INOTEK, Vol.7 Agustus 2023
ISSN: 2580-3336 (Print) / 2549-7952 (Online)
Url: https://proceeding.unpkediri.ac.id/index.php/inotek/

Optimalisasi Keamanan Data Teks Menggunakan Kombinasi Algoritma Kriptografi ElGamal Dan Vigenere Cipher

Diterima:
10 Mei 2023
Revisi:
10 Juli 2023
Terbit:
1 Agustus 2023

[1*]Bonifacius Vicky Indriyono, [2]Natalinda Pamungkas, [3]Wildan Mahmud, [4]Zudha Pratama, [5]Imelda Dimentieva, [6]Pita Mellati, [7]Sanina Quamila Putri
[1-7]Universitas Dian Nuswantoro

Abstrak— Tidak dapat disangkal bahwa perkembangan teknologi informasi saat ini menyebabkan peningkatan kebutuhan akan informasi. Peningkatan ini memicu timbulnya kejahatan terhadap informasi yang ditukar, baik dalam bentuk pencurian maupun penyadapan informasi. Akibatnya, informasi yang seharusnya bersifat rahasia menjadi dapat diakses oleh pihak yang tidak berkepentingan. Untuk menjaga kerahasiaan informasi, diperlukan metode tertentu. Salah satu metode yang bisa dipakai adalah algoritma kriptografi ElGamal dan Vigenere Cipher. Algoritma ElGamal adalah algoritma kriptografi kunci publik yang menggunakan kunci publik untuk enkripsi dan untuk dekripsi nya menggunakan kunci privat. Sementara itu, Vigenere Cipher adalah metode enkripsi alfabetik di mana teks dienkripsi melalui pergeseran karakter yang berbeda dalam teks. Penelitian ini bertujuan untuk meningkatkan keamanan pesan teks dengan menggabungkan algoritma ElGamal dan Vigenere Cipher. Hasil pengujian menunjukkan bahwa pesan teks yang dienkripsi dengan menggunakan Vigenere Cipher dan ElGamal menjadi makin sulit untuk diakses oleh pihak yang tidak berwenang karena adanya banyak pergeseran karakter serta penggunaan kunci yang lebih kompleks.
Kata Kunci—kriptografi;kriptografi asimetris;enkripsi;dekripsi;vigenere cipher; algoritma ElGamal;

Abstract— *I It is undeniable that the current advancement in information technology has led to an increased demand for information. This increase has triggered the emergence of crimes against exchanged information, both in the form of theft and interception of information. Consequently, information that should be kept confidential becomes accessible to unauthorized parties. To maintain the confidentiality of information, specific methods are required. One method that can be used is the ElGamal and Vigenere Cipher cryptographic algorithms. The ElGamal algorithm is a public key cryptography algorithm that uses a public key for encryption and a private key for decryption. On the other hand, Vigenere Cipher is an alphabetical encryption method where the text is encrypted through different character shifts within the text. This research aims to enhance the security of text messages by combining the ElGamal and Vigenere Cipher algorithms. The test results indicate that text messages encrypted using Vigenere Cipher and ElGamal become increasingly difficult to access by unauthorized parties due to multiple character shifts and the use of more complex keys.*
Keywords— *cryptography; asymmetric cryptography; encryption; decryption; vigenere cipher; ElGamal algorithm;*

Penulis Korespondensi:

Bonifacius Vicky Indriyono,
Sistem Informasi,
Universitas Dian Nuswantoro,
Email: bonifacius.vicky.indriyono@dsn.dinus.ac.id
ID Orcid: https://orcid.org/0000-0001-8805-9047

