KLIK: Kajian Ilmiah Informatika dan Komputer
ISSN 2723-3898 (Media Online)
Vol 4, No 2, Oktober 2023, Hal 1143-1153
DOI 10.30865/klik.v4i2.1277
https://djournals.com/klik

Penerapan Metode Elgamal Untuk Mengamankan Teks Pada File Dokumen Word

Abdul Halim Hasugian, Raissa Amanda Putri, Annisa Shafira Zuhri*

Fakultas Sains Dan Teknologi, Program Studi Ilmu Komputer, Universitas Islam Sumatera Utara, Medan, Indonesia
Email: [1]abdulhalimhasugian@gmail.com, [2]raissa.ap@uinsu.ac.id, [3,*]zuhriannisa1@gmail.com
Email Penulis Korespondensi: zuhriannisa1@gmail.com

Abstrak−Teks yang mengandung banyak karakter di dalamnya selalu menimbulkan masalah pada media penyimpanan dan kecepatan waktu selama pengiriman data. file teks adalah file yang berisi informasi dalam bentuk teks. data yang berasal dari dokumen pengolah kata, angka yang digunakan dalam perhitungan, nama dan alamat pada database adalah contoh input data teks yang terdiri dari karakter, angka dan tanda baca. Masalahnya adalah jika file teks tersebut berisi informasi penting dan dicuri maka pencurinya dapat mengeksploitasi data yang dicuri menjadi informasi yang menguntungkan dan jika data tersebut dirusak maka pemilik data mengalami kerugian. oleh karena itu perlu diterapkan keamanan pada file teks. Penelitian ini menggunakan metode elgamal untuk keamanan file teks penting. dengan keamanan menggunakan metode elgamal, file teks penting memiliki keamanan yang baik. Algoritma ini didasarkan atas masalah logaritma diskret pada grup $\mathbb{Z}P^*$. Algoritma ElGamal terdiri dari tiga proses, yaitu proses pembentukan kunci, proses enkripsi dan proses dekripsi. Algoritma ini merupakan cipher blok, yaitu melakukan proses enkripsi pada blok-blok plainteks dan menghasilkan blok-blok cipherteks yang kemudian dilakukan proses dekripsi, dan hasilnya digabungkan kembali menjadi pesan yang utuh dan dapat dimengerti. Hasil penelitian, dapat ditarik kesimpulan bahwa mengimplementasikan aplikasi kerahasiaan pesan maka dapat mengamankan *file microsoft word*. Hasilnya adalah aplikasi ini sangat bermanfaat untuk mengamankan dokumen agar isinya tidak diketahui oleh orang lain yang tidak berhak. Program ini menghasilkan aplikasi dengan menggunakan langkah dan rumus dari algoritma elgamal, kemudian mengubah isi teks pada *file microsoft word* sebagai *input* nya maka algoritma elgamal dapat diterapkan dan berubah menjadi kode-kode yang tidak dikenal (*chipertext*). Dengan menggunakan pemrograman *visual basic* 2012 kemudian menerapkan algoritma atau tahapan dari elgamal maka dapat menghasilkan aplikasi Penerapan Metode Elgamal Untuk Mengamankan *File Microsoft Word*.

Kata Kunci: Sifat listrik; Kinerja DSSC; Partikel nano Au; Probe empat titik.

Abstract−Text that contains a lot of characters always causes problems with storage media and time speed during data transmission. Text files are files that contain information in text form. data originating from word processing documents, numbers used in calculations, names and addresses in databases are examples of input text data consisting of characters, numbers and punctuation marks. The problem is that if the text file contains important information and is stolen, the thief can exploit the stolen data into profitable information and if the data is damaged then the data owner suffers a loss. therefore it is necessary to apply security to text files. This research uses the Elgamal method for security of important text files. with security using the elgamal method, important text files have good security. This algorithm is based on the discrete logarithm problem on the group $\mathbb{Z}P^*$. The ElGamal algorithm consists of three processes, namely the key formation process, the encryption process and the decryption process. This algorithm is a block cipher, which carries out an encryption process on plaintext blocks and produces ciphertext blocks which are then decrypted, and the results are combined back into a complete and comprehensible message. As a result of the research, it can be concluded that implementing a secret message application can secure Microsoft Word files. The result is that this application is very useful for securing documents so that their contents are not known by unauthorized people. This program produces applications using steps and formulas from the Elgamal algorithm, then changes the text content in the Microsoft Word file as input, then the Elgamal algorithm can be applied and turned into unknown codes (ciphertext). By using Visual Basic 2012 programming and then applying the algorithm or stages of Elgamal, it can result in the application of the Elgamal Method for Securing Microsoft Word Files.

Keywords: Electrical properties; DSSC Performance; Au nanoparticles; Four point probe

1. PENDAHULUAN

Microsoft Word merupakan salah satu software yang sering digunakan di dunia pendidikan dan perkantoran, untuk mengolah kata seperti pembuatan surat, makalah, laporan, dan lain sebagainya. Oleh karena itu, setiap pekerja pendidikan dan perkantoran dituntut untuk mampu menguasai keterampilan penggunaan software Microsoft Word [1]. File Microsoft Word biasanya tidak menggunakan keamanan untuk membatasi siapa yang dapat membuka dan membaca isinya, sehingga jika file Microsoft Word berisi konten data penting maka hal ini akan merugikan pemilik file dan menguntungkan pencuri file. Oleh karena itu diperlukan suatu teknik yang dapat mengatasi permasalahan keamanan isi file Microsoft Word [2].

