PERANCANGAN APLIKASI KRIPTOGRAFI BERBASIS WEB DENGAN ALGORITMA DOUBLE CAESAR CIPHER MENGGUNAKAN TABEL ASCII

Endah Handayani[1)], Wheny Lebdo Pratitis[2)], Achmad Nur[3)]
Syaifudin Ali Mashuri[4)], Bagus Nugroho[5)]

[1), 2, 3, 4, 5)] Teknik Informatika STMIK AMIKOM Yogyakarta
Jl Ring road Utara, Condongcatur, Sleman, Yogyakarta 55281
Email : endah8302@students.amikom.ac.id[1)], wheny8345@students.amikom.ac.id[2)]
achmad8355@students.amikom.ac.i[3)], syaifudin8341@students.amikom.ac.id[4)],
bagus8342@students.amikom.ac.id[5)]

Abstrak

Pada zaman sekarang ini data/pesan tidak hanya dikirimkan melalui kurir atau secara tradisional saja akan tetapi sudah disesuaikan dengan perkembangan teknologi. Salah satu fenomena yang terjadi karena melibatkan tenologi Internet dalam pengiriman pesan dan pertukaran data adalah adanya isu penyadapan, pemalsuan bahkan pencurian pesan. Atas dasar pemikiran ini, perlu dibuat media atau aplikasi yang bisa digunakan untuk melakukan proses enkripsi dan deskripsi pesan sehingga pesan yang dikirimkan dapat diterima oleh penerima dalam keadaan terjamin legitimasinya. Penelitian ini menggunakan algoritma kriptografi Double Caesar Cipher yang menekankan kombinasi dari 2 algoritma Caesar cipher yang chipertextnya diterjemahkan menggunakan tabel ASCII. Dari hasil pengujian terhadap aplikasi yang dibangun, penggabungan Double caesar Cipher dan tabel ASCII dalam melakukan proses enkripsi maupun deskripsi maka dapat terbukti menjamin kemananan maupun kerahasiaan pesan.

Kata Kunci :Keamanan, kerahasiaan, double caesar cipher, ASCII

1. Pendahuluan

Sejak berpuluh-puluh tahun yang lalu, kriptografi hanya digunakan dan dipelajari oleh pihak militer untuk mengamankan komunikasi mereka dari ancaman pihak luar. Namun persaingan dalam dunia kriptografi semakin lama semakin berkembang sehingga akhir-akhir ini kriptografi tidak hanya dimonopoli oleh pihak militer saja, hal yang sama juga dilakukan oleh individu-individu yang menginginkan pesan dan komunikasi mereka tidak diketahui oleh pihak lain. Pesan yang dikirimkan saat ini bukan lagi pesan yang bersifat konvensional, tidak lagi dikirimkan melalui kurir akan tetapi sudah melibatkan peranan internet.

Dengan menggunakan kriptografi yang sudah ada hal-hal diatas tidak perlu ditakutkan lagi. Akan tetapi dengan menggunakan algoritma kriptografi yang sudah ada kode-kode yang digunakan untuk menyandikannya sangat mudah untuk dipecahkan. Oleh karena itu diperlukan pengembangan atau penggabungan dari algoritma yang sudah ada sehingga tercipta algoritma yang aman untuk proses enkripsi dan deskripsi pesan tetapi algoritma tersebut tetap mudah untuk diterapkan. Dari berbagai algoritma kriptografi yang ada, Caesar Cipher adalah algoritma yang sangat mudah untuk diterapkan dengan ditambahkan rule-rule baru yang tidak diketahui oleh orang lain dan ditampilkan dengan menggunakan tabel ASCII maka algoritma ini akan menjadi algoritma yang sulit untuk dipecahkan.

Berdasarkan latar belakang ini, maka permasalahan yang dapat dirumuskan adalah bagaimana merancang aplikasi enkripsi-deskripsi dengan menggunakan algoritma *Double Caesar Cipher* menggunakan Tabel ASCII berbasis web. Sementara itu penelitian ini juga membatasi ruang lingkup diantaranya adalah aplikasi ini dibuat khusus berbasis web algoritma yang digunakan adalah algoritma Caesar Cipher yang digabungkan dengan tabel ASCII, aplikasi ini dibuat menggunakan bahasa pemrograman php, dan kunci yang digunakan berupa angka dengan panjang maksimal 10 karakter.