I. PENDAHULUAN

Bersama dengan kemajuan teknologi informasi di dunia, masyarakat semakin membutuhkan akses informasi dalam berbagai bentuk dan konteks. Informasi sudah menjadi kebutuhan pokok dalam keseharian semua orang dibelahan bumi manapun. Namun, pertukaran informasi antara individu dan entitas juga membawa risiko terjadinya kejahatan. Pencurian, penyadapan, dan pemalsuan informasi semakin sering terjadi, mengakibatkan informasi menjadi rentan saat dipertukarkan dan kehilangan sifat kerahasiaannya. Untuk mengatasi masalah ini, diperlukan upaya untuk menjaga kerahasiaan informasi. Salah satu metode yang umum digunakan adalah dengan cara mengenkripsi isi pesan informasi, yang dikenal dengan istilah kriptografi.. Menurut sumber [2], kriptografi merujuk pada ilmu pengetahuan yang mempelajari metode yang berkaitan dengan keamanan informasi. Sumber [3] mendefinisikan kriptografi sebagai metode untuk menjaga kerahasiaan pesan dengan mengubah teks menjadi teks sandi dengan format khusus yang isinya susah dimengerti atau bahkan disembunyikan dengan sama sekali tidak dapat dipahami. Beberapa algoritma kriptografi yang bisa digunakan ialah prosedur pemecahan ElGamal serta Vigenere Cipher. Algoritma ElGamal merupakan kriptografi kunci publik yang melakukan proses enkripsi di blok-blok teks asli, membentuk blok-blok teks tersandi, dan kemudian didekripsi balik buat menerima teks asli [4]. Menurut sumber [5] algoritma ElGamal memiliki tingkat kesulitan dalam perhitungan logaritma diskrit, sehingga sulit untuk ditembus. Algoritma ElGamal tersusun dari tiga proses dasar: pembentukan kunci, kemudian enkripsi yang membentuk sebuah blok chipertext, dan dekripsi untuk mengembalikan pesan ke nilai asli. Algoritma ElGamal merupakan jenis cipher blok, di mana enkripsi dilakukan pada blok-blok teks asli serta menghasilkan blok-blok teks tersandi, yang lalu dikembalikan menjadi pesan asli [6]. Di sisi lain, Vigenere Cipher merupakan metode enkripsi teks huruf abjad yang menggunakan sekelompok cipher Caesar yang digeser per karakter yang berbeda setiap indeknya berdasarkan huruf-huruf dalam kata kunci [7]. Penelitian ini bertujuan untuk meningkatkan tingkat keamanan pesan teks dengan menggabungkan algoritma ElGamal dan Vigenere Cipher. Hasil pengujian menunjukkan bahwa kombinasi kedua algoritma kriptografi ini membuat pesan teks semakin sulit untuk didekripsi atau dikembalikan ke bentuk semula karena penggunaan kunci yang intensif dalam proses enkripsi dan dekripsi.

Beberapa penelitian sebelumnya telah dilakukan mengenai pemanfaatan algoritma ElGamal dan Vigenere Cipher. Salah satunya adalah penelitian yang ditulis oleh [8] yang mengimplementasikan Algoritma Kriptografi ElGamal dengan Steganografi End Of File (Eof) untuk Pengamanan Email pada aplikasi Berbasis Web di Kantor Konsultan Pajak Handi. Selain

itu, ada penelitian yang ditulis oleh [9] penggunaan ElGamal untuk keamanan gambar. Penelitian ini menjelaskan konsep penggunaan algoritma ElGamal untuk mengamankan file gambar bitmap dengan format 24 bit. Berikutnya kami menemukan artikel ilmiah penggunaan Algoritma Vigenere untuk pengamanan informasi pada Aplikasi Chatting Berbasis Desktop [10], dijelaskan bagaimana teknik pengamanan data percakapan internal perusahaan menggunakan algoritma Vigenere Cipher dalam aplikasi chatting berbasis desktop. Penelitian yang dilakukan oleh [11] menerapkan Kriptografi Pesan Teks dengan yang juga menggunakan Vigenere Cipher yang diimplementasikan pada aplikasi berbasis Android. Tujuannya untuk membuat aplikasi kriptografi pesan teks pada smartphone berbasis Android menggunakan metode Vigenere Cipher. Selanjutnya, penelitian yang ditulis oleh [12] melakukan Kombinasi Kriptografi antara Algoritma Vigenere Cipher dengan Algoritma AES dalam mengamankan Teks Pesan. Disana penulis menjelaskan konsep kombinasi dua algoritma kriptografi, yaitu Vigenere Cipher dan AES, untuk pengamanan pesan teks. Selanjutnya artikel [13] berisi bagaimana Implementasi Vigenere Cipher untuk mengamankan Data Medis, dijelaskan tentang cara menyandikan citra dan menggunakan citra sebagai kunci dengan menggunakan algoritma Vigenere Cipher dalam pengamanan data medis. Selanjutnya, penelitian yang dilakukan oleh [14] melakukan Analisis dan Implementasi Gabungan antara metode Kriptografi dan Steganografi yang digunakan untuk Kunci Citra Digital. Artikel tersebut memaparkan pengembangan algoritma kriptografi dan steganografi yang menggabungkan algoritma ElGamal dan steganografi frame.