Implementasi merupakan proses penterjemahan dari pemodelan menjadi bentuk aplikasi sesuai dengan kebutuhan informasi pengguna. Proses implementasi adalah proses penterjemahan dari pemodelan ke dalam pengkodean atau pembentukan antarmuka [3]. Dalam ilmu komputer, teknik yang dikenal adalah kriptografi. Kriptografi merupakan ilmu yang mempelajari bagaimana menjaga data atau pesan tetap aman ketika dikirim dari pengirim ke penerima tanpa campur tangan pihak ketiga [4]. Teknik mengacak suatu pesan sehingga tidak dapat diketahui maknanya disebut dengan enkripsi, dan membentuk suatu bidang ilmu yang disebut kriptografi, namun untuk menggunakan kriptografi diperlukan suatu metode yang baik agar keamanan data menjadi lebih baik [5].

Oleh karena itu peneliti menggunakan metode Elgamal untuk keamanan teks di Microsoft Word. Algoritma Elgamal merupakan algoritma yang didasarkan pada konsep kunci publik. Algoritma ini umumnya digunakan untuk tanda tangan digital, namun kemudian dimodifikasi sehingga dapat digunakan untuk enkripsi dan dekripsi [6]. Keamanan

algoritma Elgamal terletak pada sulitnya menghitung logaritma diskrit pada modul prima yang besar, sehingga upaya penyelesaian masalah logaritma ini menjadi sulit untuk diselesaikan [7]. Algoritma ini mempunyai keunggulan pada pembangkitan kunci yang menggunakan logaritma diskrit dan metode enkripsi dekripsi yang menggunakan proses komputasi besar sehingga hasil enkripsi menjadi dua kali lipat dari ukuran aslinya [8]. Pengguanaan metode elgamal ini telah pernah dilakukan oleh [9] tentang Analisa Algoritma Elgamal Dalam Penyandian Data Sebagai Keamanan Database. Penerapan Metode Elgamal berhasil dalam mengamankan isi database menjadi isi teks rahasia yang tidak dapat dibaca oleh orang yang tidak diizinkan [10]. Demikian juga pada penelitian yang dilakukan oleh [2] tentang Perancangan Aplikasi Keamanan Pesan Menggunakan Algoritma Elgamal Dengan Memanfaatkan Algoritma One Time Pad Sebagai Pembangkit Kunci. Pemaktoran bilangan prima menjadikan kunci pada elgamal menjadi lebih kuat untuk penyandian pesan. Hasil penelitian ini menjelaskan bahwa pesan yang digunakan hanya berjenis teks sehingga tidak diterapkan pada jenis gambar atau dokumen [11]. Sedangkan penelitian yang dilakukan oleh [12] tentang Kriptografi Database Menggunakan Algoritma El-Gamal Berbasis Web didapatkan hasil bahwa data tanpa merusak isi data dengan menggunakan algoritma golongan kunci publik.

2. METODOLOGI PENELITIAN

2.1 Waktu dan Jadwal Pelaksanaan

Waktu dan jadwal pelaksaan penelitian ini menggunakan algoritma Elgamal dilakukan dalam jangka waktu kurang lebih 3 bulan, mulai dari Desember 2021 s/d Februari 2022.
Langkah-langkah metode Elgamal untuk enkrip dapat dilihat sebagai berikut [13].

a. Algoritma Pembentukan Kunci Kriptografi
Input:

1. Sembarang bilangan prima, *p*.
2. Sembarang bilangan acak *g*.
3. Sembarang bilangan acak *x*.

Proses*:*
Hitung nilai *y*, dengan persamaan:

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

Output:

1. Keluaran berupa bilangan *y*.
2. Kunci publik (*y*, g, *p*).
3. Kunci *private* (*x*, *p*).

b. Algoritma Enkripsi
Input:

1. Susun *plaintext* menjadi blok-blok *m1*, *m2*, dst.
2. Tentukan bilangan acak *k* sepanjang jumlah *plaintext*.

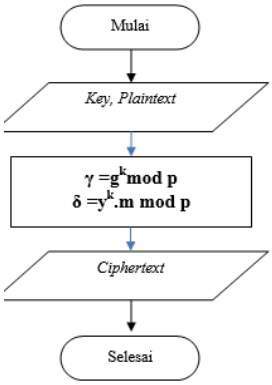
Proses*:*
Setiap blok *m* di enkripsi dengan persamaan:

$$a = gk \ mod \ p \quad (2)$$

$$b = ykm \ mod \ p \quad (3)$$

Output [14]*:*

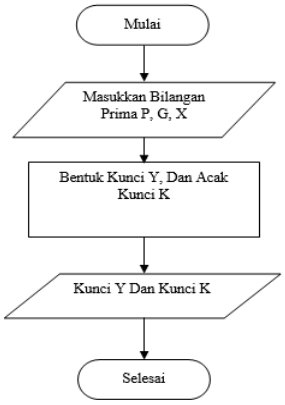
1. Pasangan *a* dan *b* adalah *ciphertext* untuk blok pesan *m*.



