IMPLEMENTASI KOMBINASI AFFINE CIPHER DAN ONE-TIME PAD DALAM PENGAMANAN PENGIRIMAN PESAN

[1]Ahmad Suhendri, [2]Bayu Dwi Juniansyah, [3]M Joko Priono,[4]Dedi Darwis

[123]Informatika, Universitas Teknokrat Indonesia
[4]Sistem Informasi, Universitas Teknokrat Indonesia
Jl.H. Zainal Abidin Pagar Alam 9-11, Bandar Lampung - Indonesia 35242
Telp. (0721) 702022 Fax. (0721) 702022
email : [1]ahmadsuhendri87@gmail.com, [2]bayudwij27@gmail.com, [3]jokopriono950@gmail.com, [4]darwisdedi@teknokrat.ac.id

ABSTRACT

In an exchange of messages that occur offline and online is very vulnerable to the threat of information theft with a combination of Affine Cipher and One-time Pad is expected to secure a message that is difficult to solve from information theft (Cryptanalysis).
Affine Cipher works by using the two integer and One-time Pad keys using keys that match the existing text and the key is randomly generated.
The combination of two algorithms is expected to secure information and can return back to its original form (Plainteks), so as not to cause any data lost or excessive. Plainteks, Affine Cipher, Ciphertеks, One-time Pad, Ciphertеks, Plainteks.

Keywords**:** *Cryptography, Affine Cipher, OTP.*

ABSTRAK

Dalam sebuah pertukaran pesan yang terjadi secara offline maupun online sangat rentan dengan ancaman pencurian informasi dengan kombinasi Affine Cipher dan One-time Pad diharapkan untuk mengamankan sebuah pesan yang sulit untuk dipecahkan dari pencurian informasi(Kriptanalisis).
Affine Cipher bekerja dengan menggunakan kunci dua buah bilangan integer dan One-time Pad menggunakan kunci yang sesuai dengan teks yang ada dan kunci nya dibuat secara random. Kombinasi dua buah algoritma ini diharapkan bisa mengamankan informasi dan bisa mengembalikan kembali ke bentuk aslinya(Plainteks), sehingga tidak menyebabkan adanya data yang hilang maupun berlebihan. Plainteks, Affine Cipher, Ciphertеks, One-time Pad, Ciphertеks, Plainteks.

Kata Kunci**:** *Kriptografi, Affine Cipher, OTP.*

I. PENDAHULUAN

Pada era zaman modern ini jaringan komputer memungkinkan kita untuk berkomunikasi melalui pengiriman pesan melalui sistem komputer. Salah satu nya menggunakan tulisan dan masih banyak contoh yang lain seperti suara, gambar, maupun vidio. Banyak sekali informasi yang disampaikan menggunakan tulisan(teks) dan terkadang dalam teks

tersebut terdapat informasi yang rahasia. [1]

Karena ingin menjaga kerahasiaan tersebut maka terdapat beberapa cara atau teknik tertentu untuk mengamankan pesan tersebut. Seperti hal nya kriptografi yang berfungsi untuk merubah teks menjadi kode dengan algoritma tertentu.

Affine Cipher Dan One-time Pad merupakan salah satu algoritma cipher yang sudah lama, metode Affine cipher merupakan kriptografi dengan kunci simetris, sebuah kunci yang digunakan untuk mengenkripsi dan medeskripsi itu harus sama. [2]

Sedangkan metode One-time Pad adalah algoritma dimana berisi deretan karakter-karakter kunci yang dibangkitkan secara acak dalam pengertian ini yang dimaksud dengan karakter kunci yang dibangkitkan secara acak adalah mengenkripsi sebuah pesan(teks) setiap karakter memiliki satu kunci yang bersifat random(acak). [3]

Sehingga dalam penelitian ini dapat menggabungkan dua algoritma tersebut agar dapat keamanan dari pesan dan dapat ditingkatkan walaupun dalam penggabungan tersebut akan memakan sedikit waktu, namun dengan penggabungan kedua algoritma tersebut dapat bersaing dengan algoritma modern dan supaya sulit dipecahkan oleh kriptanalisis.