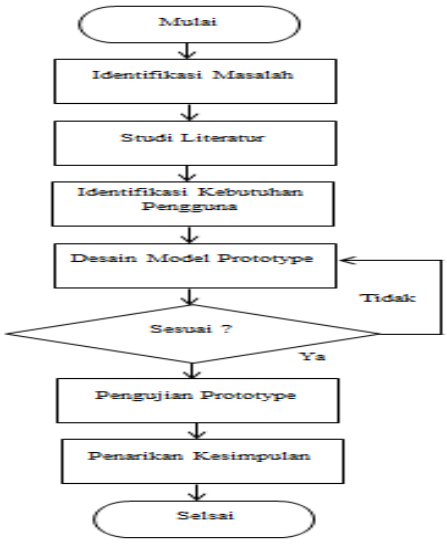
Dalam keseluruhan penelitian-penelitian tersebut, telah dilakukan berbagai pengembangan dan implementasi terkait dengan penggunaan algoritma ElGamal dan Vigenere Cipher dalam berbagai aplikasi dan skenario pengamanan informasi.

ISSN: 2580-3336 (Print) / 2549-7952 (Online)
Url: https://proceeding.unpkediri.ac.id/index.php/inotek/

II. METODE

A. Metode Penelitian

Langkah-langkah dalam metode penelitian ini ditunjukkan seperti pada gambar 1.



Gambar 1. Langkah Penelitian

B. Analisis Algoritma ElGamal

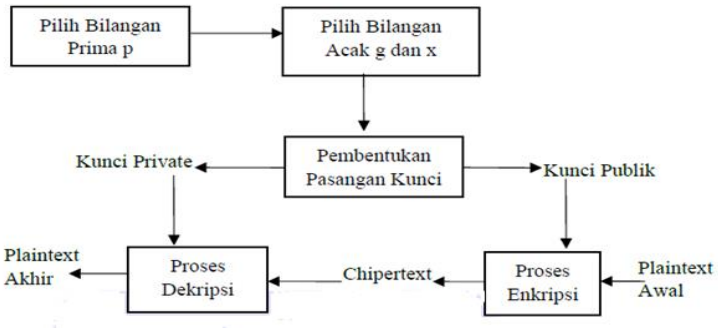
Kelebihan algoritma ElGamal ini adalah dari sisi enkripsi. Untuk teks asli yang sama, algoritma ini memberikan file hasil enkripsi yang berbeda (dengan kepastian yang dekat) setiap kali teks asli di enkripsi [15].

1. Langkah-Langkah Enkripsi ElGamal.

   Beberapa langkah diperlukan dalam menyelesaikan persoalan menggunakan metode kriptografi ElGamal antara lain [16] :

   a. Memilih sembarang bilangan prima *p*
   b. Memilih dua bilangan acak, *g* dan *x* dimana g<*p* dan 1<=*x*<=*p*-2
   c. Melakukan pembentukan pasangan kunci yaitu publik dan privat
   d. Memasukkan teks asli yang akan dienkripsi
   e. Melakukan enkripsi dengan kunci publik
   f. Keluar hasil enkripsi
   g. Melakukan proses dekripsi dengan kunci privat.

Adapun tahapan penyelesaian dengan algoritma ElGamal ditunjukkan seperti pada gambar 2.



