IMPLEMENTASI KRIPTOGRAFI *CHATTING* MENGGUNAKAN METODE *VIGENERE* DAN *AES 128* BERBASIS WEB

Mohammad Arifin[1)], **Mufti**[2)]
[1]Program studi, Fakultas Teknologi Informasi, Universitas Budi Luhur
[1,2]Jl. Raya Ciledug, Petukangan Utara, Kebayoran Lama, Jakarta Selatan 12260
E-mail : ipinscania1@gmail.com[1)], muftyhayat@gmail.com[2)]

Abstrak

Pada PT ITPro Citra Indonesia tidak semua pesan atau pembicaraan bisa dikonsumsi publik, ataupun diketahui karyawan biasa terutama pada pesan atau pembicaraan penting. Dan selama ini pesan yang penting hanya disampaikan melalui pesan pribadi. Mengakses aplikasi Whatsapp kita bisa langsung membukanya di smartphone tanpa harus mengisi password. Meskipun aplikasi Whatsapp memiliki enkripsi di tiap pesannya, baik chatting perseorangan maupun chatting grup, namun tidak menutup kemungkinan untuk kehilangan pesan penting bisa saja terjadi melalui cara apapun. Salah satu caranya bisa dengan pencurian smartphone langsung, maka pencuri bisa langsung melihat pesan penting yang ada pada chatting Whatsapp yang tidak dilindungi password untuk mengakses aplikasi. Oleh karena itu dibutuhkan aplikasi yang tidak hanya bisa mengenkripsi pesan, namun untuk bisa mengakses aplikasi juga harus memasukkan password atau kunci untuk bisa mengakses aplikasi. Metode kritografi yang digunakan untuk mengamankan pesan pada penelitian tugas akhir ini adalah Vigenere dan AES 128. Dengan adanya aplikasi ini, para pegawai PT ITPro Citra Indonesia bisa mengamankan percakapan antara Manager, Direktur dan juga dengan Karyawan lainnya agar tidak bisa diketahui bahkan dicuri oleh orang yang tidak berkepentingan dan tidak bertanggung jawab. Dan juga bisa menjaga kerahasiaan informasi penting melalui percakapan dalam group chatting ini.

Kata kunci : Chatting, Kriptografi, Enkripsi Vigenere, AES 128

1. PENDAHULUAN

Seiring dengan melesatnya pekembangan Teknologi, kini setiap orang lebih mudah untuk mengakses berbagai sumber data dan informasi dari dalam maupun luar negeri serta tidak menutup kemungkinan terjadinya pencurian data oleh pihak tidak bertanggung jawab. Menjaga keamanan sebuah data yang dimiliki seseorang maupun perusahaan menjadi suatu hal yang sangat penting untuk dilakukan demi menjaga keutuhan sebuah data dari kerusakan maupun pencurian oleh pihak-pihak yang tidak bertanggung jawab, sehingga data yang disimpan tidak mengalami perubahan atau sesuai dengan aslinya.

Berdasarkan hal tersebut, rumusan masalah dalam penulisan ini adalah sebagai berikut:

a. Bagaimana cara yang dapat dilakukan untuk melindungi informasi pesan chatting tersebut dengan menggunakan metode Vigenere dan metode AES 128 bit?
b. Bagaimana mengembalikan data chatting yang sudah di enkripsi menjadi data asli tanpa mengubah isi data tersebut ?

2. LANDASAN TEORI

2.1 Keamanan Data

Keamanan data merujuk pada langkah-langkah untuk melindungi kerahasiaan informasi digital yang diterapkan untuk mencegah akses dari pihak yang yang tidak berwenang baik itu komputer, basis data, website dan lainnya. Keamanan data juga dikenal dengan keamanan informasi ataupun keamanan komputer. Teknologi keamanan data meliputi Enkripsi software/hardware, data masking, backup, dan juga penghapusan data (data erasure).

