Faktor Exacta

Vol. 13, No. 4, Dec 2020, pp. 208~215
eISSN: 2502-339X, pISSN: 1979-276X, DOI: 10.30998/faktorexacta.v13i4.7429

Analisis Dan Perancangan Simulasi Algoritma *Paillier Cryptosystem* Pada Pesan *Text* Dengan *Presentation Format Binary, Octal, Hexadecimal* dan *Base64*

Muhamad Femy Mulya[1], Nofita Rismawati[2], Dedy Trisanto[3]
[1] Program Studi Sistem Informasi, Tanri Abeng University, Indonesia
[2] Program Studi Informatika, Universitas Indraprasta PGRI, Indonesia
[3] Program Studi Sistem Informasi Industri Otomotif, Politeknik STMI Jakarta, Indonesia

Article Info

Article history:

Received Sep 9, 2019
Revised November 20, 2020
Accepted December 11, 2020

Keywords:

Cryptography
Paillier Cryptosystem
Cryptool2

ABSTRACT

The paillier cryptosystem algorithm is an asymmetric probabilistic algorithm for cryptography public key. The paillier cryptosystem algorithm is used because the computation of encryption and decryption in the paillier cryptosystem algorithm is quite complicated: it requires two power operations, one multiplication operation, and one modulo operation. The purpose of this research is to analyze, to design and to implement simulation of encryption and decryption of text messages (in the form of text writing or text files) using the paillier cryptosystem algorithm with 4 (four) presentation formats, namely, binary, octal, hexadecimal and base64. Thus, text messages (in the form of text writing or text files) will be safer when sent via email, SMS or chat from sender to message recipient. The software that will be used to simulate the paillier cryptosystem algorithm is Cryptool2. The results showed that the binary presentation format is the fastest for the encryption and decryption process time (ms), while the base64 presentation format is the slowest for the time (ms) for the encryption and decryption process.

ABSTRAK

Algoritma *paillier cryptosystem* merupakan sebuah algoritma asimetris *probabilistic* untuk kriptografi kunci publik. Algoritma *paillier cryptosystem* digunakan karena komputasi enkripsi dan dekripsi pada algoritma *paillier cryptosystem* cukup rumit, yakni diperlukan dua kali operasi perpangkatan, satu kali operasi perkalian, dan satu kali operasi modulo. Tujuan dari penelitian ini adalah untuk menganalisis, merancang, serta mengimplementasikan simulasi enkripsi dan dekripsi dari pesan *text* (berupa *text writing* maupun *text file*) menggunakan algoritma *paillier cryptosystem* dengan *presentation format* sebanyak 4 (empat) *format* yaitu, *binary*, *octal*, *hexadecimal* dan *base64*. Dengan demikian, pesan *text* (berupa *text writing* maupun *text file*) akan lebih aman pada saat dikirimkan melalui surat-e, *SMS* maupun *chatting* dari pengirim ke penerima pesan. Adapun perangkat lunak (software) yang akan digunakan untuk membuat simulasi algoritma *paillier cryptosystem* ini adalah *Cryptool2*. Hasil penelitian ini menunjukkan bahwa *presentation format binary* menjadi yang paling cepat untuk waktu (ms) proses enkripsi dan dekripsi, sedangkan *Presentation format base64* menjadi yang paling lamban untuk waktu (ms) proses enkripsi dan dekripsi.

Corresponding Author:

Muhamad Femy Mulya,
Program Studi Sistem Informasi
Tanri Abeng University
Jl. Swadarma Raya No.58, Ulujami, Pesanggrahan, Jakarta 12250.
Email: femy.mulya@tau.ac.id

1. PENDAHULUAN

Saat ini perkembangan teknologi informasi sudah semakin merambah hingga ke semua sendi kehidupan. Kemajuan teknologi informasi pun memberikan banyak keuntungan bagi setiap kehidupan manusia. Akan tetapi keuntungan yang ditawarkan oleh teknologi informasi juga dapat menimbulkan kejahatan seperti pencurian data. Oleh karena itu, dibutuhkan suatu teknik atau metode untuk mengamankan data agar pengguna teknologi informasi selalu merasa aman dalam menggunakan dan mengakses data dari manapun berada.