Gambar 1. Flowchart Enkripsi Metode Elgamal [15]

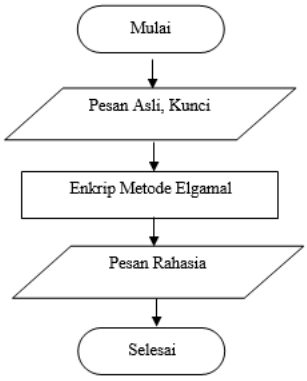
Metode Elgamal

1. *Flowchart Diagram* Pembentukan Kunci



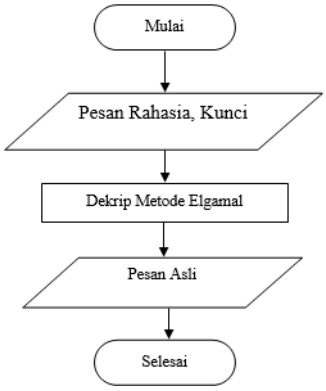
Gambar 2. Flowchart Diagram Pembentukan Kunci

2. *Flowchart Diagram* Enkrip Pesan



Gambar 3. Flowchart Diagram Enkrip Pesan

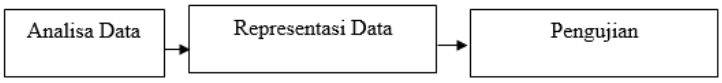
3. *Flowchart Diagram* Dekrip Pesan Rahasia



Gambar 4. Flowchart Diagram Dekrip Pesan Rahasia

2.2 Kerangka Penelitian

Kerangka dalam penelitian ini meliputi beberapa tahapan yaitu :



Gambar 5. Kerangka Penelitian

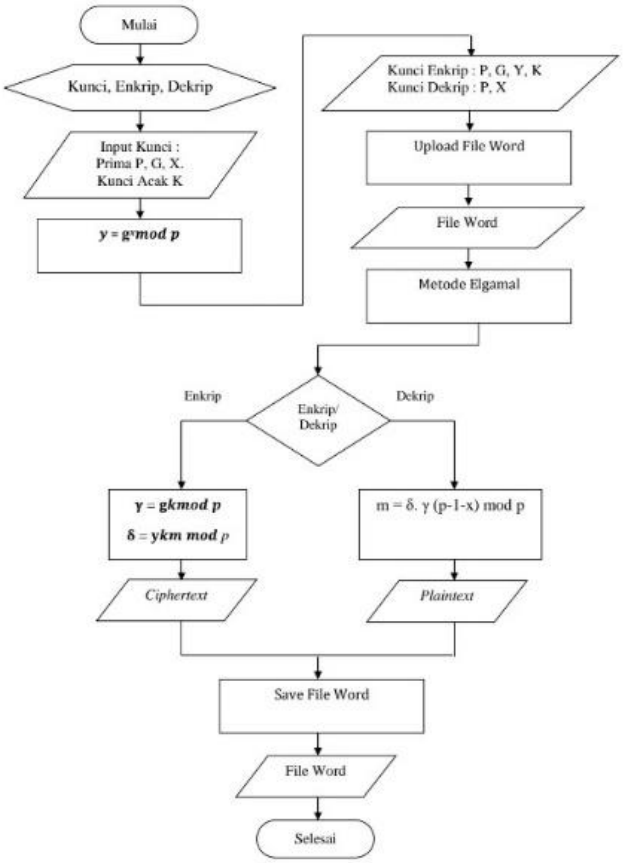
Pada analisa data, adapun hal-hal yang dibutuhkan dalam penelitian ini sebagai berikut:

a. Alat dan bahan
b. Materi lengkap mengenai metode Elgamal

c. Materi bahasa pemrograman *visual basic* untuk membantu mengimplementasian metode Elgamal dalam pengamanan data
d. Hasil dan pembahasan penelitian [16]

2.3 Perancangan Sistem

Perancangan sistem biasanya berisikan tentang pengembangan dalam tahapan kebutuhan yang diubah ke dalam *Flowchart*, diagram blok, dan lainnya, agar para peneliti dengan mudah memahami alur maupun fungsi rancangan yang akan dibuat. Dalam penelitian ini perancangan terdiri dari *Flowchart* Sistem dalam keamanan data sebagai lanjutan dari proses analisis kebutuhan [17].



Gambar 6. Flowchart Sistem

3. HASIL DAN PEMBAHASAN

3.1 Hasil Analisis Data

Maka dari itu beberapa analisis dan metode yang dibuat dalam penelitian ini adalah:

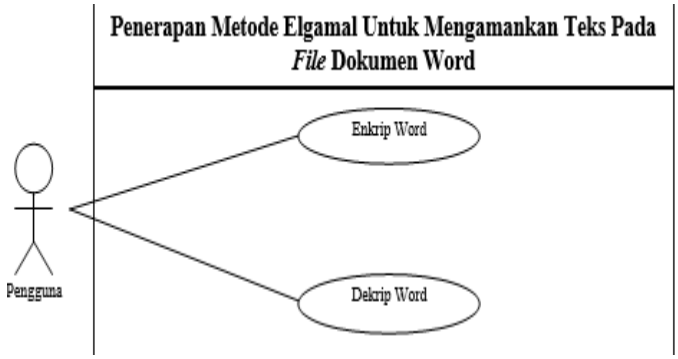
a. Teks Word
   Pada *file*yang tersimpan berisi teks yang digunakan untuk proses enkripsi dan dekripsi.
b. Metode Elgamal
   Metode elgamal digunakan untuk enkripsi dan dekripsi isi *file*word yang berupa teks.
c. Pembentukan Kunci
   Sebelum menggunakan elgamal dibutuhkan kunci yang dibentuk menggunakan bilangan prima.
d. Enkripsi Pesan Teks
   Proses enkripsi berfungsi untuk mengubah teks asli pada isi *file*word menjadi teks rahasia.
e. Dekripsi Pesan Teks
   Proses dekripsi berfungsi untuk mengubah teks rahasia pada isi *file*word menjadi teks asli [18].

