JAINS (Journal of Artificial Intelligence and Network Systems)
Vol. 1 No. 1, September 2025

PERBANDINGAN TEKNIK ALGORITMA RSA DENGAN ALGORITMA ELGAMAL DALAM MENINGKATKAN NILAI ENTROPY DALAM CHIPERTEXT

Tengku Didi Ferdillah[1)], Achmad Fauzi[2)]

[1,2)]STMIK Kaputama
Jl. Veteran No.4A, Tangsi, Kec. Binjai Kota, Kota Binjai, Sumatera Utara 20714
Email: tengkudidiferdillah23@gmail.com

ABSTRACT

This study examines the entropy values of the RSA and ElGamal algorithms in the context of cryptographic data security. Both algorithms are widely used asymmetric encryption methods in various information security applications. Entropy is utilized to measure the level of randomness and uncertainty in the encrypted data, which correlates to the system's security level. The research analyzes the output of both algorithms using the same input data and various cryptographic key sizes. This study provides in-depth insights into the performance of RSA and ElGamal algorithms from the perspective of entropy, aiding in the selection of the appropriate algorithm based on specific application needs.

Keywords: *Ciphertext, Data_Security, ElGamal, Entropy, RSA.*

1. PENDAHULUAN

Dizaman sekarang Data telah menjadi aset yang sangat berharga bagi individu, organisasi, dan pemerintahan di era digital yang semakin berkembang. Perkembangan teknologi informasi dan komunikasi telah meningkatkan efisiensi pengelolaan data besar, tetapi juga meningkatkan ancaman keamanan data. Beberapa ancaman yang sering terjadi termasuk kebocoran data, pencurian identitas, dan serangan siber, yang dapat menyebabkan kehilangan uang, reputasi, dan pelanggaran privasi[1]. Oleh karena itu, keamanan data menjadi prioritas utama di banyak bidang, seperti keuangan, kesehatan, dan pemerintahan. Salah satu metode yang paling efektif untuk melindungi data adalah enkripsi, yang merupakan proses mengubah data menjadi format yang tidak dapat dibaca dengan menggunakan kunci tertentu, yang memungkinkan hanya pihak yang berwenang yang dapat mengaksesnya[2]. Enkripsi telah menjadi teknologi kunci yang sangat penting untuk menjaga kerahasiaan, integritas, dan ketersediaan data, baik secara online maupun offline.

Adapun nama algoritma RSA berasal dari kode kriptografi kunci publik, penyelidik Ron Rivest, Adi Shamir, dan Leonard Adleman. MIT membuat RSA pada tahun 1977, dan mendapatkan paten pada tahun 1983. Patent tersebut berakhir pada September 2000, dan sejak saat itu, semua orang dapat menggunakannya dengan bebas.

Algoritma RSA adalah algoritma yang mudah digunakan dan dipahami. RSA menggunakan banyak teori, seperti algoritma Euclid yang diperluas, fungsi Euler hingga teoremafermat[1].

Sedangkan bagi algoritma Elgamal untuk menyelesaikan masalah dengan logaritma diskrit pada modul prima yang besar, namun algoritma ini memiliki keunggulan dalam pembangkitan kunci yang menggunakan logaritma diskrit dan metode enkripsi dekripsi yang memerlukan proses komputasi yang besar, yang membuat hasil enkripsi dua kali lipat dari ukuran aslinya.Dalam Analisa Algoritma

Elgamal Dalam Penyandian Data Sebagai Keamanan Database, metode elgamal telah digunakan dengan sukses untuk melindungi konten database menjadi teks rahasia yang tidak dapat dibaca oleh orang yang tidak diizinkan[2].
Keamanan informasi sangat penting, terutama dengan meningkatnya kebutuhan untuk melindungi data sensitif dari ancaman pihak yang tidak berwenang. Penggunaan ciphertext untuk menyembunyikan informasi asli (plaintext) melalui berbagai metode enkripsi adalah komponen penting dalam kriptografi[3]. Dalam konteks ini, evaluasi keamanan ciphertextseringkali dikaitkan dengan sifat statistiknya, salah satunya adalah entropi.

Dalam kriptografi, entropi digunakan untuk mengukur kerandomanciphertext yang dibuat oleh algoritma enkripsi. Nilai entropi suatu ciphertext menunjukkan bahwa lebih sulit bagi pihak tidak berwenang untuk memprediksi informasi yang terkandung di dalamnya Akibatnya, tingkat keamanan ciphertext meningkat seiring dengan nilai entropinya
Karena ada banyak teknik serangan pada sistem kriptografi, pendekatan berbasis entropi ini menjadi relevan.

2. METODOLOGI PENELITIAN

2.1 Jenis Penelitian

Penelitian ini adalah penelitian eksperimental, bertujuan untuk membandingkan algoritma RSA dan ElGamal dalam meningkatkan nilai entropy pada ciphertext yang dihasilkan.