II. METODE PENELITIAN

Dengan melakukan literatur terhadap beberapa sumber baikyang berasal dari buku maupun jurnal ilmiah nasional yang terkait dengan masalah pengamanan data, maka pada penelitian ini dilakukan pengamanan sebuah data khusus nya data berupa teks, dalam penelitian ini menggunakan metode-metode kriptografi klasik yaitu *Affine cipher dan One-time Pad.* Kombinasi kedua metode tersebut dibagi dalam beberapa tahap dimana metode *affine cipher* berfungsi untuk melakukan enkripsi plainteks tahap pertama sebelum dilakukan penenkripsian tahap kedua yaitu menggunakan metode *One-time Pad*. Enkripsi dengan metode *Affine cipher* dapat dinyatakan dalam perumusan

$C = a\text{P} + \text{b} \pmod{26}$

Ket :
C = Cipher Teks
a = bilangan bulat relatif prima (kunci pertama)
b = bilangan bulat relatif prima (kunci kedua)
P = Plainteks
mod 26 = untuk mengetahui sisa bagi

Kemudian untuk deskripsi pada metode *affine cipher* dapat dinyatakan

$\text{P} = a^{-1}(C - b) \pmod{26}$

Metode *One-time Pad* digunakan pada tahapan untuk meenkripsi cipher teks atau hasil enkripsi dari *Affine cipher* dan juga

digunakan mendekripsi cipher teks yang dihasilkan oleh *one-time pad* menjadi plainteks yang akan di dekripsi oleh *affine cipher*. Adapun rumus enkripsi dan dekripsi *One-time Pad* dapat dinyatakan sebagai berikut

$c_i = (p_i + k_i) \bmod 26$

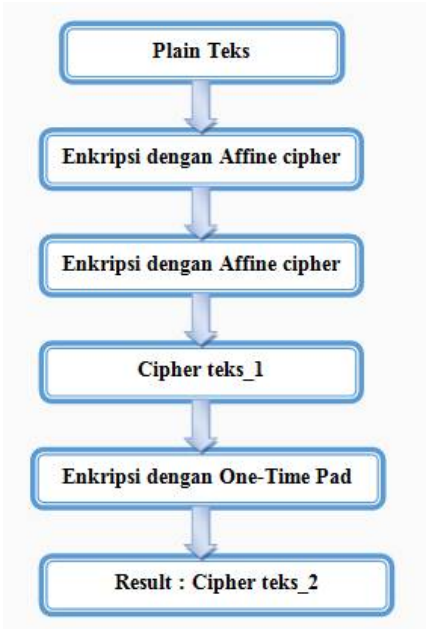
Ket :

p_i = karakter plainteks
k_i = karakter kunci
c_i = karakter cipherteks
mod 26 = untuk mengetahui sisa bagi

sedangkan untuk dekripsi pada metode *One-time Pad* dapat dinyatakan

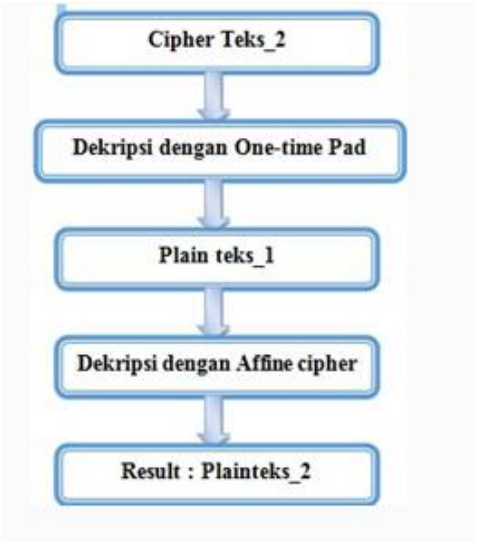
$p_i = (c_i - k_i) \bmod 26$

untuk tahapan enkripsi plainteks dengan menggunakan kombinasi dari *Affine cipher dan One-time Pad*