Tujuan utama dari keamanan data ialah untuk memastikan sekaligus melindungi data baik milik pribadi ataupun perusahaan. Keamanan data tidak hanya bergantung pada teknologi saja, tetapi dari aspek prosedur dan kebijakan keamanan yang diterapkan serta kedisiplinan sumber daya manusia, jika panduan keamanan tidak diikuti maka data ataupun informasi sensitif yang tersimpan akan sangat beresiko untuk diakses oleh pihak yang tidak berwenang. [8]

2.2 Algoritma

Algoritma merupakan urutan barisan langkah–langkah atau instruksi untuk menyelesaikan suatu permasalahan. Walaupun sejauh ini tidak ada standarisasi tentang bagaimana menyusun algoritma, tetapi secara prinsip bentuk algoritma dapat bebas ditentukan setiap orang, baik menggunakan *pseudocode*, atau bahkan diagram alir (*flowchart*) untuk implementasi suatu algoritma. Kriteria algoritma yang baik [16] adalah :

(1) Ada output-nya dimana output merupakan solusi dari masalah yang disediakan,
(2) Algoritma menghasilkan suatu solusi yang sesuai dengan masalanya (efektif) dan algoritma tersebut mempunyai waktu proses

realtif lebih singkat dan penggunaan memorinya relatif lebih sedikit.

(3) Jumlah langkahnya berhingga, tujuannya waktu proses relatif lebih singkat, dan memperoleh hasil yang sesuai dan apabila solusi diperoleh proses akan berhenti.

Hal yang perlu diperhatikan dalam menyusun suatu algoritma, diantaranya :

(1) *Finiteness* menyatakan suatu algoritma harus berakhir untuk semua kondisi setelah memproses sejumlah langkah.
(2) *Definiteness* menyatakan setiap langkah harus dinyatakan dengan jelas (tidak rancu/bermakna ganda).
(3) Masukan (*Input*) merupakan suatu besaran yang diberikan di awal sebelum algoritma diproses.
(4) Keluaran (*Output*) merupakan besaran yang mempunyai kaitan atau hubungan dengan masukan.
(5) Efektivitas artinya semua operasi yang dilaksanakan oleh algoritma harus sederhana dan dapat dikerjakan dalam waktu terbatas. Secara prinsip, setiap instruksi dalam algoritma dapat dikerjakan oleh orang dengan hanya menggunakan kertas dan pensil.

2.3 Kriptografi

Kriptografi (Cryptography), berasal dari Bahasa Yunani,cryptos berarti secret atau rahasia sedangkan graphein berarti writing atau tulisan. [3] kriptografi adalah ilmu dan seni untuk menjaga keamanan pesan ketika pesan dikirim dari suatu tempat ke tempat lain.

Kriptografi pada awalnya dijabarkan sebagai ilmu yang mempelajari bagaimana menyembunyikan pesan. Namun pada pengertian modern, kriptografi adalah ilmu yang bersandarkan pada teknik matematika untuk berurusan dengan keamanan informasi seperti kerahasiaan, keutuhan data dan otentikasi entitas. Jadi pengertian kriptografi modern saja tidak berurusan hanya dengan penyembunyian pesan, namun lebih pada sekumpulan teknik yang menyediakan keamanan informasi [12].

2.4 Algoritma Vigenere

Vigenere adalah suatu algoritma kriptografi klasik yang ditemukan oleh Giovan Battista Bellaso [3]. Pada bukunya beliau menuliskan metodenya tersebut yang berjudul *La Cifra del Sig. Giovan Battista Bellaso* yang ditulis pada tahun 1553. Nama Vigenere sendiri diambil dari nama Biaise de Vigenere kemudian Vigenere diambil sebagai nama algoritma ini karena beliau yang menemukan kunci tersebut yang lebih kuat lagi untuk algoritma ini dengan menggunakan metode autokey *cipher* meskipun algoritma ini dasarnya telah ditemukan lebih dahulu oleh Giovan Battista Bellaso.

