MEDIA PEMBELAJARAN INTERAKTIF ENKRIPSI *CAESAR CIPHER*, *VIGENERE CIPHER*, DAN ALGORITMA RSA

Interactive Learning Media of Caesar Cipher, Vigenere Cipher, and RSA Algorithm Encryption

Wina Ayu Lestari[1], Rohmat Tulloh, S.T., M.T.[2], Atik Novianti, S.ST.,M.T.[3]

[1,2,3]Prodi D3 Teknik Telekomunikasi, Fakultas Ilmu Terapan, Telkom University

[1]lestariwinaayu@gmail.com, [2] rohmatulloh@tass.telkomuniversity.ac.id, [3]atiknovianti@tass.telkomuniversity.ac.id

Abstrak

Salah satu contoh penyalahgunaan teknologi adalah pencurian data atau informasi oleh pihak yang tidak diizinkan. Maka dari itu, terciptalah metode enkripsi untuk melindungi informasi tesebut. Enkripsi dibagi menjadi beberapa metode diantaranya adalah Caesar Cipher, Vigenere Cipher, dan algoritma RSA. Pentingnya enkripsi harus diketahui oleh pengguna internet.

Enkripsi memiliki perhitungan yang rumit sehingga tidak semua orang bisa memahaminya dengan baik termasuk bagi mahasiswa D3 Teknik Telekomunikasi di Universitas Telkom yang mengambil mata kuliah Keamanan Jaringan. Berdasarkan kuesioner yang telah disebarkan, sebanyak 80% responden kesulitan untuk mempelajari metode Caesar Cipher, Vigenere Cipher, dan algoritma RSA yang berkaitan dengan kelengkapan materi, sumber materi hingga teknik penjelasannya. Maka pada Proyek Akhir ini dibuat media pembelajaran interaktif mengenai algoritma Caesar Cipher, Vigenere Cipher dan RSA menggunakan *software* Adobe Flash Professional CS6 dan MATLAB R2017a. Didalamnya memuat materi, video penjelasan, beberapa latihan soal hingga aplikasi konverter. Hasil dibuatnya media pembelajaran ini adalah meningkatkan pemahaman pada setiap pelajar serta meningkatkan motivasi dan keinginan belajar pada materi enkripsi khususnya algoritma Caesar Cipher, Vigenere Cipher dan RSA.

Media pembelajaran yang telah dibuat dari hasil pengujian yang dilakukan menunjukan pada pengujian fungsionalitas dimana semua fungsi berjalan 100% sebagaimana mestinya. Berdasarkan kuisioner, tampilan dari media pembelajaran mendapatkan nilai rata-rata sebesar 4.36 dari skala 1-5 yang artinya tampilan pada media pembelajaran tergolong baik.

kata kunci : media pembelajaran interaktif, Caesar Cipher, Vigenere Cipher, Algoritma RSA, MATLAB R2017a.

Abstract

One example of misuse of technology is theft of data or information by unauthorized parties. Therefore, it creates an encryption method to protect the information. Encryption is divided into several methods including Caesar Cipher, Vigenere Cipher, and RSA algorithm. The importance of encryption must be known by internet users.

Encryption has complex calculations so that not everyone can understand it well, including for D3 Telecommunications Engineering students at Telkom University who take Network Security courses. Based on the questionnaire that was distributed, as many as 80% of respondents had difficulty learning the Caesar Cipher method, Vigenere Cipher, and RSA algorithm related to the completeness of the material, the source of the material to the explanation technique. So in this Final Project an interactive learning media was created regarding the Caesar Cipher, Vigenere Cipher and RSA algorithm using Adobe Flash Professional CS6 and MATLAB R2017a *software*. It contains material, explanatory videos, some practice questions to the converter application. The result of this learning media is to increase the understanding of each student as well as increase motivation and desire to learn on encryption materials, especially the Caesar Cipher algorithm, Vigenere Cipher and RSA.

Learning media that have been made from the results of tests carried out show the functionality testing where all functions run 100% as they should. Based on the questionnaire, the display of the learning media got an average value of 4.36 from a scale of 1-5, which means the display on the learning media was good.

keywords: interactive learning media, Caesar Cipher, Vigenere Cipher, RSA Algorithm, MATLAB R2017a.

1. Pendahuluan

Sejalan dengan perkembangan internet yang memberikan banyak keuntungan, kemudahan, dan manfaat bagi masyarakat luas, tidak menutup kemungkinan adanya resiko atau ancaman dan aspek negatif lainnya yang ikut terbawa akibat dari penyalahgunaan internet[1].

Untuk meminimalkan hal-hal tersebut, maka para ilmuan dan ahli komputer menemukan cara agar informasi tidak bisa dibaca atau diambil oleh pihak yang tidak diizinkan dengan menggunakan enkripsi. Enkripsi ini bisa dipelajari oleh semua kalangan termasuk mahasiswa. Namun didalam dunia pendidikan, enkripsi kurang diminati oleh mahasiswa karena perhitungannya yang rumit sehingga susah dipahami[2] termasuk bagi mahasiswa D3 Teknik Telekomunikasi di Telkom University yang mengambil mata kuliah Keamanan Jaringan.

Dari hasil kuisioner yang telah disebar, didapatkan hasil sebagai berikut. Berdasarkan kuisioner, 80% dari 20 responden merasa kesulitan untuk mempelajari materi enkripsi khususnya pada materi Caesar Cipher, Vigenere Cipher, dan Algoritma RSA dengan menggunakan metode pembelajaran diskusi dan presentasi. Sebanyak 85% membutuhkan metode pembelajaran yang digunakan lebih menarik agar mudah dipahami, karena responden mengalami kesulitan dalam mempelajari materi berkaitan dengan kelengkapan materi, sumber materi hingga teknik penjelasannya.