Data merupakan informasi yang belum diolah, data biasanya terdiri dari berbagai macam jenis, seperti Gambar/citra, tulisan/*text*, suara, dan video. Dengan adanya kemajuan teknologi, berbagai jenis data tersebut dapat dinikmati secara digital dan dapat disebarluaskan dan didistribusikan secara bebas. Namun tidak bisa dipungkiri, bahwa data yang telah tersebar luas dan bebas tersebut akan rentan terhadap keamanannya, karena data tersebut dapat diubah, dihapus, maupun dimanipulasi oleh orang yang tidak bertanggung jawab. Salah satu jenis data yang sering dimanipulasi adalah data tulisan atau *text*. Oleh karena itu, perlu diterapkan pengamanan terhadap data. Salah satu teknik untuk mengamankan suatu data adalah teknik penyandiaan data atau yang biasa disebut dengan teknik kriptogafi.

Dalam setiap penggunaan kriptografi sebagai pengamanan data, maka diperlukan sebuah algoritma kriptografi sebagai pendukung utama dalam meningkatkan kerahasian masing-masing sistem kriptografi. Jenis algoritma yang biasa dipergunakan dalam teknik kriptografi adalah algoritma simetris dan algoritma asimetris. Algoritma simetri adalah jenis algoritma yang menggunakan kunci yang sama dalam proses enkripsi dan dekripsinya. Sementara algoritma asimetri menggunakan kunci yang berbeda dalam proses enkripsi dan dekripsinya.

Masalah yang umum-nya dan rentan terjadi pada algoritma simetri adalah personal yang ingin meng-enkripsi ataupun men-dekripsi data harus memiliki kunci yang sama, dimana jalan satu-satunya adalah dengan menyebarluaskan kunci tersebut. Dengan demikian, pada penelitian ini, peneliti akan menggunakan algoritma asimetri, karena dalam proses penyebarluasan kuncinya tidak memerlukan jalur khusus, karena proses enkripsi dan dekripsinya dapat menggunakan kunci yang berbeda [1].

Algoritma *paillier cryptosystem* adalah algoritma asimetris probabilistik yang efisien untuk kriptografi kunci publik.[2] Pada algoritma *paillier cryptosystem* proses enkripsinya dilakukan per-karakter. Selain itu, salah satu kelebihan dari Algoritma *Paillier Cryptosystem* adalah adanya sifat *homormofisme* dan *self-blinding*. Beberapa sifat inilah yang membuat algoritma *paillier cryptosystem* dapat dipergunakan untuk berbagai keperluan, salah satunya untuk pengamanan pesan *text* [3].

Penelitian ini penting dilakukan, karena pada penelitian-penelitian yang sudah dilakukan hanya menggunakan algoritma *paillier cryptosystem* dengan 1 (satu) *presentation format* saja, sedangkan pada penelitian ini menggunakan algoritma *paillier cryptosystem* dengan *presentation format* sebanyak 4 (empat) *format* yaitu, *binary*, *octal*, *hexadecimal* dan *base64*. Selain itu, pada penelitian ini juga akan dilakukan uji coba terhadap simulasi enkripsi dan dekripsi pesan *text* (berupa *text writing* maupun *text file*) menggunakan algoritma *paillier cryptosystem* dengan *software Cryptool2*.

Dari uraian yang telah diberikan sebelumnya, pada penelitian ini akan dijawab permasalahan bagaimana pemanfaatan algoritma *paillier cryptosystem* untuk proses enkripsi dan dekripsi pesan *text* (berupa *text writing* maupun *text file*) sehingga dapat diimplementasikan dalam bentuk simulasi proses enkripsi dan dekripsi pada suatu proses pengiriman pesan *text* melalui media *email*, *sms* maupun *chatting*, dengan demikian mampu menjaga integritas dan keamanan data serta informasi tersebut.

Tujuan dari penelitian ini adalah untuk menganalisa, merancang serta mengimplementasikan simulasi enkripsi dan dekripsi dari pesan *text* (berupa *text writing* maupun *text file*) menggunakan algoritma *paillier cryptosystem*, sehingga pesan *text* (berupa *text writing* maupun *text file*) akan lebih aman pada saat dikirimkan melalui *email*, *sms* maupun *chatting* dari pengirim ke penerima pesan. Perangkat lunak yang digunakan untuk membuat simulasi algoritma *paillier cryptosystem* ini menggunakan *Cryptool2*.

