Jurnal Unitek
Vol.15 No.2 Juli - Desember 2022
e-ISSN : 2580-2582, p-ISSN: 2089-3957

Algoritma Hybrid dengan Kombinasi Elgamal Algorithm dan *Electronic Code Book* untuk Mengatasi Masalah *Key Distribution*

Agung Purnomo Sidik
Fakultas Sains & Teknologi, Universitas Pembangunan Panca Budi
Jalan Gatot Subroto Km. 4,5 - Kota Medan - Sumatera Utara
agung@dosen.pancabudi.ac.id

ABSTRAK

Tujuan dari penelitian ini adalah mengombinasikan algoritma kunci publik Elgamal dengan model operasi *Electronic Code Book* (ECB) untuk menghasilkan algoritma yang cepat dan aman yang terbebas dari masalah *key distribution*. Masalah *key distribution* terjadi dikarenakan adanya proses pengiriman kunci rahasia dalam jaringan publik. Model operasi *Electronic Code Book* (ECB) digunakan untuk proses enkripsi dengan panjang blok 128-bit. Algoritma Elgamal digunakan untuk mengenkripsi kunci simetris 128-bit yang berbentuk acak untuk menghasilkan *cipher key* yang bersifat publik atau tidak rahasia. Hasil penelitian menunjukkan masalah *key distribution* berhasil teratasi. *Cipher text* yang dihasilkan sangat kuat karena terdapat 2^{128} kombinasi acak dari *cipher text* per blok dan 2^{128} kombinasi kunci acak yang mungkin. Waktu proses dekripsi lebih cepat dari pada waktu proses enkripsi. Waktu proses enkripsi dan dekripsi sangat cepat sehingga cocok digunakan untuk mengenkripsi dan mendekripsi data yang berukuran besar. Sifat kunci yang acak sepanjang 128-bit dan terenkripsi dengan algoritma Elgamal membuat kunci sulit untuk dipecahkan.

Kata kunci: Elgamal, ECB, Enkripsi, Dekripsi, Key Distribution.

ABSTRACT

This research aimed to combine the Elgamal public key algorithm with the Electronic Code Book (ECB) operating model to produce fast and secure algorithms, and overcome key distribution problems. Key distribution problems occured due to sending a secret key to a public network. The Electronic Code Book (ECB) operating model was used for the encryption process with a block length of 128 bits. The Elgamal algorithm was used to encrypt a random 128-bit symmetric key to generate a non-secret cypher key. The results showed that the key distribution problem was successfully resolved. The resulting cypher text was very strong because there are 2^{128} random combinations of ciphertext per block and 2^{128} possible random key combinations. The decryption process time was faster than the encryption process. The encryption and decryption process time was very fast, so it was suitable for encrypting and decrypting large data. The random nature of the 128-bit key and encrypted with the Elgamal algorithm made the key difficult to crack.

Keywords: *Elgamal, ECB, Encrypt, Decrypt, Key Distribution.*

Pendahuluan

Pesatnya pertumbuhan teknologi informasi dan komunikasi saat ini memungkinkan setiap orang untuk mengirimkan dan menerima informasi secara bebas dan cepat, tanpa memandang ruang dan waktu (Khairatunnisa, 2021). Keamanan data yang tidak memadai akan memungkinkan pihak luar mengakses, memanfaatkan, atau memanipulasi pesan yang disampaikan (Andriyanto et al, 2020). Sehingga diperlukan suatu upaya khusus untuk meningkatkan keamanan pesan agar bersifat private (Ilaga & Sari, 2018).

Peningkatan keamanan pesan dapat dilakukan dengan mengenkripsi pesan yang dikirimkan (Widarma et al, 2019). Terdapat dua jenis algoritma enkripsi yang dapat digunakan berdasarkan jenis kuncinya, yaitu algoritma simetris (kunci private) dan algoritma asimetris (kunci publik) (Sidik, 2019) (Urva, 2017). Kelemahan dari algoritma simetris adanya masalah pada *key distribution*, dimana kunci yang dihasilkan seluruhnya bersifat rahasia sehingga tidak memungkinkan untuk dikirimkan melalui jalur publik dengan aman, namun kelebihannya algoritma simetris memiliki proses enkripsi dan dekripsi yang cepat (Tampubolon, 2021). Sebaliknya, algoritma asimetris memiliki kelemahan pada proses enkripsi dan dekripsi yang cukup lambat, namun tidak memiliki masalah *key distribution* (Pljonkin, 2021).