Sehingga untuk memenuhi kebutuhan mahasiswa dibuatlah suatu media pembelajaran interaktif mengenai enkripsi agar meningkatkan pemahaman. Dimana didalamnya dijelaskan tentang kriptografi caesar chipper dan vigenere chipper serta algoritma RSA menggunakan *software* Adobe Flash Professional CS6. Sebelumnya, pada jurnal "An RGB Image Encryption using RSA Algorithm" dari Samson Chepuri[3] menjelaskan bahwa proses enkripsi-dekripsi dilakuan hanya dengan merubah warna gambar. Sedangkan, pada proposal ini penulis membuat suatu teks yang tersimpan dalam gambar. Dibuatnya media pembelajaran ini, bisa mempermudah proses belajar tentang materi enkripsi, menigkatkan pemahaman tentang pentingnya enkripsi dalam keamanan jaringan.

Dasar Teori

2.1 Mata Kuliah Keamanan Jaringan

Mata kuliah keamanan jaringan adalah mata kuliah wajib pada program D3 Teknologi Telekomunikasi pada tahun ajaran 2018/2019 yang memiliki 3 sks dengan nilai kelulusan minimal C. Mata kuliah keamanan jaringan sangat penting bagi mahasiswa untuk memahami aspek dari keamanan jaringan hingga klasifikasi kejahatan komputer. Dalam mata kuliah inipun diajarkan tentang bagaimana suatu data atau informasi memiliki kesempatan kebocoran data. Mata kuliah keamanan jaringan memiliki banyak materi menarik yang sangat menantang, karena memiliki teori yang membutuhkan penjelasan secara rinci juga banyak menggunakan bahasa pemograman. Sehingga mahasiswa dituntut untuk membaca dan memahami materi sehingga saat dikelas diharapkan mahasiswa hanya mempelajari atau memahami materi yang penting saja, selebihnya bisa dipelajari dari bahan-bahan pustaka. Namun walaupun membutuhkan penjelasan secara rinci, mata kuliah keamanan jaringan memiliki inovasi untuk meningkatkan pemahaman mahasiswa dengan memberikan simulasi dan latihan soal pada setiap topik-topik materi yang disampaikan, misal pada topik materi enkripsi dengan tujuan mahasiswa memiliki ketepatan dalam proses enkripsi yang menggunakan jenis enkripsi kriptografi (Caesar Cipher, Vigenere Cipher, dan algoritma RSA) dengan inovasi membuat latihan soal pada Adobe Flash CS6 dan converter pada Matlab.

2.2 Keamanan Jaringan

Keamanan jarigan digunakan untuk membantu mengamankan jaringan tanpa menghalangi penggunanya dan menempatkan antisipasi ketika jaringan berhasil ditembus. Selain itu, keamanan jaringan memasitikan bahwa pengguna memiliki pengetahuan yang cukup mengenai keamanan dan memastikan pengguna menerima dan memahami rencara keamanan yang telah dibuat[4]. Keamanan jaringan dapat di definisikan sebagain 5 poin dibawah ini:

1. *Confidentiality* : Informasi (data) hanya bisa diakses oleh pihak yang berwenang.
2. *Integrity* : Informasi (data) hanya bisa diubah oleh pihak yang berwenang.
3. *Availability* : Informasi (data) hanya tersedia pada pihak yang berwenang.
4. *Authentication* : Pengirim suatu informasi dapat diidentifikasi dengan benar dan ada jaminan bahwa identitas yang didapatkan tidak palsu.
5. *Nonrepudiation* : Pengirim atau penerima informasi tidak dapat menyangkal pengiriman dan penerimaan palsu.

2.3 Keamanan Jaringanr

Kriptografi adalah metode yang memungkinkan informasi dikirim dalam bentuk yang aman sehingga satu-satunya orang yang dapat mengambil informasi ini adalah penerima yang dituju[4].

Berikut adalah tujuan layanan keamanan kriptografi[5]:

a. Kerahasiaan (*Confidentiality*)
   Informasi dirahasiakan dari semua pihak yang tidak berwenang.
b. Keutuhan Data (*Integrity*)
   Pesan tidak berubah dalam proses pengiriman hingga pesan diterima oleh si penerima.
c. Autentikasi (*Message Autentication*)
   Kepastian terhadap identitas yang terlibat dan keaslian sumber data.
d. Ketersediaan (*Avaibility*)
   Layanan dimana user mempunyai hak untuk diberi akses tempat waktu dan tidak terkendala apapun.
e. Nirpenyangkalan (*Nonrepudiation*)
   Semua pihak yang berkomunikasi tidak dapat menolak atau menyangkal atas data yang telah dikirim atau diterima.

2.3.1 Istilah dalam Bidang Kriptografi

a. *Plaintext* (M) = Pesan yang hendak dikirimkan (data asli) yang dapat dimengerti.
b. *Ciphertext* (C) = Pesan ter-enkrip (tersandi) / hasil enkripsi.
c. Enkripsi (E) = Proses pengubahan plaintext menjadi chipertext.
d. Dekripsi (D) = Mengubah ciphertext menjadi plaintext (data asli).
e. Kunci (K) = Suatu bilangan yang dirahasiakan untuk digunakan dalam proses enkripsi dan dekripsi.

2.4 *Caesar Cipher*

Menurut Turyadi dalam makalah dengan judul "Enkripsi dan Dekripsi menggunakan Metode Caesar Cipher dan Operasi XOR" Caesar Cipher memiliki langkah – langkah sebagai berikut[6]:

1. Menghitung panjang karakter / huruf yang diinputkan dalam plaintext.
2. Tiap huruf diubah menjadi kode ASCII menggunakan proses looping.
3. Untuk melakukan pergeseran / proses enkripsi maka kode ASCII tersebut digeser dengan cara ditambah sebanyak pergeseran. Misalnya, pergeseran 5 huruf maka kode ASCII ditambah dengan 5.
4. Jika ditemukan spasi (ASCII=31), maka tidak usah dilakukan penambahan.
5. Hasil pergeseran bilangan ASCII dikembalikan lagi menjadi huruf / karakter.