Algoritma *Paillier Cryptosystem*

Paillier cryptosystem algorithm yang ditemukan oleh Pascal Paillier pada tahun 1999 merupakan sebuah algoritma asimetris *probabilistic* pada kriptografi untuk kunci publik. Sekuritas dari algoritma paillier ini bergantung pada problema perhitungan *n-residue class* yang dipercaya sangat sulit untuk komputasi.[4] Pada *paillier cryptosystem* berdasarkan pada *Composite Residuosity* (CR), yaitu jika diberikan $x \in Z^*_{N^2}$, tentukan apakah x adalah residu ke-N modulo N^2 [5].

Elemen x dikatakan sebuah residu ke-N jika terdapat elemen lain, $y \in Z^*_{N^2}$ yang memenuhi: $x = y^N \bmod N^2$. Setiap x memiliki tepat N buah akar di $Z^*_{N^2}$ atau memiliki N buah solusi berbeda. Oleh karena itu, sulit menentukan mana solusi yang sebenarnya [6].

Paillier Cryptosystem Algorithm merupakan jenis kriptografi berbasis *keypair*, maksudnya setiap pengguna mendapatkan kunci publik dan pribadi, dan pesan yang dienkripsi dengan kunci publik mereka hanya

dapat didekripsi dengan kunci pribadi mereka [7]. *Paillier Cryptosystem Algorithm* tidak banyak digunakan sebagai algoritma lain seperti RSA, dan ada beberapa implementasi yang tersedia secara online. Kelebihan dari *paillier cryptosystem algorithm* tidak seperti banyak *cryptosystem* lainnya *keypair*, *paillier cryptosystem algorithm* menyediakan *homomorfisme aditif*. Ini berarti bahwa pesan dapat ditambahkan bersama ketika dienkripsi, dan pihak lain tidak akan mendekripsi dengan benar [8].

Pembangkitan Kunci Algoritma *Paillier Cryptosystem*

Untuk melakukan enkripsi dan dekripsi pesan *text*, pada algoritma *paillier cryptosystem* juga memerlukan kunci publik dan kunci privat [9]. Kunci publik, seperti namanya, dapat diketahui oleh publik dan digunakan untuk mengenkripsi pesan *text*. Pesan *text* yang dienkripsi dengan kunci publik hanya dapat didekripsi dengan menggunakan kunci privat padanannya yang tentunya bersifat rahasia. Kunci publik dan kunci privat yang digunakan dalam algoritma *paillier cryptosystem* dibangkitkan dengan mekanisme sebagai berikut[10]:

1. Misal *k* adalah parameter keamanan.
2. Pilih dua buah bilangan prima berukuran besar sembarang secara acak *k*-bit dua buah bilangan ini juga umum disebut *p* dan *q*.
3. Menghitung nilai *N*, dimana *N* adalah hasil perkalian antara nilai *p* dan nilai *q*. Hitung $N=pq$.

$$|Z_N^*| = \phi(N) = (p-1)(q-1) \quad (1)$$

$$\left|Z_{N^2}^*\right| = \phi(N^2) = N \cdot \phi(N) \quad (2)$$

4. Mengitung Nilai λ

$$\lambda(N) = lcm(p-1, q-1) \quad (3)$$

5. Memilih bilangan bulat acak *g*, dimana *N* membagi orde *g*.

$$L\left(g^{\lambda(N)} \bmod N^2\right) = \frac{\left(g^{\lambda(N)} \bmod N^2\right)-1}{N} \quad (4)$$

6. Pilih basis g yang memenuhi:

$$\gcd\left(L\left(g^{\lambda(N)} \bmod N^2\right), N\right) = 1 \quad (5)$$

Atau

$$g = (\alpha N + 1) \cdot \beta^N \bmod N^2 \quad (6)$$

Dengan α dan β adalah suatu bilangan bulat. *N* membagi order dari g.

Yang perlu diperhatikan dalam algoritma pembangkitan kunci publik dan kunci privat pada algoritma *paillier cryptosystem*, yaitu nilai bilangan prima *p* dan *q* dipilih secara acak dan independen satu sama lain. Hasil dari algortima pembangkitan pasangan kunci di atas adalah sebuah kunci publik yang merupakan pasangan nilai *N* dan *g*, serta λ sebagai kunci privat [11].