Lebih jauh, kontribusi penting dalam penelitian ini adalah diharapkan dapat membantu mengamankan pesan yang bersifat rahasia dari ancaman orang-orang yang tidak bertanggungjawab sehingga pesan yang dikirimkan pengirim dapat diterima oleh penerima tanpa diketahui oleh siapapun.

Kriptografi adalah suatu ilmu yang mempelajari bagaimana cara menjaga agar data atau pesan tetap aman saat dikirimkan dari pengirim ke pengirim lain tanpa mengalami gangguan dari pihak ketiga. Menurut terminologinya kriptografi adalah ilmu dan seni untuk menjaa keamanan pesan ketika pesan dikirim dari suatu tempat ke tempat yang lain. Kriptografi berasal dari bahasa Yunani, menurut bahsa dibagi menjadi dua yaitu kripto dan graphia, kripto berarti secret (rahasia) dan graphia berarti writing (tulisan)[1]

Algoritma Caesar Cipher adalah algoritma kriptografi klasik yang menggunakan teknik subtitusi.[2] Inti dari Algoritma ini adalah melakukan pergeseran terhadap semua karakter pada plaintext dengan menggunakan kunci yang sudah ditentukan. Contoh :

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

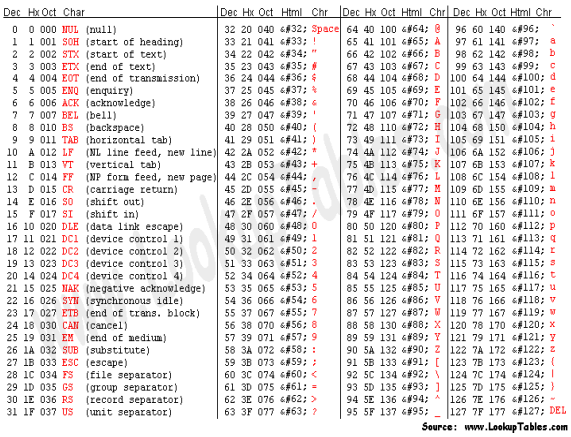
menjadi :

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

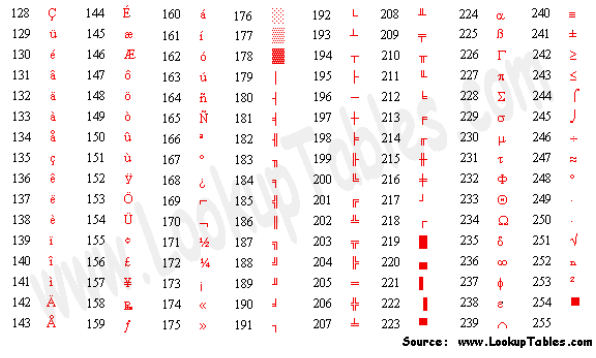
pada contoh diatas pergeseran dilakukan sebanyak tiga kali atau 3 langkah maka kuncinya adalah 3. Pergeseran kunci yang dilakukan dapat disesuaikan dengan keinginan pengirim pesan. Misalkan a = 1, b = 3, dan seterusnya. Pada algoritma Caesar Cipher untuk plaintext disimbolkan "P" dan chipertext "C" sedangkan untuk kunci "K". Terdapat cara lain untuk melakukan perhitungan enkripsi-deskripsi dengan algoritma Caesar Cipher yaitu dengan menggunakan rumus dibawah ini :

E = (Pi + K) mod 26 .....(1)
D = (Ei-K) mod 26 .....(2)
E = (Pi + K) mod 256 .....(1)
D = (Ei-K) mod 256 .....(2)

Keterangan :
Pi = nilai desimal karakter dari plaintext ke-i
Ei = nilai desimal karakter dari ciphertext ke-i
K = Key/kunci yang digunakan
Mod 256 digunakan jika menggunakan table ASCII
Mod 26 digunakan jika menggunakan alphabet 26



