p-ISSN: 2527-967X
e-ISSN: 2549-2845

PERANCANGAN SIMULASI METODE CAESAR CIPHER MENGGUNAKAN MICROSOFT EXCEL – ALTERNATIF MEDIA PEMBELAJARAN KRIPTOGRAFI

Endaryono
Program Studi Informatika, Universitas Indraprasta PGRI
Email: endaryono612@gmail.com

Abstrak

Dalam perkuliahan kriptografi, mahasiswa perlu mendapat ilustrasi dalam bentuk simulasi. Diperlukan media pembelajaran yang dapat menjelaskan secara visual proses kerja enkripsi dan dekripsi termasuk pada metode caesar cipher. Metode caesar cipher adalah satu dari beberapa algoritma dalam proses kriptografi. Meski algoritma ini dinilai banyak kelemahan karena mudah ditebak tetapi algoritma ini merupakan dasar dari proses kriptografi. Penelitian ini merupakan penelitian terapan, yaitu membuat perancangan aplikasi *microsoft excel* (*MS. Excel*) untuk simulasi proses enkripsi dan dekripsi menggunakan metode caesar cipher. Aplikasi *microsoft excel* ini dipilih karena mudah dalam pengoperasiannya dan luas penggunaannya. Hasil dari penelitian ini adalah program aplikasi *microsoft excel* untuk simulasi kerja metode caesar cipher. Penelitian menunjukkan bahwa perancangan simulasi yang dibuat dapat berfungsi dan berjalan dalam pelaksanaan enkripsi dekripsi. Dalam simulasi dapat ditunjukkan bagaimana proses kerja enkripsi dan dekripsi yang menyangkut pengubahan isi pesan. Hasil penelitian diharapkan menjadi alternatif media pembelajaran kriptografi yang secara langsung dapat dirasakan manfaatnya bagi para dosen dan mahasiswa dalam pembelajaran kriptografi.
Kata Kunci : *MS Excel*, enkripsi, dekripsi, kristografi, caesar cipher

Abstract

In cryptography lectures, students need to get illustrations in the form of simulations. Learning media is needed that can visually explain the work processes of encryption and decryption, including the caesar cipher method. The caesarean cipher method is one of several algorithms in the cryptographic process. Although this algorithm is considered a lot of weaknesses because it is easy to guess, but this algorithm is the basis of the cryptogratic process. This research is applied research, which is making the design of Microsoft Excel application (MS.Excel) for the simulation of the encryption and decryption process using the caesar cipher method. This Microsoft Excel application was chosen because it is easy to operate and widely used. The result of this study was the Microsoft Excel application program for working simulations of the Caesar Cipher method. Research showed that the design of simulations made can function and run in the implementation of decryption encryption. In the simulation it can be shown how the process of encryption and decryption work that involves changing the contents of the message. The results of the study are expected to be an alternative medium for cryptographic learning that can directly benefit the lecturers and students in cryptographic learning..
Key Words : *MS Excel, encryption, description, crystallography, caesarean cipher*

PENDAHULUAN

Informasi dalam suatu kegiatan merupakan hal yang penting. Banyak informasi yang sesungguhnya bukan merupakan konsumsi publik secara luas. Ada informasi yang bersifat terbatas atau hanya pihak-pihak tertentu yang mempunyai otoritas mengetahui suatu informasi tersebut. Untuk kebutuhan keamanan suatu pesan maka kajian kriptografi dan algoritma persandian dilakukan dan dikembangkan untuk melindungi isi pesan. Satu dari algoritma kriptologi adalah caesar chiper. Algoritma ini meski terdapat kelemahan tetapi algoritma ini merupakan dasar dari algoritma selanjutnya. Dalam perkuliahan kriptografi, mahasiswa perlu diberikan media pembelajaran yang dapat mengilustrasikan proses kerja suatu algoritma.

p-ISSN: 2527-967X
e-ISSN: 2549-2845

Media pembelajaran adalah segala sesuatu baik berupa fisik maupun teknis dalam proses pembelajaran yang dapat membantu pengajar menyampaikan materi pengajaran sehingga memudahkan pencapaian tujuan pembelajaran [1].