Enkripsi Pada Algoritma *Paillier Cryptosystem*

Mekanisme enkripsi algoritma *paillier cryptosystem* jauh lebih sederhana dari pada algoritma pembangkitan kuncinya. Algoritma enkripsi *paillier cryptosystem* secara lengkap adalah sebagai berikut[10]:

1. Mengambil kunci publik penerima pesan, yang secara umum disebut m, dan nilai *N* dengan $m < N$
2. Memilih sebuah bilangan bulat acak $r \in Z_N^*$
3. *Cipherteks* dihitung dengan rumus sebagai berikut:

$$c = g^m r^N \bmod N^2 \quad (7)$$

dengan *c* adalah cipherteks hasil enkripsi dan *m* adalah plainteks yang dienkripsi

Dekripsi Pada Algoritma *Paillier Cryptosystem*

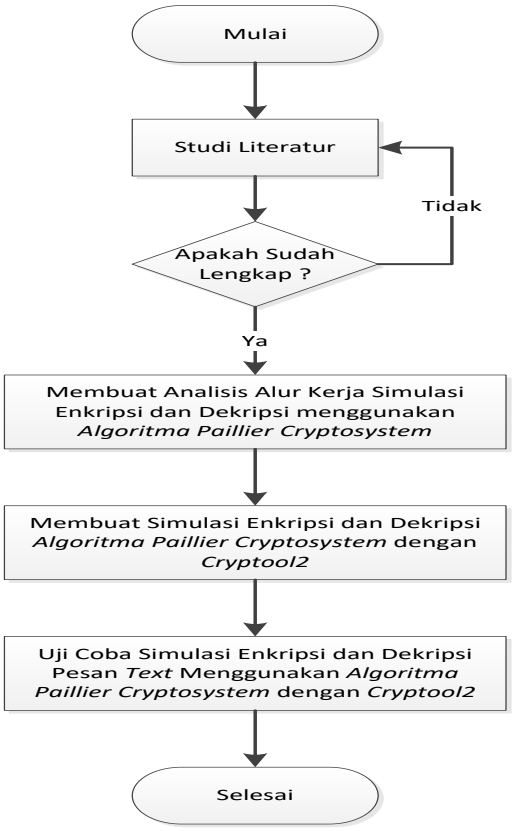
Mekanisme dekripsi *paillier cryptosystem* sedikit lebih rumit dari pada mekanisme enkripsinya. Adapun Algoritma dekripsi *paillier cryptosystem* secara lengkap adalah sebagai berikut [5]:

1. Periksa apakah $c < N^2$
2. Jika ya, pesan m dapat diperoleh dari:

$$m = \frac{L(c^{\lambda(N)} mod\ N^2)}{L(g^{\lambda(N)} mod\ N^2)} \quad (8)$$

2. METODE

Pada simulasi enkripsi dan dekripsi dianalisa dan dirancang pada pesan *text* (berupa *text writing* ataupun *text file*) dengan menggunakan algoritma *paillier cryptosystem* pada penelitian ini, menggunakan studi literatur dan metode kuantitatif. Pada studi literatur dilakukan studi pustaka yang membahas teknik enkripsi dan dekripsi dengan algoritma *paillier cryptosystem*. Kemudian pada metode kuantitatif dilakukan 3 (tiga) tahap penelitian mulai dari membuat analisis alur kerja simulasi enkripsi dan dekripsi menggunakan algoritma *paillier cryptosystem*, selanjutnya membuat simulasi enkripsi dan dekripsi algoritma *paillier cryptosystem* dengan *Cryptool2*, dan yang terakhir melakukan uji coba simulasi enkripsi dan dekripsi pesan *text* menggunakan algoritma *paillier cryptosystem* dengan *cryptool2*. Adapun detail *flowchart* untuk tahapan penelitian ini, terlihat pada gambar 1 berikut.