Penelitian ini bertujuan untuk menghasilkan sebuah algoritma hybrid yang memiliki kemampuan pemrosesan enkripsi dan dekripsi yang cepat, aman, dan tidak memiliki masalah *key distribution*. Algoritma hybrid dihasilkan dari kombinasi algoritma Elgamal dan *Electronic Code Book* (ECB) 128-bit dengan teknik dasar XOR untuk mempercepat proses enkripsi dan dekripsi serta kunci acak sepanjang 128-bit.

Metode Penelitian

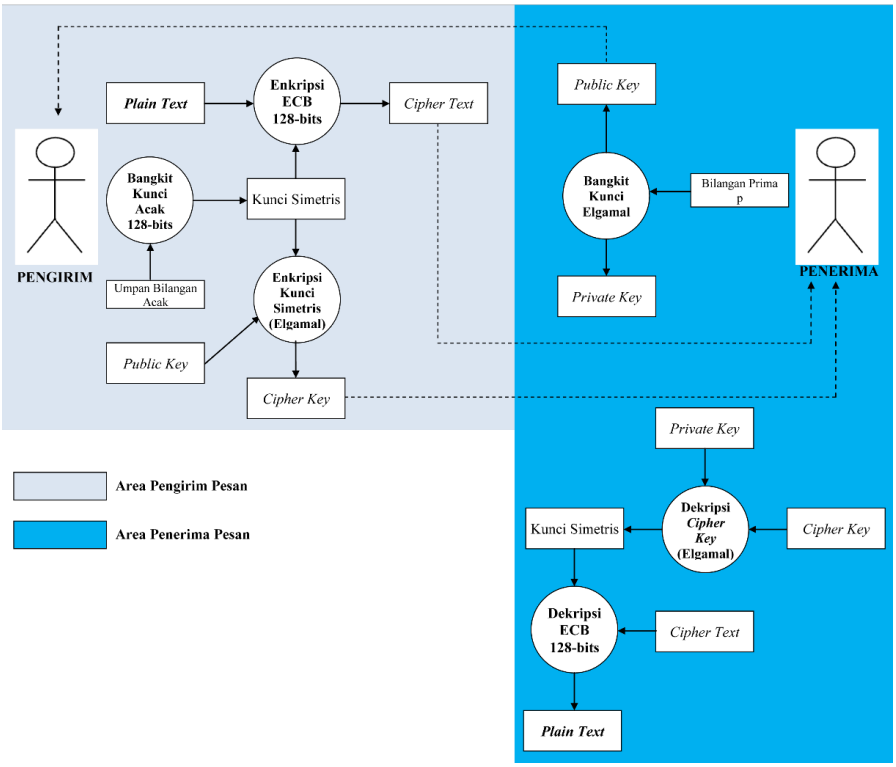
Objek pada penelitian ini adalah pesan teks yang bisa dikirim melalui SMS, email, atau lainnya. Algoritma simetris yang digunakan adalah algoritma XOR dengan model operasi *Electronic Code Book* (ECB) dengan panjang blok 128-bit yang digunakan untuk mengenkripsi dan dekripsi pesan teks (Eka & Putra, 2020). Kunci simetris menggunakan kunci acak 128-bit. Algoritma asimetris yang digunakan adalah algoritma Elgamal yang digunakan untuk mengenkripsi kunci simetris menjadi *cipher key* agar bersifat publik (tidak rahasia), dan mendekripsi kembali menjadi kunci simetris (Rachmawati et al, 2018).

