Universitas Maritim Raja Ali Haji
Student Online Journal
Online ISSN 2746-8461

KOMBINASI ALGORITMA *CAESAR CIPHER* DAN *ONE TIME PAD* (OTP) UNTUK PENGAMANAN PESAN TEKS MENGGUNAKAN TABEL *ASCII*

Dwi Kurnia Vionita[1], Tekad Matulatan[2], Alena Uperiati[3]
vionitadwikurnia@gmail.com
Program Studi Teknik Informatika, Fakultas Teknik, Universitas Maritim Raja Ali Haji

Abstract

Text message security can be maintained by using cryptographic techniques. The purpose of cryptography is to make text messages that are sent difficult to read by third parties, these messages can only be read by authorized people. By using a combination of the Caesar cipher and One Time Pad (OTP) Algorithm for Text Message Security using ASCII tables, which is the text messages will be encrypted first with the Caesar Cipher algorithm then the results (ciphertext) will be re-encrypted using the One Time Pad (OTP) algorithm. Then the decryption process will be carried out using the One Time Pad algorithm first, then the results (plaintext) will be decrypted again using the Caesar Cipher algorithm. The results of the message decryption test return to the original message (plaintext) using the same key from the encryption process.

Keywords: Message Security, Caesar Cipher, One Time Pad (OTP), Plaintext, Ciphertext, ASCII

I. Pendahuluan

Caesar cipher merupakan salah satu algoritma tertua dan merupakan salah satu jenis cipher subtitusi yang membentuk cipher dengan cara melakukan pergeseran terhadap semua karakter pada plainteks dengan nilai pergeseran yang sama. Algoritma One Time Pad (OTP) pertama kali ditemukan oleh Gilbert Vernam di tahun 1917 menggunakan karakter-karakter kunci yang berisi huruf-huruf yang tersusun secara acak. Secara teoritis, teknik one-time pad merupakan teknik enkripsi yang sempurna (perfect encryption) asalkan proses pembuatan kunci benar acak (Kromodimoeljo, 2010).

Data yang di kirim merupakan data yang sangat rahasia dan penting. Dan pengiriman data tersebut melalui media seperti *Local Area Network* (LAN), internet, *email* dan media lainnya. Jika terjadi penyadapan melalui jalur pengiriman tersebut, dengan mudah penyadap dapat langsung membaca isi data tersebut karena belum dilakukan pengamanan data. Untuk menghindari terjadinya hal seperti itu, dibutuhkan suatu metode untuk mengamankan data yang akan di kirim, dimana data yang di kirim akan diacak dengan suatu metode penyadian agar data tersebut hanya bisa di baca oleh orang yang berhak.

Dalam hal tersebut, dilakukanlah penelitian dengan judul "Kombinasi Algoritma *Caesar Cipher* dan *One Time Pad* (OTP) Untuk Pengamanan Pesan Teks Menggunakan Tabel *ASCII*". Pada penelitian ini pesan teks akan di enkripsi terlebih dahulu dengan algoritma *Caesar Cipher* kemudian hasilnya (*ciphertext*) akan di enkripsi kembali menggunakan algoritma *One Time Pad* (OTP).
Kemudian untuk proses dekripsi akan dilakukan menggunakan algoritma *One Time Pad* (OTP) terlebih dahulu kemudian hasilnya (*plaintext*) akan di dekripsi kembali menggunakan algoritma caesar cipher.

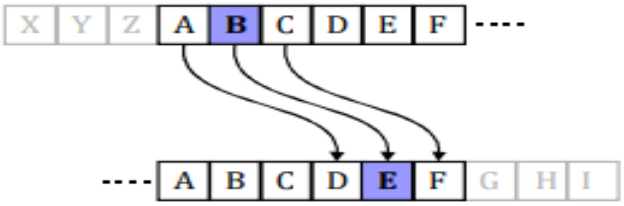
II. Metode Penelitian

2.1 Kriptografi

Secara etimologi, kriptografi berasal dari Bahasa Yunani yaitu kryptos yang bermakna tersembunyi dan graphein yang bermakna tulisan. Kriptografi adalah ilmu menulis pesan rahasia dengan tujuan menyembunyikan makna pesan tersebut (Harahap, 2016). Kriptografi adalah ilmu mengenai teknik enkripsi dimana data diacak menggunakan suatu kunci enkripsi menjadi sesuatu yang sulit dibaca oleh seseorang yang tidak memiliki kunci dekripsi. Dekripsi menggunakan kunci dekripsi mendapatkan kembali data asli. (Kromodimoeljo, 2010).