Gambar 1. Tabel ASCII (teks) [3]



Gambar2. Tabel ASCII(simbol)[3]

Penelitian terhadap metode enkripsi dan deskripsi sudah diteliti oleh banyak orang oleh karena itu penulis melakukan tinjauan studi dari beberapa penelitian sebelumnya. Penelitian sebelumnya tentang *"Implementasi pengamanan data menggunakan enkripsi Caesar cipher menggunakan tabel ASCII"*, dari penelitian ditemukan pengubahan cara enkripsi pada Caesar cipher yang telah ditambahkan table ASCII dan juga tabel huruf perulangan maka plaintext diubah menggunakan pola yang ada akan menghasilkan deretan yang terdiri dari angka dan huruf. Dengan begitu keamanan data atau pesan yang dikirimkan kepada orang lain dapat lebih aman dan tidak dapat di bobol oleh orang yang tidak bertanggung jawab karena pesan yang dikirimkan berupa deretan angka dan huruf yang tak beraturan, sehingga orang lain sulit untuk memecahkan pesan tersebut [4].

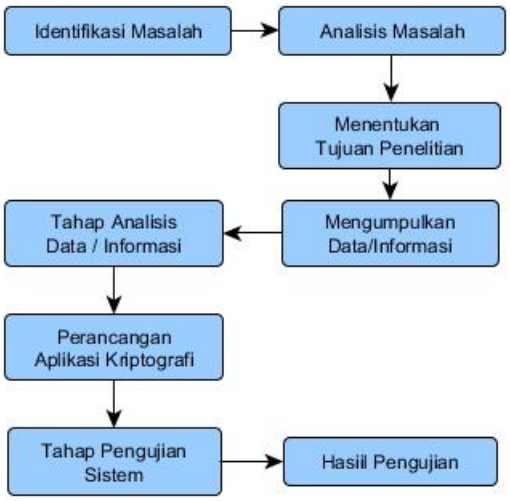
Penelitian sebelumnya tentang *"Implementasi algoritma kriptografi kode caesar, vigenere, dan transposisi untuk sistem proteksi penggunaan pesan singkat (sms) pada smartphone android", dimana dalam* implementasi algoritma Caesar Cipher, Program mengambil jumlah karakter dari kata kunci sebagai penentu banyaknya pergeseran masing-masing karakter teks biasa. Program mengubah masing-masing karakter teks biasa dengan menggesernya sebanyak variabel pengubah sesuai jumlah karakter kunci. Proses kerja variabel pengubah pada program ini dapat dilakukan secara manual dengan melakukan pergeseran karakter [5].

Selain penelitian yang sudah dijelaskan diatas, penelitian lain yang dijadikan tinjauan studi adalah penelitian tentang *"Implementasi Cipher Hill pada kode ASCII dengan Memanfaatkan Digit Desimal Bilangan Euler"* kode ASCII memberikan kemungkinan yang luas pada lebih banyak karakter yang tercakup, tidak hanya terbatas pada 26 alfabet, tetapi juga mencakup karakter-karakter seperti . ,", ',=,@,#,% dan sebagainya [6]

2. Pembahasan

2.1 Kerangka Kerja Penelitian

Pada tahap ini akan dideskripsikan lagkah – langkah yang akan diilakukan dalam penyelesaian. masalah yang akan dibahas. Berikut gambaran kerangka kerja penelitian :



Gambar 3. *Kerangka Kerja Penelitian*

2.2 Analisis Aplikasi

Dalam penelitian ini dilakukan beberapa analisis, yaitu analisis kebutuhan fungsional dan analisis kebutuhan non fungsional. Kebutuhan fungisonal digunakan untuk menganalisis fungsi-fungsi yang nantinya dapat dikerjakan oleh sistem. Adapun kebutuhan fungsional pada aplikasi enkripsi-deskripsi pesan dengan menggunakan algoritma Double Caesar Cipher dengan menggunakan Tabel ASCII adalah sebagai berikut :