Gambar 1.Tahapan Enkripsi

Pada gambar 1 tersebut, dapat dilihat bahwa enkripsi diawali dengan menyiapkan plainteks yang akan kita enkripsi. Enkripsi tahap pertama dilakukan menggunakan *Affine Cipher*, dimana setelah enkripsi affine cipher akan menghasilkan cipherteks pertama, cipherteks pertama kemudian dienkripsi kembali dengan menggunakan *One-time Pad,* hasil dari kedua proses enkripsi tersebut adalah Cipher teks_2.Sedangkan untuk tahapan dekripsi dapat digambarkan sebagai berikut.Dekripsi diawali dengan sebuah cipher teks yang dihasilkan sebelumnya yang akan didekripsikan kemudian di lanjutkan dengan dekripsi tahap pertama menggunakan *One-time Pad*, yang akan dihasilkan plainteks tahap pertama. Plainteks tersebut akan di dekripsikan kembali oleh *Affine cipher* setelah melakukan dekripsi tahap kedua tersebut maka akan menghasilkan plainteks terakhir(bentuk semula).



Gambar 2 tahapan dekripsi

III. HASIL DAN PEMBAHASAN

Kombinasi Kriptografi Affine Cipher dan One-time Pad

a. Affine Cipher berkombinasi dengan *One-time Pad* Proses enkripsi ini merupakan proses dua kali peenkripsian, yang pertama enkripsi dengan Affine Cipher lalu cipherteks yang diperoleh dari peenkripsian Affine cipher dienkripsi kembali dengan menggunakan One-time Pad. Berikut adalah proses peenkripsian Affine cipher berkombinasi dengan One-time Pad.

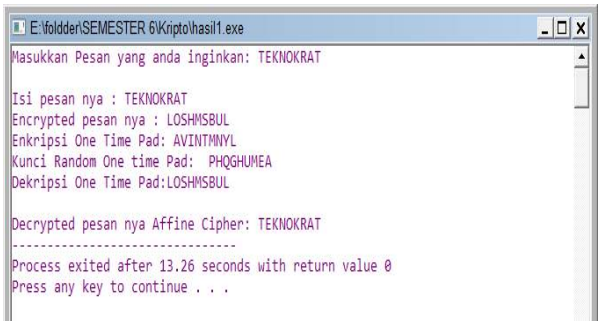
$$C = E_{otp}(E_{aff}(P))$$
$$= E_{otp}(aP + b)$$
$$= (aP + b) + K$$

Keterangan :
$Eaff$ = proses enkripsi *affine cipher*
$Eotp$ = proses enkripsi *one time pad*
P = *plaintext*
= *ciphertext*
a, = kunci untuk *affine cipher*
= kunci untuk *one time pad cipher*

Dan berikut ini adalah proses pendekripsian *one time pad cipher* berkombinasi dengan *affine cipher:*

$$P = D_{aff}(D_{otp}(C))$$
$$= D_{aff}(C - K)$$
$$= a^{-1}((C - K) - b)$$

Keterangan :
D_{otp} = proses dekripsi *one time pad*
D_{aff} = proses dekripsi *affine cipher*



Gambar 3. Tampilan Program

Pada gambar 3 merupakan tampilan program dengan contoh : Plainteks "TEKNOKRAT" diubah kedalam kode ASCII karakter menjadi (84, 69, 75, 78, 79, 75, 82, 65, 84) dienkripsi ke Affine cipher dengan kunci a=5 dan b=7 dan di mod 26, kemudian dalam hasil ASCII tersebut akan diubah kembali ke huruf, dimana huruf tersebut disusun dimulai dengan angka 0. Berikut adalah proses enkripsi dan dekripsi algoritma Affine cipher berkombinasi dengan One-time Pad :

c_1 = 5 x 84 + 7 mod 26
c_1 = 11
c_2 = 5 x 69 + 7 mod 26
c_2 = 14
c_3 = 5 x 75 + 7 mod 26
c_3 = 18
c_4 = 5 x 78 + 7 mod 26
c_4 = 7
c_5 = 5 x 79 + 7 mod 26
c_5 = 12
c_6 = 5 x 75 + 7 mod 26
c_6 = 18
c_7 = 5 x 82 + 7 mod 26
c_7 = 1
c_8 = 5 x 65 + 7 mod 26
c_8 = 20
c_9 = 5 x 84 + 7 mod 26
c_9 = 11

Diperoleh C = (11, 14, 18, 7, 12, 18, 1, 20,11) hasil dari enkripsi Affine Cipher, dan dalam program ini memiliki kunci random(P, H, Q, G, H, U, M, E, A), jika dibuat dalam bentuk angka maka (15, 7, 16, 6, 7, 20, 12, 4, 0).