2.5 *Vigenere Cipher*

Vigenere Cipher merupakan salah satu kriptografi klasik yang dikenalkan pada abad 16 atau sekitar tahun 1986. Cara kerja Vigenere Cipher mirip dengan Caesar Cipher yaitu mengenkripsi plaintext pada pesan dengan cara menggeser huruf pada pesan tersebut sejauh nilai kunci pada deret alfabet[2]. Kunci yang berbentuk deretan kata tersebut akan memungkinkan setiap huruf plaintext untuk di enkripsi dengan kunci yang berbeda. Jika panjang kunci yang digunakan lebih pendek dari panjang plaintext maka kunci akan diulang sampai panjang kunci sama dengan panjang plaintext. Berikut adalah algoritma Vigenere Cipher dengan A=0; B=1; C=2; D=3; E=4; F=5; G=6; H=7; I=8; J=9; K=10; L=11; M=12; N=13; O=14; P=15; Q=16; R=17; S=18; T=19; U=20; V=21; W=22; X=23; Y=24; Z=25.

$$C = E (M) = (M + K) \bmod 26 \text{ (enkrispi)}$$

$$M = D (C) = (C – K) \bmod 26 \text{ (dekripsi).}$$

2.6 Algoritma RSA

Algoritma RSA dibuat oleh 3 (tiga) orang peneliti dari MIT (Massachusset Institute of Technology) pada tahun 1976 yaitu Ron Riverst, Adi Shamir, dan Leonard Adleman. Algoritma RSA juga merupakan kriptografi kunci umum yang paling popular dikarenakan algoritma ini melakukan pemfaktoran bilangan yang sangat besar sehingga dianggap paling aman (Al Azad 2012)[7][4]. Algoritma RSA adalah salah satu kriptografi asimetris yang memiliki kunci publik dan kunci privat[8].

Beberapa hal yang harus dilakukan untuk melakukan enkripsi menggunakan algoritma RSA, yaitu:

1. Nilai p dan q merupakan bilangan prima. Dengan syarat p > q dan q > 1
2. Nilai n = p.q
3. Nilai m = (p-1)(q-1)
4. Nilai e adalah kunci publik untuk enkripsi dimana nilai e harus relatif prima terhadap nilai m.
5. Nilai d merupakan kunci privat untuk dekripsi dimana nilai didapat dari persamaan invers e mod n atau e.d = 1 k(m).

2.7 Steganografi

Steganografi yaitu seni penyembunyian pesan ke dalam pesan lainnya sedemikian rupa sehingga orang lain tidak menyadari ada sesuatu didalam pesan tersebut. Biasanya, pengaplikasian steganografi terdapat pada media gambar. Metode tersebut akan menyamarkan pesan teks pada file gambar yang dikirimkan, sehingga pengirim dapat dengan nyaman mengirim pesan rahasia[2][9].

2.8 *Adobe Flash Professional CS6*

"Adobe Flash adalah program animasi yang mendukung pemograman dengan action script-nya, sangat cocok untuk dikembangkan pada pembelajaran interaktif karena mendukung animasi, gambar, teks dan pemograman." (Nurtianto dan Syarif, 2013)[10]. Pada proyek akhir ini, Sofware Flash digunakan sebagai tempat pembuatan media pembelajaran secara keseluruhan.

2.9 *Storyboard*

Storyboard adalah gambar sketsa sebagai alat perencanaan untuk menunjukkan secara visual aksi dari sebuah cerita atau naskah yang berbentuk gambar untuk memudahkan cameraman dalam pengambilan gambar[11]. Keuntungan dari storyboard yaitu memicu reaksi dan ketertarikan pembaca pada suatu cerita. Pembuat storyboard harus bisa membuat sebuah cerita yang menarik. Dengan cara mengetahui berbagai film, mengetahui pengertian tampilan yang bagus, komposisi, gambaran berurut dan editing[12]. Storyboard digunakan untuk merancang alur media pembelajaran yang akan dibuat sehingga mudah untuk dimengerti saat proses pengeditan.

2.10 *Adobe Photoshop* dan *CorelDraw*

Adobe Photoshop adalah *software* yang sering digunakan untuk mengedit *image*/gambar karena memiliki fasilitas yang lengkap. Baik itu berupa tools untuk mengedit gambar hingga memberi filter pada gambar dengan kualitas terbaik[10]. *Corel Draw* memiliki fungsi untuk mengolah dan mengedit gambar, oleh karena itu banyak orang yang menggunakan untuk menunjang pekerjaan dalam bidang publikasi, percetakan ataupun pekerjaan di bidang lain yang membutuhkan proses visualisasi[13][14]. Kedua *software* ini digunakan untuk membantu proses edit gambar yang dibutuhkan *Adobe Flash*.

2.11 Wondershare Filmora

Software Filmora adalah *software* editing video sederhara namun sangat profesional. Sangat cocok digunakan bagi pemula yang ingin mencoba membuat sebuah karya. Filmora digunakan untuk membuat video pembelajaran yang akan disisipkan pada media pembelajaran[15].

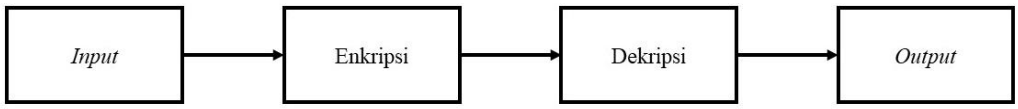
2.12 MATLAB R2017A

Matlab adalah sebuah software pemrograman untuk analisa matrix, desain kontrol, identifikasi sistem dan teknik penggambaran grafik[16]. Matlab merupakan singkatan dari Matrix Laboratory. Matlab mampu mengintegrasikan komputasi, visualisasi, dan pemrograman untuk dapat digunakan secara mudah[17]. Penggunaan Matlab diantranya adalah (Wahid, 2010)[18]:

1. Matematika dan komputasi.
2. Pengembangan algoritma.
3. Pemodelan, simulasi, dan *prototype*.
4. Pengolahan grafik untuk sains dan teknik.
5. Pengembangan aplikasi berbasis GUI (Graphical User Interface)

