Available *online* at : http://bit.ly/InfoTekJar

InfoTekJar : Jurnal Nasional Informatika dan Teknologi Jaringan

ISSN (Print) 2540-7597 | ISSN (Online) 2540-7600

Kriptografi

Pengamanan File Teks Menggunakan Algoritma RSA – LUC dan Algoritma Zig-Zag dalam Hybrid Crypto Sistem

Rahmi Suliani Lubis [1], Tulus [2], Erna Budhiarti Nababan [3]

[1,3]*Fakultas Ilmu Komputer dan Teknologi Informasi, Universitas Sumatera Utara, Medan, Indonesia*
[2]*Fakultas Matematika dan Ilmu pengetahuan Alam, Universitas Sumatera Utara Medan, Indonesia*

KEYWORDS

Kriptografi, RSA, LUC, Zig Zag, hybrid crypto sistem

CORRESPONDENCE

Phone: +6281375094001

E-mail: tulus@usu.ac.id

A B S T R A C T

Kriptografi adalah ilmu yang berdasarkan pada teknik matematika untuk berurusan dengan keamanan informasi seperti kerahasiaan, keutuhan data dan otentifikasi entitas. Hybrid crypto metode untuk mengunci plainteks dengan algoritma simetris dan menggunakan algoritma asimetris untuk mengunci algoritma simetris. Tujuan dari penelitian ini adalah kriptografi masih memiliki kelemahan oleh karena itu peneliti menggabungkan zig-zag dan RSA dengan kunci LUC dalam mengenkripsi pesan. Dalam penelitian digunakan pembangkit kunci pada algoritma LUC. hybrid kriptosistem merupaka metode untuk mengunci algortima plainteks dengan algoritma simetris dan asimetris digunakan untuk mengamankan algoritma simetris. Algoritma digunakan untuk mengenkripsi plainteks sedangkan algoritma RSA-LUC untuk mengenkripsi kunci zig-zag. Hasil dari penelitian ini adalah Semakin panjang jumlah karakter maka semakin lama proses yang dibutuhkan untuk proses enkripsi pada file teks. Dan semakin besar ukuran file, maka semakin besar ukuran ciphertext yang dihasilkan.

PENDAHULUAN

Pesan merupakan suatu informasi yang dapat dibaca dan dimengerti maknanya. Masalah keamanan merupakan salah satu aspek terpenting dari sebuah pesan . Keamanan adalah masalah besar dan mengamankan data yang sangat penting, sehingga data tidak dapat disadap atau disalah gunakan untuk tujuan yang tidak baik dan merugikan orang lain[1]. Data yang disampaikan terkadang sering mengandung informasi penting bahkan sangat rahasia dan harus dijaga keamanannya [2].

Kriptografi juga disebut sebagai “tulisan rahasia”, adalah ilmu dan seni mengubah pesan menjadi teks rahasia yang tidak dapat dibobol oleh pengguna yang tidak berwenang [3]. Salah satu algoritma kriptografi yang dapat digunakan adalah RSA merupakan algoritma kriptografi modern yang termasuk salah satu algoritma kriptografi asimetris. Algoritma RSA dianggap sebagai sebagai algoritma enkripsi kunci public yang paling baik sejauh ini. Ini telah banyak diterapkan untuk enkripsi dan dekripsi. Panjang kunci RSA meningkat seiring dengan peningkatan tingkat kerahasiaan[4] .

Algoritma LUC adalah untuk pengkodean teks dilakukan menggunakan generator kunci (publik dan pribadi), prosesnya menggunakan enkripsi dan dekripsi. Selain itu algoritma LUC dapat memproses enkripsi dan dekripsi dengan baik untuk huruf kapital [5].

Algoritma zig-zag merupakan salah satu algoritma kriptografi klasik yang menggunakan teknik transposisi. Teknik transposisi adalah memanfaatkan karakter permutasi, dimana dengan menggunakan teknik ini pesan asli tidak dapat terbaca kecuali orang yang memiliki kunci untuk mengembalikan pesan dalam bentuk aslinya [1].