Media pembelajaran dapat membangkitkan minat, motivasi, rangsangan dan pengaruh psikologis lainnya terhadap peserta belajar. Secara umum manfaat media pembelajaran adalah memperlancar interaksi antara pengajar dengan peserta belajar sehingga proses pembelajaran efektif dan efisien [2].

Tulisan ini menunjukkan aplikasi *microsoft excel* dapat digunakan sebagai alternatif media pembelajaran yang membantu peserta belajar memahami cara kerja algoritma caesar (caesar cipher) dalam kriptografi.

Jurnal yang membahas aplikasi caesar cipher antara lain: (1) Implementasi Kriptografi Caesar Cipher Menggunakan Matlab R2013a. Jurnal ini membahas bagaimana proses enkrpsi dan dekripsi dalam kriptografi metode caesar cipher berjalan melalui simulasi menggunakan perancangan aplikasi matlab R2013a [3]. (2) Perancangan Apliksi Enkripsi Dekripsi Menggunakan Metode Caesar Cipher dan Operasi XOR. Jurnal ini membahas perancangan aplikasi enkripsi dan dekripsi berbasis visual studio 2005 dengan algoritma caesar chiper dan operasi XOR [4]. Hasil penelitian berupa perancangan simulasi diharapkan menjadi pilihan media pembelajaran bagi dosen dan mahasiswa dalam kajian kriptografi.

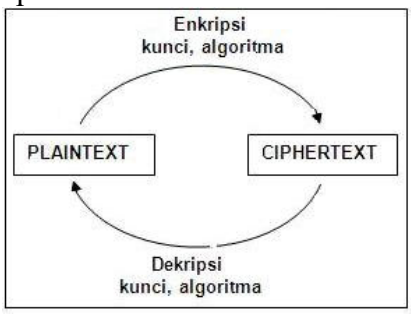
Dasar Kriptografi

Kriptografi berasal dari bahasa Yunani, *cryptos* berarti menyembunyikan, rahasia dan *graphein* berarti menulis. Kriptografi dapat dipahami sebagai bagian matematika yang mempelajari aspek keamanan informasi, kerahasiaan, validitas, integritas dan otentikasi suatu data. Kriptografi juga dipandang sebagai seni menjaga keamanan pesan [5].

Unsur utama dari kriptografi ada 4 hal, yaitu: Plaintext yaitu pesan yang dapat dibaca, Ciphertext yaitu pesan yang tidak dapat dibaca, Key yaitu kunci dari pelaksanaan kriptografi, dan Algorithma atau *cipher* yaitu aturan untuk *enchipering* dan *dechipering* atau metode pelaksanaan dalam enkrispi dan dekripsi. [6]

Proses dasar dari kriptografi terdiri dari: (1) enkripsi (*encryption*, *enciphering*), proses mengubah pesan yang terbaca atau *plaintext* menjadi pesan yang sudah diacak atau *ciphertext*, (2) dekripsi (*decryption*, *deciphering*) adalah proses kebalikan dari enkripsi, yaitu mengubah ciphertext menjadi plaintext [7].

Ilustrasi proses dasar kriptografi dapat dilihat pada Gambar 1 berikut:



Gambar 1. Operasi Kriptografi

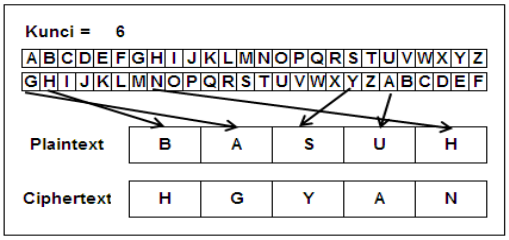
Algoritma Caesar (Caesar Cipher)

Algoritma caesar atau caesar cipher adalah algoritma yang tertua dalam kriptografi. Algoritma ini pertama kali digunakan pada masa kekuasaan Raja Julius Caesar. Ia mengubah setiap huruf dalam pesan yang disampaikan menjadi tiga huruf sesudah huruf dalam pesan asli pada urutan alfabet. Metode yang dilakukan ini dikenal dengan algoritma ROT3. Langkah-langkah yang dilakukan dari metode Caesar Cipher adalah menentukan jumlah atau nilai langkah pergeseran setiap huruf atau karakter untuk mengubah dari ciphertext

p-ISSN: 2527-967X
e-ISSN: 2549-2845

ke paintext, dan menukarkan setiap huruf atau karakter pada setiap isi pesan plaintext menjadi kalimat yang disandikan atau ciphertext.