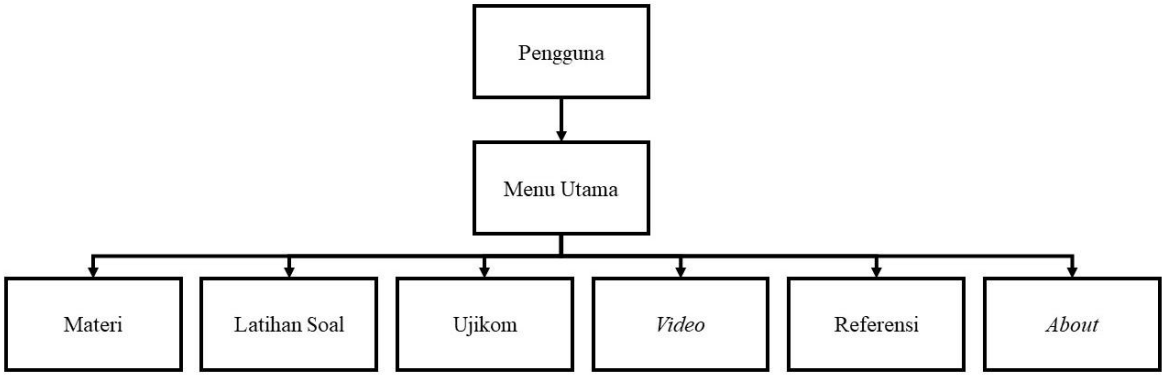
2. Perancangan Sistem

3.1 Blok Diagram Sistem



Gambar 3. 1 Blok Diagram Sistem Konverter

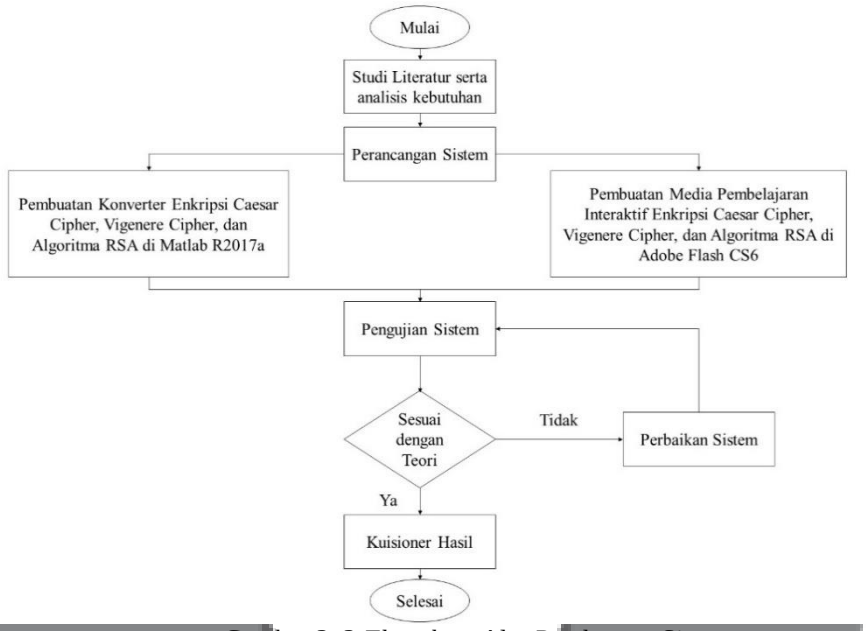
Berdasarkan blok diagram tersebut, data yang diinputkan secara manual pada konverter merupakan sebuah *plain text*. Kemudian plain text tersebut akan dienkripsi menjadi sebuat *cipher text* menggunakan suatu algoritma yang digunakan pada jenis enkripsi tersebut. Selanjutnya *cipher text* akan didekripsi menggunakan proses yang sama hingga menghasilkan *plain text* awal sebagai *output* nya.



Gambar 3. 2 Blok Diagram Sistem Media Pembelajaran Interaktif

Berdasarkan Gambar 3.2, saat pengguna menggunakan media pembelajaran interaktif disuguhkan Menu Utama. Jika pengguna menekan tombol Menu Utama maka beberapa submenu. Submenu tersebut adalah Materi, Latihan Soal, Ujikom, *Video*, Referensi, dan *About*.

3.2 Flow Chart Sistem



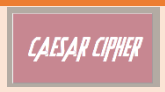
Gambar 3. 3 *Flowchart* Alur Pembuatan Sistem

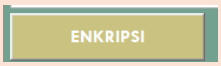
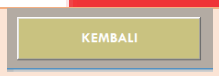
Gambar 3.3 adalah flowchart alur pembuatan sistem. Dimulai dari menganalisis kebutuhan yang sesuai dengan metode pembelajaran enkripsi Caesar Cipher, Vigenere Cipher, dan algoritma RSA sesuai dengan mata kuliah keamanan jaringan. Lalu pada tahap selanjutnya, membuat sistem media pembelajaran interaktif pada software Adobe Flash Professional CS6 dan MATLAB R2017a untuk membuat konverter enkripsinya. Tahap berikutnya, pengujian dilakukan untuk mengetahui hasil yang sudah sesuai atau belum dengan materi teoritisnya. Apabila terdapat perbedaan maka dilakukan perbaikan sistem ulang. Sedangkan apabila sudah sesuai dengan materi teoritisnya dilakukan hasil untuk melakukan pengujian tingkat pemahaman kepada mahasiswa/i. Dengan cara membandingkan hasil nilai sebelum dan sesudah melakukan simulasi untuk membantu pembelajaran.