Algoritma Vigenere menjadi terkenal karena sulit untuk dipecahkan. Seorang matematikawan Charles utwidge Dodgson menyatakan bahwa algoritma ini tidak dapat terpecahkan. Pada tahun 1917, ilmuan amerika juga menyebutkan bahwa Vigenere adalah suatu algoritma yang tidak mungkin dapat dipecahkan. Namun kemudian hal tersebut terbantahkan oleh Kasiski yang berhasil memecahkan algoritma Vigenere ini pada abad ke-19.

Algoritma Vigenere menggunakan bujur sangkar Vigenere yang terlihat seperti ada tabel untuk melakukan proses enkripsi. Pada bujur sangkar tersebut, kolom bagian paling kiri menyatakan huruf kunci, dan bagian baris kolom paling atas menyatakan plaintext, kemudian karakter-karakter lainnya yang menunjukkan karakter dari ciphertext. Karakter ciphertext ditentukan dengan menggunakan metode prinsip Caesar Cipher.

Tabel 1. Bujur Sangkar Vigenere

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

2.5 Algoritma AES

Dalam kriptografi, Advanced Encryption Standard (AES), juga dikenal sebagai Rijndael, AES adalah algoritma enkripsi dengan sebuah block cipher yang dijadikan standar enkripsi oleh pemerintah Amerika Serikat. Enkripsi ini diharapkan juga digunakan secara luas diseluruh dunia dan dianalisa secara luas, seperti pada pendahulunya, Data Encryption Standard (DES). Rijndael (AES) diumumkan oleh National Institute of Standards and Technology (NIST) pada tanggal 26 November 2001, setelah lima tahun proses standarisasi. Metode enkripsi ini menjadi standar secara efektif mulai tahun 2002. Pada tahun 2006, AES adalah salah satu algoritma populer yang digunakan dalam kriptografi kunci simetris.

Algoritma AES menggunakan substitusi, permutasi, dan sejumlah putaran yang dikenakan pada tiap blok yang akan dienkripsi/ dekripsi. Untuk setiap putarannya, Rijndael menggunakan kunci yang berbeda. Rijndael beroperasi dalam orientasi byte sehingga memungkinkan untuk implementasi algoritma yang efisien ke dalam *software* dan *hardware*. [8]

2.6 Chatting

Menurut Kamus Istiah Komputer, Teknologi Informasi & Komunikasi, *chat* atau *chatting* merupakan obrolan yang berbentuk tulisan secara online.

Chatting pada dasarnya bisa menggunakan beberapa jejaring social seperti *Facebook, Yahoo Massenger* maupun media *Chatting* lainnya [9].

3. ANALISIS PERMASALAHAN DAN RANCANGAN PROGRAM

3.1 Analisis Masalah

Permasalahan keamanan menjadi salah satu aspek yang sangat penting dari sebuah sistem informasi. Tapi yang sangat disayangkan, masalah kemanan kurang mendapat perhatian. Seringkali masalah keamanan menjadi urutan kedua atau bahkan urutan yang terakhir dalam daftar perancangan sebuah program. Apabila mengganggu performansi sistem, masalah kemanan Ini sering dikurangi atau bahkan ditiadakan.

Sangat pentingnya sebuah nilai informasi menyebabkan seringkali informasi diinginkan hanya boleh diakses oleh orang-orang tertentu saja. Jatuhnya informasi ke tangan pihak lain (misalnya pihak tidak dikenal) dapat menimbulkan kerugian bagi pemilik informasi dan juga perusahaan. Sebagai contoh, banyak informasi dalam sebuah perusahaan yang hanya boleh diakses oleh orang-orang tertentu di dalam perusahaan tersebut, seperti misalnya informasi tentang produk yang sedang dijual maupun yang akan, algoritma-algoritma dan teknik yang digunakan untuk menghasilkan produk tersebut, untuk itu keamanan dari sistem informasi harus terjamin dalam batas yang bisa diterima.

