APLIKASI PENGAMANANAN EMAIL DENGAN ALGORITMA *ADVANCED ENCRYPTION STANDARD* (AES), RIVEST CIPHER 4 (RC4) DAN CAESAR CIPHER

Ryfan Aditya Indra[*] dan Wahyu Pramusinto
Program Studi Teknik Informatika, Fakultas Teknologi Informasi, Universitas Budi Luhur
Jl. Raya Ciledug, Petukangan Utara, Jakarta Selatan 12260
[*]Email: ryfandotnet@gmail.com[1], wahyu.pramusinto@budiluhur.ac.id[2]

Abstrak

Teknologi informasi sangat dibutuhkan oleh perusahaan. Salah satu teknologi yang banyak digunakan oleh perusahaan adalah email. Terkadang data-data yang dikirim via email adalah data rahasia yang isinya tidak boleh diketahui orang lain. Akan tetapi sebagian besar provider email tidak menyediakan fitur untuk mengamankan pesan sehingga email yang dikirimkan hanya berbentuk plain text yang isinya bisa langsung dibaca oleh orang yang tidak berhak menerimanya. Untuk mengamankan data dalam email dapat dilakukan dengan teknik penyamaran atau penyandian data yang disebut dengan kriptografi. Kriptografi merupakan ilmu dan seni teknik penyamaran atau penyandian pesan untuk melindungi data dengan mengubah kode tertentu dan hanya orang tertentu (encryptor) mempunyai kunci yang dapat menjamin kerahasiaan data. Pada penelitian ini dibuat sebuah aplikasi berbasis web untuk mengirim dan menerima email dengan menerapkan metode kriptografi yakni Algoritma Advanced Encryption Standard dengan jumlah bit 128 (AES-128) dan Algoritma Rivest Cipher 4 (RC4) untuk pengamanan isi email serta Caesar Cipher untuk pengamanan kunci. Dengan menerapkan kedua algoritma tersebut isi email akan diubah menjadi suatu informasi yang tidak dapat dimengerti oleh siapapun dan diharapkan keamanan dalam pengiriman informasi melalui email dapat terjamin kerahasiaan dari sebuah informasi tersebut.

Kata kunci : *algoritma AES-128, algoritma RC4,caesar cipher, aplikasi email, kriptografi*

1. PENDAHULUAN

1.1. Latar Belakang

Dahulu, untuk berkomunikasi sangatlah sulit, namun dengan seiringnya waktu berjalan munculah era teknologi informasi yang dapat mempermudah berkomunikasi. Salah satu cara untuk melakukan komunikasi adalah menggunakan email. Terkadang data-data yang dikirim via email adalah data rahasia yang isinya tidak boleh diketahui orang lain. Akan tetapi sebagian besar provider email tidak menyediakan fitur untuk mengamankan pesan sehingga email yang dikirimkan hanya berbentuk *plain text* yang isinya bisa langsung dibaca oleh orang yang tidak berhak menerimanya.

Untuk mengamankan data dalam email yang dikirim dapat dilakukan dengan teknik penyamaran atau penyandian data yang disebut dengan kriptografi. Pada penelitian ini dibuat sebuah aplikasi berbasis web untuk mengirim dan menerima email dengan menerapkan metode kriptografi yakni Algoritma Advanced Encryption Standard dengan jumlah bit 128 (AES-128), Algoritma Rivest Cipher 4 (RC4) dan Caesar Cipher.

1.2. Rumusan Masalah

a. Bagaimana menjaga kerahasiaan data yang dikirimkan via email?
b. Bagaimana menerapkan metode kriptografi AES-128, RC4 dan Caesar Cipher untuk mengamankan email?

1.3. Tujuan Penelitian

Penelitian ini bertujuan membuat aplikasi email yang mengimplementasikan metode kriptografi AES-128, RC4 dan Caesar Cipher untuk mengamankan data email yang dikirim.

1.4. Batasan Permasalahan

a. Aplikasi ini dibuat menggunakan bahasa pemrograman PHP.
b. Username dan password untuk masuk ke aplikasi ini menggunakan akun Gmail.
c. Algoritma AES dan RC4 digunakan untuk mengenkripsi isi pesan dan lampiran.
d. Algoritma Caesar Cipher digunakan untuk mengenkripsi kunci/*password.*

2. METODOLOGI

2.1. Kriptografi

Secara umum kriptografi dapat diartikan sebagai ilmu dan seni penyandian yang bertujuan untuk menjaga keamanan dan kerahasiaan suatu data. Kriptografi juga tidak berarti hanya memberikan keamanan informasi saja, namun kriptografi lebih ke arah teknik-tekniknya (Bhaudhayana dan Widiartha, 2015).