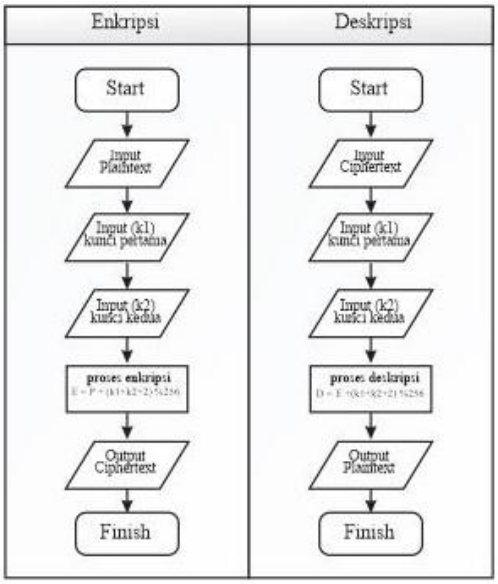
1. Sistem bisa menerima inputan dari user, berupa plaintext.
2. User dapat menginputkan key pertama dan key kedua sesuai dengan yang diinginkan (batasan jumlah key = 8).
3. Sistem dapat melakukan enkripsi dan deskripsi pesan.
4. Sistem dapat menampilkan hasil dari enkripsi dan deskripsi pesan.
5. Sistem dapat melakukan edit dan delete pesan yang sudah diinputkan.

Sedangkan analisis kebutuhan non fungsional yang yang dilakukan adalah dengan melakukan analisis kebutuhan perangkat lunak sebagai berikut :

1. Google Chrome
2. Sublime
3. XAMPP Control Panel v3.1.0
4. Apache
5. Windows 8

Deskripsi dan Flowchart Aplikasi

Pada program kriptografi ini inputan yang diberikan oleh user berupa plaintext dan ciphertext. Pada proses enkripsi meminta user untuk menginputkan plaintext (teks yang ingin di enkripsi) kemudian jumlah angka pertama dan jumlah angka kedua dimana jumlah angka tersebut merupakan kunci yang digunkan untuk mengenkripsi. Jumlah angka untuk masing-masing pegeseran yang bisa digunakan untuk mengenkripsi. Jumlah angka untuk masing-masing pergeseran yang biasa digunkan sudah kami tentukan yaitu maksimal 8. Jadi user tidak bias menginputkan angka kunci lebih dari 8. Rumus atau formula yang digunakan sesuai dengan algoritma Caesar Cipher, karena kami menggunakan double Caesar Cipher maka jumlah angka kunci pertama dijumlahkan dengan angka kedua, mislakan jumlah angka pertama= 6 dan jumlah angka kedua = 8, maka 6+8=14 akan tetapi jika hanya seperti itu saja akan mudha dipahami oleh nkarena itu kami menambahkan formula +2 pada hasil enkripsi 6+8 bukan =14, tetapi = 16. Begitu juga sebaliknya saat proses deskripsi, perbedaanya adalah inputan dari user berupa ciphertext dan jumlah angka pertama, jumlah angka kedua harus sama dengan yang dimasukkan pada sata proses enkripsi. Output dari program ini dihitung dengan formula menggunakan tabel ASCII. Untuk lebih jelasnya alur dan langkah kerja dari aplikasi yang dibuat dapat digambarkan secara umum melalui flowchart dibawah ini :



Gambar 4. *Flowchart aplikasi*

2.3 Pembuatan Aplikasi

Aplikasi ini dibuat dengan menggunakan bahasa pemrograman php dengan aplikasi sublime. Berikut adalah source code dari algoritma yang digunakan :

```
<?php
if(!empty($_POST)){ //if do action
  $plus = $_POST['n1']+1+$_POST['n2'];
  $string = $_POST['plaintext'];
  $newstring = $_POST['plaintext'];
  if(isset($_POST['btn_encrypt'])) {//jika melakukan encrypt
    for ($i=0;$i<strlen($string);$i++) {
      $ascii = ord($string[$i]);
      $ascii = $ascii + ($plus);
      if($ascii == 90) {
          $ascii = 65;
      }
      else if($ascii == 122) {
          $ascii = 97;
      }
      else {
        $ascii++;
      }
      $newstring[$i] = chr($ascii);
    }
  }else
```