3.2 Hasil Perancangan

32.1 *Unified Modelling Language* (UML)

a. *Use Case Diagram*

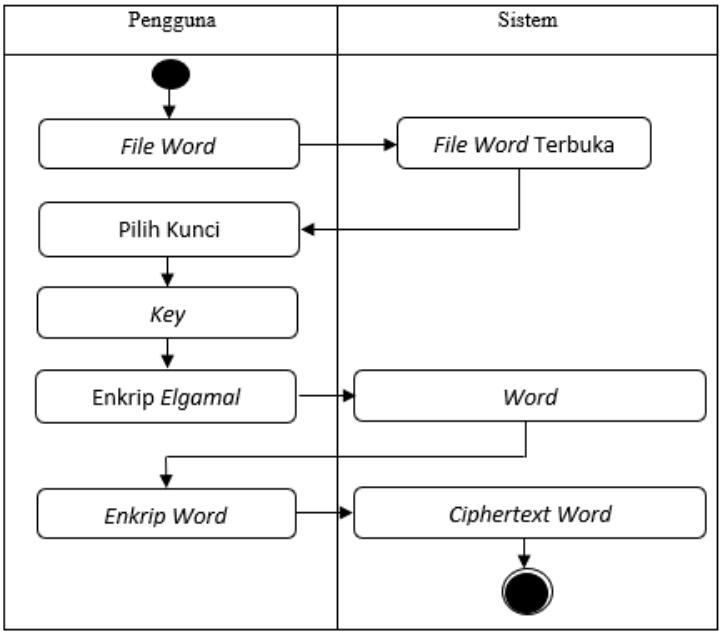
Perancangan dimulai dari identifikasi aktor dan bagaimana hubungan antara aktor dan use case didalam sistem [19]. Perancangan *Use Case* Diagram dapat dilihat pada gambar sebagai berikut:



Gambar 7. *Use Case* Penerapan Metode Elgamal Untuk Mengamankan Teks Pada *File* Dokumen Word

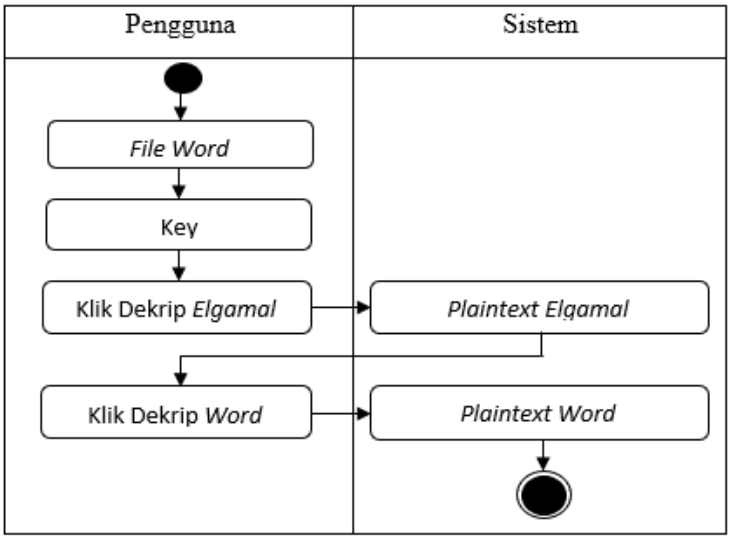
b. *Activity Diagram*

Rangkaian kegiatan pada setiap terjadi *event* sistem digambarkan pada *activity* diagram berikut :



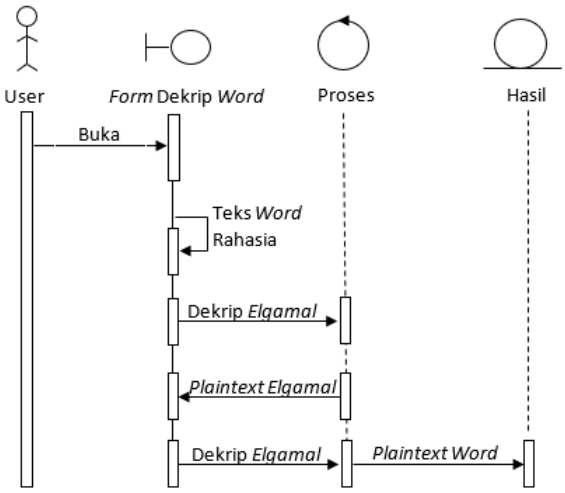
Gambar 8. *Activity Diagram Enkrip*

Serangkaian kerja melakukan enkrip dapat terlihat seperti pada Gambar 8.