Dalam penelitian ini pengamanan File Teks menggunakan Algoritma RSA-LUC dan Algoritma zig-zag dalam hybrid crypto sistem. Kriptografi masih memiliki kelemahan oleh karena itu penelitian ini menggabungkan zig-zag dan RSA dengan kunci LUC dalam mengenkripsi pesan. Dalam penelitian ini digunakan pembangkit kunci pada algoritma LUC. Hybrid kriptosistem merupakan metode untuk mengunci algoritma plainteks dengan algoritma simetris dan asimetris digunakan untuk mengamankan algoritma simetris. Algoritma zig-zag digunakan untuk mengenkripsi plainteks sedangkan algoritma RSA-LUC untuk mengenkripsi kunci zig-zag.

https://doi.org/10.30743/infotekjar.v6i2.4717

METODOLOGI PENELITIAN

A. Algoritma RSA

RSA dikenal sebagai algortima kriptografi modern yang dapat mengatur panjang kunci. Kunci akan sulit dipecahkan apabila nilai bit panjang karena pemfaktoran bilangan yang besar menjadi lebih sulit.untuk mengurangi serangan digunakan RSA yaitu algoritma kriptografi yang efektif untuk memperbanyak langkah dalam mengurangi serangan. Jika terdapat penyusup maka pengirim dapat dihentikan dan tidak akan menerima pesan yang dikirim[6] .

Proses pembangkitan kunci pada kriptografi RSA adalah sebagai berikut [7]:

Step 1 : membangkitkan kunci

1. Pilih dua buah bilangan prima sembarangan p dan q. Jaga kerahasiaan p dan q.
2. Hitung $n = p * q$ Besaran n ini tidak perlu dirahasiakan.
3. Hitung $\phi(n) = (p-1) * (q-1)$. Sekali m telah dihitung, p dan q dapat dihapus untuk mencegah diketahuinya oleh pihak lain.
4. Pilih sebuah bilangan acak untuk kunci publik, sebut namanya e, yang relatif prima terhadap ϕ (relatif prima berarti GCD(e, ϕ) = 1dengan syarat $1 < e < \phi(n)$.
5. Hitung kunci dekripsi d, dengan kekongruenan $ed \equiv 1(mod\ \phi(n))$.

Step 2 : mencari enkripsi

Proses enkripsi pesan menggunakan kunci publik dari hasil pembangkitan kunci dengan menggunakan rumus :

$$C = M^e \ mod\ N \qquad (1)$$

Menggunakan kunci yang diperoleh diatas kita akan mencoba untuk melakukan enkripsi pesan

Step 3 : mencari dekripsi

Untuk mengembalikan pesan *ciphertext* menjadi *plaintext* (pesan asli) adalah dengan menggunakan rumus dekripsi RSA sebagai berikut :

$$M = C^d \ mod\ N \qquad (2)$$

Dengan menggunakan pesan hasil enkripsi dari kunci yang diperoleh diatsa dapat dilakukan dekripsi pesan.

B. Algoritma LUC

Ditahun 1993, Smith dan Lennon memperkenalkan algoritma kriptografi asimetris yang berbasis pada fungsi lucas (*Lucas Function)*. Fungsi Lucas (*lucas function*) dapat dijabarkan sebagai berikut[8]