Gambar 5. *Source code Enkripsi*

```
if(isset($_POST['btn_decrypt'])) { //jika melakukan decrypt

  for ($i=0;$i<strlen($string);$i++) {
    $ascii = ord($string[$i]);
    $ascii = $ascii - ($plus+2);
    if($ascii == 90) {
        $ascii = 65;
    }
    else if($ascii == 122) {
        $ascii = 97;
    }
    else {
      $ascii++;
    }
    $newstring[$i] = chr($ascii);
  }
}
```

Gambar 6. *Source code Deskripsi*

2.4 Uji Coba Program

Pada tahap pengujian program dilakukan dengan cara perhitungan manual terlebih dahulu sehingga terdapat sinkronisasi antara perhitungan manual dengan perhitungan dari program yang dibuat. Berikut adalah perhitungan manual dari program yang dibuat :

Plaintext : Amikom sukses
Key 1 : 3
Key 2 : 4

Rumus : $E = P + (K_1+K_2+'2') \bmod 256$

A	: 65 + (3+4+2) mod 256	= 74	= J
m	: 109 + (3+4+2) mod 256	= 118	= v
i	: 105 + (3+4+2) mod 256	= 114	= r
k	: 107 + (3+4+2) mod 256	= 116	= t
o	: 111 + (3+4+2) mod 256	= 120	= x
m	: 109 + (3+4+2) mod 256	= 118	= v
(space)	: 32 + (3+4+2) mod 256	= 41	=)
s	: 115 + (3+4+2) mod 256	= 124	= |
u	: 117 + (3+4+2) mod 256	= 126	= ~
k	: 107 + (3+4+2) mod 256	= 116	= t
s	: 115 + (3+4+2) mod 256	= 124	= |
e	: 101 + (3+4+2) mod 256	= 110	= n
s	: 115 + (3+4+2) mod 256	= 124	= |

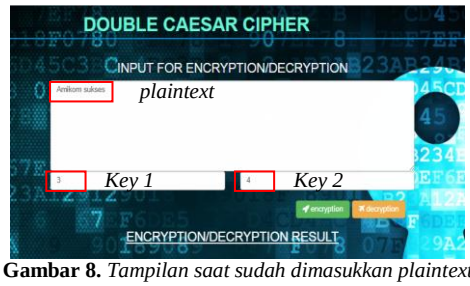
Jadi, Plaintext "Amikom sukses" dengan key 1 = 3 dan key 2 = 4 menghasilkan chipertext "Jvrtxv)|~t|n|"

Adapun aplikasi kriptografi dengan algoritma double Caesar cipher dan tabel ASCII yang sudah dibuat seperti dibawah ini :

1. Tampilan Awal
   Antar muka aplikasi

Gambar 7. *Tampilan awal aplikasi*

2. Proses Enkripsi
   Langkah-langkah enkripsi adalah sebagai berikut :
   a. memasukkan plaintext, pada contoh percobaan dibawah ini plaintext nya adalah "Amikom sukses".
   b. Memasukkan jumlah angka pertama "3".
   c. Memasukkan jumlah angka kedua "4".
   d. Klik tombol "Encryption"



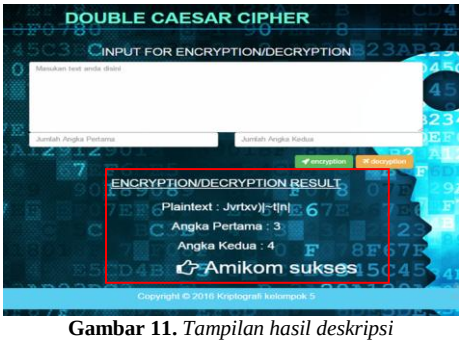
Gambar 8. *Tampilan saat sudah dimasukkan plaintext dan kunci*

   e. Setelah itu akan muncul hasil dari enkripsi pesan pada bagian bawah seperti gambar dibawah ini :

Gambar 9. *Tampilan hasil enkripsi*

3. Proses Deskripsi
   Adapun langkah-langkah saat melakukan deskripsi adalah sama seperti melakukan enkripsi. perbedaannya adalah inputan yang dimasukkan berupa ciphertext dan tombol yang dipilih tombol "Descryption".