Gambar 9. *Activity Diagram* Dekrip

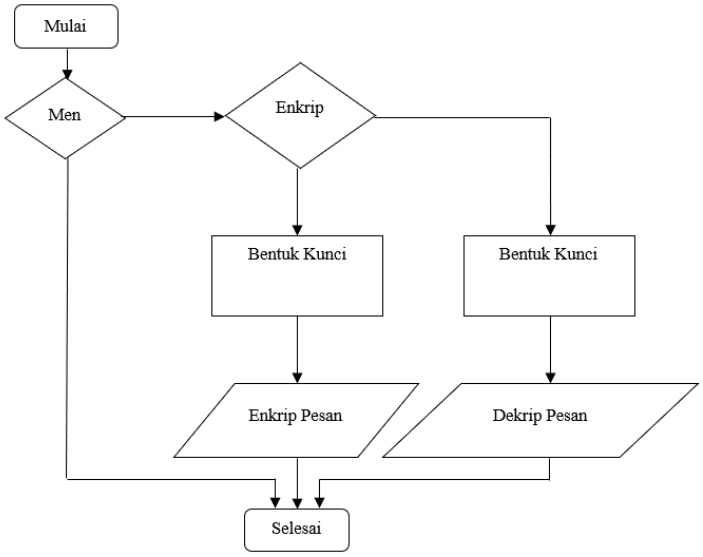
Gambar 9 menunjukkan *activity diagram dekrip*. Aktivitas yang dilakukan untuk melakukan Dekrip dapat dilihat seperti pada berikut :



Gambar 10. *Sequence Diagram* Dekrip

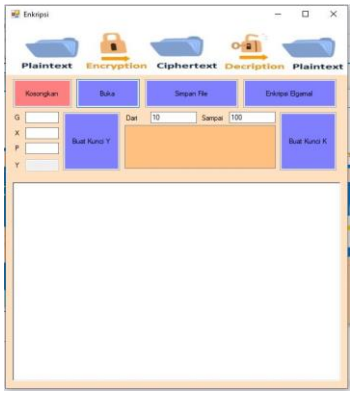
Flowchart ditujukan untuk mempermudah pembuatan program. Dalam penelitian ini *flowchart* dibuat untuk mengetahui langkah-langkah apa saja yang harus diterapkan, dalam bahasa pemrograman, agar sistem yang dibuat dapat menghasilkan output yang sesuai dengan harapan dari inputan yang dimasukkan oleh *user* berupa hasil dari proses enkripai file yang diinputkan [20].

Flowchart merupakan gambar atau bagan yang berisi proses dan penjelasan alur kerja program. *Flowchart* aplikasi yang telah dibuat terdapat pada gambar di bawah ini:



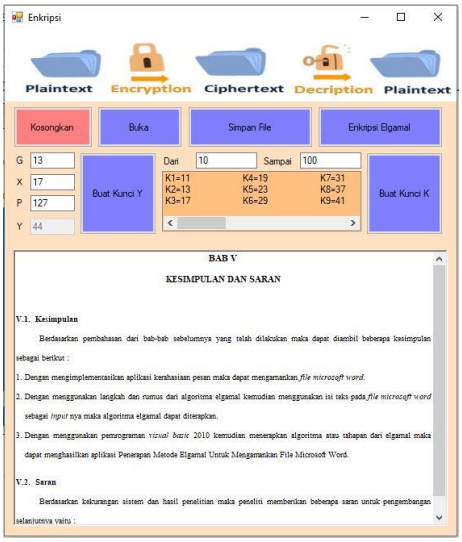
Gambar 11. Flowchart

Setelah merancang dan membuat sistem aplikasi. Kemudian langkah selanjutnya adalah menguji penerapan aplikasi metode Elgamal untuk mengamankan file Microsoft Word dan dapat dilihat pada gambar di bawah ini:



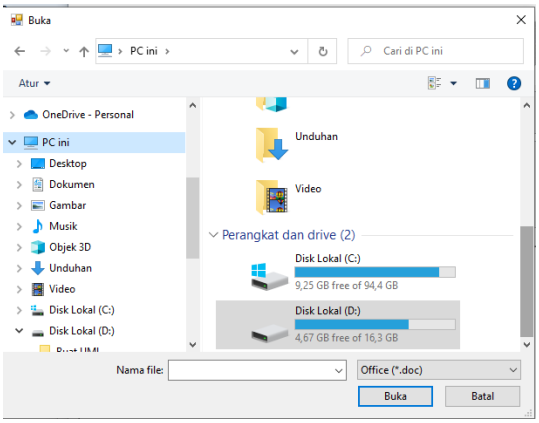
Gambar 12. Tampilan Form Enkripsi

Gambar 12 merupakan bentuk enkripsi pesan, penggunaan aplikasi dimulai dari pengambilan gambar pada tombol pencarian file, selanjutnya pengguna harus menginput kunci G, X, P dan klik tombol Buat Kunci Y. Kemudian pengguna juga harus menginput angka pada tombol from dan Until kemudian klik tombol Create Key agar semua kunci dapat terbentuk.



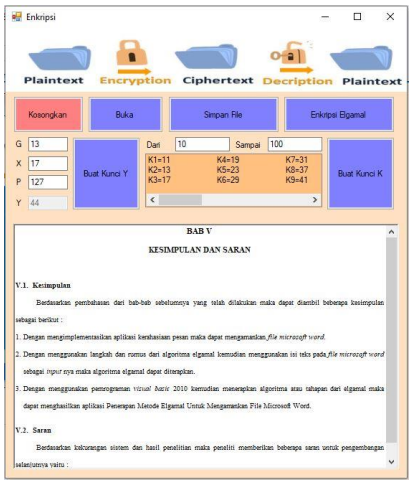
Gambar 13. Tampilan Form Pembentukan Kunci

Gambar 13 menunjukkan hasil dari form pembentukan kunci setelah enskripsi pesan dibuat. Setelahnya tekan tombol enkripsi, akan muncul jendela penyimpanan dan pengguna dipersilakan menyimpan file sesuai lokasi yang diinginkan .