Gambar 2. Tahap Penyelesaian ElGamal

2. Proses Pembentukan Kunci pada Algoritma ElGamal

   Dalam algoritma kriptografi ElGamal, diperlukan pasangan kunci yang dibentuk dengan pemilihan bilangan prima *p* serta dua buah bilangan acak *g* dan *x*, dengan catatan bahwa nilai bilangan acak (*g* & *x*) harus lebih kecil dari *p* sesuai persamaan.

   $$y = g^x mod\ p \qquad (1)$$

3. Proses Enkripsi pada Algoritma ElGamal

   Pada proses ini digunakan kunci publik yakni (p,g,y). Proses enkripsi algoritma ElGamal diselesaikan melalui pemilihan bilangan acak k yang berada pada himpunan $1 \leq k \leq p\text{-}2$. Pada setiap blok teks asli *m* dienkripsi menggunakan persamaan berikut :

   $a = g.k \bmod p \qquad (2)$

   $b = y.k.\ m \bmod p \qquad (3)$

4. Proses Dekripsi pada Algoritma ElGamal

   Proses dekripsi ElGamal membutuhkan kunci privat x dan p untuk melakukan dekripsi a dan b sehingga terbentuk kembali plaintext (m) pada persamaan berikut :

   m = b . a ^ (p-1-x) mod p (4)

   $(ax)\text{-}1 = a^{p-1-x} \bmod p \qquad (5)$

C. Enkripsi Vigenere Cipher

Proses enkripsi dengan Vigenere Cipher dapat menggunakan sebuah tabel/array yang terdiri dari x baris untuk mengenkripsikan teks asli [17]. Untuk proses enkripsi dan dekripsi pada algoritma Vigenere Cipher digunakan persamaan berikut :

Proses enkripsi : Cn = (Pn + Kn) mod x (6)

Proses dekripsi : Pn = (Cn – Kn) mod x jika Cn-Kn > 0 (7)

Pn = ((Cn - Kn)+x) mod 26 jika Cn-Kn < 0 (8)

Dimana :

ISSN: 2580-3336 (Print) / 2549-7952 (Online)
Url: https://proceeding.unpkediri.ac.id/index.php/inotek/

C = Ciphertext (Pesan Acak)

P = Plaintext (Pesan Asli)

K = Kunci

x = Panjang Tabel/Arrray dari kamus

III. HASIL DAN PEMBAHASAN

A. Perhitungan Enkripsi ElGamal kombinasi dengan Vigenere

Berikut ini diberikan contoh proses enkripsi dan dekripsi menggunakan kombinasi algoritma ElGamal dengan Vigenere Cipher.

1. Teks Asli = “DATA RAHASIA”
2. Dari teks asli, karakter diubah sesuai dengan Kode ASCII sehingga bernilai **68 65 84 65** 32 82 65 72 65 83 73 65.
3. Dari teks asli akan di contohkan memproses teks : **Data** dengan kode insput ASCII **68 65 84 65,** sehingga nilai M (teks asli)= 68658465.
4. Ditentukan bilangan prima (p): 541, Generator (g): 10, Kunci publik (h): 259

Enkripsi Pesan Teks :

Dalam langkah persiapan, kita sudah memiliki kunci publik (p, g, h). Diberikan pesan M = 68658465 yang ingin dienkripsi dan bilangan acak r = 137, langkah-langkah enkripsi adalah sebagai berikut:

1. Hitung elemen pertama dari ciphertext: c1 = g^r mod p = 10^137 mod 541 = 458.
2. Hitung elemen kedua dari ciphertext: c2 = (h^r * M) mod p = (259^137 * 68658465) mod 541 = 49, sehingga, ciphertext yang dihasilkan dari pesan M = 68658465 adalah (c1, c2) = (458, 49).