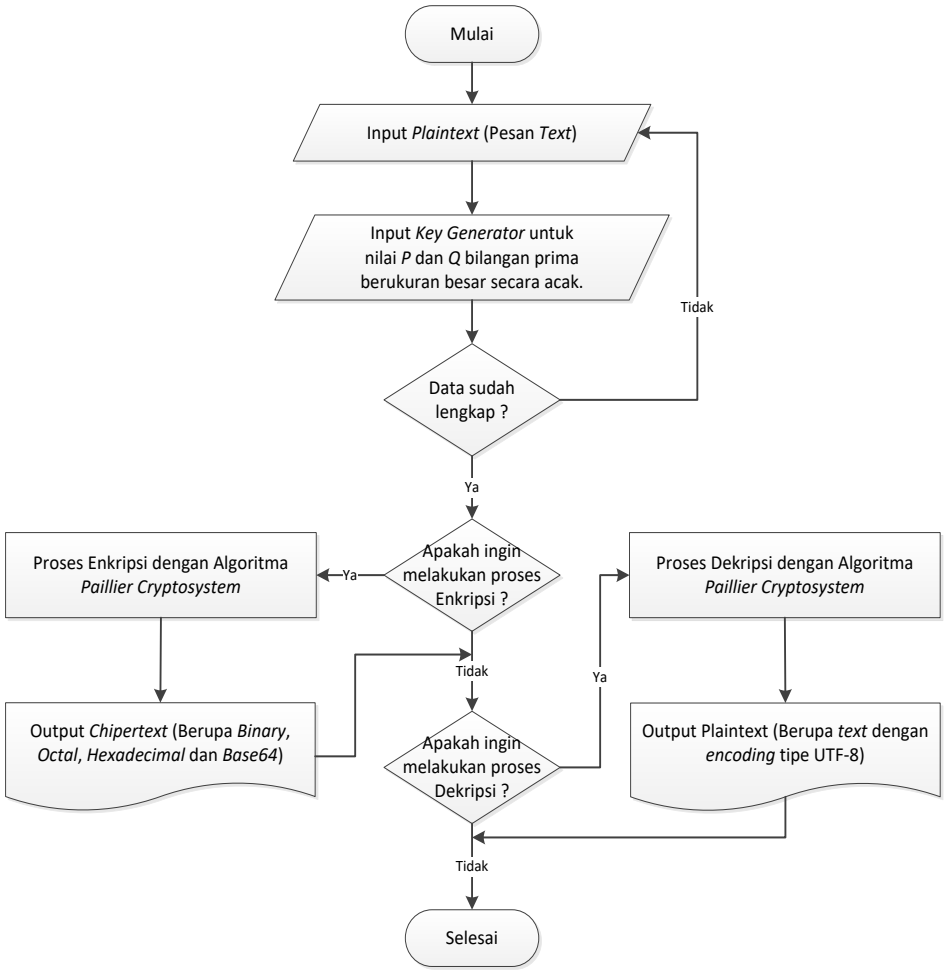


Gambar 1. *Flowchart* Tahapan Penelitian

3. HASIL DAN PEMBAHASAN

Analisis Alur Kerja Simulasi Enkripsi dan Dekripsi menggunakan Algoritma *Paillier Cryptosystem*

Analisis ini dilakukan guna memahami alur kerja simulasi algoritma *paillier cryptosystem* untuk proses enkripsi dan dekripsi pada pesan *text*. Berikut adalah gambaran *flowchart* untuk simulasi enkripsi dan dekripsi pesan *text* dengan Algoritma *Paillier Cryptosystem*.



Gambar 2. *Flowchart* simulasi enkripsi dan dekripsi pada Algoritma *Paillier Cryptosystem*