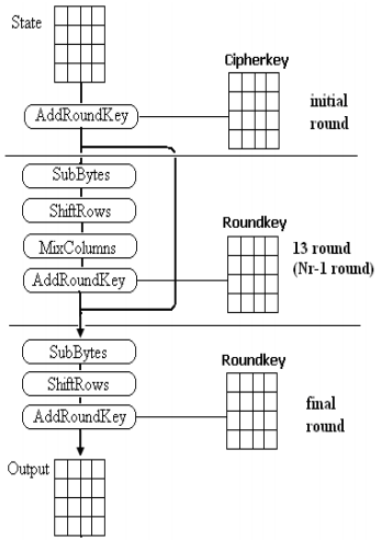
Konsep kriptografi yang bertujuan untuk menjaga kerahasiaan pesan/data adalah dengan cara menyamarkan pesan/data menjadi bentuk tersandi yang tidak dapat dibaca oleh siapapun. Pesan/data yang akan disandikan disebut *plaintext*, sedangkan yang telah disamarkan (telah disandikan) disebut *ciphertext*. Proses penyamaran dari *plaintext* ke *ciphertext* disebut dengan enkripsi, sedangkan proses pengembalian dari *ciphertext* menjadi *plaintext* disebut dengan dekripsi (Primartha, 2013).

Kriptografi memiiki 4 komponen utama yaitu:

1) *Plaintext*, yaitu pesan/data yang dapat dibaca.
2) *Ciphertext*, yaitu pesan/data sandi acak yang tidak bisa dibaca oleh siapapun.
3) *Key*, yaitu metode untuk melakukan teknik kriptografi sebagai kunci.
4) Algoritma, yaitu metode untuk melakukan proses enkripsi dan proses dekripsi.

2.2. Algoritma AES (Advanced Encryption Standard)

Algoritma AES (*Advanced Encryption Standard*) merupakan algoritma blok *cipher* yang aman untuk melindungi data atau informasi yang bersifat rahasia. AES (*Advanced Encryption Standard*) dipublikasikan oleh NIST (*National Institute of Standard and Technology*) pada tahun 2001 yang digunakan untuk menggantikan algoritma DES (*Data Encryption Standard*) yang sudah dianggap kuno dan mudah dibobol.



Gambar 1. Proses Enkripsi Pada AES (Ibrahim, 2017)

Garis besar algoritma *Advanced Encryption Standard* (AES) adalah sebagai berikut :

1) *AddRoundKey* yakni melakukan XOR antara awal (*plaintext*) dengan *cipher key*.
2) Putaran sebanyak Nr-1 kali.

Proses yang dilakukan pada setiap putaran adalah :

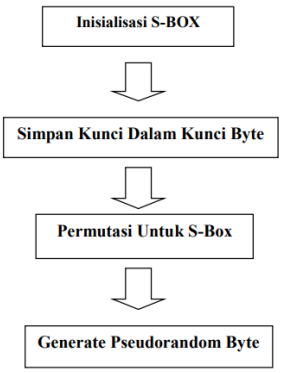
a. *SubBytes*, yakni subsitusi *byte* menggunakan *table* subsitusi (S-Box).
b. *ShiftRows*, yakni pergeseran baris-baris *array state* secara *wrapping*.
c. *MixColumns*, yakni mengacak data di masing-masing kolom *array state*.
d. *AddRoundKey*, yakni melakukan XOR antara *state* saat *round key*.

3) *Final round*, proses untuk putaran terakhir meliputi:
a. SubBytes
b. ShiftRows
c. *AddRoundKey*

ISBN 978-602-99334-9-9

2.3. Algoritma RC4 (Rivest Cipher 4)

Algoritma RC4 (*Rivest Cipher 4*) ini sederhana dan mudah diimplementasikan. RC4 (*Rivest Cipher 4*) dibuat oleh Ron Rivest dari laboratorium RSA (RC adalah singkatan dari Ron's Code). Gambar berikut memperlihatkan rangkaian proses yang dijalankan untuk mengenkripsi data.