Selanjutnya untuk melapisi Elgamal dengan Vigenere maka ada sedikit penyesuaian tabel aplhabet yang digunakan, mengingat chipertext hasil Elgamal adalah angka, dan juga kita akan menggunakan simbol # sebagai pemisah ketika kedua chipertext digabung menjadi satu teks. Langkah-langkah proses adalah sebagai berikut :

1. Membuat Tabel alphabet Modifikasi pada array: A = [1, 2, 3, 4, 5, 6, 7, 8, 9, 0, '#']
2. Konversi Plaintext dan Kunci ke Angka: Plaintext: "458#49" -> Konversi setiap karakter menjadi angka berdasarkan posisi dalam array : [4, 5, 8, 11, 4, 9]. Misal Kunci: "123", kemudian dikonversi setiap karakter dalam array: [1, 2, 3]
3. Plaintext angka: [4, 5, 8, 11, 4, 9]
4. Kunci angka: [1, 2, 3] sehingga menjadi [1, 2, 3, 1, 2, 3]
5. Ciphertext angka: [(4 + 1) % 11 = 5, (5 + 2) % 11 = 7, (8 + 3) % 11 = 0 , (11 + 1) % 11 = 1, (4 + 2) % 11 = 6 , (9 + 3) % 11 = 1] = 570161

Deskripsi Pesan Teks Lapisan Vigenere Cipher :

Untuk proses deskripsi, langkah awal adalah mendeskripsi lapisan Vigenere. Ciphertext yang dihasilkan "570161" di konversi kembali ke karakter menggunakan tabel alfabet sehingga prosesnya adalah : Plaintext angka: [(5- 1) % 11 = 4 , (7- 2) % 11 = 5, (11- 3) % 11 = 8 , (11 - 0) % 11 = 11 , (6 - 2) % 11 = 4 , (12 - 3) % 11 = 9] = 4, 5, 8, 11, 4, 9 = **4, 5, 8,** #, **4, 9 = 458 , 49**

Deskripsi Pesan Teks Lapisan Elgamal :

Setelah berhasil mendekripsi lapisan pertama yang terlindungi oleh enkripsi Vigenere Cipher, selanjutnya hasil proses di dekripsi kembali dengan ElGamal.

1. Diketahui kunci publik: (p, g, h) = (541, 10, 259)
2. Ciphertext: (c1, c2) = (**458**, **49**)

Langkah Deskripsi:

1. Diberikan ciphertext (c1, c2) = (458, 49), langkah-langkah berikut dilakukan untuk mendekripsi pesan tersebut:
2. Hitung shared secret: s = (c1^x) mod p = (458^x) mod 541.
3. Hitung invers modulo dari s: s_inv = s^(-1) mod p.
4. Hitung pesan asli: M = (s_inv * c2) mod p.
5. Private key x = 137 sebagai contoh, maka langkah-langkah deskripsi menjadi:
6. Hitung shared secret: s = (458^137) mod 541 = 207.
7. Hitung invers modulo dari s: s_inv = 207^(-1) mod 541 = 64.
8. Hitung pesan asli: M = (64 * 49) mod 541 = 68658465.
9. Dari hasil 68658465 kemudian di sesuaikan dengan karakter dalam tabel ASCII menjadi teks : “DATA”

IV. KESIMPULAN

Dari hasil pengujian dapat disimpulkan bahwa enkripsi yang dilakukan menggunakan kombinasi algoritma ElGamal dengan Vigenere Cipher berjalan dengan baik dan optimal. Pesan teks memiliki keamanan yang berlapis karena memiliki banyak kunci dan pergeseran apfabet yang tidak mudah ditembus perhitungannya oleh kriptanalis. Proses enkripsi berjalan dengan sangat baik dan hasil enkripsi dapat di kembalikan ke bentuk semula dengan benar serta tidak ada kerusakan pada hasil deskripsinya.

DAFTAR PUSTAKA

[1] M.M. Amin, "Implementasi Kriptografi Klasik Pada Komunikasi Berbasis Teks," Jurnal Pseudocode, vol. III, no. 2, pp. 129–136, 2016.

[2] B.S. Hasugian, "Peranan Kriptografi Sebagai Keamanan Sistem Informasi Pada Usaha Kecil Dan Menengah" Jurnal Warta, No 53, 2017, DOI: https://doi.org/10.46576/wdw.v0i53.269, ISSN. 1829 - 7463

[3] F.N. Pabokory, I.F. Astuti and A.H. Kridalaksana, "Implementasi Kriptografi Pengamanan Data Pada Pesan Teks, Isi File Dokumen, Dan File Dokumen Menggunakan Algoritma Advanced Encryption Standard", Jurnal Informatika Mulawarman, Vol. 10, No. 1, pp. 20–31, 2015.