4. Pengujian Sistem

4.1 Pengujian Fungsionalitas

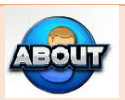
Tabel 4. 1 Pengujian Fungsi Button pada Konverter Enkripsi

NO	GAMBAR	NAMA *BUTTON*	FUNGSI	BERFUNGSI
1		*Caesar Cipher*	Membuka menu *Caesar Cipher*	Sesuai
2		*Vigenere Cipher*	Membuka menu *Vigenere Cipher*	Sesuai

NO	GAMBAR	NAMA *BUTTON*	FUNGSI	BERFUNGSI
3		Algoritma RSA	Membuka menu algoritma RSA	Sesuai
4		Steganografi	Membuka menu steganografi	Sesuai
5		Enkripsi	Memproses perhitungan setiap metode enkripsi	Sesuai
6		Dekripsi	Memproses perhitungan setiap metode dekripsi	Sesuai
7		Kembali	Kembali ke menu utama	Sesuai
8		Reset	Kembali ke reset semula	Sesuai

Tabel 4. 2 Pengujian Fungsi Button pada Media Pembelajaran Interaktif

NO	GAMBAR	NAMA *BUTTON*	FUNGSI	BERFUNGSI
1		*Close*	Menutup media pembelajaran	Sesuai
2		*Log-in*	Masuk untuk ke halaman menu utama	Sesuai
3		*Home*	Kembali ke halaman awal	Sesuai
4		Materi	Menampilkan sub menu *Caesar Cipher*, *Vigenere Cipher*, algoritma RSA	Sesuai
5		Latihan Soal dan Ujikom	Menampilkan halaman untuk latihan soal	Sesuai
6		Konverter	Membuka menu konverter yang ada di MATLAB R2017a	Sesuai
7		Referensi	Menampilkan beberapa referensi yang menjadi acuan dalam pembuatan media pembelajaran	Sesuai
8		Kembali	Mengembalikan ke halaman awal	Sesuai
9		Menu Kriptografi dan Steganografi	Menampilkan materi dan latihan soal mengenai kriptografi dan steganografi	Sesuai

NO	GAMBAR	NAMA *BUTTON*	FUNGSI	BERFUNGSI
10		Menu RSA	Menampilkan materi dan latihan soal mengenai Algoritma RSA	Sesuai
11		Menu *Caesar Cipher*	Menampilkan materi dan latihan soal mengenai *Caesar Cipher*	Sesuai
12		Menu *Vigenere Cipher*	Menampilkan materi dan latihan soal mengenai *Vigenere Cipher*	Sesuai
13		*Back*	Kembali ke halaman sebelumnya	Sesuai
14		*Next*	Menampilkan halaman selanjutnya	Sesuai
15		*About*	Menampilkan informasi tentang penulis	Sesuai

Dari hasil Tabel 4.1 dan Tabel 4.2 dengan demikian dapat disimpulkan fungsionalitas proyek akhir ini berjalan sesuai harapan untuk menjalankan sistem.

4.2 Pengujian Akurasi Perhitungan

Pada pengujian ini dimaksudkan untuk membuktikan jawaban yang dihasilkan konventer sesuai dengan jawaban menggunakan rumus atau algoritma yang digunakan.

a. *Caesar Cipher*

(Contoh ke 1)

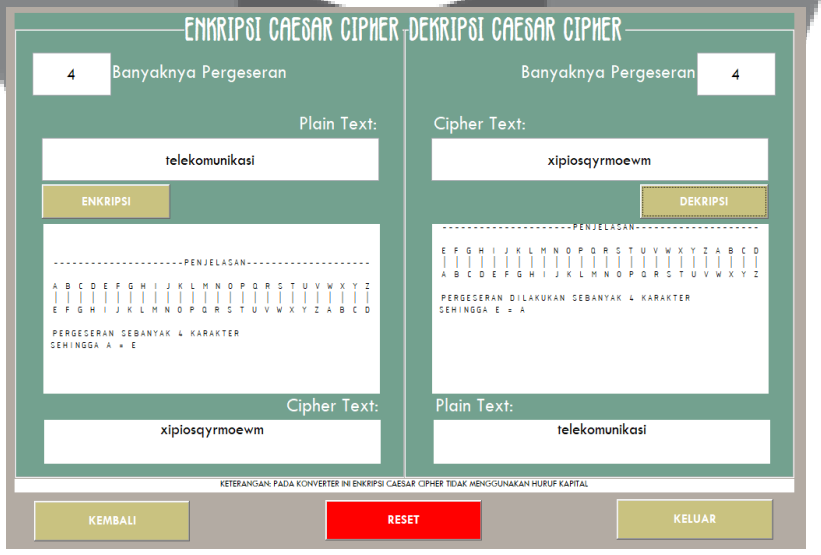
Diketahui :

Plain Text = selamat datang

Banyaknya pergeseran = 5

Cipher Text = xjqfrfy ifyfsl

Berikut adalah hasil dari konverter yang dibuat menggunakan MATLAB R2017a.



Gambar 4. 1 Hasil Enkripsi dan Dekripsi *Caesar Cipher* menggunakan Konverter

Berdasarkan Gambar 4.1, dijelaskan bahwa pengguna menginput banyaknya pergeseran sebanyak 4 karakter dengan *plain text* “telekomunikasi” yang memiliki hasil atau *Cipher Text* “xipiosqyrmoewm”. Selanjutnya, hasil enkripsi dan dekripsi melalui perhitungan/pergeseran menggunakan tabel.

Tabel 4. 1 Perhitungan *Caesar Cipher* secara manual

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
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

t=x; e=i; l=p; e=i; k=o; o=s; m=q; u=y; n=r; i=n; k=o; a=e; s=w; i=m

Cipher Text = xipiosqyrnoewm

Pergeseran karakter dilakukan seperti pada Tabel 4.3 dimana a = e karena pergeseran sebanyak 4 karakter. Dari jawaban yang dihasilkan antara konverter dengan perhitungan manual memiliki hasil yang sama.

b. *Vigenere Cipher*

(Contoh ke 3)

Diketahui :

Plain Text = VIGENERE

Key = CIPHER

Cipher Text = XQVLRVTM

Berikut adalah hasil dari konverter yang dibuat menggunakan MATLAB R2017a.

Gambar 4. 2 Hasil Enkripsi dan Dekripsi *Vigenere Cipher* menggunakan Konverter

Pada Gambar 4.2, pengguna menggunakan *plain text* “VIGENERE” dan kata kunci “CIPHER” dengan hasil atau *Cipher Text* “XQVLRVTM”. Selanjutnya, hasil enkripsi dan dekripsi melalui perhitungan menggunakan tabel.