Masukkan nilai a dan b menjadi persamaan akar polinomial x^2 - Px + Q = 0. Kemudian P = a + b dan Q = ab. Pada umumnya kedua linier berulang tersebut adalah:

$$U_n = (a^n - b^n) / (a - b) \qquad (1)$$

$$V_n = a^n + b^n \qquad (2)$$

Ada dua fungsi yang bisa diturunkan dari persamaan (1) dan (2). adalah:

$$U_{n+1} = PU_n - QU_{n-1} \qquad (3)$$

$$V_{n+1} = PV_n - QV_{n-1} \qquad (4)$$

Kemudian, pada persamaan (4) dapat diturunkan,

$$V_n = PV_{n-1} - V_{n-2} \qquad (5)$$

Di mana n ≥ 2, V0 = 2 dan V1 = P

Beberapa persamaan saling berkaitan dan digunakan dengan menambahkan teknik. :

$$V_{2n} = V_{n2-2} \qquad (6)$$

$$V_{2n+1} = PV_{n2} - V_nV_{n-1} - P \qquad (7)$$

$$V_{2n-1} = V_nV_{n-1} - P \qquad (8)$$

Algoritma LUC merupakan algoritma kunci publik dalam kriptografi. Terdapat tiga bagian utama dalam algoritma LUC, yaitu [9]:

Proses Pembangkit Kunci dengan Algoritma LUC

a. Anbil dua buah bilangan prima, misalkan p dan q dimana p ≠ q.
b. Hitunglah nilai n = p x q.
c. Hitung nilai t = (p-1).(q-1).(p+1).(q+1).
d. Ambil sebuah bilangan acak di mana bilangan tersebut (1< e < t) kemudian bilangan acak tersebut merupakan bilangan bulat. Bilangan acak disimbolkan dengan e.
e. Kemudian hitung nilai gcd(e,t)=1 atau e *relative* prima terhadap t.
f. Hitung nilai R(n) dengan rumus: R(n) = LCM (p-1, q-1, p+1, q+1).

C. Algoritma zig-zag

zig-zag *cipher* adalah salah satu dari algoritma kriptografi klasik yang menggunakan teknik transposisi.teknik transposisi menggunakan permutasi karakter, yang mana dengan menggunakan teknik ini pesan yang asli tidak dapat dibaca kecuali orang yang memiliki kunci untuk mengembalikan pesan seperti semula [10].cara agar algoritma zig-zag sama kuatnya dengan algoritma modern yaitu memakai bilangan ASCII.

Jika transposisi zig-zag dilakukan berturut-turut, maka pesan yang akan dibaca dalam mode zig-zag berdasarkan angka dalam kunci. Jika kuncinya adalah j, maka pesan akan dibaca dalam urutan sebagai berikut dalam posisi *matrix.*

(j, 1) (j+1, 2) (j, 3) (j+1 , 4) (j, 5)

Jika dilakukan sama yang dilakukan kolom, maka pesan akan dibaca sebagai berikut :

(1, j) (2, j+1) (3 , j) (4 , j+1) (5, j)

Jumlah digit pada kunci *(key)* yang digunakan pada algoritma zig-zag tergantung pada jumlah baris jika menggunakan kolom transposisi.

Rancangan penelitian

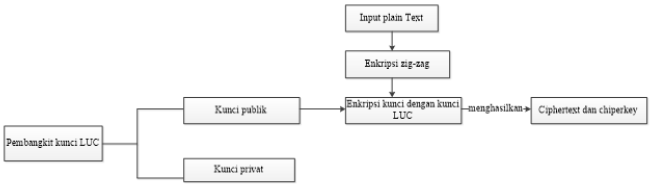
Penelitian ini menggunakan algoritma zig-zag dan algoritma RSA dengan kunci LUC yang dapat dilihat dalam gambar arsitektur penelitian. Arsitektur umum proses enkripsi dan dekripsi dapat dilihat pada gambar dibawah ini :

 https://doi.org/10.30743/infotekjar.v6i2.4717

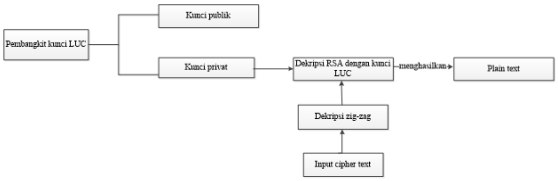
HASIL DAN PEMBAHASAN

A. Enkripsi Algoritma RSA-LUC dan Algoritma zig-zag

Pada penelitian ini, melakukan pengujian enkripsi untuk pengamanan file teks menggunakan algoritma RSA-LUC dan algoritma zig-zag dalam hybrid crypto sistem. Dalam pengujian ini mengetahui jumlah karakter yang menggunakan ASCII 8 bit dan kunci yang digunakan dengan kunci LUC. pengujian terhadap 10 karakter yang berbeda-beda. Hasil pengujian enkripsi terhadap algoritma RSA-LUC dan algoritma zig-zag sebagai berikut :