[4] A.I. Warnilah and S.N. Nugraha, "Komparasi Algoritma Kriptografi Elgamal Dan Caesar Cipher Untuk Enkripsi Dan Dekripsi Pesan", IJCIT (Indonesian Journal on Computer and Information Technology), Vol.3, No.2, pp. 243-252, 2018.

[5] A.Y.N. Harahap, H. Gunawan, A.B. Nasution and R.E. Sari, "Penerapan Elgamal Guna Meningkatkan Keamanan Data Text dan Docx", IT Journal, Vol. 10, No. 1, pp. 76-86, 2022.

[6] Maxrizal and S. Irawadi, "Analisis Sistem Kriptografi ElGamal Untuk Membentuk Sistem Kunci Publik Berbasis Grup Non-Komutatif", Jurnal Matematika Integratif, Vol. 16, No. 2, pp. 117-125, 2020.

[7] A. Amrulloh, E.I.H.Ujianto, "Kriptografi Simetris Menggunakan Algoritma Vigenere Cipher", Jurnal CoreIT, Vol. 5, No. 2, pp. 71-77, 2019.

[8] E. Setiasih and M. Syafrullah, "Implementasi Algoritma Kriptografi Elgamal Dan Steganografi End Of File (Eof) Pada Aplikasi Pengamanan Email Berbasis Web Pada Kantor Konsultan Pajak Handi", SKANIKA, Vol. 1, No.1, pp. 316-322, 2018.

[9] M.T. Thamam, W. Dwiono and T. Hartanto, "Penerapan Algoritma Kriptografi ElGamal untuk Pengaman File Citra", Jurnal EECCIS, Vol. IV, No. 1, pp. 8-11, 2010.

[10] Marchandi and Ferdiansyah, "Implementasi Algoritma Vigenere Cipher Dalam Aplikasi Chatting Untuk Pengamanan Informasi Berbasis Desktop", SKANIKA, Vol. 1, No. 1, pp. 340-345, 2018.

[11] A.A. Permana, "Penerapan Kriptografi Pada Teks Pesan dengan Menggunakan Metode Vigenere Cipher Berbasis Android", Jurnal AL-AZHAR INDONESIA SERI SAINS DAN TEKNOLOGI, Vol. 4, No. 3, pp. 110-115, 2018.

[12] H. Triansyah, A. Pratama, M.H.D.F. Syahputra and I. Gunawan, "Kombinasi Kriptografi Algoritma Vigenere Cipher Dan Algoritma Aes Untuk Pengamanan Pesan Teks", TECHSI, Vol. 11, No. 3, pp. 408-418, 2019.

[13] A. Riski, A. Kamsyakawuni and M. Z. Arif, "Implementasi Vigenere Cipher Pada Pengamanan Data Medis", Vol. 02, No. 01, pp. 23-30, 2019.

[14] I.K.R.Y. Negara and E. Triandini, "Analisis Dan Implementasi Gabungan Kriptografi Elgamal Dan Steganografi Frame Dengan Menggunakan Kunci Citra Digital", EKSPLORA INFORMATIKA, Vol. 3, No. 2, pp. 141-150, 2014.

[15] F. Al-Anshori and E. Aribowo, "Implementasi Algoritma Kriptografi Kunci Publik Elgamal Untuk Proses Enkripsi Dan Dekripsi Guna Pengamanan File Data", Jurnal Informatika, Vol. 2, No.2, pp. 376-384, 2014.

[16] S.N. Nugraha, "Implementasi Algoritma Kriptografi Elgamal Untuk Enkripsi Dan Dekripsi Pesan.", Tugas Akhir, Program Studi Manajemen Informatika, AMIK BSI Tasikmalaya, 2018.

[17] M.R. Darmawan and Windarto, "Implementasi Algoritma Kriptografi Vigener Cipher Dan Affine Cipher Untuk Mengamankan Pesan Pada Aplikasi Chatting Berbasis Android", Jurnal SKANIKA, Vol. 1, No. 2, pp. 583-590, 2018