Tabel 4. 2 Perhitungan *Vigenere Cipher* secara Manual

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
0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25

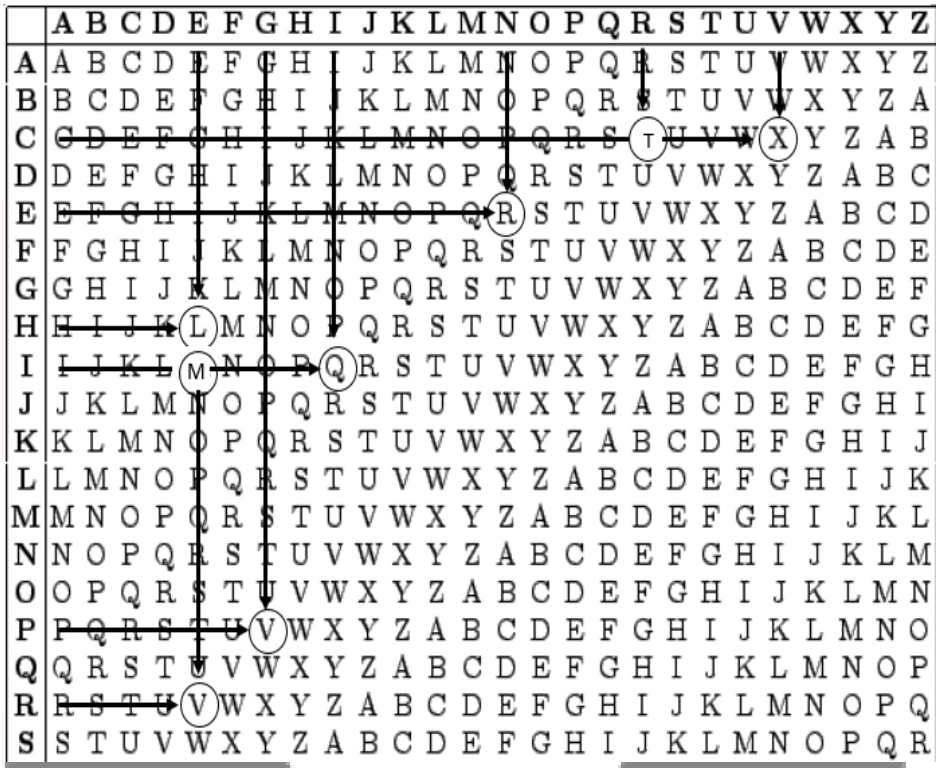
V	I	G	E	N	E	R	E
C	I	P	H	E	R	C	I

21	8	6	4	13	4	17	4
2	8	15	7	4	17	2	8

Mod 26

23	16	21	11	17	21	19	12
X	Q	V	L	R	V	T	M

Cipher Text = XQVLRVTM

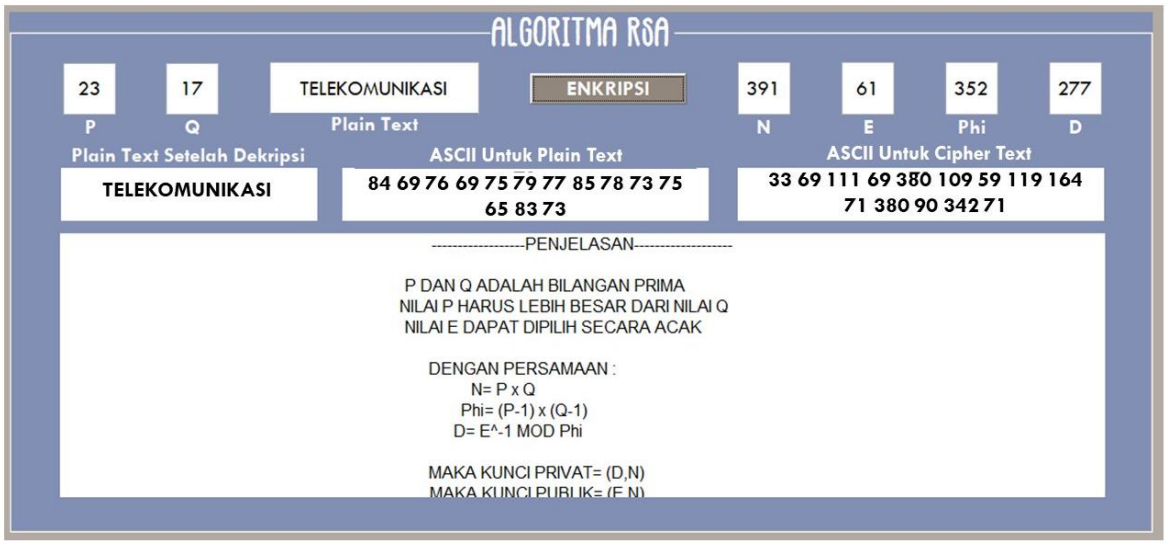


Gambar 4. 3 Tabel *Vigenere Cipher*

Pada Gambar 4.3, diketahui perhitungan menggunakan tabel *Vigenere Cipher* dan memiliki hasil yang sama dengan yang dihasilkan konverter.

c. Algortima RSA

Berikut adalah hasil dari konverter yang dibuat menggunakan MATLAB R2017a.



Gambar 4. 4 Hasil Perhitungan Algortima RSA menggunakan Konverter

Pada Gambar 4.4 dijelaskan bahwa inputan nya adalah P = 23, Q = 17. P dan Q adalah bilangan prima, nilai P lebih besar dari nilai Q. *Plain Text* = TELEKOMUNIKASI.

Setelah di enkripsi, didapatkan hasil sebagai berikut.