Gambar 10. *Tampilan saat sudah dimasukkan plaintext dan kunci*



Gambar 11. *Tampilan hasil deskripsi*

Seperti gambar diatas tampilan setelah text mengalami proses deskripsi, hamper sama seperti proses enkripsi

3. Penutup

3.1 Kesimpulan

Penelitian yang sudah dilakukan menghasilkan aplikasi kriptografi berbasis web yang merupakan kombinasi algoritma Double Caesar Cipher dan Tabel ASCII. Aplikasi ini dapat melakukan proses enkripsi-deskripsi yang tidak terbatas pada 26 alphabet tetapi juga dapat mencakup semua karakter dan simbol. Pada aplikasi enkripsi-deksripsi ini juga terdapat dua key yang di inputkan user dengan batasan jumlah key maksimal 8.

Dengan demikian maka keamanan data atau pesan tetap dapat terjaga kerahasiaannya dari para kriptanalis.

3.2 Saran

Di karenakan aplikasi kriptografi dengan menggunakan algoritma *double cesar chipper dan ASCII* berbasis web ini masih memiliki beberapa kekurangan.
Maka saran yang dapat diberikan untuk pengembangan sistem agar menjadi lebih baik diantaranya :

1. Perlunya pengembangan lagi dalam penerapan algoritma *Double cesar chippe*r dan *ASCII* sehingga lebih baik dalam melakukan enkripsi.
2. Perlu pengembangan aplikasi dengan algoritma lain dan penerapan dalam media yang lebih banyak lagi selain web tentunya.
3. Perlunya interface yang lebih menarik perhatian lagi atau *eye catching* namun tetap mudah untuk digunakan.

Daftar Pustaka

[1] Ariyus, D. (2005). *Computer Security.* Yogyakarta: Andi Offset.

[2] Ariyus, D. (2006). *Kriptografi keamanan data dan komunikasi.* Yogyakarta: Graha Ilmu.

[3] **2016.** www.asciitable.com. *AsciiTable.* [Online] Desember 2016.

[4] Zulfidar, A. F. (2014). *Implementasi Pengamanan Data Menggunakan Enkripsi Caesar Cipher Dengan Menggunakan Kombinsasi Tabel ASCII.*

[5] Damai Subimawanto, F. I. (2014, Oktober 14 - 15). *Implementasi Algoritma Kriptografi Kode Caesar, Vigenere, Dan Transposisi Untuk Sistem Proteksi Penggunaan Pesan Singkat (Sms) Pada Smartphone Android. 8.*

[6] Hernawati, K. (2006). Implementasi Cipher Hill pada kode ASCII dengan Memanfaatkan Digit Desimal Bilangan Euler. *Penelitian, Pendidikan, dan Penerapan MIPA serta Peranannya dalam Peningkatan Keprofesionalan Pendidik dan Tenaga Kependidikan".* Yogyakarta: FMIPA Universitas Negeri Yogyakarta.

Biodata Penulis

Endah Handayani, mahasiswa aktif semester 5 Jurusan Teknik Informatika angkatan 2014 STMIK AMIKOM YOGYAKARTA.
Wheny Lebdo Pratitis, mahasiswa aktif semester 5 Jurusan Teknik Informatika angkatan 2014 STMIK AMIKOM YOGYAKARTA.
Achmad Nur, mahasiswa aktif semester 5 Jurusan Teknik Informatika angkatan 2014 STMIK AMIKOM YOGYAKARTA.
Syaifudin Ali Mashuri, mahasiswa aktif semester 5 Jurusan Teknik Informatika angkatan 2014 STMIK AMIKOM YOGYAKARTA.
Bagus Nugroho, mahasiswa aktif semester 5 Jurusan Teknik Informatika angkatan 2014 STMIK AMIKOM YOGYAKARTA.

ISSN : 2302-3805