Metode penyelesaian masalah pada penelitian ini terbagi menjadi tiga tahapan, yaitu: (Pal et al, 2021)

1. Tahap Pembangkitan Kunci
    a. Membangkitkan Kunci Simetris
       Kunci simetris digunakan untuk mengenkripsi pesan teks menjadi *cipher text*, dan mendekripsi *cipher text* menjadi *plain text* (pesan teks asal) (Fauzi, 2019).
    b. Membangkitkan Kunci Asimetris
       Kunci asimetris terdiri dari *public key* da *private key* (Ordonez et al, 2018). *Public key* digunakan untuk mengenkripsi kunci simetris menjadi *cipher key*, sedangkan *private key* digunakan untuk mendekripsi *cipher key* kembali menjadi kunci simetris Imran et al, 2020).

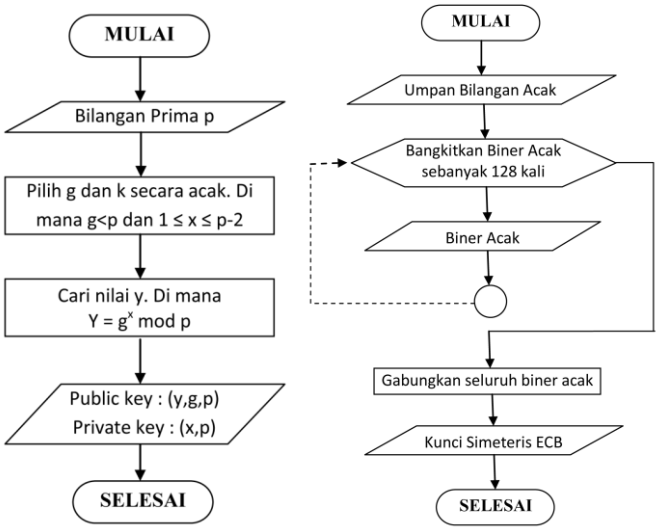
2. Tahap Enkripsi
   Mengenkripsi pesan teks menjadi *cipher text* dan mengenkripsi kunci simetris menjadi *cipher key*.
3. Tahap Dekripsi
   Mendekripsi *cipher key* menjadi kunci simetris dan mendekripsi *cipher text* menjadi *plain text*.

Metode penyelesaian masalah tersebut dapat dilihat dalam diagram berikut:

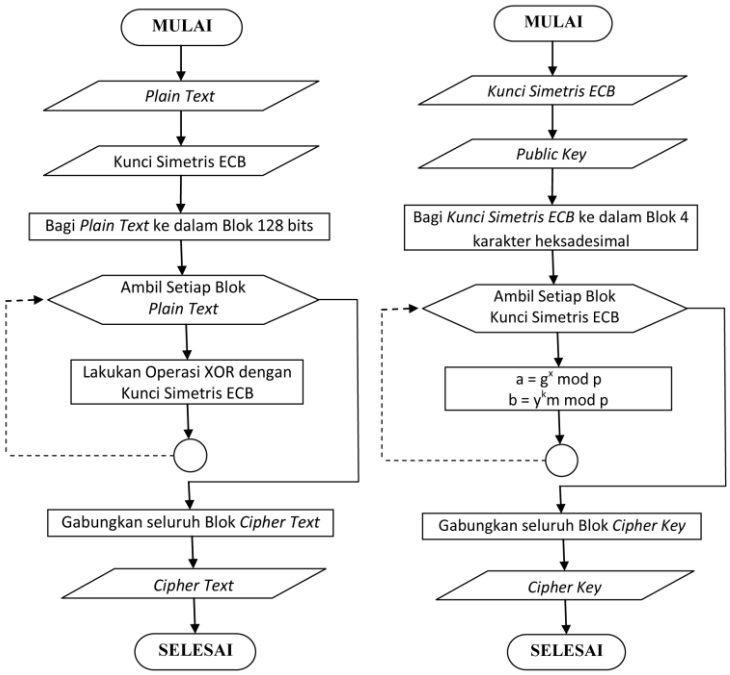


Gambar 1. Diagram Proses Penyelesaian Masalah yang Diusulkan

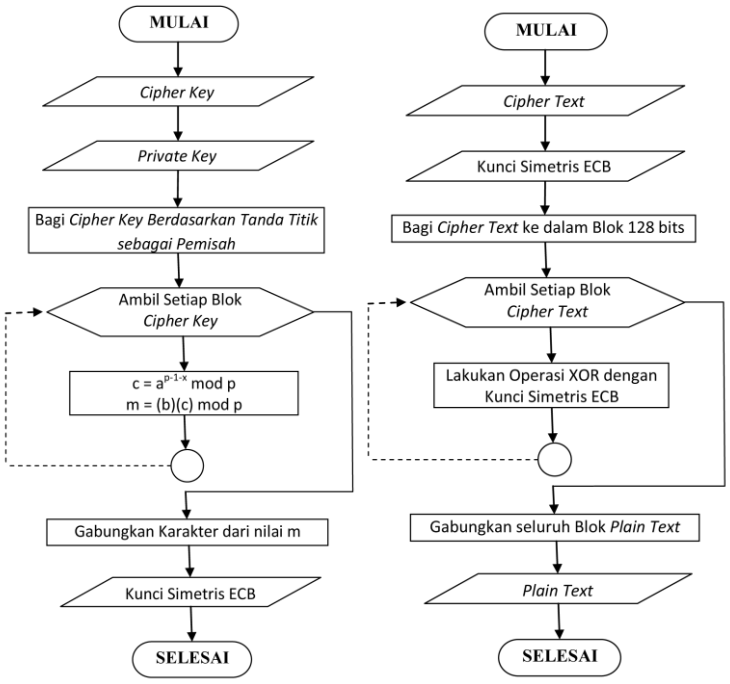
Flowchart dari setiap tahapan dapat dilihat pada gambar berikut:



Gambar 2. Alur Proses Tahapan Pembangkitan Kunci Simetris dan Kunci Asimetris



Gambar 3. Alur Proses Tahapan Enkripsi Plain Text dan Kunci Simetris

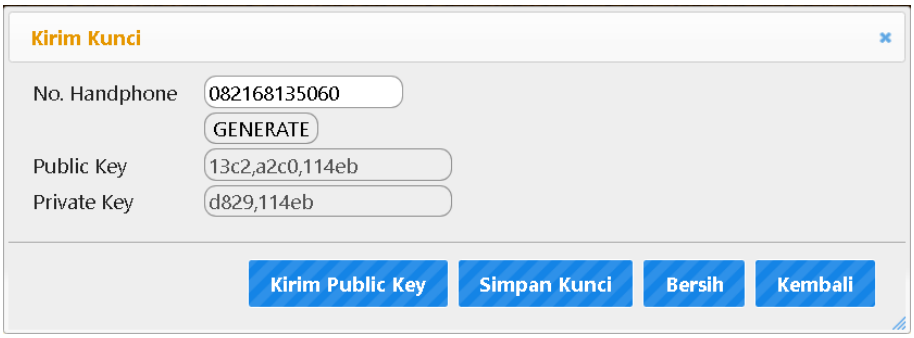


Gambar 4. Alur Proses Tahapan Dekripsi *Cipher* Text dan *Cipher* Key

Metode penyelesaian masalah pada penelitian ini diimplementasikan ke dalam bentuk aplikasi pengiriman pesan dengan bahasa pemrograman PHP.

