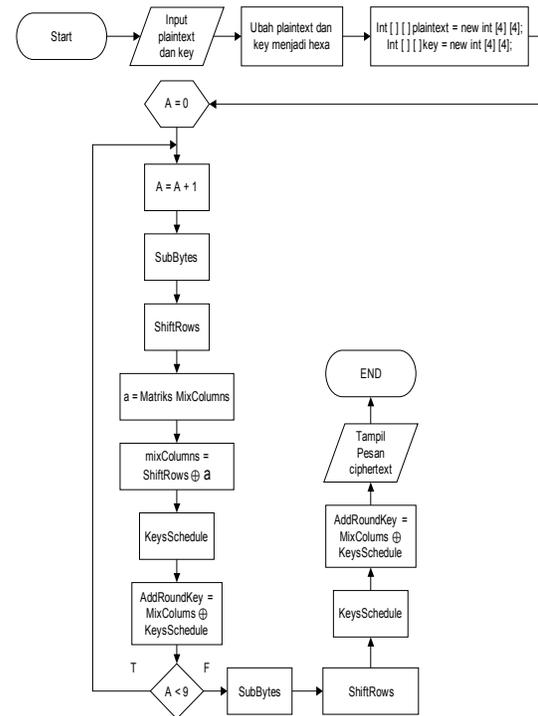
Flowchart ini menjelaskan perubahan kembali dari *ciphertext* menjadi *plaintext* dari algoritma GOST.



Gambar 4: Proses Dekripsi AES 128

3.4 Flowchart Proses Enkripsi Algoritma AES 128

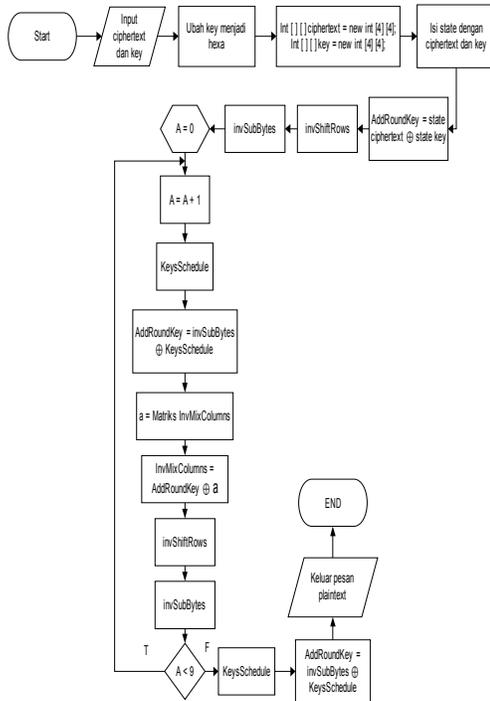
Flowchart ini menjelaskan perubahan dari *plaintext* menjadi *chipertext* dari algoritma AES 128.



Gambar 5: Flowchart Enkripsi AES 128

3.5 Flowchart Proses Dekripsi Algoritma AES 128

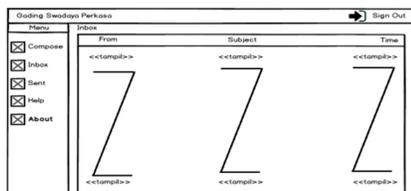
Flowchart proses perubahan dari *chipertext* menjadi *plaintext* dari algoritma AES 128.



Gambar 6: Flowchart Proses AES 128

3.6 Rancangan Layar Menu Utama

Dibawah ini adalah rancangan dari halaman utama dari aplikasi ini, disini ada menu *compose*, *inbox*, *sent*, *about* dan *help* yang mempunyai fungsinya masing-masing.



Gambar 7: Tampilan Rancangan Layar Menu utama

4. HASIL DAN PEMBAHASAN

4.1 Tampilan Layar

Berikut ini merupakan tampilan dari beberapa fungsi utama yang ada di aplikasi ini.

a. Tampilan Layar Form Login

Berikut ini tampilan form *login*, merupakan yang akan tampil pertama kali ketika *user* menjalankan aplikasi dan menjadi penghubung ke halaman utama yang langsung membuka menu *inbox*.

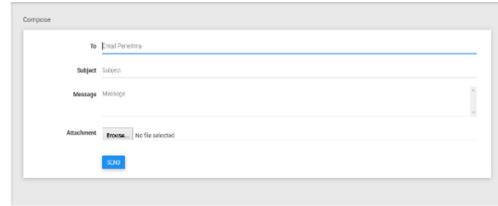


Berbasis Web Pada CV. Gading Swadaya Perkasa

Gambar 8: Tampilan Layar Form Login

b. Tampilan Layar Form Compose

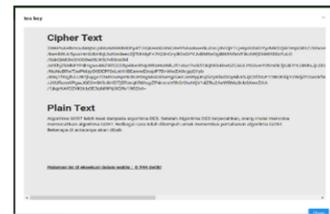
Pada tampilan *form compose*, *user* bisa mengirim pesan baru kepada seseorang.



Gambar 9: Tampilan Layar Menu Compose

c. Tampilan Layar Form Inbox

Pada tampilan *form inbox*, *user* dapat melihat list pesan masuk yang tampil di *form* ini.



Gambar 10: Tampilan Layar Form Inbox

d. Tampilan Layar Form Sent

Pada tampilan *form Sent*, *user* dapat melihat list pesan keluar yang tampil di *form* ini.