Ilustrasi dari langkah ini dapat dilihat pada Gambar 2.



Gambar 2. Ilustrasi Ekripsi Kunci 6

Sebagai contoh, misalkan nilai pergeseran adalah 6, maka huruf A diubah menjadi G, huruf B diubah menjadi H dan selanjutnya. Demikian pesan yang berisi : BASUH maka setelah melalui proses enkripsi algortima Caesar Cipher dengan kunci = 6 menjadi ciphertext : HGYAN.

Aritmatika Modular

Aritmatika modular atau dikenal dengan aritmatika jam adalah sistem operasi dua buah bilangan bulat sehingga mencapai nilai sisa atau modulus. Konsep ini dipublikasikan oleh Carl Friedrich Gauss tahun 1801 [8].

Pemahaman dasar aritmatika modular sebagai berikut:
Definisi:
Misalkan n adalah suatu bilangan bulat positif, a dan b adalah suatu bilangan bulat, maka a dikatakan kongruen b modulo n, ditulis : $a \equiv b (\mathrm{mod}\, n)$
jika dan hanya jika $a - b$ adalah kelipatan n
Sebagai contoh:
$5 \equiv 12 \pmod 7$
$2 \equiv 23 \pmod 7$
$1 \equiv 36 \pmod 7$, dan seterusnya
$5 \equiv 12 \pmod 7$
$2 \equiv 23 \pmod 7$
$1 \equiv 36 \pmod 7$, dan seterusnya.

Proses enkripsi dan dekripsi metode caesar cipher melibatkan operasi matematika khususnya pembahasan aritmatika modular. Persamaan enkripsi, ditulis :

$y = E(x)$ ---------- Pers. 1

y = adalah hasil enkripsi atau ciphertext
$x = \{x_1, x_2, .., x_m\}$, adalah plaintext, yaitu karakter atau huruf dalam isi pesan terbaca.

m = jumlah elemen atau jumlah karakter.

Persamaan tersebut melibatkan aritmatika modulo, sehingga dapat ditulus:

$E_n \equiv (x + n) \bmod 26$ ---------- Pers. 2

Dan persamaan dekripsi ditulis :

$x = D(y)$ ---------- Pers. 3

x = adalah hasil dekripsi berbentu plaintext
$y = \{y_1, y_2, .., y_m\}$, adalah ciphertext, yaitu karakter atau huruf yang disandikan.

m = jumlah elemen atau jumlah karakter.

Persamaan 3 melibatkan aritmatika modulo, ditulus:

$D_n \equiv (y - n) \bmod 26$ ---------- Pers. 4

Ilustrasi proses enkripsi menggunkan persamaan 2 misalnya:
Plaintext (x) : B A S U H
Kunci (n) : 6

B	$E_1 \equiv (1+6) \bmod 26 \equiv 7$	H
A	$E_2 \equiv (0+6) \bmod 26 \equiv 6$	G
S	$E_3 \equiv (18+6) \bmod 26 \equiv 24$	Y
U	$E_4 \equiv (20+6) \bmod 26 \equiv 0$	A
H	$E_1 \equiv (7+6) \bmod 26 \equiv 13$	N

Sebagai ilustrasi proses dekripsi dengan persamaan persamaan 4, adalah:

p-ISSN: 2527-967X
e-ISSN: 2549-2845

Ciphertext (y) : H G Y A N
Kunci (n) : 6

H	$D_1 \equiv (7-6) \bmod 26 \equiv 1$	B
G	$D_2 \equiv (6-6) \bmod 26 \equiv 0$	A
Y	$D_3 \equiv (24-6) \bmod 26 \equiv 18$	S
A	$D_4 \equiv (0-6) \bmod 26 \equiv 20$	U
N	$D_5 \equiv (13-6) \bmod 26 \equiv 7$	H

METODE

Penelitian ini merupakan penelitian terapan, yaitu membuat perancangan aplikasi *microsoft excel* untuk simulasi proses enkripsi dan dekripsi menggunakan metode caesar cipher. Hasil penelitian diharapkan menjadi alternatif media pembelajaran bidang kriptografi sehingga manfaatnya dapat dirasakan secara langsung bagi para dosen, mahasiswa atau peminat matematika kriptografi. Metode penelitian adalah studi pustaka dan penerapan pada aplikasi *microsoft excel*.