Dan terakhir meenkripsi C menggunakan One-time Pad dengan kunci K.

$c'_1 = 11 + 15 \ mod \ 26$
$c_1 = 0$
$c'_2 = 14 + 7 \ mod \ 26$
$c_2 = 21$
$c'_3 = 18 + 16 \ mod \ 26$
$c_3 = 8$
$c'_4 = 7 + 6 \ mod \ 26$
$c_4 = 13$
$c'_5 = 12 + 7 \ mod \ 26$
$c_5 = 19$
$c'_6 = 18 + 20 \ mod \ 26$
$c_6 = 12$
$c'_7 = 1 + 12 \ mod \ 26$
$c_7 = 13$
$c'_8 = 20 + 4 \ mod \ 26$
$c_8 = 24$
$c'_9 = 11 + 0 \ mod \ 26$
$c_9 = 11$

Diperoleh C'(0, 21, 8, 13, 19, 12, 13, 24, 11).

Jadi plainteks "TEKNOKRAT" dienkripsi dengan metode Affine cipher dikombinasikan dengan One-time Pad menjadi "AVINTMNYL" dengan a^{-1} sama seperti sebelumnya dan rumus pendekripsian Affine cipher berkombinasi dengan One-time Pad bisa dikembalikan menjadi plainteks "TEKNOKRAT" melalui tahapan didekripsi.

IV. SIMPULAN

Berdasarkan rumusan masalah dalam penelitian terdapat beberapa kesimpulan diantaranya sebagai berikut :

a) Kunci dari One-time Pad dapat dibangun dari beberapa formula, dan kunci tersebut memiliki sistem random dimana seseorang sulit untuk memecahkan kunci tersebut.
b) Peenkripsian dan pendekripsian dari kedua algoritma tersebut menggunakan beberapa konsep matematik dimana konsep matematik tersebut memiliki beberapa tahapan diantaranya komposisi fungsi, kongruensi, faktor persekutuan terbesar dan grup.
c) Dengan adanya kombinasi kedua algoritma tersebut dapat mengamankan sebuah pesan dengan aman tanpa harus diketahui kriptanalisis.

SARAN

Dari hasil penelitian yang diperoleh, terdapat beberapa saran yang perlu diperhatikan agar menjadi lebih baik untuk selanjutnya diantara sebagai berikut :

1) Penerapatan algoritma kriptograpi dalam pengamanan pesan dapat menggunakan metode lain.
2) Penggunaan algoritma Affine Cipher, dan One-time Pad untuk

meningkatkan keamanan pesan bisa dijadikan sebagai referensi agar dapat dikembangkan menjadi lebih baik.

3) Penggunaan kedua algoritma untuk proses enkripsi dan deskripsi pesan tidak terpaku pada Affine cipher dan One-time Pad saja.

Penerapan algoritma Affine cipher dan One-time Pad tidak hanya untuk di terapkan untuk pengaman pesan saja, melainkan bisa untuk pengamanan database ataupun juga untuk yang lain.

DAFTAR PUSTAKA

[1] Dian Rahmawati, Ade Candra, 2015, *Implementasi Kombinasi Caesar dan Affine Cipher untuk keamanan data teks*, Sumatera Utara

[2] Juliadi, Bayu Pri Handono, Nilamsari Kusumastuti, 2013 *Kriptografi Klasik dengan metode modifikasi Affine Cipher yang diperkuat dengan Vigenere Cipher*, Pontianak

[3] Rinaldi Munir. *Kriptografi*. Bandung:Informatika;2004

[4] Muhammad Fadlan, & Hadriansah, 2017 *Rekayasa Aplikasi Kriptografi dengan penerapan kombinasi algoritma Knapsack Merkle Hellman dan Affine Cipher*, Kota Tarakan

[5] Yoga Religia, 2015 *Implementasi Algoritma Affine Cipher dan Vigenere Cipher untuk keamanan login sistem inventori tb nita jepara*. Semarang,Informatika