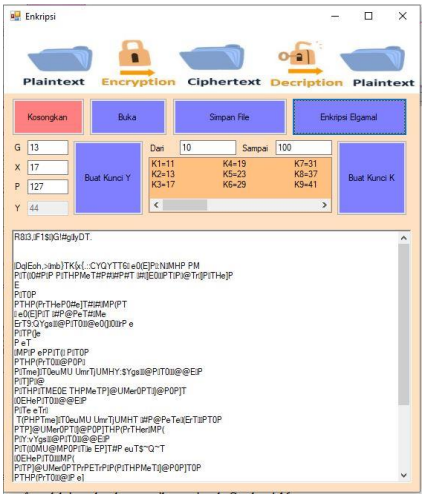
Gambar 14. Tampilan jendela pemilihan file

Setelah file word dipilih untuk dimasukkan ke dalam aplikasi, maka akan muncul tampilan seperti pada Gambar 14.



Gambar 14. Tampilan file Word yang dipilih

Setelah muncul file word maka pengguna dapat melakukan enkripsi dengan menekan tombol enkripsi elgamal maka akan muncul tampilan seperti pada Gambar 15.

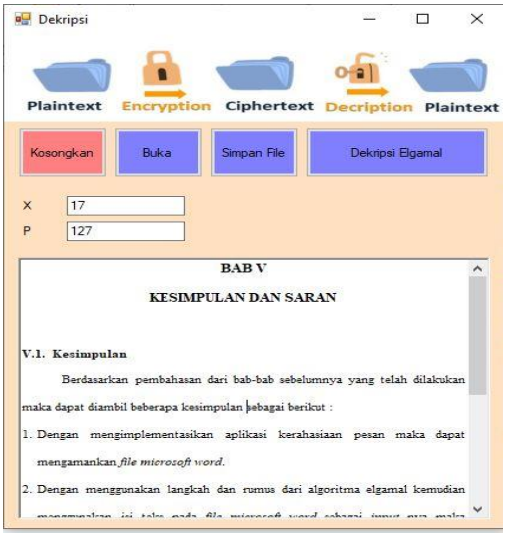


Gambar 15. Tampilan file Word terenkripsi

Jika pengguna ingin mendekripsi atau mengembalikan teks dapat menggunakan bentuk deskriptif, maka akan muncul tampilan seperti pada Gambar 16.

Gambar 16. Tampilan Form Dekripsi

Lakukan langkah pemilihan file word, kemudian pengguna memasukkan tombol X dan P dan mengklik tombol dekripsi elgamal. Akan muncul tampilan seperti pada Gambar 17.

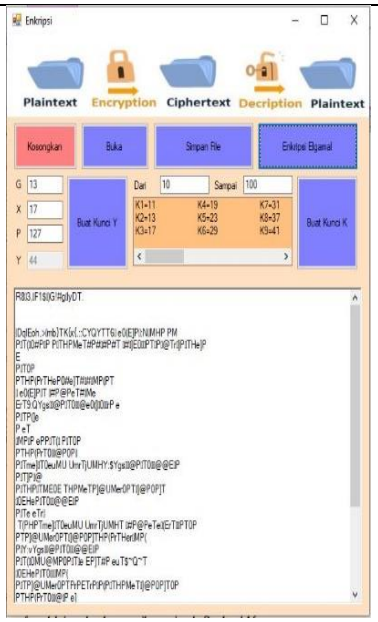
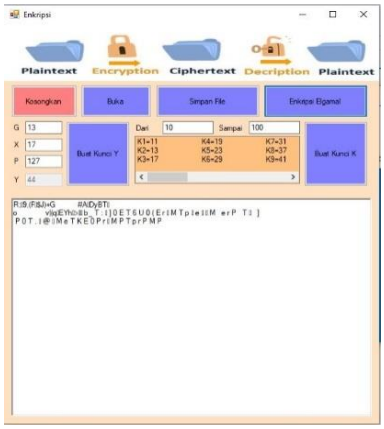
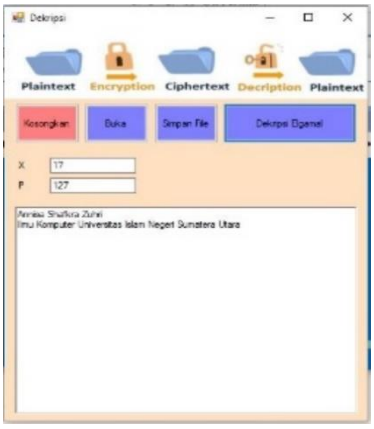
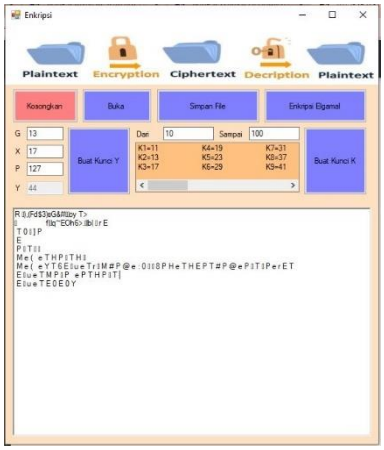
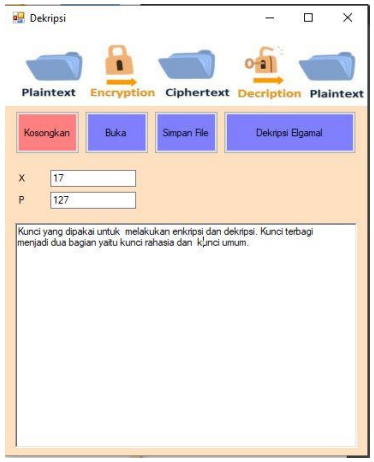