Gambar 11: Tampilan Layar Form Sent

4.2 Tabel Pengujian

Pengujian kali ini menampilkan proses enkripsi dan dekripsi *file attachment*. *File attachment* yang diuji adalah jenis *file attachment* berformat file docx dan xlsx. Pengujian ini dilakukan untuk membandingkan ukuran *file attachment* asli dan ukuran *file attachment* setelah proses enkripsi dilakukan serta waktu saat enkripsi dan waktu proses dekripsi.

Tabel 1: Tabel Pengujian

Nama file	Ukuran File			Waktu	
	Asli	Enkripsi	Dekripsi	Enkrip (s)	Dekrip (s)
Po upload.docx	76 Kb	101 Kb	76 Kb	3.244	0.207
sample.xls	215 Kb	286 Kb	215 Kb	3.721	0.066

4.3 Evaluasi Program

Setelah dilakukan pengujian aplikasi ditemukan adanya kelebihan dan kekurangan pada aplikasi ini, beberapa yang telah didapat diantaranya sebagai berikut :

a. Kelebihan Aplikasi

- 1) Aplikasi mudah digunakan karena tampilannya dibuat secara umum.
 - 2) Berbasis *web*, sehingga tidak membutuhkan instalasi pada klien
 - 3) Aplikasi dapat berjalan dengan baik selama ada koneksi internet
 - 4) Isi pesan akan lebih aman, karena pesan telah dienkripsi
- b. Kekurangan Aplikasi
- 1) Fitur yang terdapat pada aplikasi masih sedikit.
 - 2) Aplikasi tidak dapat berjalan jika tidak ada koneksi internet.
 - 3) Jika terjadi gangguan koneksi internet akan mempengaruhi kinerja aplikasi ini
 - 4) Hanya bisa mengirim file satu saja tidak bisa lebih.

5. KESIMPULAN

5.1 Kesimpulan

Setelah proses pembuatan dan pengujian dalam penelitian ini telah dilakukan, dapat diberikan kesimpulan yang dapat diambil, antara lain:

- a. Aplikasi ini diatur sistem agar isi pesan dan data yang di dalam akun email tersebut otomatis telah dienkripsi.
- b. Dengan adanya aplikasi enkripsi dan dekripsi email berbasis web yang menggunakan proses enkripsi maka pesan yang dikirim melalui email menjadi lebih aman.

To	SUBJECT	TIME
hadi@...@gmail.com	Pesan Compose Email	Thu, 19 Dec 2017 11:49:28 (GMT)
hadi@...@gmail.com	Pesan Compose Email	Wed, 20 Dec 2017 12:01:28 (GMT)
hadi@...@gmail.com	See Mail	Wed, 20 Dec 2017 12:04:28 (GMT)
hadi@...@gmail.com	See Mail	Thu, 21 Dec 2017 09:00:00 (GMT)
hadi@...@gmail.com	See Mail	Thu, 19 Dec 2017 11:49:28 (GMT)
hadi@...@gmail.com	See Mail	Thu, 19 Dec 2017 11:49:28 (GMT)
hadi@...@gmail.com	Pesan Compose Email	Fri, 19 Dec 2017 10:16:16 (GMT)
hadi@...@gmail.com	See Mail	Wed, 20 Dec 2017 12:04:28 (GMT)
hadi@...@gmail.com	Pesan Compose Email	Fri, 19 Dec 2017 12:14:47 (GMT)
hadi@...@gmail.com	Pesan Compose Email	Fri, 19 Dec 2017 10:16:16 (GMT)

- c. Meminimalisir kemungkinan pencurian atau penyadapan pesan pada email oleh pihak yang tidak bertanggung jawab.
- d. Aplikasi ini tidak hanya isi pesan tetapi bisa juga meng-Attachment.
- e. Waktu untuk mengirim pesan bergantung dengan panjang teks dan besar *file attachment* yang dienkripsi, semakin pendek ukuran teks dan filenya maka semakin cepat proses pengirimannya.

5.2 Saran

Beberapa saran yang dapat diberikan untuk pengembangan aplikasi dengan harapan menghasilkan penelitian yang lebih baik lagi selanjutnya, berikut saran yang dapat diberikan:

- a. Dapat membalas email secara langsung di email tersebut tanpa membuka menu compose.

- b. Dapat ditambahkan domain email lain seperti yahoo, hotmail, live serta email host lainnya.
- c. Tampilan yang sederhana, diharapkan dapat ditambahkan beberapa fitur yang nantinya bisa membuat aplikasi ini lebih baik.

6. DAFTAR PUSTAKA

- [1] Basri., 2016, *Kriptografi Simetris Dan Asimetris Dalam Perspektif Keamanan Data Dan Kompleksitas Komputasi*, Jurnal Ilmiah Ilmu Komputer, 2(2), pp.2442–4512.
- [2] Pressman., R.S., 1997. *Software Engineering : A Practitioer’s Approach* 5th ed. B. Jones, ed., Americas, New York: Thomas Casson.
- [3] Nugraha, Ucu., dan Marisa, Fitrya., 2009, *Perbandingan Algoritma Rc4 Dengan Algoritma Gost Untuk Meningkatkan Keamanan Data*, InSearch, Universitas Informatika dan Bisnis Indonesia, (2), pp1.
- [4] Primartha, R., 2013, *Penerapan Enkripsi dan Dekripsi File menggunakan Algoritma Advanced Encryption Standard (AES)*, Journal of Research in Computer Science and Applications, 2(1), pp13–18.