- N = 391

  Sesuai dengan perhitungan manual, dimana N = P x Q; N = 23 x 17 = 391
- E = 61
- Phi = 352
- D = 277
- ASCII untuk *Cipher Text* = 33 69 111 69 380 109 59 119 164 71 380 90 342 71

  ASCII ini digunakan pada setiap karakter *Plain Text* yang diinputkan. Seperti pada Tabel 4.5.

Tabel 4. 3 ASCII untuk *Cipher Text*

33	69	111	69	380	109	59	119	164	71	380	90	342	71
T	E	L	E	K	O	M	U	N	I	K	A	S	I

- ASCII untuk *Plain Text* = 84 69 76 69 75 79 77 85 78 73 75 65 83 73

  ASCII ini digunakan pada setiap karakter *Plain Text* yang diinputkan. Seperti pada Tabel 4.6.

Tabel 4. 4 ASCII untuk *Plain Text*

84	69	76	69	75	79	77	85	78	73	75	65	83	73
T	E	L	E	K	O	M	U	N	I	K	A	S	I

- Hasil Dekripsi = TELEKOMUNIKASI

d. Steganografi

Berikut adalah hasil dari konverter yang dibuat menggunakan MATLAB R2017a.

Gambar 4. 5 Hasil Enkripsi Dekripsi Steganografi Menggunakan Konverter

Seperti pada Gambar 4.5, untuk melakukan proses enkripsi sebuah *file* yang diunggah pengguna akan terlihat isi pesannya juga tempat penyimpanannya. Lalu, setelah itu pengguna menggunggah gambar yang menjadi media penyimpanan *file* rahasia. Sementara itu, untuk melakukan proses dekripsi sebuah *file* dekripsi yang berbentuk gambar diunggah terlebih dahulu, setelah di proses *file* rahasia akan terbaca dan diketahui letak penyimpanannya.

4.3 Survey Pengguna

Pengujian ini dilakukan dengan menyebarkan kuisioner secara acak yang akan dijawab oleh pengguna aplikasi pembelajaran. Telah tercatat sekitar 25 responden ikut serta dalam pengisian kuisioner.

Tabel 4. 5 Skala Penilaian

NO	KETERANGAN	BOBOT NILAI
1.	Sangat Setuju	5
2.	Setuju	4
3.	Netral	3
4.	Tidak Setuju	2
5.	Sangat Tidak Setuju	1

Pada Tabel 4.7 merupakan tabel skala penilaian MOS dari kuesioner untuk nilai bobot 5 dengan keterangan sangat setuju, nilai bobot 4 dengan keterangan setuju, nilai bobot 3 dengan keterangan netral nilai bobot 2 dengan keterangan tidak setuju dan nilai bobot 1 keterangan sangat tidak setuju.

Tabel 4. 6 Kuesioner Media Pembelajaran Interaktif

No.	Pertanyaan	Jawaban				
		1	2	3	4	5
1.	Kecukupan isi materi tentang teori Kriptografi dan Steganografi	-	-	3	5	17
2.	Kecukupan isi materi tentang Caesar Cipher	-	-	5	9	11
3.	Kecukupan isi materi tentang contoh soal Caesar Cipher	-	-	7	6	12
4.	Kecukupan isi materi tentang teori Vigenere Cipher	-	-	6	7	12
5.	Kecukupan materi mengenai contoh soal Vigenere Cipher	-	-	3	10	12
6.	Kecukupan isi materi mengenai teori Algoritma RSA	-	-	6	9	10
7.	Gambar, animasi, dan video yang ditampilkan sesuai dengan materi	-	-	2	10	13
8.	Media pembelajaran ini dapat membantu mahasiswa dalam proses belajar mandiri	-	-	-	8	17

Dari Tabel 4.8 didapatkan hasil seperti ini.

1. Kecukupan isi materi tentang teori kriptografi dan steganografi.

$$\text{MOS} = \frac{(1 \times 0) + (2 \times 0) + (3 \times 3) + (4 \times 5) + (5 \times 17)}{25} = 4.56$$

2. Kecukupan isi materi tentang *Caesar Cipher*.

$$\text{MOS} = \frac{(1 \times 0) + (2 \times 0) + (3 \times 5) + (4 \times 9) + (5 \times 11)}{25} = 4.24$$

3. Kecukupan isi materi tentang contoh soal *Caesar Cipher*.

$$\text{MOS} = \frac{(1 \times 0) + (2 \times 0) + (3 \times 7) + (4 \times 6) + (5 \times 12)}{25} = 4.2$$

4. Kecukupan isi materi tentang teori *Vigenere Cipher*.

$$\text{MOS} = \frac{(1 \times 0) + (2 \times 0) + (3 \times 6) + (4 \times 7) + (5 \times 12)}{25} = 4.24$$

5. Kecukupan materi mengenai contoh soal *Vigenere Cipher*.

$$\text{MOS} = \frac{(1 \times 0) + (2 \times 0) + (3 \times 3) + (4 \times 10) + (5 \times 12)}{25} = 4.36$$

6. Kecukupan isi materi mengenai teori Algoritma RSA.

$$\text{MOS} = \frac{(1 \times 0) + (2 \times 0) + (3 \times 6) + (4 \times 9) + (5 \times 10)}{25} = 4.16$$

7. Gambar, animasi dan Video yang ditampilkan sesuai dengan materi.

$$\text{MOS} = \frac{(1 \times 0) + (2 \times 0) + (3 \times 2) + (4 \times 10) + (5 \times 13)}{25} = 4.44$$

8. Media pembelajaran ini dapat membantu mahasiswa dalam proses balajar mandiri.

$$\text{MOS} = \frac{(1 \times 0) + (2 \times 0) + (3 \times 0) + (4 \times 8) + (5 \times 17)}{25} = 4.68$$

9. Nilai rata-rata MOS

$$\text{MOS} = \frac{4.56 + 4.24 + 4.2 + 4.24 + 4.36 + 4.16 + 4.44 + 4.68}{8} = 4.68$$