Perancangan Aplikasi Proses Enkripsi

Tahap pertama pelaksanaan kerja adalah membuat rancangan proses enkripsi pada aplikasi *microsoft excel*.

Modulo yang terapkan adalah 27, yaitu $-= 0$, $a = 1$, $b = 2$ dan seterusnya sampai $z = 26$. Tanda – digunakan untuk spasi antar kata dalam kalimat.

Selanjutnya dari masukan kalimat yang dilakukan sebapai plaintext, pada kolom perhitungan-1 setiap karakter dikonversi sebagai angka berdasarkan fungsi satu-satu, misalnya: L = 12, A = 1, K = 11 dan seterusnya. Rancangan proses enkripsi dapat dilihat pada Gambar 3.

PROGRAM ENKRIPSI																													
A. RUMUS AWAL																													
-	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	26			
MASUKAN KALIMAT :	L	A	K	U	K	A	N	-	S	E	M	U	A	N	Y	A	-	T	I	D	A	K	-	S	I	S	A		
B. PELAKSANAAN ENKRIPSI																													
KUNCI :	6																												
PERHITUNGAN-1 :	12	1	11	21	11	1	14	0	19	5	13	21	1	14	25	1	0	20	9	4	1	11	0	19	9	19	1		
PERHITUNGAN-2 :	18	7	17	0	17	7	20	6	25	11	19	0	7	20	4	7	6	26	15	10	7	17	6	25	15	25	7		
C. HASIL ENKRIPSI :	R	G	Q	-	Q	G	T	F	Y	K	S	-	G	T	D	G	F	Z	O	J	G	Q	F	Y	O	Y	G		

Gambar 3. Rancangan Proses Enkripsi

Formula *MS Excel* yang digunakan adalah:
H17=IF(enkripsi!$I$6="";"";IF(H10="";"";(LOOKUP(H10;$B$6:$AG$6;$B$7:$AG$7))))

Selanjutnya pada kolom perhitungan-2, setiap angka-angka dikonversi berdasarkan aritmatika modulo sesuai banyak pergeseran, misalkan angka 12 dikonversikan menjadi angka 18, yaitu:
En ≡ (12 + 6) mod 27
En ≡ (18) mod 27
En ≡ 18

Formula *MS Excel* yang digunakan:
H18=IF(enkripsi!$I$6="";"";IF(H10="";"";(MOD((H$17+enkripsi!$I$6);27))))

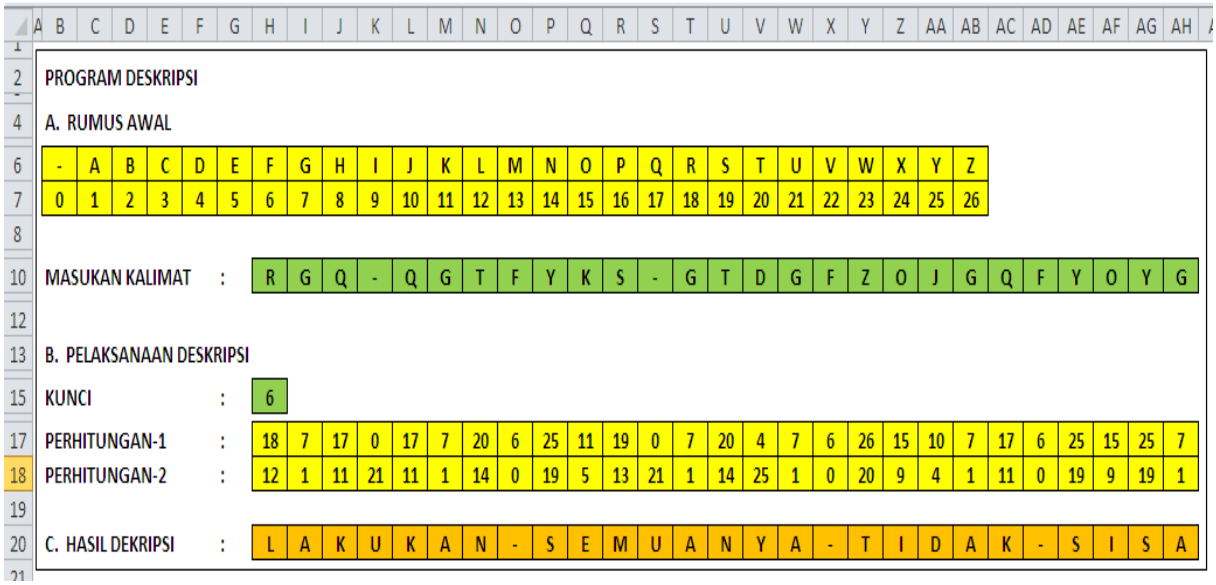
Selanjutnya pada baris hasil enkripsi, setiap nilai pada baris hasil enkripsi diubah menjadi huruf berdasarkan fungsi satu-satu, misalnya angka 18 menjadi huruf R, 7 menjadi G, 17 menjadi Q dan seterusnya.
Formula MS Excel yang digunakan:
H20=IF(H18="";"";(LOOKUP(H$18;$B$7:$AG$7;$B$6:$AG$6)))