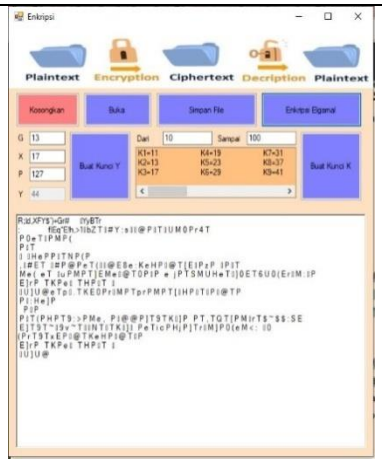
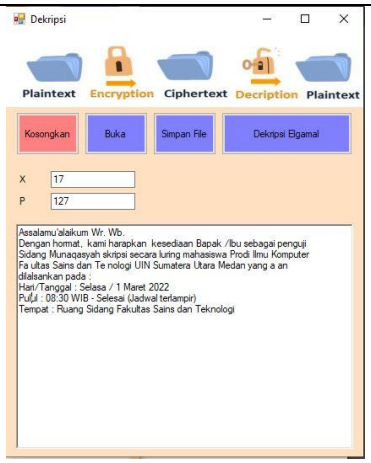
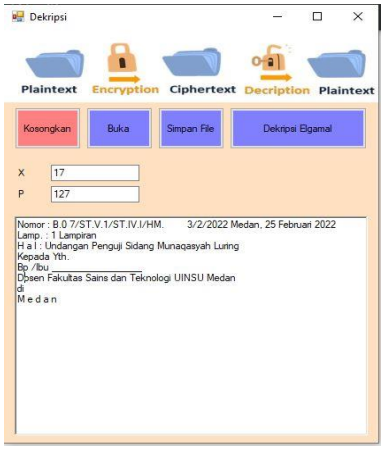
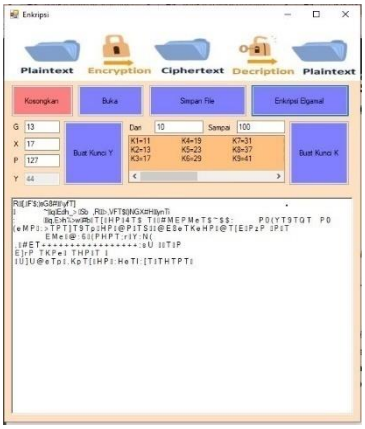
Gambar 17. Tampilan Form Hasil Dekripsi

4.2 Hasil tes

Hasil pengujian program meliputi hasil proses enkripsi dan hasil proses deskripsi. Pengujian enkripsi dan deskripsi pada penelitian ini menggunakan 5 sampel file word. Hasil pengujian enkripsi dan dekripsi teks rekaman meliputi kunci, enkripsi, deskripsi, hasil.

Table 1. Data Test Results

No	Key	Encryption	Decryption	Result
1.	Enkrip: G=13 X=17 P=127 Dekrip: X=17 P=127			Appropriate
2.	Enkrip: G=13 X=17 P=127 Dekrip: X=17 P=127			Appropriate
3.	Enkrip: G=13 X=17 P=127 Dekrip: X=17 P=127			Appropriate

4.	Enkrip: G=13 X=17 P=127 Dekrip: X=17 P=127			Appropriate
5.	Enkrip: G=13 X=17 P=127 Dekrip: X=17 P=127			Appropriate

Berdasarkan tabel pengujian diatas dapat disimpulkan bahwa program aplikasi berhasil mengenkripsi dan mendekripsi file word pada aplikasi keamanan file word.

4. KESIMPULAN

Berdasarkan hasil Penelitian maka dapat diambil kesimpulan dengan mengimplementasikan aplikasi kerahasiaan pesan maka dapat mengamankan file Microsoft Word. Hasilnya aplikasi ini sangat berguna untuk mengamankan dokumen agar isinya tidak diketahui oleh orang lain yang tidak berhak, Program ini menghasilkan aplikasi menggunakan langkah-langkah dan rumus dari algoritma elgamal, kemudian mengubah isi teks pada file Microsoft Word sebagai masukan , maka algoritma elgamal dapat diterapkan dan diubah menjadi kode-kode yang tidak diketahui (chipertext), Dengan menggunakan pemrograman Visual Basic 2012. Selain itu juga menerapkan algoritma atau tahapan elgamal. Sehingga dapat dihasilkan suatu penerapan metode elgamal untuk mengamankan teks pada dokumen file word. Hasilnya adalah aplikasi ini sangat bermanfaat untuk mengamankan dokumen agar isinya tidak diketahui oleh orang lain yang tidak berhak. Program ini menghasilkan aplikasi dengan menggunakan langkah dan rumus dari algoritma elgamal, kemudian mengubah isi teks pada *file microsoft word* sebagai *input* nya maka algoritma elgamal dapat diterapkan dan berubah menjadi kode-kode yang tidak dikenal (*chipertext*). Dengan menggunakan pemrograman *visual basic* 2012 kemudian menerapkan algoritma atau tahapan dari elgamal maka dapat menghasilkan aplikasi Penerapan Metode Elgamal Untuk Mengamankan *File Microsoft Word*.