Gambar 2. Rangkaian Proses Pada RC4 (Putra dkk, 2017)

2.4. Algoritma Caesar Cipher

Caesar Cipher adalah metodologi enkripsi pertama. Metode enkripsi ini berjenis *cipher* subtitusi, dimana setiap huruf pada *plaintext*-nya digantikan dengan huruf lain. Misalnya dengan pergeseran 3 langkah, A akan digantikan oleh D, B akan menjadi E, dan seterusnya

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	Q	R	S	T	U	V	W	X	Y	Z
D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C

Gambar 3. Contoh pergeseran tiga langkah

Untuk menyandikan sebuah pesan, cukup mencari setiap huruf yang hendak disandikan di alfabet biasa, lalu tuliskan huruf yang sesuai pada alfabet sandi. Untuk memecahkan sandi tersebut gunakan cara sebaliknya.

2.5. Landasan Teori

(Fairuzabadi, 2010) membuat penelitian untuk mengimplementasikan kriptografi klasik menggunakan Borland Delphi. Metode kriptografi klasik yang digunakan adalah tehnik substitusi, shift chiper, monoalphabetic chiper, polyalphabetic chiper dan tehnik transposisi. Penelitian dilakukan pada plain teks, bukan pada file dokumen. Secara teknik kriptograsi klasik mudah diimplementasikan menggunakan Borland Delphi

Penelitian lain tentang kriptografi RC4 pernah dilakukan oleh (Nugroho dkk, 2016) untuk mengamankan pesan email. Penelitiannya untuk membuat aplikasi yang dapat membantu menjaga keamanan pesan pada email sehingga penyusup tidak bisa mengambil informasi pribadi pada email. Dalam penelitian ini digunakan 1 algoritma saja yaitu RC4 untuk mengenkripsi pesan email.

(Ibrahim,2017) membuat penelitian berjudul Perancangan Pengamanan Data Menggunakan Algoritma AES (Advanced Encyption Standard) yang membuat aplikasi untuk mengamankan data dengan menggunakan algoritma AES. Menurut penelitian ini kriptografi mempunyai tiga unsur penting yaitu pembangkitan kunci, enkripsi dan deskipsi

3. HASIL DAN PEMBAHASAN

3.1. Perancangan Aplikasi

Aplikasi yang akan dibuat terdiri dari beberapa halaman yakni Halaman *Login*, *Dashboard*, Kirim *Email*, Pesan Masuk, Lihat Pesan, Bantuan Penggunaan dan Halaman Tentang Aplikasi. Dalam penggunaan aplikasi pengamanan *email* ini, pengguna (*user*) wajib melalukan *login* dengan *email Google* (*Gmail*). Setelah itu *user* diarahkan ke halaman beranda (*dashboard*) sebagai tanda bahwa *user* telah melakukan autentikasi *user email*. Untuk menggunakan aplikasi pengiriman *email* yang terenkripsi, pengguna dapat memilih menu Kirim *Email* dibagian *sidebar* halaman. Pengguna

(*user*) mengisikan *form* kirim *email* dengan *input*an tujuan *email*, judul pesan, isi pesan, lampiran dan memberikan *password* pesan sebagai kunci dalam mengenkripsi dan memproses serta mengirim *email* menggunakan *SMTP* (*Simple Mail Transfer Protocol*) *Gmail*. Pesan dan lampiran akan dienkripsi AES-128 kemudian RC4. Sementara *password*/kunci akan dienkripsi dengan Caesar Cipher

Untuk membaca *email* masuk yang telah dienkripsi, pengguna memilih *email* di menu Pesan Masuk kemudian akan diarahkan ke halaman Lihat Pesan. sebelum membuka isi *email*, pengguna dimintai untuk memasukkan password/kunci yang pertama kali dibuat untuk mendekripsi pesan dan lampiran.

3.2. Komponen Yang Digunakan

3.2.1. Perangkat Lunak (*Software*)

Perangkat lunak yang dipakai untuk mengembangan aplikasi ini yaitu sebagai berikut:

1) Sistem Operasi *Windows* 7
2) *Notepad++*
3) Browser Google Chrome
4) *Xampp* 5.5.19

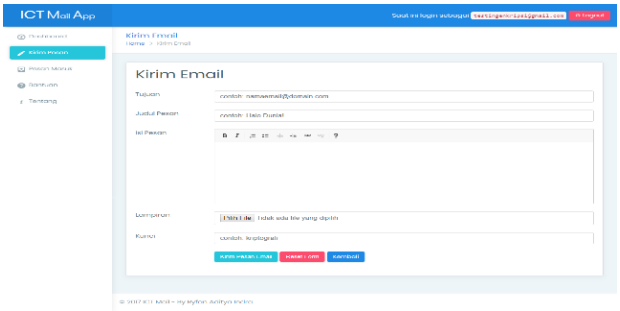
3.2.2. Perangkat Keras (*Hardware*)