p-ISSN: 2527-967X
e-ISSN: 2549-2845

Perancangan Aplikasi Proses Dekripsi

Tahap kedua penelitian adalah pembuatan rancangan proses dekripsi pada aplikasi microsoft excel. Modulo yang gunakan sama dengan modulo pada enkripsi yaitu 27. Pada pelaksanaan proses dekripsi, user memasukkan ciphertext yang akan diubah menjadi plaintext.

Selanjutnya, pada perhitungan-1, setiap karakter pada ciphertext diubah menjadi angka sesuai dengan fungsi satu-satu, misalnya R = 18, G = 7, Q = 17 dan seterusnya. Formula MS Excel digunakan:
H17=IF(deskripsi!$I$6="";"";IF(H10="";"";LOOKUP(H10;$B$6:$AG$6;$B$7:$AG$7)))



Gambar 4. Rancangan Proses Dekripsi

Pada kolom perhitungan-2, setiap angka dikonversi berdasarkan aritmatika modulo dengan invers algoritma, misalkan nilai 12 dikonversikan menjadi angka 18, yaitu:
En ≡ (18 - 6) mod 27
En ≡ 12
Dalam MS excel formula yang digunakan:
H18=IF(deskripsi!$I$6="";"";IF(H10="";"";(MOD((H$17-deskripsi!$I$6);27))))
Selanjutnya setiap angka diubah menjadi karakter pada baris hasil dekripsi. Proses ini berdasarkan fungsi satu-satu. Formula MS Excel yang digunakan:
H20=IF(H18="";"";(LOOKUP(H$18;$B$7:$AG$7;$B$6:$AG$6)))

HASIL DAN PEMBAHASAN

Hasil dari penelitian ini adalah perancangan program aplikasi *microsoft excel* untuk simulasi proses enkripsi dan dekripsi menggunakan metode caesar cipher. *Microsoft excel* merupakan aplikasi yang relatif mudah pengoperasiannya dan luas penggunaannya.

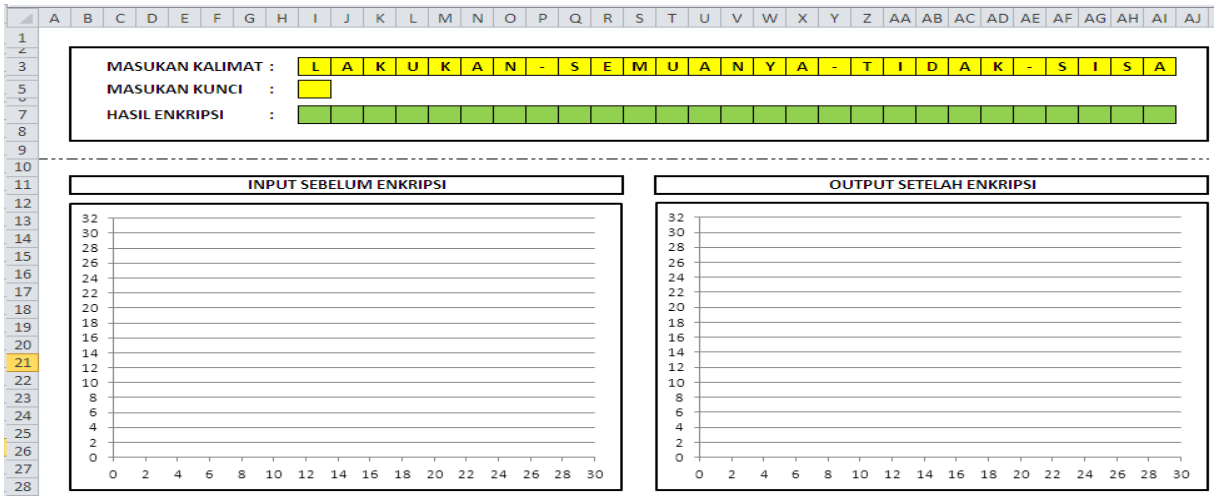
Hasil penelitian ini berupa program aplikasi *microsoft excel* untuk simulasi kerja metode caesar cipher, selanjutnya dilakukan pengecekan apakah perancangan berfungsi dengan baik. Uji coba ditampilkan dalam dua halaman tampilan, yaitu tampilan pelaksanaan enkripsi dan tampilan pelaksanaan dekripsi.