3.2 Penanganan Masalah

Dari permasalahan yang telah diuraikan pada analisis masalah maka, diperlukanadanya sebuah sistem yang dapat menjaga kerahasiaan sebuah informasi. Sehingga isi tersebut tidak bisa dibaca atau tidak bisa diketahui oleh pihak lain yang tidak berhak atas informasi tersebut. Aplikasi ini nantinya akan mengamankan sebuah grup chatting yang isi chat-nya tidak bisa dibaca dan tidak bisa diketahui, jika *user* tidak memasukkan password atau kunci yang benar untuk masuk mengakses grup chat tersebut. Kemudian mengembalikan isi chat tersebut menjadi seperti semula tanpa mengalami perubahan sedikitpun ketika sudah memasukkan password atau kunci dengan benar.

Pada aplikasi ini penulis menggunakan algoritma Vigenere dan AES 128 bit sebagai metode kriptografi, aplikasi ini dapat mengenkrip pesan dengan cepat dan juga aman,

sehingga masalah-masalah seperti pencurian informasi dapat diminimalisir.

3.3 Skema Proses Sistem Aplikasi

Skema proses sistem aplikasi pada aplikasi ini, pada proses chatting dimulai saat user melakukan login di aplikasi Chat UTAMA menggunakan *device* yan dimiliki *user* kemudian *user* melakukan login dengan menggunakan *user* name dan password yang dimiliki *user*. Kemudian setelah sukses login, *user* akan diarahkan ke form dashboard, kemudian user memilih topik yang sudah tersedia di dalam Form Dashboard, selanjutnya untuk memulai percakapan di dalam topik, *user* terlebih dahulu harus memasukkan password atau kunci untuk bisa mengakses atau masuk kedalam grup chat. Kunci yang dimasukkan pada saat masuk ke dalam grup chat selain berfungsi untuk masuk ke grup chat juga berfungsi untuk mendekrip pesan.

3.4 Perancangan Aplikasi

Pada aplikasi ini tampilan dibagi menjadi dua jenis, yaitu tampilan untuk admin dan tampilan untuk user. Tampilan untuk admin yaitu, tampilan Form Login, tampilan Form Menu Dashboard, tampilan Form Menu User Profile, tampilan Form Menu Tabel Referensi yang memiliki submenu tampilan Form Menu Create New User dan tampilan Form Menu Unit Organisasi. Sedangkan pada tampilan untuk user yaitu, tampilan Form Login, tampilan Form Menu Dashboard, tampilan Form Menu Create New Topic, tampilan Form Menu User Profile dan tampilan Form Chat. Untuk memulai sebuah chatting, user dapat memilih topik yang sudah tersedia pada menu Dashboard saat setelah login. Untuk bisa mengakses grup chat *user* harus memasukkan password. Jika *user* salah memasukkan password maka form chat tidak bisa diakses dan *user* akan tetap diarahkan ke tampilan PopUp Form Topic Password.

3.5 Rancangan Database MySQL

Berikut ini adalah beberapa spesifikasi *database* dalam aplikasi teks *editor* yang dibuat :

a. Tabel *AccessPass*

Nama Tabel	: accesspass
Isi	: notifikasi status akses
Organisasi	: Index Sequential
Primary Key	: idaccess

Nama *Field*	Tipe	Panjang	Deskripsi
idtopik	integer	11	Id topik
iduser	integer	11	Id user
title_topik	varchar	255	Judul topik
deskripsi	varchar	255	Deskripsi topik
iduo	integer	11	Id unit organisasi
status_topik	Enum (open, closed)	6	Status topik
createddate	Time stamp	19	Waktu topik dibuat
keypass	varchar	16	Password topik

Tabel 2. Struktur tabel *access*

b. Struktur tabel tblchat

Nama Tabel : tblchat
Isi : *Chat* dalam topik
Organisasi : *Index Sequential*
Primary Key : idchat