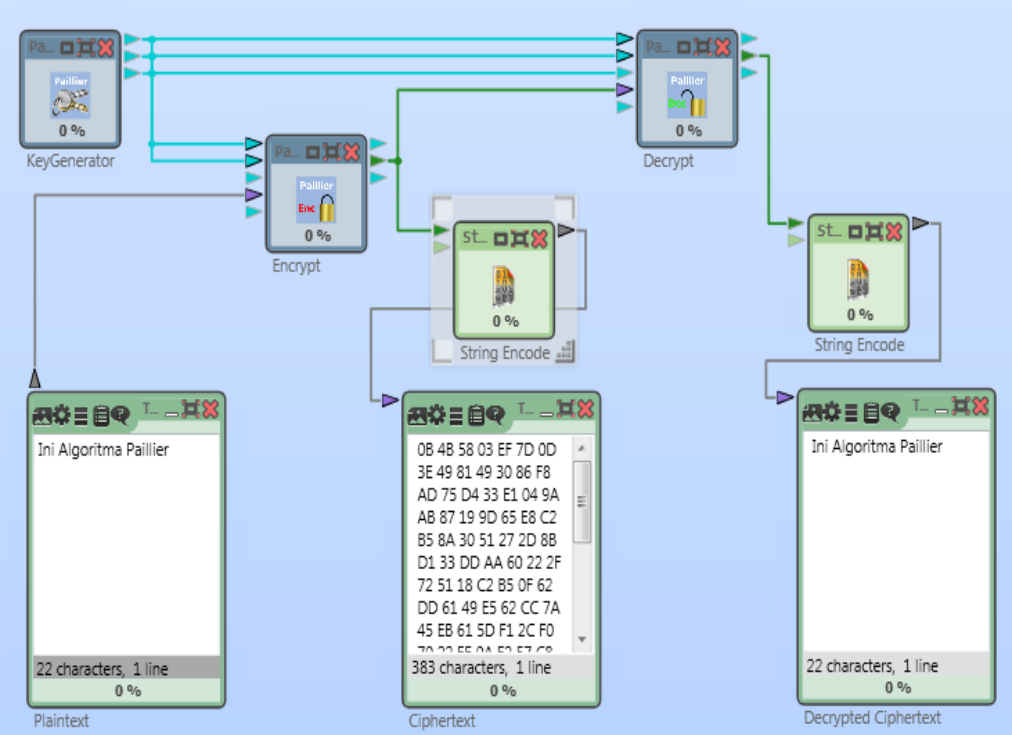
Pada *flowchart* simulasi enkripsi dan dekripsi algoritma *paillier cryptosystem* yang terlihat pada gambar 2, langkah pertama untuk melakukan simulasi enkripsi dan dekripsi pada algoritma *paillier cryptosystem*, dibutuhkan inputan berupa *plaintext* (dengan *presentattion format* tipe *text* dan tipe *encoding* UTF-8), lalu langkah kedua dibutuhan inputan *key generator* untuk nilai *P* dan *Q* berupa bilangan prima berukuran besar secara acak. Kemudian jika semua data telah selesai diinput, proses selanjutnya akan dilakukan proses perhitungan enkripsi dan dekripsi pada algoritma *paillier cryptosystem* pada setiap kali eksekusi program simulasi dijalankan. kemudian akan dihasilkan *output* enkripsi berupa *chipertext* (dengan *presentation format* yang dapat dipilih sesuai dengan *format* sebagai berikut: *binary*, *octal*, *hexadecimal* dan *base64*). Serta akan dihasilkan *output* dekripsi dari hasil proses enkripsi sebelumnya berupa *plaintext* (*text* dengan *encoding* tipe UTF-8).

Simulasi Enkripsi dan Dekripsi Algoritma *Paillier Cryptosystem* dengan *Cryptool2*

Pembuatan simulasi enkripsi dan dekripsi pada algoritma *paillier cryptosystem* menggunakan *cryptool2* kita harus membuat desain seperti pada gambar 3 (desain enkripsi dan dekripsi mengikuti alur *flowchart* yang sudah dibuat dalam sekali eksekusi). Adapun beberapa *Properties*/*Tools* yang dibutuhkan antara lain sebagai berikut:

1. *Text input* sebanyak 1 (satu) buah, yang digunakan untuk pesan *text* yang akan dirubah ke *chipertext* (untuk proses enkripsi) dan *decrypted chipertext* (untuk proses dekripsi).
2. Key Generator sebanyak 1 (satu) buah, yang digunakan untuk menginput nilai *P* dan *Q* berupa bilangan prima berukuran besar secara acak.
3. Satu buah *encrypt paillier* yang akan digunakan untuk melakukan proses enkripsi algoritma *paillier cryptosystem*.
4. Satu buah *decrypt paillier* yang akan digunakan untuk melakukan proses dekripsi algoritma *paillier cryptosystem*.

5. Dua buah *string encode*, yang pertama untuk melakukan *encode* pada proses enkripsi menjadi *presentation format* (*binary*, *octal*, *hexadecimal* dan *base64*). Kemudian *string encode* yang kedua untuk melakukan *encode* pada proses dekripsi menjadi *presentation format* (*text* dengan *encoding* tipe *UTF-8*).
6. Dua buah *text output*, yang perama digunakan untuk menampilkan data *output* dari hasil proses enkripsi *encode*, sedangkan *text output* yang kedua digunakan untuk menampilkan data *output* dari hasil proses dekripsi *encode*.