Perangkat keras yang digunakan untuk membuat aplikasi ini yaitu sebagai berikut:

1) *Processor* Intel Core i5-5200U *Processor* 2.70 *GHz*
2) *Memory* 4 GB RAM
3) VGA Intel(R) HD *Graphics Family*
4) *Harddisk space* 500 GB

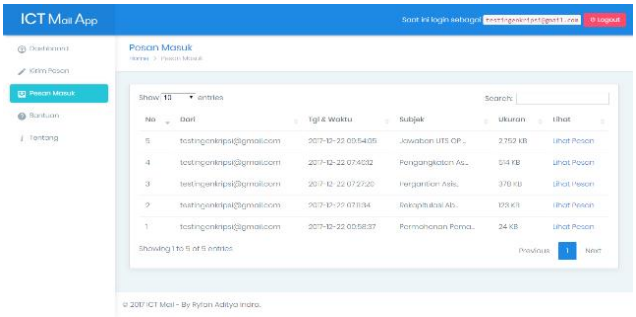
3.3. Tampilan Layar

Gambar 4 merupakan tampilan layar halaman Kirim *Email*, *user* wajib memasukan alamat *email* yang dituju, subjek pesan, isi pesan, lampiran dan kunci enkripsi.



Gambar 4. Tampilan Layar Halaman Kirim Email

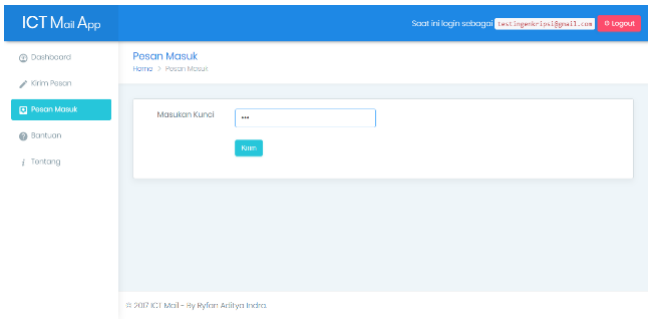
Gambar 5 adalah tampilan layar halaman Pesan Masuk dimana *user* dapat melihat pesan-pesan yang masuk yang bertujuan ke email *user*. Pada halaman ini terlihat email pengirim, tanggal kirim, judul dan ukuran. Untuk melihat isi email, klik Lihat Pesan.



Gambar 5. Tampilan Layar Halaman Pesan Masuk

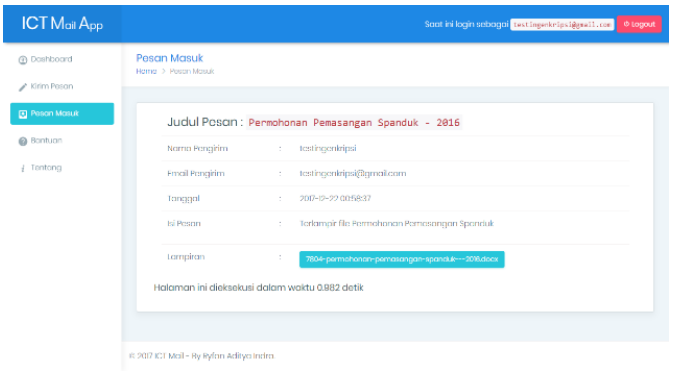
ISBN 978-602-99334-9-9

Setelah mengklik Lihat Pesan pada gambar sebelumnya, *user* diminta untuk memasukan kunci agar pesan dapat didekripsi seperti Gambar 6.



Gambar 6. Tampilan Layar Halaman Masukan Kunci Dekripsi

Jika kunci sesuai, pesan asli akan ditampilkan seperti Gambar 7.