Nama *Field*	Tipe	Panjang	Deskripsi
iduo	integer	14	Id uo
nmuo	varchar	150	Nama uo
parentuo	integer	14	*Parent* dalam unit organisasi
deskripsi	varchar	200	Deskripsi unit organisasi

Tabel 3. Struktur tabel tblchat

c. Struktur tabel tbltopik

Nama Tabel : tbltopik
Isi : keseluruhan topik
Organisasi : *Index Sequential*
Primary Key : idtopik

Tabel 4. Struktur tabel tbltopik

Nama *Field*	Tipe	Panjang	Deskripsi
idacceess	integer	11	id access untuk bisa mengakses topik
idtopik	integer	11	id tiap topik yang dibuat super admin
iduser	integer	11	id user
tgljoin	timestamp	19	waktu bergabung di *chat*

d. Struktur tabel tbluo

Nama Tabel : tbluo
Isi : unit organisasi
Organisasi : *Index Sequential*
Primary Key : iduo

Tabel 5. Struktur tabel tbluo

Nama *Field*	Tipe	Panjang	Deskripsi
idchat	integer	11	id chat
idtopik	integer	11	id topik
iduser	integer	11	id user di *chat*
pesan	text	5000	pesan atau *chat*
dates	timestamp	19	waktu chat dibuat

e. Struktur tabel tbluser

Nama Tabel : tbluser
Isi : keseluruhan topik
Organisasi : *Index Sequential*
Primary Key : idtopik

Tabel 6. Struktur tabel tbluser

Nama *Field*	Tipe	Panjang	Deskripsi
iduser	Integer	11	Id user
nmuser	Varchar	100	Nama user
passwords	Varchar	255	Kata sandi
iduo	Integer	11	Id unit organisasi
idgrup	Integer	11	Id grup
email	Varchar	255	Email *user*
notelp	Varchar	20	Nomor telepon *user*
profpict	Varchar	255	Foto *user*
jointdate	Time stamp	19	Waktu bergabung sebagai *user*

3.6 Rancangan Layar

Agar suatu aplikasi mudah digunakan, maka diperlukan tampilan yang dapat mudah dimengerti oleh *user*. Berikut ini adalah rancangan layar untuk Aplikasi :

a. Rancangan Layar *Form Login*

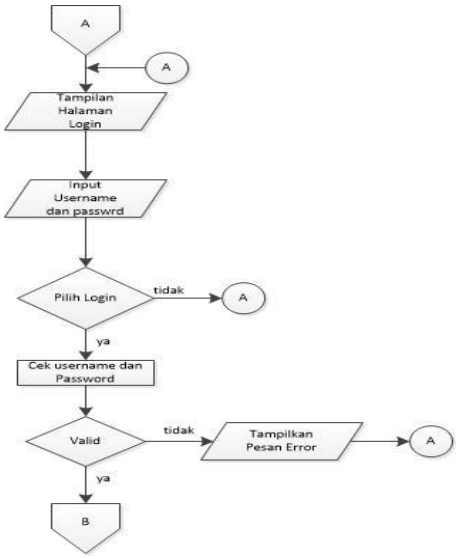
Fungsi Form Login yaitu, agar *user* dapat masuk(login) atau menggunakan aplikasi ini. Untuk login, *user* terlebih dahulu harus