Gambar 3. Simulasi Enkripsi dan Dekripsi pada *Algoritma Paillier Cryptosystem* dengan *Cryptool2*

Uji Coba Enkripsi dan Dekripsi Pesan *Text* Menggunakan Algoritma *Paillier Cryptosystem* dengan *Cryptool2*

Pada penelitian ini akan dilakukan pengujian terhadap simulasi enkripsi dan dekripsi pesan *text* dengan algoritma *paillier cryptosystem* menggunakan perangkat lunak *cryptool2*. Kemudian akan dilakukan uji coba *sampling* sebanyak 10 kali uji coba untuk masing-masing proses enkripsi dan dekripsi terhadap pesan *text* dengan algoritma *paillier cryptosystem*, lalu untuk sampling yang digunakan adalah ukuran/besaran pesan *text* (dengan format *.txt), lalu untuk variabel pembanding berupa waktu proses untuk enkripsi dan dekripsi. Adapun hasil uji cobanya terlihat pada tabel 1 sebagai berikut.

Tabel 1. Hasil Uji Coba Enkripsi dan Dekripsi Pesan *Text* Menggunakan Algoritma *Paillier Cryptosystem* dengan *Cryptool2*

No	Pesan Text Asli (Plaintext)		Enkripsi								Dekripsi	
			Binary (Chipertext)		**Octal (Chipertext)**		**Hexadecimal (Chipertext)**		**Base64 (Chipertext)**		**Decrypted Chipertext (Plaintext)**	
	Nama File (*.txt)	**Ukuran (Byte)**	**Ukuran (Byte)**	**Waktu (ms)**	**Ukuran (Byte)**	**Waktu (ms)**	**Ukuran (Byte)**	**Waktu (ms)**	**Ukuran (Byte)**	**Waktu (ms)**	**Ukuran (Byte)**	**Waktu (ms)**
1	Sampel 1	12,56	13,59	0,14	16,37	0,26	18,26	0,41	19,36	0,5	12,56	1,3
2	Sampel 2	54,67	55,89	0,52	58,67	0,64	60,56	0,79	61,66	0,88	54,67	1,68
3	Sampel 3	107,54	108,63	0,93	111,41	1,05	113,3	1,2	114,4	1,29	107,54	2,09
4	Sampel 4	534,89	535,99	1,68	538,77	1,8	540,66	1,95	541,76	2,04	534,89	2,84
5	Sampel 5	1132,11	1134,31	2,79	1137,09	2,91	1138,98	3,06	1140,08	3,15	1132,11	3,95

6	Sampel 6	5651,23	5654,29	4,83	5657,07	4,95	5658,96	5,1	5660,06	5,19	5651,23	5,99
7	Sampel 7	13212,45	13216,64	9,74	13219,42	9,86	13221,31	10,01	13222,41	10,1	13212,45	10,9
8	Sampel 8	57652,21	57657,38	14,35	57660,16	14,47	57662,05	14,62	57663,15	14,71	57652,21	15,51
9	Sampel 9	114232,78	114239,89	27,67	114242,67	27,79	114244,6	27,94	114245,66	28,03	114232,78	28,83
10	Sampel 10	521342,66	521351,71	39,34	521354,49	39,46	521356,4	39,61	521357,48	39,7	521342,66	40,5

4. PENUTUP

Simpulan

Berdasarkan penelitian dan hasil pengujian yang dilakukan terhadap simulasi enkripsi dan dekripsi pada pesan *text* menggunakan *algoritma paillier cryptosystem*, maka didapatkan kesimpulan sebagai berikut:

1. Ukuran pesan *text* (*byte*) sangat mempengaruhi lamanya proses enkripsi dan dekripsi suatu pesan. Semakin besar ukuran pesan *text* (*byte*), maka akan semakin lama waktu (ms) proses yang diperlukan perangkat lunak *cryptool2* untuk melakukan enkripsi dan dekripsi pesan *text*.
2. Ukuran *text file* (*byte*) dari hasil proses enkripsi mengalami kenaikan ukuran *text file* (*byte*) dari *file* originalnya. Sedangkan Ukuran *text file* (*byte*) dari hasil proses dekripsi sama dengan ukuran *text file* (*byte*) dari file originalnya.
3. *Presentation format binary* menjadi yang tercepat untuk waktu (ms) proses enkripsi dan dekripsi, sedangkan *presentation format base64* menjadi yang terlama untuk waktu (ms) untuk proses enkripsi dan dekripsi.
4. Jika nilai *P* dan *Q* yang diinputkan saat pembangkitan kunci yang bernilai cukup besar dan ukuran *text file* (*byte*) yang akan diinputkan cukup besar, maka waktu enkripsi dan dekripsi akan memerlukan waktu yang relatif lebih lama.
5. Pada proses dekripsi pesan *text* menggunakan algoritma *paillier cryptosystem*, memerlukan waktu (ms) yang relatif lebih lama dari pada proses enkripsi pesan *text*.