Gambar 1. Enkripsi pesan



Gambar 2. Dekripsi pesan

Tahap enkripsi dan dekripsi yang berurtan. Tahap awal membangkitkan pembangkit kunci LUC. pada langkah ini menghasilkan kunci pribadi. Setelah mendapatkan nilai p dan q selanjutnya akan dihitung nilai d untuk menghasilkan kunci privat yang mana kunci privat digunakan untuk proses enkripsi. Langkah kedua input plainteks dimana akan dimasukkan dokumen yang dienkripsi. Langkah ketiga pengirin akan melakukan enkripsi dengan algoritma zig-zag dan algoritma RSA menggunakan kunci LUC dan akan dihasilkan kunci chipertext yang kemudian akan dikirim kepada sipenerima.

Tahap dekripsinya adalah membangkitkan kunci LUC pada langkah ini menghasilkan kunci pribadi. Setelah mendapatkan nilai p dan q selanjutnya akan dihitung nilai d untuk menghasilkan kunci privat yang mana kunci privat digunakan untuk proses dekripsi. Langkah kedua input ciphertext diamana akan memasukkan hasil enkripsi yang telah diproses oleh enkripsi. Selanjutnya melakukan dekripsi terhadap chiphertext dengan menggunakan kunci privat. Setelah melakukan dekripsi penerima akan mendapatkan plainteks atau pesan asli.

Tabel 1. hasil enkripsi algoritma RSA-LUC dan algoritma zig-zag

No	Plain Teks	Algoritma RSA + LUC	Algoritma Zig-Zag
1	TEKNIK INFORMATIKA	412 17 1 1657 1807 567 2271 1011	E I ATIKNIK ONFARMKT
2	SAYA BELAJAR MOBIL	148 244 282 358 1 372 267 272	JMR A ALB S YEAA IOB L
3	S1 ILMU KOMPUTER	2709 2081 3624 3091 527 3136 1052 1	E1UOKPMT ML URSI
4	UNIVERSITAS SUMATERA UTARA	1 2542 4235 1534 2392 4032 1914 4073	URIIEAS TURATUSAR SEMA AT N V
5	SMAN 7 MEDAN	1 358 92 361 894 629 898 96	SNA7 MEN DA M
6	SISWA KELAS X	1327 147 3083 2803 2874 1466 2238 1	X AEL IS KAS SW
7	PERPANJANG SIM	1 3333 600 175 1012 2556 4009 995	PPNSAA MI ERNJG
8	KELUARGA BAHAGIA	1139 1373 1330 1 1060 900 905 1072	AALR HKUIEGBAGAA
9	RAHMI SULIANI LUBIS	1152 737 196 941 131 871 1 809	A MU IBLSALU II NRIHS
10	DINDA AGUSTINA LUBIS	1550 1000 1257 1947 2168 1 1702 153	SAI I DG NU LSBDANI ATU

Pada tabel 1 menjelaskan hasil enkripsi algoritma RSA-LUC dan Algoritma zig-zag sehingga menghasilkan chipertext yang acak. Berdasarkan ciphertext dari algoritma RSA-LUC dan Algoritma zig-zag misalkan contohnya “TEKNIK INFORMATIKA” langkah pertama adalah mengambil dua bilangan prima p = 83 q =59 setelah itu langkah selanjutnya adalah mengalikan p dan q dan diperoleh nilai n = 4897 dan diperoleh nilai e = 47 dan d = 297503. Dengan menggunakan rumus enkripsi maka hasil chiperkeynya adalah 1 4179 73 1132 204 3302 4418 62 setelah itu hasil chipertextnya adalah TIKFARI A E ONNIKMKT