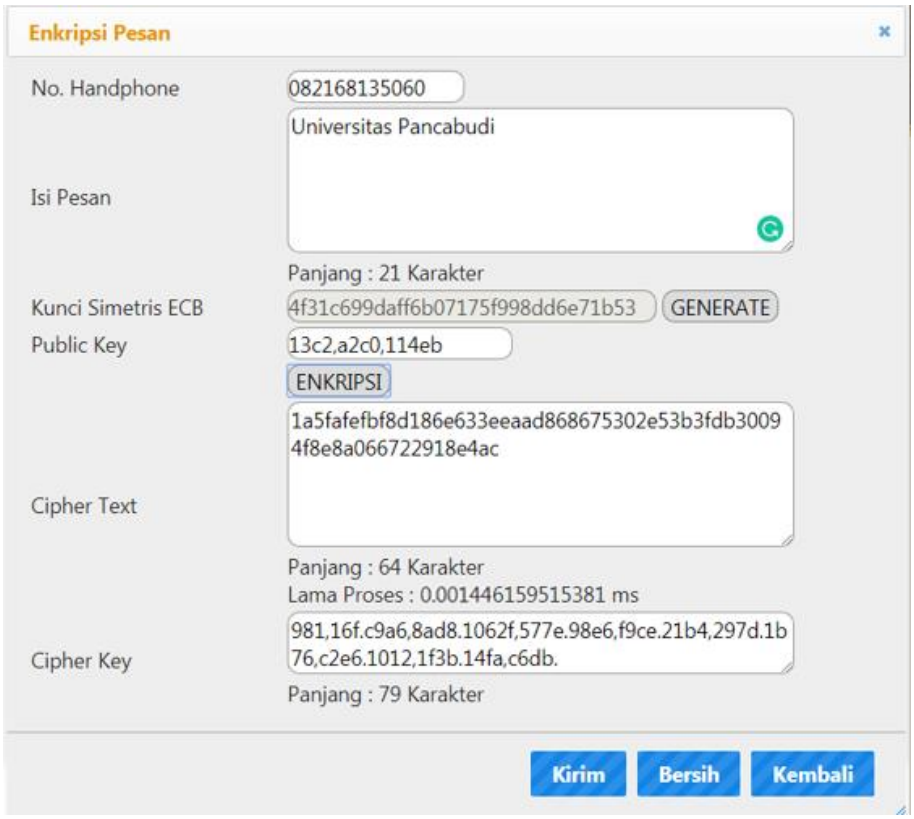
Hasil dan Pembahasan

Hasil percobaan yang dilakukan dengan aplikasi yang berhasil dibangun dapat dilihat pada gambar berikut:



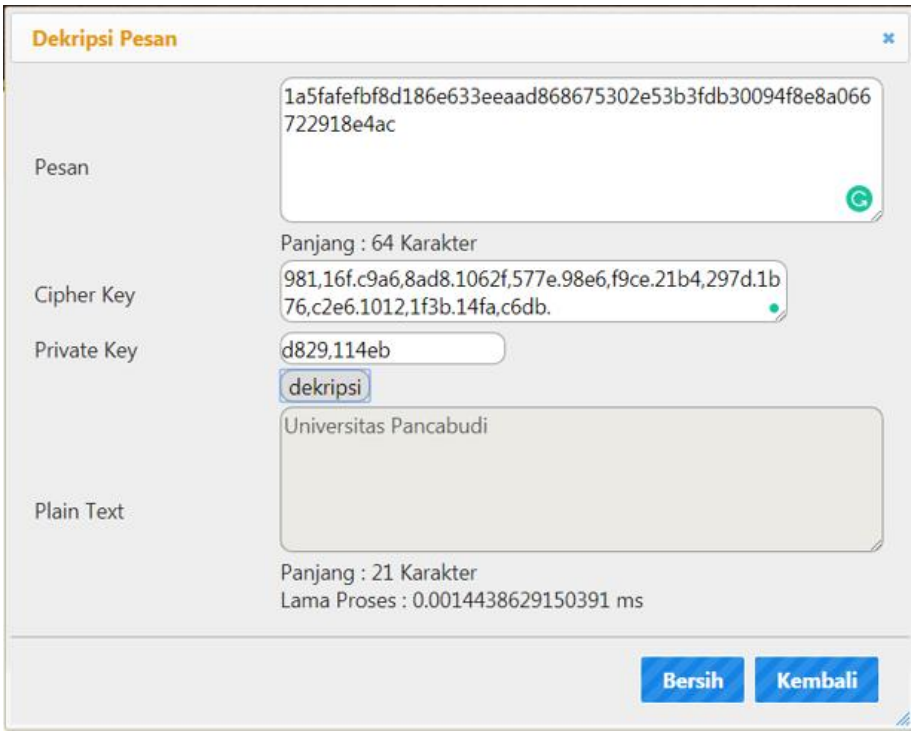
Gambar 5. Hasil Pembangkitan Kunci Asimetris

Proses pembangkitan kunci asimetris menghasilkan dua buah kunci, yaitu *public key* yang bersifat tidak rahasia yang digunakan untuk enkripsi kunci simetris, serta *private key* yang bersifat rahasia yang digunakan untuk dekripsi *cipher key*. Proses ini dilakukan oleh penerima pesan. Setelah kunci asimetris dibangkitkan, penerima pesan mengirimkan *public key* kepada pengirim pesan, sedangkan *private key* tetap tersimpan di aplikasi.