Saran

Berdasarkan hasil dari penelitian yang telah dilakukan oleh peneliti, berikut ini beberapa saran untuk pengembangan simulasi enkripsi dan dekripsi menggunakan algoritma *paillier cryptosystem* dengan perangkat lunak *cryptool2*, antara lain:

1. Untuk pengembangan penelitian ini, bisa dikembangkan suatu simulasi enkripsi dan dekripsi dengan *presentation format* selain *binary*, *octal*, *hexadecimal* maupun *base64* atau bisa juga mengkombinasikan antara algoritma simetris dan asimetris (secara *hybrid*), sehingga tingkat keamanan terhadap data dan informasi menjadi semakin terjamin dan aman.
2. Pada perancangan simulasi enkripsi dan dekripsi menggunakan Algoritma *Paillier Cryptosystem* diharapkan kedepannya dapat men-support file ekstensi selain *.txt seperti file bertipe *.pdf, *.jpeg, *.doc, video, dan audio.

DAFTAR PUSTAKA

[1] S. Roychowdhury, T. T. Allen, and N. B. Allen, "A genetic algorithm with an earliest due date encoding for scheduling automotive stamping operations," *Comput. Ind. Eng.*, vol. 105, pp. 201–209, Mar. 2017, doi: 10.1016/j.cie.2017.01.007.

[2] "Effective Key Distribution Scheme using Paillier Cryptosystem in Wireless Sensor Networks," doi: 10.35940/ijitee.I8164.078919.

[3] C. Jost, H. Lam, A. Maximov, and B. Smeets, "Encryption Performance Improvements of the Paillier Cryptosystem."

[4] C. Zaraket, M. Chamoun, and T. Nicolas, "Calculating the average using Paillier's cryptosystem," 2019.

[5] I. W. Aditya Eka Prabawa -, K. Kunci, K. Privat, and K. Publik, "Analisis Perbandingan dan Pengujian Algoritma Kunci Publik RSA dan Paillier."

[6] J. A. N. Purba, T. Zebua, and R. K. Hondro, "IMPLEMENTASI ALGORITMA PAILLIER CRYPTOSYSTEM PENGAMANAN CITRA DIGITAL PADA APLIKASI CHAT," *KOMIK (Konferensi Nas. Teknol. Inf. dan Komputer)*, vol. 3, no. 1, Nov. 2019, doi: 10.30865/komik.v3i1.1605.

[7] F. Knirsch, A. Unterweger, M. Unterrainer, and D. Engel, "Comparison of the Paillier and ElGamal

Cryptosystems for Smart Grid Aggregation Protocols." Accessed: Aug. 31, 2020. [Online]. Available: https://orcid.org/0000-0002-6346-5759.

[8] U. P. Setyaningrum, "ALGORITMA PAILLIER CRYPTOSYSTEM UNTUK MENGAMANKAN CITRA DIGITAL," 2017.

[9] "IJESRT INTERNATIONAL JOURNA An Enhanced Paillier's Algorithm Using Homomorphic Encryption," 2013. Accessed: Jan. 13, 2021. [Online]. Available: http://www.ijesrt.com.

[10] T. Lia, "Pemanfaatan Paillier Cryptosystem untuk Low Cost Secure Direct-Recording Electronic (DRE." Accessed: Aug. 31, 2020. [Online]. Available: https://www.academia.edu/29725537/Pemanfaatan_Paillier_Cryptosystem_untuk_Low_Cost_Secure_Direct_Recording_Electronic_DRE.

[11] J. A. N. Purba, D. Sinaga, and S. R. Purba, *Seminar Nasional Teknologi Komputer & Sains (SAINTEKS)*, vol. 1, no. 1. 2019.