B. Dekripsi Algoritma RSA-LUC dan Algoritma zig-zag

Pada penelitian ini, melakukan pengujian dekripsi untuk pengamanan file teks menggunakan algoritma RSA-LUC dan algoritma zig-zag dalam hybrid crypto sistem. Dalam pengujian ini mengetahui jumlah karakter yang menggunakan ASCII 8 bit dan kunci yang digunakan dengan kunci LUC. pengujian terhadap 10 karakter yang berbeda-beda. Hasil pengujian dekripsi terhadap algoritma RSA-LUCdan algoritma zig-zag sebagai berikut :

Tabel 2. hasil dekripsi algoritma RSA-LUC dan algoritma zig-zag

No	Algoritma RSA + LUC	Algoritma Zig-Zag	Plain Teks
1	412 17 1 1657 1807 567 2271 1011	E I ATIKNIK ONFARMKT	TEKNIK INFORMATIKA
2	148 244 282 358 1 372 267 272	JMR A ALB S YEAA IOB L	SAYA BELAJAR MOBIL
3	2709 2081 3624 3091 527 3136 1052 1	E1UOKPMT ML URSI	S1 ILMU KOMPUTER
4	1 2542 4235 1534 2392 4032 1914 4073	URIIEAS TURATUSAR SEMA AT N V	UNIVERSITAS SUMATERA UTARA
5	1 358 92 361 894 629 898 96	SNA7 MEN DA M	SMAN 7 MEDAN
6	1327 147 3083 2803 2874 1466 2238 1	X AEL IS KAS SW	SISWA KELAS X
7	1 3333 600 175 1012 2556 4009 995	PPNSAA MI ERNJG	PERPANJANG SIM
8	1139 1373 1330 1 1060 900 905 1072	AALR HKUIEGBAGAA	KELUARGA BAHAGIA
9	1152 737 196 941 131 871 1 809	A MU IBLSALU II NRIHS	RAHMI SULIANI LUBIS
10	1550 1000 1257 1947 2168 1 1702 153	SAI I DG NU LSBDANI ATU	DINDA AGUSTINA LUBIS

Pada tabel 2 menjelaskan hasil dekripsi algoritma RSA-LUC dan algoritma zig-zag. Hasil dari chiperteks "TIKFARI A E ONNIKMKT " akan kembali plainteks menjadi "TEKNIK INFORMATIKA". Dimana hasil akhir kembali keplainteks awal.

C. Pengujian

Hasil pengujian ini untuk mengetahui panjang plainteks terhadap lama proses enkripsi pesan dengan menggunakan algoritma RSA-LUC dan algoritma zig-zag

Tabel 3. Hasil panjang plainteks dan kecepatannya

No	Plain Teks	waktu
1	TEKNIK INFORMATIKA	4,1987 ms
2	SAYA BELAJAR MOBIL	3,324 ms
3	S1 ILMU KOMPUTER	3,6193 ms
4	UNIVERSITAS SUMATERA UTARA	2,687 ms
5	SMAN 7 MEDAN	3,2388 ms
6	SISWA KELAS X	2,4245 ms
7	PERPANJANG SIM	3,6257 ms
8	KELUARGA BAHAGIA	3,8271 ms
9	RAHMI SULIANI LUBIS	3,0623 ms
10	DINDA AGUSTINA LUBIS	3,4211 ms

Hasil pengujian ini untuk mengetahui panjang chipertext terhadap lama proses dekripsi.