Berdasarkan data kuesioner diatas, dapat disimpulkan nilai rata-rata media pembelajaran interaktif enkripsi caesar cipher, vigenere cipher dan algoritma RSA mendapatkan total rata-rata mencapat 4.36 sehingga aplikasi media pembelajaran yang dibuat sudah melebihi nilai 4 dan dapat diartikan aplikasi media pembelajaran dalam segi penampilan menarik,

5 Kesimpulan dan Saran

Dari Bab 4 dapat diambil kesimpulan jika :

1. Dari hasil pengujian fungsionalitas, disimpulkan bahwa semua fungsi di dalam media pembelajaran interaktif menggunakan Adobe Flash CS6 dan Konverter Enkripsi menggunakan MATLAB R2017a ini berjalan 100%, sesuai yang telah direncanakan.
2. Dari hasil pengujian akurasi perhitungan. Dengan cara membandingkan hasil nilai konverter dengan hitung manual pada contoh ke 1, contoh ke 2, dan contoh ke 3 didapatkan nilai yang sama. Sehingga konverter enkripsi yang telah dibuat layak untuk digunakan.
3. Berdasarkan hasil kuesioner, tampilan dan penggunaan dari media pembelajaran mendapatkan nilai rata-rata MOS yaitu 4.36 dari skala 1 sampai 5. Dapat disimpulkan bahwa pengaruh penggunaan media pembelajaran ini berdampak baik.

Berikut ini adalah saran untuk pengembangan dan penyempurnaan media pembelajaran interaktif dan konverter ini.

1. Dapat menghubungkan antara media pembelajaran yang menggunakan Adobe Flash CS6 dan konverter enkripsi yang menggunakan MATLAB R2017a.
2. Dapat menambahkan beberapa animasi pada contoh soal agar terlihat lebih menarik dan tidak monoton.
3. Menambahkan setiap materi yang lebih lengkap dan detail. Karena masih banyak responden yang menilai cukup (MOS mengenai isi Materi masih <4.5). Maka, menyatakan masih ada kekurangan yang harus dibenahi supaya responden lebih mudah dalam penggunaannya.

Daftar Pustaka

[1] R. Eko Indrajit, “FENOMENA KEBOCORAN DATA Mencari Sumber Penyebab dan Akar Permasalahnnya,” Guru Besar Institus Perbanas, vol. 4, no. ii, pp. 1–5, 2015.

[2] I. Mu’alimin Arrijal, R. Efendi, and B. Susilo, “PENERAPAN ALGORTIMA KRIPTOGRAFI KUNCI SIMETRIS DENGAN MODIFIKASI VIGENERE CIPHER DALAM APLIKASI KRIPTOGRAFI TEKS,” J. Pseudocode, vol. III, no. 01, pp. 69–82, 2016.

[3] S. Chepuri, “An RGB Image Encryption using RSA Algorithm,” Int. J. Curr. Trends Eng. Res., vol. 3, no. 3, pp. 1–7, 2017.

[4] R. Kurniawan, “RANCANG BANGUN APLIKASI PENGAMAN ISI FILE DOKUMEN DENGAN ALGORTIMA RSA,” Algoritm. J. Ilmu Komput. dan Inform., vol. 01, no. 01, pp. 46–52, 2017.

[5] I. Gunawan, "Kombinasi Algoritma Caesar Cipher dan Algoritma RSA untuk Pengamanan File Dokumen dan Pesan Teks," J. Nas. Inform. dan Teknol. Jar., vol. 2, no. 1, pp. 124–129, 2018.

[6] Turyadi, "ENKRIPSI DAN DEKRIPSI MENGGUNAKAN METODE CAESAR CIPHER DAN OPERASI XOR," 2016.

[7] S. F. Yousif, "ENCRYPTION AND DECRYPTION OF AUDIO SIGNAL BASED ON RSA ALGORITHM," Int. J. Eng. Technol. Manag. Res., vol. 5, no. July, pp. 57–64, 2018.

[8] A. Ginting, R. R. Isnanto, and I. P. Windasari, "Implementasi Algoritma Kriptografi RSA untuk Enkripsi dan Dekripsi E-mail," J. Teknol. dan Sist. Komput., vol. 3, no. 2, pp. 253–258, 2015.

[9] T. P. Utomo, "Steganografi Gambar Dengan Metode Least Significant Bit Untuk Proteksi Komunikasi Pada Media Online," J. Tek. Inform. UNI Sunan Gunung Djati Bandung, vol. 1, no. 1, pp. 2–14, 2013.

[10] K. Firmantoro, Anton, and E. R. Nainggolan, "Animasi Interaktif Pengenalan Hewan Untuk Pendidikan Anak Usia Dini," J. Techno Nusa Mandiri, vol. XIII, no. 2, pp. 14–22, 2016.

[11] Y. Indrawaty Nurhasanah and S. Destyany, "IMPLEMENTASI MODEL CMIFED PADA MULTIMEDIA INTERAKTIF UNTUK PEMBELAJARAN ANAK USIA TK DAN PLAYGROUP," J. Inform., vol. 2, no. 2, 2011.

[12] N. Hadi W, "Storyboard Dalam Media Pembelajaran Interaktif," 2016.

[13] P. Beirne and M. Bowllon, CorelDRAW X3. 2013.

[14] K. Manuel, CorelDRAW GRAPHOCS SUITE X4. 2007.

[15] Wondershare Filmora, Wondershare Filmora User Guide (for Windows). 2017.

[16] K. D. M. AlSabti and H. R. Hashim, "A New Approach for Image Encryption in the Modified RSA Cryptosystem Using MATLAB," Glob. J. Pure Appl. Math., vol. 12, no. 4, pp. 3631–3640, 2016.

[17] J. S. Farha, M. Yamini, N. Sandhya, and M. Puneeth, "AES Algorithm Using MATLAB," Int. J. Eng. Manag. Sci., vol. 2, no. 6, pp. 17–21, 2015.

[18] N. Wahid and N. Hassan, "Self-Tuning Fuzzy PID Controller Design for Aircraft Pitch Control," 2012 Third Int. Conf. Intell. Syst. Model. Simul., vol. 10, no. 27, pp. 19–24, 2012.