memasukkan *user name* dan *password*, seperti pada gambar berikut

Gambar 1. Rancangan layar Form Login

b. Flowchart login

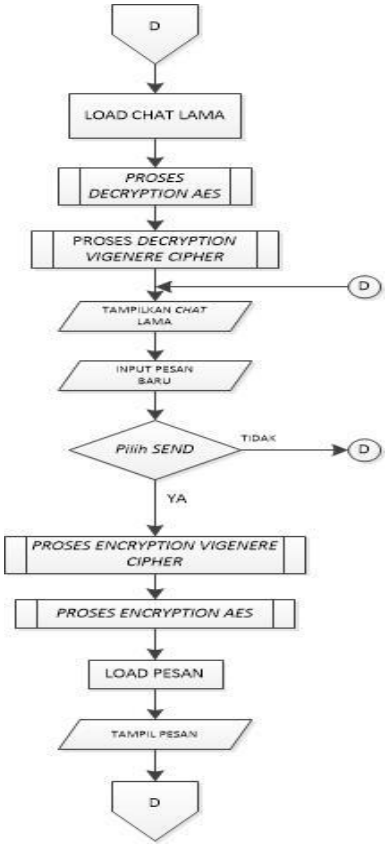
Pada *flowchart* yang menggambarkan proses *login*



Gambar 2. Flowchart Login

c. Flowchart form chat

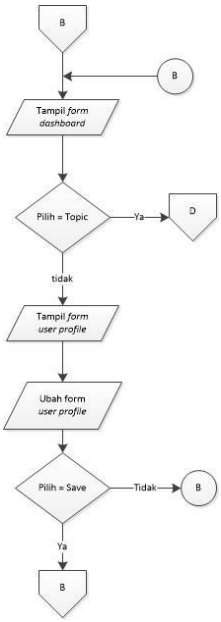
Flowchart Form chat pada gambar 3.16 berikut ini adalah alur untuk proses *chatting*.



Gambar 3. Flowchart Chat

d. Flowchart Dashboard User

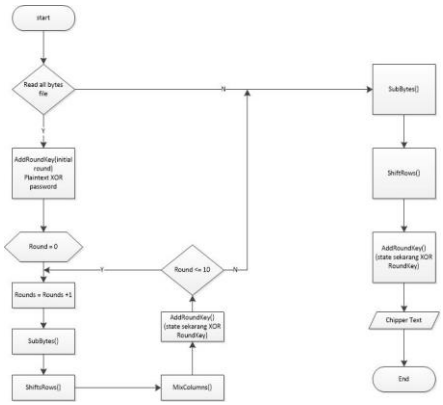
Pada *Flowchart Form Dashboard* ini akan menjelaskan proses *user* memiih topik dan jika user salah memasukkan *password* saat berada di *PopUp Form Password Topic*, secara otomatis *user* akan diarahkan ke *PopUp Form Password Topic* kembali.



Gambar 4. Flowchart Dashboard User

e. *Flowchart Enkripsi AES*

Flowchart dibawah ini menjelaskan alur proses dari algoritma AES 128 mulai dari proses AddRoundKey, SubBytes, ShiftRows, dan MixColumns, sehingga nantinya terbentuk file chipper dari dokumen yang dienkripsi.



Gambar 5. Proses Enkripsi AES

3.7 Pembahasan Algoritma

Beberapa urutan-urutan proses yang harus di lalui digambarkan dalam bentuk algoritma. Algoritma dari setiap proses pada sebuah aplikasi akan dibahas pada penjelasan sebagai berikut.

a. Algoritma *login*

Algoritma Form Login menjelaskan tentang awal mula *user* menggunakan aplikasi ini, sebelum menggunakan aplikasi ini *user* terlebih dahulu harus mengisi Form Login agar dapat masuk ke menu dashboard dan dapat menggunakan.

1. Tampilkan *Form Login*
2. Input *User Name*, *Password*
3. Cek *User Name* dan *Password*
4. If *User Name* dan *Password == TRUE* then
5. Tampilkan Menu *Dashboard*
6. Else
7. Kembali ke baris 1
8. End if

b. Algoritma *Create New Topic*

Algoritma Form Menu Create New Topic menjelaskan proses *user* membuat topik baru dan setelah selesai akan diarahkan ke PopUp Form Topic Password.