2.2 *Caesar Cipher*

Caesar cipher merupakan salah satu algoritma tertua dan merupakan salah satu jenis cipher subtitusi yang membentuk cipher dengan cara melakukan pergeseran terhadap semua karakter pada plainteks dengan nilai pergeseran yang sama. Kelemahan caesar cipher adalah kita bisa memperoleh pesan asli dengan memanfaatkan metode brute force dan presentasi frekuensi huruf yang paling sering muncul dalam suatu kalimat (Gunawan, 2018).



Gambar 1. Pergeseran pada *Caesar Cipher*

Dari gambar 2 ditunjukkan telah terjadi pergeseran 3 (tiga) buah karakter, yaitu A berubah menjadi D, B berubah menjadi E dan C berubah menjadi F dan seterusnya. Untuk mengenkripsi/ dekripsi pesan yang disusun oleh karakter-karakter teks (*ASCII*, 256 karakter), maka persamaan ditulis sebagai berikut (Munir, 2004):

$$C_i = E(P_i) = (P_i + K) \bmod 256$$
$$P_i = D(C_i) = (C_i - K) \bmod 256$$

2.3 *One Time Pad* (OTP)

Pada tahun 1949, Shannon mathematically membuktikan bahwa OTP dapat mencapai informasi secara teoritis keamanan, yaitu kerahasiaan yang sempurna bahkan dapat diperoleh musuh dengan kekuatan komputasi tak terbatas. Sedangkan OTP adalah mampu memberikan kerahasiaan yang sempurna, penerapannya terbatas mungkin karena penyediaan kunci yang aman dan efisien (Hu dkk. 2020). Prinsip enkripsi pada algoritma OTP adalah dengan mengkombinasikan setiap karakter *plaintext* dengan satu karakter *key*. Karena itu panjang key harus sama dengan panjang *plaintext.* Secara teoritis, tidak mungkin untuk mendeskripsi *ciphertext* tanpa kuncinya karena bila *key* yang digunakan adalah *key* yang salah maka yang diperoleh bukan *plaintext* yang seharusnya. Setiap *key* hanya boleh digunakan untuk sekali pesan, pengambilan dilakukan secara acak agar tidak dapat diterka, dan jumlah karakter *key* harus sebanyak jumlah karakter pesan (Siregar dan Hasrul, 2016).

Tabel **1**. Operasi *XOR* (Kromodimoeljo, 2010)

Bit naskah	Bit kunci	Bit hasil operasi
0	0	0
1	0	1
0	1	1
1	1	0

Suhardi (2016) Algoritma enkripsi menggunakan *XOR* adalah dengan meng-*XOR*-kan *plaintext* (P) dengan kunci (K) menghasilkan *ciphertext* (C):

$$C = P \oplus K$$

Algoritma dekripsi menggunakan *XOR* adalah dengan meng-*XOR*-kan *ciphertext* (C) dengan kunci (K) menghasilkan *plaintext* (P):

$$P = C \oplus K$$

2.4 Kombinasi Algoritma Caesar Cipher dan One Time Pad (OTP)

Kombinasi *Caesar cipher* dan algoritma *One Time Pad* (OTP) bertujuan untuk mengatasi kelemahan dari *Caesar cipher*, karena *Caesar cipher* bekerja hanya dengan melakukan pergeseran karakter, sehingga memungkinkan untuk dipecahkan dengan menggunakan *brute force.* Metode *brute force* yang paling sering digunakan adalah dengan menggunakan statistika frekuensi kemunculan huruf yang paling sering muncul. Kombinasi *Caesar cipher* dengan algoritma OTP bekerja dengan cara mengenkripsi pesan terlebih dahulu dengan *Caesar cipher*, selanjutnya hasil pesan (*ciphertext*) dienkripsi kembali menggunakan OTP, sehingga pola kemunculan statistika dari pesan tidak dapat dideteksi.