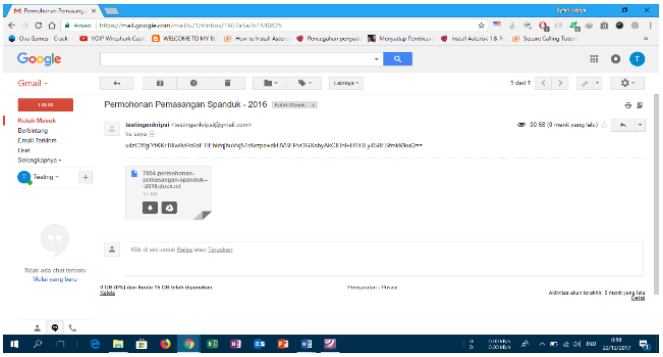


Gambar 7. Tampilan Layar Halaman Lihat Pesan

3.4. Pengujian Program

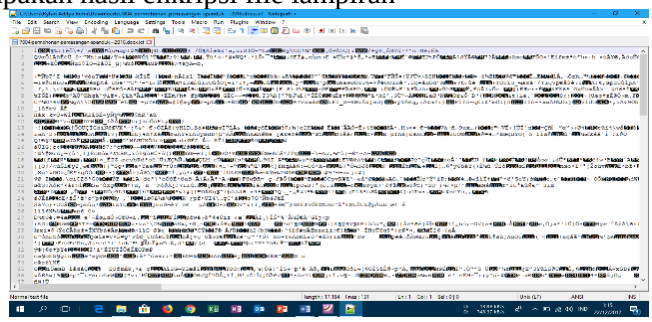
Judul Pesan : Permohonan Pemasangan Spanduk - 2016
Isi Pesan : Terlampir *file* Permohonan Pemasangan Spanduk
Isi Lampiran : File permohonan.docx

Gambar 8 merupakan hasil enkripsi isi pesan dan lampiran yang terdapat di *Inbox Gmail*.



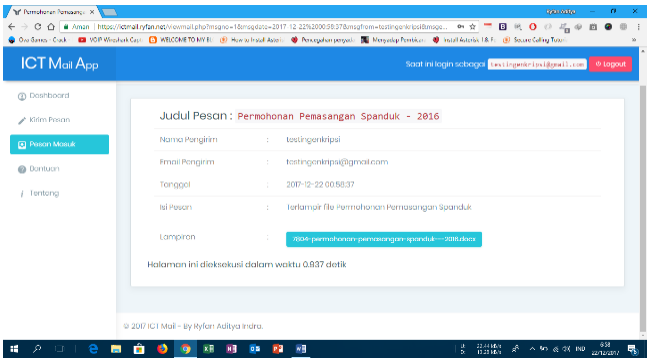
Gambar 8. Hasil Enkripsi Inbox Gmail

Gambar 9 merupakan hasil enkripsi file lampiran



Gambar 9. Hasil Enkripsi File Lampiran

Gambar 10 menunjukan hasil dekripsi pesan *email* yang terenkripsi user masuk ke kotak masuk. Pengguna memilih pesan yang ingin didekrip kemudian masukan kunci. Jika benar akan menghasilkan pesan utuh sesuai yang dikirim diawal.



Gambar 10. Hasil Dekripsi Pesan

4. KESIMPULAN

a. Algoritma *Advanced Encryption Standard* (AES-128), *Rivest Cipher 4* (RC4) dan *Caesar Cipher* dapat diimpllementasikan pada pesan *email* dalam bahasa pemrograman PHP untuk mengenkripsi dan mendekripsi suatu isi pesan dan *file* lampiran.
b. Program aplikasi pengamanan email ini berbasis web sehingga memudahkan untuk penggunaan dan hanya memerlukan koneksi internet dan browser.
c. Waktu yang dibutuhkan untuk melakukan enkripsi dan dekripsi isi pesan dan file lampiran berbeda-beda tergantung pada jumlah karakter isi pesan, ukuran file lampiran dan koneksi internet.

DAFTAR PUSTAKA

Bhaudhayana, G. W. and Widiartha, I. M. (2015) 'Implementasi algoritma kriptografi aes 256 dan metode steganografi lsb pada gambar bitmap', Jurnal ilmu komputer Universitas Udayana, 8(2), pp. 15–25.

Ibrahim, A. A. (2017) 'Perancangan Pengamanan Data Menggunakan Algoritma AES (Advanced Encyption Standard)', III(1), pp. 53–60.

Fairuzabadi,M., "Implementasi Kriptografi Klasik Menggunakan Borland Delphi", Jurnal Dinamika Informatika Vol 4 No 2, September 2010.

Nugroho, N. B., Azmi, Z. and Arif, S. N. (2016) 'Aplikasi Keamanan Email Menggunakan Algoritma Rc4', Jurnal SAINTIKOM, 15(3), pp. 81–88.

Primartha, R. (2013) 'Penerapan Enkripsi dan Dekripsi File menggunakan Algoritma Advanced Encryption Standard (AES)', Journal of Research in Computer Science and Applications, 2(1), pp. 13–18. doi: 2301-8488.

Putra, D. et al. (2017) 'IMPLEMENTASI ALGORITMA RC4 DAN PLAYFAIR CIPHER Permutasi Untuk S-Box', 16, pp. 328–334.

ISBN 978-602-99334-9-9