1. Tampilkan *Form Create New Topic*
2. *Input Tittle Topic*, Deskripsi, ID *User* dan *Password*
3. Cek *Tittle Topic*, Deskripsi, ID *User* dan *Password*
4. If *Tittle Topic*, Deskripsi, ID *User* dan *Password* kosong then
5. Tampilkan Pesan *Alert*
6. Else If Password <= 24 then
7. Tampilkan *PopUp Form Topic Password*
8. Else
9. Kembali ke baris 1
10. End if

c. Algoritma *pop up form topic*

Algoritma *PopUp Form Topic Password* menjelaskan proses *input password* untuk mengakses halaman atau *Form Chatting.*

1. Tampilkan *PopUp Form Topic Password*
2. *Input Password*
3. If *Password == TRUE* then
4. Tampilkan *Form Chatting*
5. Else
6. Kembali ke baris 1
7. End if

d. Algoritma *Form Chat*

Algoritma ini menjelaskan proses *Form Chat*. Proses dari *user input* pesan *text* sampai proses enkripsi pesan.

1. Tampilkan *Form Chat*
2. *Load Chat* Lama
3. Proses Dekripsi AES 128
4. Proses Dekripsi Vigenere
5. Tampilkan *Chat* Lama
6. *Input* Pesan Baru
7. If *pilih Send == TRUE* then
8. Proses Enkripsi Pesan dengan Vigenere
9. Proses Enkripsi Pesan dengan AES 128
10. Else
11. Kembali kebaris 5
12. End if

4. HASIL DAN PEMBAHASAN

Aplikasi kriptografi dengan menggunakan algoritma Vigenere dan AES 128dapat diimplementasikan dengan baik. Chat hanya berupa pesan text. Hal ini dilakukan agar user tidak terlalu lama saat proses pengiriman pesan maupun menerima pesan. Setelah dilakukan analisis dari hasil pengujian aplikasi, akan dijelaskan tentang hasil evaluasi, kelebihan dan kekurangan dari aplikasi ini, yakni :

a. Kelebihan Aplikasi

(1) *User* dapat menggunakan aplikasi dengan mudah karena *user interface* dirancang *user friendly*.
(2) Pesan dan informasi pada topik dalam aplikasi akan aman karena sudah dienkripsi.
(3) Pesan dari hasil enkripsi, tidak mengalami perubahan sedikitpun dan dapat dibaca kembali setelah didekripsi.

b. Kekurangan Aplikasi

(1) Pesan yang bisa dikirim hanya berupa pesan text saja.
(2) Aplikasi yang dijalankan hanya berbasis web *browser* dan masih digunakan di *local* saja belum bisa digunakan pada untuk publik.

5. KESIMPULAN

Berdasarkan permasalahan dan cara untuk menyelesaikannya pada bahasan sebelumnya, dapat disimpulkan bahwa program aplikasi pengaman chatting menggunakan algoritma Vigenere dan AES 128 sangat diperlukan karena :

(1) Aplikasi yang mengimplementasikan algoritma kriptografi Vigenere dan AES 128 telah berhasil diimplementasikan untuk enkripsi dan dekripsi chatting.
(2) Dengan adanya aplikasi ini maka chatting yang dianggap penting dapat terjaga kerahasiaannya dari siapapun.
(3) Menggunakan aplikasi chatting yang dibangun sendiri untuk kebutuhan bertukar informasi dalam institusi lebih aman dan lebih mudah diperbaiki jika ada permasalahan.

DAFTAR PUSTAKA

[1] Abimanyu, Adi, Nurhidayat dan Jumari., 2013. "Implementasi Algoritma Vigenere MenggunakanMikrokontroler untuk Pengiriman SMS pada Sistem Pemantau Pengangkutan Zat Radioaktif", Prosiding seminar Penelitian dan Pengelolaan Perangkat Nuklir, ISSN 1410-8178 Pusat Teknologi Akselerator dan Proses Bahan, Yogyakarta.