Gambar 6. Hasil Pembangkitan Kunci Simetris, Enkripsi Plain Text, dan Enkripsi Kunci Simetris

Proses enkripsi memakan waktu 0,00144 milidetik untuk 21 karakter *plain text* yang dienkripsi menjadi 64 karakter heksadesimal *cipher text* (dua blok *cipher text* dimana 1 blok *cipher text* terdiri dari 32 karakter heksadesimal). Kunci simetris yang dihasilkan sepanjang 128-bit atau 32 karakter heksadesimal. *Cipher* text dan *cipher key* yang dihasilkan menggunakan bilangan heksadesimal.



Gambar 7. Hasil Dekripsi *Cipher* Key dan *Cipher* Text

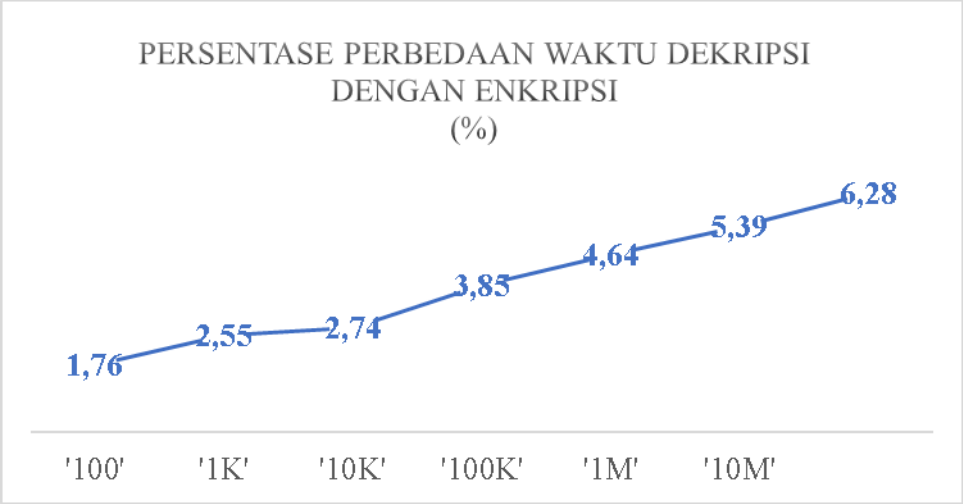
Proses dekripsi memakan waktu 0,00144 milidetik untuk mengembalikan *cipher text* menjadi *plain text* (pesan teks asli). Sehingga dapat ditarik kesimpulan bahwa proses dekripsi lebih cepat dari proses enkripsi. Waktu proses enkripsi dan dekripsi untuk pesan dengan panjang yang berbeda-beda dapat dilihat pada tabel berikut:

Tabel 1. Waktu Proses Enkripsi dan Dekripsi yang Diperlukan

Panjang Pesan (karakter)	Waktu Enkrispsi (ms)	Waktu Dekripsi (ms)	Selisih (ms)	Rasio Enkripsi/ Dekripsi (%)
100	0,00307696	0,00302277	0,00005419	1,76
1000	0,02982211	0,02906033	0,00076179	2,55
10.000	0,32335207	0,31449234	0,00885973	2,74
100.000	3,18798734	3,06521653	0,12277081	3,85
1.000.000	28,92458423	27,58129002	1,34329421	4,64
10.000.000	304,28511252	287,88244103	16,40267149	5,39
100.000.000	2871,29849423	2691,11827493	180,18021930	6,28

Tabel 1 menunjukkan hasil pengujian enkripsi dan dekripsi untuk pesan sepanjang 100, 1.000, 10.000, 100.000, 1.000.000, 10.000.000, dan 100.000.000 karakter. Hasil

pengujian menunjukkan bahwa waktu proses yang dibutuhkan enkripsi selalu lebih lama dari pada waktu yang dibutuhkan untuk proses dekripsi. Persentase perbedaan waktu dekripsi terhadap waktu enkripsi dapat dilihat pada grafik berikut:



Gambar 8. Persentase Perbedaan Waktu Dekripsi dengan Enkripsi

Gambar 8 menunjukkan bahwa semakin besar panjang pesan yang diproses maka persentase waktu dekripsi yang dibutuhkan akan semakin cepat. Oleh karena itu, algoritma ini sangat layak digunakan untuk mengenkripsi dan dekripsi data yang berukuran besar.