Hasil Tampilan Pelaksanaan Enkripsi

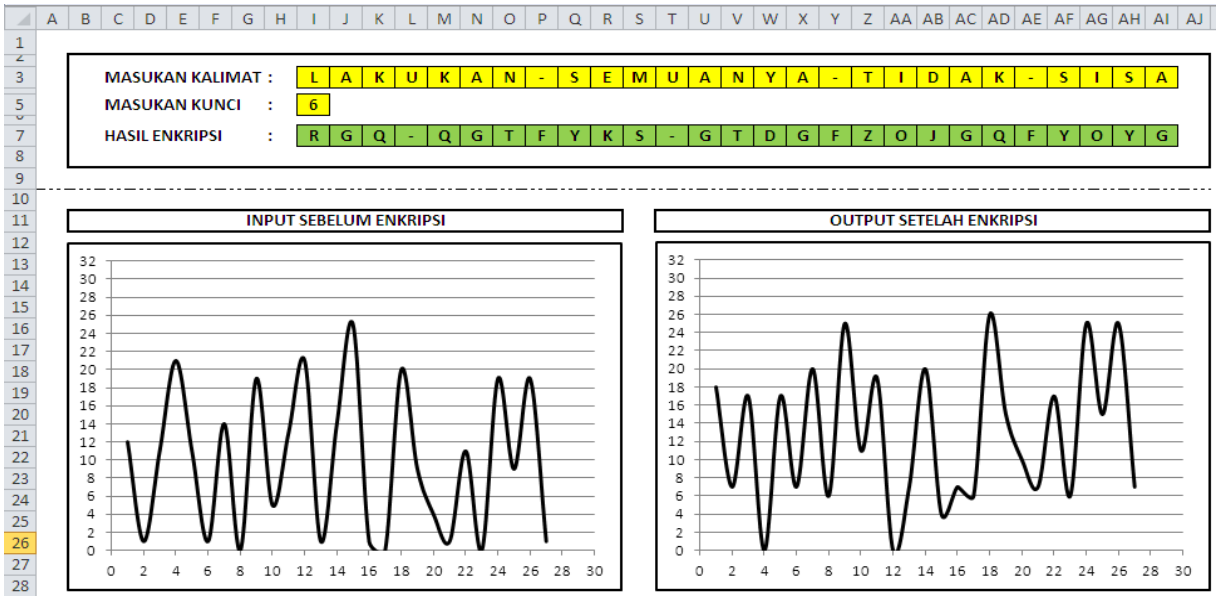
Pengecekan pelaksanaan enkripsi, pengguna memasukkan plaintext yaitu isi pesan. Tampilan pelaksanaan enkripsi sudah tentu berkaitan dengan formula *microsoft excel* yang ada pada halaman proses enkripsi. Saat pengguna mengentry plaintext dan belum memasukkan angka

p-ISSN: 2527-967X
e-ISSN: 2549-2845

kunci, maka pada tahap ini program belum menampilkan ciphertext. Tampilan awal sebelum *user* memasukkan kunci dapat dilihat pada Gambar 5.