2.5 Tabel *ASCII*

Kode *Standart* Amerika untuk pertukaran informasi atau *ASCII* (*American Standart Code for Information Interchange)* merupakan suatu *standart* internasional dalam kode huruf dan simbol seperti *Hex* dan *Unicode* tetapi *ASCII* lebih bersifat universal, contohnya 124 adalah untuk karakter "|". Ia selalu digunakan oleh komputer dan alat komunikasi lain untuk menunjukkan teks. Kode *ASCII* sebenarnya memiliki komposisi bilangan biner sebanyak 7 bit. Namun, ASCII disimpan sebagai sandi 8 bit dengan menambahkan satu angka 0 sebagai bit *significant* paling tinggi. Bit tambahan ini sering digunakan untuk uji prioritas. Karakter *control* pada *ASCII* dibedakan menjadi 5 kelompok sesuai dengan penggunaan yaitu berturut-turut meliputi *logical communication*, *Device control*, *Information separator*, *Code extention,* dan *physical communication*. *Code ASCII* ini banyak dijumpai pada papan ketik (keyboard) komputer atau instrument-instrumen digital.

Jumlah kode *ASCII* adalah 255 kode. Kode *ASCII* 0...127 merupakan kode *ASCII* untuk manipulasi teks sedangkan kode *ASCII* 128-255 merupakan kode *ASCII* untuk manipulasi grafik. Kode *ASCII* sendiri dapat dikelompokkan lagi kedalam beberapa bagian:

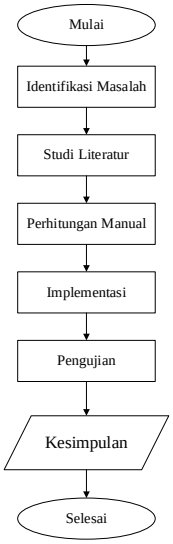
1. Kode yang tidak terlihat simbolnya seperti kode 10 (Line Feed), 13 (Carriage Return), 8 (Tab), 32 (Space).
2. Kode yang terlihat simbolnya seperti abjad (A...Z), numerik (0...9), karakter khusus (~!@#$%^&*()_+?:{}).
3. Kode yang tidak ada dikeyboard namun dapat ditampilkan. Kode ini umumnya untuk kode-kode grafik (Zaen dan Tantoni, 2018).

2.6 Bahan atau Materi Penelitian

Bahan penelitian yang digunakan dalam penelitian adalah data berupa teks.

2.7 Kerangka Pikir Penelitian

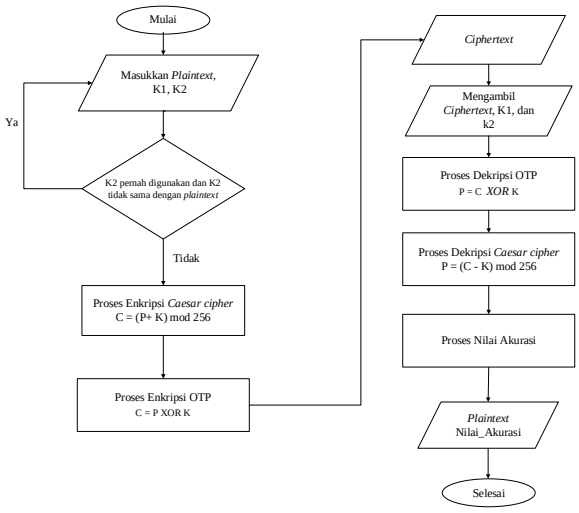
Kerangka pikir penelitian ditunjukkan pada gambar 2 sebagai berikut:



Gambar 2. Kerangka Pikir Penelitian

Kerangka pikir penelitian diawali dengan dimulai dengan mengidentifikasi masalah, mencari masalah di mana sutu objek tertentu sebagai suatu masalah. Selanjutnya Studi literatur dengan mencari referensi informasi yang diperoleh dari jurnal-jurnal ilmiah, dan hasil-hasil penelitian mahasiswa dalam berbagai bentuk misalnya skripsi, tesis, laporan praktikum, dan sebagainya. Selanjutnya focus penelitian dalam melakukan penelitian, kemudian membangun aplikasi. Setelah aplikasi selesai maka akan dilakukan pengujian, jika aplikasi sesuai dengan yang diharapkan maka peneliti menarik kesimpulan jika tidak maka Kembali ke proses pembangunan aplikasi dan selesai.