Analisis Keamanan

Kunci simetris yang dibangkitkan terdiri dari 128-bit acak yang tidak dapat diprediksi. Oleh karena itu, terdapat 2^{128} atau 3,40282 x 10^{38} kombinasi kunci acak yang mungkin (Murdowo, 2019). Kombinasi kunci ini sangat sulit dipecahkan karena bersifat acak dan memiliki kombinasi kunci yang sangat banyak. Kelemahan pada kunci simetris ini ada pada sifatnya yang private atau rahasia (Andriyanto, 2020). Proses enkripsi kunci simetris dengan menggunakan *public key* dari algoritma Elgamal menghasilkan *cipher key* yang bersifat publik atau tidak rahasia (Jintcharadze & Iavich, 2020). Sehingga kelemahan kunci simetris telah terjawab. Sifat *cipher key* yang bersifat publik ini menghilangkan masalah *key distribution* (Tampubolon, 2021) (Shenoy-Hejamadi et al, 2017). Hal ini dikarenakan pengirim pesan dapat mengirimkan *cipher text* dan *cipher key* di dalam jaringan terbuka (publik) karena sifat *cipher text* dan *cipher key* yang tidak lagi private atau rahasia (Kumar et al, 2019).

Cipher text dihasilkan dari proses enkripsi *plain text* dengan kunci simetris acak pada blok 128-bit dengan model operasi *electronic code book*. Proses enkripsi *plain text* dengan kunci simetris yang acak akan menghasilkan *cipher text* yang seluruhnya benar-benar acak sehingga metode pemecahannya yang paling memungkinkan adalah dengan metode *exhaustive search* atau metode bruto-force yaitu mencoba satu per satu kemunginan (Das & De, 2018). Blok 128-bit akan menghasilkan 2^{128} atau 3,40282 x 10^{38} kemungkinan *cipher text* untuk masing-masing blok sehingga akan dibutuhkan waktu yang sangat lama untuk memecahkan *cipher text* tanpa kunci walau dengan komputer yang sangat cepat (Sidik, 2019). Andai digunakan komputer dengan kecepatan 1 Sekstiliun per detik atau 10^{21} operasi

per detik, masih dibutuhkan 10,79 x 10^9 tahun untuk memecahkan setiap blok dari *cipher text*. Oleh karena itu, dapat disimpulkan *cipher text* yang dihasilkan masih sangat aman.

Simpulan

Hasil penelitian menunjukkan bahwa kombinasi dari algoritma Elgamal dengan model operasi *electronic code book* menghasilkan algoritma hybrid yang cepat, aman, dan mampu mengatasi masalah *key distribution* sehingga proses pengiriman pesan dan kunci menjadi lebih aman. Waktu proses yang dibutuhkan untuk dekripsi lebih cepat dari pada waktu proses enkripsi dimana semakin panjang pesan yang diproses maka persentase kecepatan waktu dekripsi terhadap enkripsi akan semakin meningkat.

Daftar Pustaka

Andriyanto, R., Khairijal, K., & Satria, D. (2020). Penerapan Kriptografi AES Class Untuk Pengamanan URL WEBSITE Dari Serangan SQL INJECTION. *JURNAL UNITEK*, 13(1), 34-48.

Das, J. C., & De, D. (2018). QCA Based Secure Nanocommunication Block Cipher Design Based on Electronic Code Book. *Malaysian Journal of Computer Science,* 31(2), 130-142.

Eka, I. A. W. A. P., & Putra, W. H. C. G. B. (2020). Perbandingan Waktu Enkripsi Antara Metode Electronic Codebook (ECB) dan Chipher Block Chaining (CBC) Dalam Algoritma Blowfish. *JURNAL ILMU KOMPUTER INDONESIA,* 5(1), 50-54.