Table 4. hasil panjang chipertext dan kecepatannya

No	chipherteks	waktu
1	E I ATIKNIK ONFARMKT	21,5564 ms
2	JMR A ALB S YEAA IOB L	0,7112 ms
3	E1UOKPMT ML URSI	53,7919 ms
4	URIIEAS TURATUSAR SEMA AT N V	53,1954 ms
5	SNA7 MEN DA M	0,5847 ms
6	X AEL IS KAS SW	13,7199 ms
7	PPNSAA MI ERNJG	10,1713 ms
8	AALR HKUIEGBAGAA	5,4588 ms
9	A MU IBLSALU II NRIHS	1,0963 ms
10	SAI I DG NU LSBDANI ATU	2,4526 ms

Berdasarkan tabel 3 dan 4 dapat diketahui bahwa lama waktu proses enkripsi dan dekripsi berbeda sehingga sistem membutuhkan waktu yang lama untuk melakukan proses enkripsi pesan dibandingkan dengan proses enkripsi.

KESIMPULAN

Berdasarkan hasil akhir dari pengujian yang diperoleh dapat disimpulkan adalah pada penelitian ini algoritma RSA- LUC yang digunakan pada saat enkripsi harus sama jumalah chiphertext yang digunakan untuk pada saat dekripsi untuk menghasilkan plainteks yang sama. Semakin panjang jumlah karakter maka semakin lama proses yang dibutuhkan untuk proses enkripsi pada file teks. Dan semakin besar ukuran file, maka semakin besar ukuran ciphertext yang dihasilkan.

DAFTAR PUSTAKA

[1] D. Rachmawati, M. A. Budiman, and R. S. Lubis, "A hybrid cryptosystem based on zig-zag algorithm and Rivest Shamir Adleman (RSA) algorithm," *IOP Conf. Ser. Mater. Sci. Eng.*, vol. 434, p. 012046, Dec. 2018, doi: 10.1088/1757-899X/434/1/012046.

[2] H. Mawengkang, A. F. Siregar, and S. Efendi, "Combination analysis of ElGamal algorithm and LUC algorithm in file security," *IOP Conf. Ser. Mater. Sci. Eng.*, vol. 420, p. 012130, Oct. 2018, doi: 10.1088/1757-899X/420/1/012130.

[3] F. J. Aufa, Endroyono, and A. Affandi, "Security System Analysis in Combination Method: RSA Encryption and Digital Signature Algorithm," in *2018 4th International Conference on Science and Technology (ICST)*, Yogyakarta, Aug. 2018, pp. 1–5. doi: 10.1109/ICSTC.2018.8528584.

[4] A. Chhabra and S. Mathur, "Modified RSA Algorithm: A Secure Approach," in *2011 International Conference on Computational Intelligence and Communication Networks*, Gwalior, India, Oct. 2011, pp. 545–548. doi: 10.1109/CICN.2011.117.

[5] M. Annalakshmi, "Zigzag Ciphers: A Novel Transposition Method," *Int. J. Comput. Appl.*, p. 5.

[6] M. Shankar and A. P, "Hybrid Cryptographic Technique Using RSA Algorithm and Scheduling Concepts," *Int. J. Netw. Secur. Its Appl.*, vol. 6, no. 6, pp. 39–48, Nov. 2014, doi: 10.5121/ijnsa.2014.6604.

[7] N. P. Smart, *Cryptography Made Simple*. Cham: Springer International Publishing, 2016. doi: 10.1007/978-3-319-21936-3.

[8] P. P. Sari, E. Budhiarti Nababan, and M. Zarlis, "Comparative Study of LUC, ElGamal and RSA Algorithms in Encoding Texts," in *2020 3rd International Conference on Mechanical, Electronics, Computer, and Industrial Technology (MECnIT)*, Medan, Indonesia, Jun. 2020, pp. 148–151. doi: 10.1109/MECnIT48290.2020.9166586.

[9] Z. M. Ali, M. Othman, M. R. M. Said, and M. N. Sulaiman, "Two Fast Computation Algorithms for LUC Cryptosystems," p. 5, 2007.