REFERENCES

[1] A. Andikos, "Perancangan Aplikasi Multimedia Interaktif Sebagai Media Pembelajaran Pengenalan Hewan Pada Tk Islam Bakti 113 Koto Salak," *J. Sakinah*, vol. 11, pp. 34–39, 2019.

[2] A. Fauzi and Y. Maulita, "Perancangan Aplikasi Keamanan Pesan Menggunakan Algoritma Elgamal Dengan Memanfaatkan Algoritma One Time Pad Sebagai Pembangkit Kunci," *JTIK (Jurnal Tek. Inform. Kaputama)*, vol. 1, no. 1, pp. 1–9, 2018.

[3] N. Oktaviani and S. Sauda, "Pemodelan dan Implementasi Aplikasi Mobile Umrah Guide Menggunakan Unified Modeling Language," *J. Sains dan Inform.*, vol. 5, no. 2, pp. 177–18, 2019.

[4] S. M. Hardi, D. Hamonangan, and M. Zarlis, "Implementasi Kriptografi Hibrid Dengan Algoritma Elgamal Dan Algoritma Onetime Pad (Otp) Dalam Pengamanan File Audio Berbasis Desktop," *TECHSI-Jurnal Tek. Inform.*, vol. 10, no. 2, pp. 129–140, 2018.

[5] T. Zebua, "Pengamanan Data Teks Dengan Kombinasi Cipher Block Chaining dan LSB-1," 2018.

[6] J. S. B. Tambunan, M. I. Sukmana, and S. N. Siregar, "Penyandian Pesan Berdasarkan Algoritma RC5 dan El-Gamal," *Sink. J. dan Penelit. Tek. Inform.*, vol. 2, no. 2, pp. 1–5, 2018.

[7] R. P. Sugijanto, H. N. Palit, and L. W. Santoso, "Implementasi Sistem Inventori pada Prodi Informatika Universitas Kristen Petra," *J. Infra*, vol. 8, no. 2, pp. 223–227, 2020.
[8] J. Susilo, T. Pujiatna, and S. Firmasari, "Pembinaan Tata Bahasa dan Bentuk Surat-Menyurat Indonesia Berbasis Microsoft di Desa Mandala, Dukupuntang Kabupaten Cirebon," *(Jurnal Pengabdi. Dan Pemberdaya. Masyarakat)*, vol. 4, no. 1, pp. 173–177, 2020.
[9] Y. Sari, W., Maulita and A. Fauzi, "Analisa Algoritma Elgamal Dalam Penyandian Data Sebagai Keamanan Database," *J. Inform. Kaputama*, vol. 2, no. 1, pp. 60–70, 2018.
[10] H. Santoso and M. Fakhriza, "erancangan Aplikasi Keamanan File Audio Format Wav (Waveform) Menggunakan Algoritma Rsa," *Algoritm. J. Ilmu Komput. Dan Inform.*, vol. 2, no. 1, pp. 47–54, 2018.
[11] T. Rahmasari, "Perancangan Sistem Informasi Akuntansi Persediaan Barang Dagang Pada Toserba Selamat Menggunakan Php Dan Mysql.," *Account. Inf. Syst. Inf. Technol. Bus. Enterp.*, vol. 4, no. 1, pp. 411–425, 2019.
[12] H. Santoso and M. Fakhriza, "Perancangan Aplikasi Keamanan File Audio Format Wav (Waveform) Menggunakan Algoritma Rsa," *Algoritm. J. Ilmu Komput. Dan Inform.*, vol. 2, no. 1, pp. 47–54, 2018.
[13] Kusrini, "Konsep dan Aplikasi Sistem Pendukung Keputusan," 2019.
[14] T. Wijaya, *Analisis Data Penelitian Menggunakan SPSS*. Yogyakarta: CV Andi Offset, 2009.
[15] H. Ghodang, *Path analysis (analisis jalur)*. Medan: PT Penerbit Mitra Grup, 2020.
[16] V. Jainuri and T. Sukmono, "Optimization of Inventory Costs Using the Continuous Review System (CRS) Method in Controlling the Need for Raw Materials for the Crimean Industry," *Acad. Open*, vol. 5, pp. 1–14, 2021, doi: 10.21070/acopen.5.2021.2205.
[17] I. Magdalena, A. Salsabila, D. A. Krianasari, and S. F. Apsarini, "Implementasi Model Pembelajaran Daring Pada Masa Pandemi Covid-19 Di Kelas III SDN Sindangsari III," *PANDAWA*, vol. 3, no. 1, pp. 119–128, 2021.
[18] S. Calderwood, K. McAreavey, W. Liu, and J. Hong, "Context-dependent Combination of Sensor Information in Dempster-Shafer Teory for BDI," *Knowl Syst 51*, 2016, doi: 10.007/s10115-016-0978-0.
[19] R. E. Putri, "Perancangan Aplikasi Rekam Medis Menggunakan Bahasa Pemograman VB. Net 2010," *J. Tek. dan Inform.*, vol. 5, no. 1, pp. 49–55, 2018.
[20] S. Sumanto, "Metode AHP Dan SAW Untuk Penerimaan Siswa Baru (Studi kasus:Sekolah Menengah Kejuruan (SMK) Sandikta)," *J I M P - J. Inform. Merdeka Pasuruan*, vol. 3, no. 3, pp. 50–56, 2018, doi: 10.37438/jimp.v3i3.188.