Fauzi, A. (2019). Analisa Kombinasi Pesan Teks Ke Dalam File Audio Memanfaatkan Algoritma Data Encryption Standard Dan Metode End of File. *JTIK (Jurnal Teknik Informatika Kaputama), 3*(1), 1-8.

Ilaga, K. R., & Sari, C. A. (2018). Analysis of Secure Image Crypto-Stegano Based on Electronic Code Book and Least Significant Bit. *J. Appl. Intell. Syst,* 3(1), 28-38.

Imran, O. A., Yousif, S. F., Hameed, I. S., Abed, W. N. A. D., & Hammid, A. T. (2020). Implementation of El-Gamal Algorithm for Speech Signals Encryption and Decryption. *Procedia Computer Science,* 167, 1028-1037.

Jintcharadze, E., & Iavich, M. (2020). Hybrid Implementation of Twofish, AES, ElGamal and RSA Cryptosystems. *In 2020 IEEE East-West Design & Test Symposium (EWDTS)* (pp. 1-5). IEEE.

Khairatunnisa, K., & Sari, F. (2021). Sistem Informasi Donor Darah Pada Unit Tranfusi Darah Palang Merah Indonesia Kota Dumai Berbasis Website. Jurnal Unitek, 14(1), 30–37

Kumar, A., Dadheech, P., Singh, V., Poonia, R. C., & Raja, L. (2019). An Improved Quantum Key Distribution Protocol for Verification. *Journal of Discrete Mathematical Sciences and Cryptography,* 22(4), 491-498.

Murdowo, S. (2019). Mengenal Kriptografi Modern Sederhana Menggunakan Electronik Code Book (ECB). *Jurnal Ilmiah Infokam,* 15(1).

Ordonez, A. J., Medina, R. P., & Gerardo, B. D. (2018, April). Modified El Gamal Algorithm for Multiple Senders and Single Receiver Encryption. *In 2018 IEEE Symposium on Computer Applications & Industrial Electronics (ISCAIE)* (pp. 201-205). IEEE.

Pal, P., Sahana, B. C., Ghosh, S., Poray, J., & Mallick, A. K. (2021). Voice Password-Based Secured Communication Using RSA and ElGamal Algorithm. *In Progress in Advanced Computing and Intelligent* Engineering (pp. 387-399). Springer, Singapore.

Pljonkin, A. P. (2021). Vulnerability of the Synchronization Process in the Quantum Key Distribution System. *In Research Anthology on Advancements in Quantum Technology* (pp. 345-354). IGI Global.

Rachmawati, D., Budiman, M. A., & Saffiera, C. A. (2018). An Implementation Of Elias Delta Code And ElGamal Algorithm In Image Compression And Security. *In IOP Conference Series: Materials Science and Engineering* (Vol. 300, No. 1, p. 012040). IOP Publishing.

Shenoy-Hejamadi, A., Pathak, A., & Radhakrishna, S. (2017). Quantum Cryptography: Key Distribution and Beyond. *Quanta,* 6(1), 1-47.

Sidik, A. P. (2019). Rancangan Model Algoritma Hybrid Teknik Enkripsi XOR dengan Kombinasi Mode Block Cipher CBC-ECB 512-Bits dan Algoritma RSA. *Jurnal Teknik dan Informatika,* 6(2), 1-7.

Tampubolon, A. (2021). Implementasi Kombinasi Algoritma RSA dan Algoritma DES Pada Aplikasi Pengaman Pesan Teks. *Jurnal SAINTIKOM (Jurnal Sains Manajemen Informatika dan Komputer),* 20(1), 38-43.

Urva, G. (2017). Analisis Penggunaan Enkripsi End To End Pada Aplikasi Whatsapp Messengger. *Jurnal Unitek,* 10(1), 34-45.

Widarma, A., Siregar, H. F., & Irawan, M. D. (2019). Teknik Keamanan Data Menggunakan Vigenere Cipher Dan Electronic Code Book (ECB). *J-SAKTI (Jurnal Sains Komputer dan Informatika),* 3(2), 393-400.