[2] Arrijal, Irham Mu'alimin, Efendi, Rusdi dan Susilo, Boko., 2016. "Penerapan Algoritma Kriptografi Kunci Simetris dengan Modifikasi Vigenere Cipher dalam AplikasiKriptografi Teks", Jurnal Pseudocode, Volume III Nomor 1, ISSN 2355-5920 Universitas Bengkulu, Bengkulu.

[3] Ariyus, Dony, 2008. "Pengantar Ilmu Kriptografi : Teori Analisis dan Implementasi", Yogyakarta : ANDI.

[4] Budiarto, B., Raden, 2010. "Analisis Penyimpanan File Online dengan Enkripsi menggunakan Algoritma *AES* Rijndael", (Juni 2010).

[5] Endriani, N., 2014. "Implementasi algoritma enkripsi AES pada aplikasi *SMS (Short Message Service)* berbasis android", Amikom : Yogyakarta.

[6] Haryanto, H., Wiryadinata R dan Afif M. 2014. "Implementasi Kombinasi Algoritma Enkripsi AES 128 Dan Algoritma Kompresi Shannon-Fano", (Juni 2014), vol. 3

[7] Marvin Chandra Wijaya, Semuil Tjiharjadi, "Mencari Nilai Threshold Yang Tepat Untuk Perancangan Pendeteksi Kanker Trofoblas," Seminar Nasional Aplikasi Teknologi Informasi 2009, 2009.

[8] Munir, R., "Bahan Kuliah IF5054 Kriptografi", Departemen Teknik Informatika, Institut Teknologi Bandung 2004.

[9] Nasution, Helfi, Prihartini, Narti, "Pengembangan Media Chatting Online Dengan Fitur Alih Bahasa Melalui Pendekatan Metode Rule Based Dalam Proses Penerjemahan Chat" Jurnal Informatika Mulawarman, vol. 7, No. 3, September 2012, 2012

[10] Pradipta, Gede Angga., 2016. "Penerapan Kombinasi Metode Enkripsi Vigenere Chiper Dan Transposisi Pada Aplikasai Client Server Chatting", Jurnal Sistem dan Informatika,Vol. 10 No. 2/ Mei 2016, ISSN 130662, STIKOM BALI, Denpasar.

[11] Permana, Aditya, Santoso, Edy, dan Ratnawati, Dian Eka.2013. "Kriptografipada File Dokumen Microsoft Office Menggunakan Metode RSA".Jurnal Mahasiswa PTIIK UB Vol 2 No. 1 2013

[12] Sadikin, Rifki., 2012. "Kriptografi Untuk Keamanan Jaringan", Yogyakarta, Penerbit ANDI.

[13] Suryanto, Indra, Suheri, Cucu & Brianorman, Yulrio., 2017. "Pengembangan Aplikasi Chat Messenger Dengan Metode Advanced Encryption Standard (Aes) Pada Smartphone", Jurnal Coding Sistem Komputer Untan, Volume 5, Nomor 2,

ISSN 2338-493X Universitas Tanjungpura, Pontianak.

[14] Yulianingsih, Pricilia, Hamdani, Septya Maharani., 2014. "Aplikasi Chatting Rahasia Menggunakan Algoritma Vigenere Chiper, Jurnal Informatika Mulawarman", Vol. 9 No. 1/ Februari 2014, ISSN 1858-4853, Universitas Mulawarman, Samarinda.

[15] Yuniati, V, Indriyanta, G, Rachmat, C 2013, "ENKRIPSI DAN DEKRIPSI DENGAN ALGORITMA AES 128 UNTUK SEMUA JENIS FILE" Jurnal Yogyakarta : Fakultas Teknik Informatika Universitas Kristen Duta Wacana.

[16] Kurniawan, Nyoto, & Sanjaya ,Ridwan 2010, "Website Praktis dengan Google Sites". Jakarta : PT Elex Media Komputindo, dilihat pada 19 November 2016,