Gambar 5. Tampilan Halaman Proses Enkripsi Sebelum *User* Memasukkan Kunci



Gambar 6. Tampilan Halaman Proses Enkripsi Setelah *User* Memasukkan Kunci

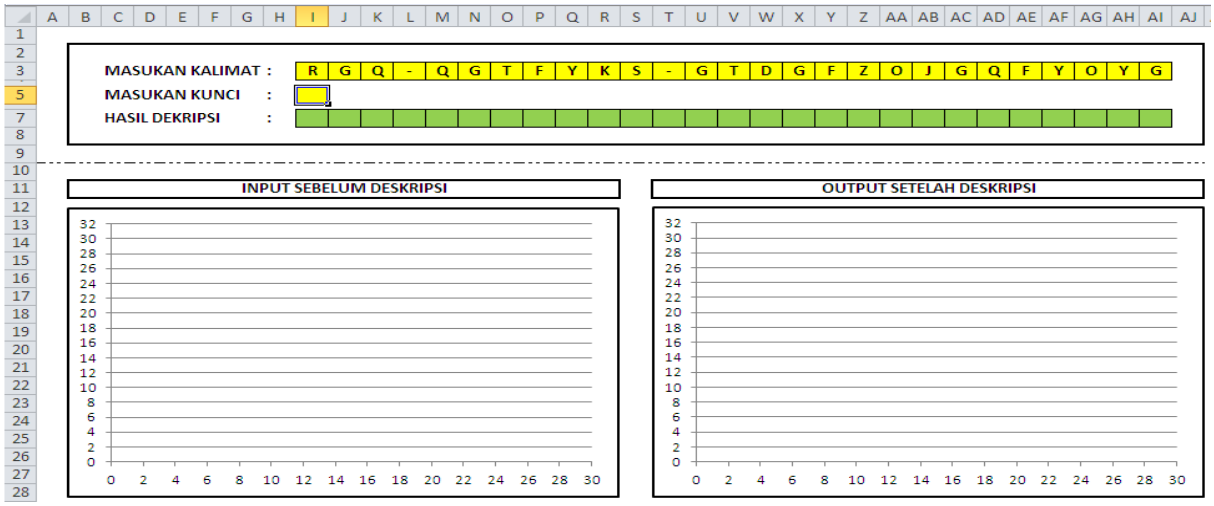
Setelah *user* memasukkan kunci, maka komputer menampilkan ciphertext dan grafik yang menggambarkan fungsi satu-satu antara nilai urutan karakter dan simbol karakter yang telah dientri. Tampilan layar komputer setelah *user* memasukkan kunci pada Gambar 6.

Hasil Tampilan Proses Dekripsi

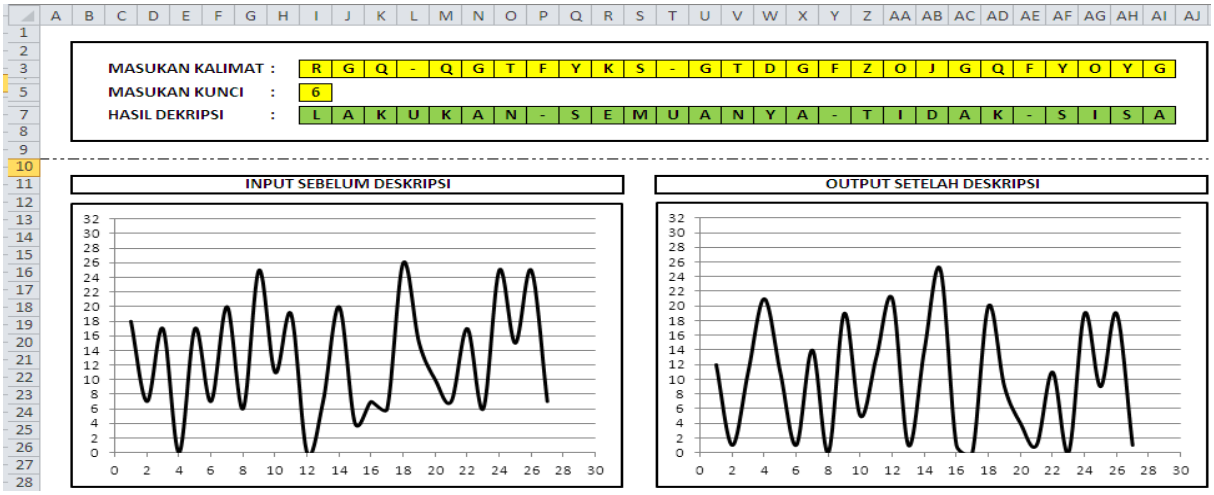
Sebagaimana dalam pelaksanaan enkripsi, maka dalam pelaksanaan dekripsi, pengguna lebih dahulu memasukkan ciphertext atau pesan yang telah disandikan. Halaman pelaksanaan dekripsi berkaitan dengan formula *microsoft excel* pada halaman proses dekripsi.