2.8 Flowchart Enkripsi dan Dekripsi



Gambar 3. *Flowchart* Enkripsi dan Dekripsi

Pada gambar 3 sistem melakukan proses input *plaintext*, K1 dan K2 terlebih dahulu, kemudian sistem akan dilakukan pengecekan apakah K2 pernah digunakan dan K2 tidak sama panjang dengan *plaintext* jika ya maka akan kembali ke proses penginputan lagi jika tidak maka akan dilakukan proses enkripsi dengan algoritma *Caesar cipher* kemudian hasilnya (*ciphertext*) akan di enkripsi lagi menggunakan algoritma *One Time Pad* (OTP) kemudian sistem akan mengeluarkan *output* berupa *ciphertext*. Kemudian pada saat proses dekripsi sistem akan mengambil *ciphertext*, K1 dan K2, kemudian proses dekripsi dilakukan dengan menggunakan algoritma *One Time Pad* (OTP) terlebih dahulu kemudian hasilnya (*plaintext*) akan di dekripsi lagi menggunakan algoritma *Caesar Cipher*. Kemudian sistem melakukan proses nilai akurasi dengan membandingkan *plaintext* inputan dengan *plaintext output* dari proses dekripsi, hasilnya adalah berupa *plaintext* dan nilai akurasi.

III. Hasil dan Pembahasan

3.1 Hasil Penelitian

Data yang akan digunakan pada penelitian adalah beberapa data berjenis teks.

3.2 Pengujian dan hasil Enkripsi dan Dekripsi

Pengujian dilakukan untuk mengetahui apakah teks dapat di enkripsi dan kemudian dapat di dekripsi Kembali ke pesan semula (*plaintext*).

Tabel 2. Hasil Pengujian

No	*Plaintext*	K1	K2	*Chipertext*	Plaintext (Hasil dekripsi)	Status
1	Kepri cyber system DISKOMINFO Kepri	3	Universitas Maritim Rajaa Ali Hajii	□□□□ Q□□□ □□;□□□□□Ng□7$31I□%;□□ □□[	Kepri cyber system DISKOMINFO Kepri	Benar
2	Kepri cyber system DISKOMINFO Kepri	7	1 2 3 4 5 6 7 8 9 10 11 12 13 14 15	cLEYC□^ \LO□M B[UT□{pkcvebu|e□cXWHE	Kepri cyber system DISKOMINFO Kepri	Benar
3	Kepri cyber system DISKOMINFO Kepri	100	%""}|{ _+)(* ~!@#$ %%%%^ !!!!@ %^&*	Šëö«±ÿç,íàþ®÷£ö˜êõ¤□ˆ'Šſ'Œ"‹'Ä□ìŠðç	Kepri cyber system DISKOMINFO Kepri	Benar
4	098765432123 4567	60	ABC ZZZ FFF WWWW	-77S(+*O(+(O'&%$	098765432123 4567	Benar
5	888 666 444 333 222 44	420	345678900987 6543212345	ïèéòíâãôèáàóáâã÷äçä÷ìí	888 666 444 333 222 44	Benar
6	747474 747474 7474	1000 005	(!)(!)(!)(!)(!)(!)	TXUQ]PM]PTXUQDUQ]P	747474 747474 7474	Benar

7	{_}{+}{=}{&}{“}{~}{#}{%}{^}{&}{**}	6	1234567891234567891234567*qwertyui	°W°µ□µ¶{º°□°µ¬µ¶¼º°□°µ□µ¶NòölñõlEê	{_}{+}{=}{&}{“}{~}{#}{%}{^}{&}{**}	Benar
8	[][][][][][][][][][]	700	I-n-f-o-r-m-a-t-i-k-a!	^4y4q4x4e4z4v4c4~4|4v8	[][][][][][][][][][]	Benar
9	!!!!!!!!!!!!!!!!!!!!??????????????	10	?_?_!_!_Teknik_Informatika_UMRAH_OK	□t□t t t□N@EB@tbEMDYFJ= "(□□□□□□□□	!!!!!!!!!!!!!!!!!!!!??????????????	Benar
10	081565486992012	45000	InformatikaAAA	±nŸ'Œ□□t—j`Ú¹¸»	081565486992012	Benar

3.3 Perhitungan Nilai Akurasi

$$\text{Nilai Akurasi} = \frac{\sum \text{proses dekripsi yang berhasil}}{\sum \text{proses uji coba}} \times 100\%$$

$$\text{Nilai Akurasi} = \frac{10}{10} \times 100\%$$

$$\text{Nilai Akurasi} = 100\%$$

IV. Kesimpulan

Berdasarkan hasil penelitian dapat disimpulkan bahwa Kombinasi algoritma *Caesar cipher* dan *One Time Pad* (OTP) dapat diimplementasikan pada aplikasi Pengamanan Pesan Teks berbasis Web, dengan mengkombinasikan algortima *Caesar cipher* dan *One Time Pad* (OTP) dapat mengamankan pesan karena sulit untuk dipecahkan dengan cara *brute force*.

V. Daftar Pustaka

Ariyus, D. dan Triwibowo, D. N., 2020, Penerapan Algoritma Coulped Linear Congurential Generator (CLCG) pada Algoritma Kriptografi One Time Pad (OTP) dalam Proses Mengamankan Pesan, *Jurnal Media Informatika Budidarma*, Vol. 4, No. 3.

Gunawan, I., 2018, Kombinasi Algoritma Caesar Cipher Dan Algoritma RSA Pengamanan File Dokumen Dan Pesan Teks, *Jurnal Nasional Informatika dan Teknologi Jaringan*, Vol. 2, No. 2.

Harahap, M. K., 2016, Analisis Perbandingan Algoritma Kriptografi Klasik Vigenere Cipher dan One Time Pad, *Jurnal Nasional Informatika dan Teknologi Jaringan*, Vol. 1, No. 1.

Hu, A., Li, G., Zhang, Z., dan Zhang, J., 2020, Encrypting Wireless Communication On the Fly Using One-Time Pad and Key Generation, *Jurnal IEEE*

Kromodimoeljo, S., 2010, Teori & Aplikasi Kriptografi, Penerbit SPK IT Consulting.

Medina, R. P., Manucom, E. M. M., dan Gerardo, B. D., 2019, Analysis of Key Randomness in Improved One-Time Pad Cryptography, *Jurnal IEEE*.

Munir, R., 2004, Diktat Kuliah IF5054 Kriptografi, Bandung.

Murhaban. dan Sutoyo, M. N., 2016, Kombinasi Algoritma Kriptografi Caesar Chiper dan Vigenere Chiper Untuk Keamanan Data, *Jurnal Mekanova*, Vol. 2, No. 1.

Santoso, N. dan Pradyatna, I., 2015, Aplikasi Messenger Kriptografi Untuk Mengamankan Pesan Teks Menggunakan Algoritma Rijndael, *Prosiding Seminar Informatika Polinema*.

Siregar, L.H. dan Hasrul, H., 2016, Penerapan Teknik Kriptografi Pada Database Menggunakan Algoritma One Time Pad, *Jurnal Elektronik Sistem Informasi dan Komputer*, Vol. 2, No. 2.

Suhardi, 2016, Aplikasi Kriptografi Data Sederhana Dengan Metode Exlusive-OR (XOR), *Jurnal Teknovasi*, Vol. 03, No. 2.

Zaen, M. T. A. dan Tantoni, A., 2018, Implementasi Double Caesar Cipher Menggunakan ASCII, *JIRE (Jurnal Informatika & Rekayasa Elektronika)*, Vol. 1, No.2.