Saat pengguna mengentry ciphertext dan belum memasukkan angka kunci, maka pada tahap ini program belum menampilkan plaintext. Tampilan awal sebelum *user* memasukkan kunci dapat dilihat pada Gambar 7.

p-ISSN: 2527-967X
e-ISSN: 2549-2845



Gambar 7. Tampilan Halaman Proses Dekripsi Sebelum *User* Memasukkan Kunci



Gambar 8. Tampilan Halaman Proses Dekripsi Setelah *User* Memasukkan Kunci

Pada Gambar 8 adalah hasil tampilan setelah *user* memasukkan kunci. Terlihat plaintext atau pesan yang dapat dibaca dihasilkan dan disertai dengan grafik yang menggambarkan fungsi satu-satu antara nilai urutan karakter dan simbol karakter tang telah dientri. Tentu saja kunci dekripsi yang dimasukkan harus sama dengan kunci yang digunakan saat enkripsi.

SIMPULAN

Perancangan yang dibuat untuk simulasi enkripsi dekripsi metode caesar cipher menggunakan *microsoft excel* dapat befungsi dan proses dapat berjalan. Modulo yang digunakan adalah 27 yang terdiri dari jumlah alfabet 26 karakter dan tanda strip (–) untuk spasi antar kata dalam kalimat. Kekurangan dari rancangan ini adalah belum digunakannya beberapa tanda baca, seperti: koma, titik, tanda seru, tanda tanya, spasi dan lain-lain. Sebagai saran, perlu dibuat rancangan simulasi lainnya yang lebih menarik dengan metode atau algoritma tertentu dalam kriptografi.

DAFTAR PUSTAKA

[1] T. Tafonao. "Peranan Media Pembelajaran dalam Meningkatkan Minat Belajar Mahasiswa". *J. Komun. Pendidik. STT Kadesi Yogyakarta*, vol. 2, no. 2, pp. 103–113, 2018.

p-ISSN: 2527-967X
e-ISSN: 2549-2845

[2] I. R. Karo-Karo. "Manfaat Media dalam Pembelajaran". *J. AXIOM*, vol. VII, no. 1, pp. 91–96, 2018.

[3] P. N. Arifah dan W. Agustiar Basuki. "Implementasi Kriptografi Caesar Cipher Menggunakan Matlab R2013a". *Proseeding Seminar Matematika dan Pendidikan Matematika UNY*, pp. 297–304, 2017.

[4] N. Azis. "Perancangan Aplikasi Enkripsi Deskripsi Menggunakan Metode Caesar Chiper dan Operasi XOR". *J. Univ. Krsnadwipayana*, vol. 2, no. 1, pp. 72–80, 2018.

[5] A. W. Sudrajat. "Implementasi Enkripsi Database Menggunakan *Transparent Data Encryption* pada *Database Engine Oracle*". *J. Ilm. STMIK GI MDP*, vol. 2, no. 3, 2006.

[6] M. Nasir. "Pengembangan Prototype Sistem Kriptografi untuk Enkripsi dan Dekripsi Data *Office* Menggunakan Metode Blowfish dengan Bahasa Pemrograman Java". *J. Format Univ. Mercubuana*, vol. 6, no. 1, pp. 87–105, 2017.

[7] R. Primartha. "Penerapan Enkripsi dan Dekripsi File Menggunakan Algoritma *Data Encryption Standard* (DES)". *J. Sist. Inf. Univ. Sriwij.*, vol. 3, no. 2, pp. 371–387, 2011.

[8] D. B. Ginting. "Peranan Aritmatika Modulo dan Bilangan prima pada Algoritma Kriptografi RSA". *J. Media Inform. Sekol. Tinggi Manaj. Inform. dan Komput. LIKMI*, vol. 9, no. 2, pp. 48–57, 2010.