2.2 Elgamal

Dalam kriptografi, algoritma ElGamal termasuk dalam kategori algoritma asimetris.
Keamanan algoritma ElGamalterletak pada masalah penghitungan logaritma diskrit pada bilangan modulo prima yang besar. Menyelesaikan masalah logaritma ini sangat sulit. ElGamal Algoritma mempunyai kunci rahasia satu bilangan dan kunci publik tiga pasang bilangan. Cipherteks algoritma ini panjangnya dua kali lipat dari plainteksnya. Walau bagaimanapun, algoritma ini memiliki kelebihan pada enkripsi karena dapat memberikan cipherteks yang berbeda dan lebih pasti untuk plainteks yang sama setiap kali plainteks dienkripsi [3].
Dalam proses enkripsi, kunci publik (p,α,β) dan sebuah bilangan integer acak k (k ε {0,1,...,p-1) digunakan, yang masing-masing dijaga rahasia oleh penerima yang mengenkripsi pesan. Bilangan k yang berbeda digunakan untuk mengenkripsi setiap karakter dalam pesan. Satu karakter yang diwakili dengan bilangan Kode dalam format bulat ASCII akan dihasilkan sebagai blok yang terdiri dari dua nilai (r, t) [3].

2.3 Algoritma RSA

Algoritma RSA adalah blok cipher yang meletakkan semua informasi ke dalam integer[4]. Kunci publik dan privat algoritma dapat diketahui oleh semua orang, tetapi kunci privat hanya diketahui oleh satu orang. diketahui oleh pemilik data baik enkripsi maupun dekripsi dilakukan dengan kunci publik pemilik data. Salah satu kekuatan algoritma RSA adalah kesulitan memfaktorkan bilangan besar menjadi faktor-faktor bilangan primanya, yang berarti bahwa bilangan prima yang lebih besar digunakan lebih aman atau baik. Cryptography menggunakan tiga langkah dalam algoritma RSA: enkripsi, pembangkitan kunci publik dan privat, dan dekripsi. Untuk membuat dua kunci, digunakan dua bilangan prima acak yang besar [4].
Dalam RSA, proses enkripsi adalah proses selanjutnya setelah pembangkitan kunci. Proses ini mengubah pesan asli (plaintext) menjadi pesan rahasia (ciphertext), dengan pesan asli terlebih dahulu diubah ke dalam bentuk desimal, kemudian pesan dalam bentuk desimal kemuadian dibagi menjadi beberapa blok desimal secara teratur. Nilai dalam setiap blok desimal harus lebih kecil dari nilai n, yang disebut P [4].

2.4 Nilai Entropy

Entropi Shannon adalah sebuah ukuran yang digunakan untuk menghitung ketidakpastian dari suatu variabel acak. Dalam konteks teori informasi, entropi ini memegang peran kunci sebagai dasar untuk memahami dan mengukur informasi. Shannon memperkenalkan konsep ini dalam karyanya yang monumental di tahun 1948 tentang teori komunikasi. Entropi Shannon dihitung menggunakan formula berikut:

$$H(P) = -\sum_{i=1}^{N} p_i \ln(p_i)$$

Di mana:

- Pi adalah probabilitas terjadinya kejadian i,
- H(P) adalah total entropi atau ukuran ketidakpastian dalam distribusi probabilitas P,
- N adalah jumlah total kejadian.

Shannon mengajukan bahwa ukuran informasi H(P) harus memenuhi tiga syarat utama, yaitu:

1. **Kontinuitas terhadap probabilitas:** Fungsi H harus bersifat kontinu terhadap nilai probabilitas Pi. Artinya, perubahan kecil dalam pip_ipi tidak akan menyebabkan perubahan drastis pada nilai H.
2. **Monotonik terhadap jumlah kejadian:** Jika semua probabilitas sama besar, maka H harus meningkat seiring bertambahnya jumlah kejadian N.
3. **Sifat aditif:** Jika sebuah sistem dapat dipecah menjadi dua subsistem independen, maka entropi total sistem sama dengan jumlah entropi dari masing-masing subsistem.

Shannon membuktikan bahwa fungsi H(P) sebagaimana dinyatakan dalam formula di atas memenuhi ketiga kondisi tersebut. Oleh karena itu, fungsi ini menjadi standar untuk mengukur informasi dalam berbagai bidang aplikasi, mulai dari telekomunikasi hingga analisis data.

Entropi Shannon sering digunakan untuk menentukan ukuran informasi yang terdapat dalam sinyal, terutama dalam aplikasi seperti registrasi citra multi-modalitas, evaluasi pola penyebaran perkotaan, dan klasifikasi sinyal biometrik seperti EKG [5].

2.5 Tahap Penelitian

a. Pengumpulan Data

Data berupa sebuah plain teks "INFORMATIKA" yang kemudian dienkripsi menggunakan algoritma RSA dan Elgamal untuk menghasilkan 2 chipertext dari masing-masing algoritma tersebut. Proses perhitungan chipertext dilakukan dengan microsoftexcel.

b. Pengukuran Nilai Entropy

Masing-masing chipertext dihitung nilai entropy-nya dengan rumus Shannon Entropy sebagai berikut :

$$H = -\sum_{i=1}^{n} p_i \log_b(p_i)$$

Pi = probabilitas kemunculan karakter i.
n = jumlah karakter unik.
b = basis logaritma

Pengukuran nilai entropy ini juga akan dilakukan peneliti dengan microsoftexcel.

c. Perbandingan dan Analisis

Membandingkan hasil nilai entropy dari ciphertext yang dihasilkan oleh algoritma RSA dan ElGamal, semakin tinggi nilai entropy maka semakin acak stringchipertext tersebut.

3. HASIL DAN PEMBAHASAN

3.1 Perhitungan Algoritma RSA

Jika diketahui :
p = 17
q = 11
n = p x q = 17 x 11 = 187
Φ(n) = (p - 1) x (q - 1) = (17 - 1) x (11 - 1) = 160
e = 7
cari nilai d
d.emodΦn = 1
d.7 mod 160 = 1
23.7 mod 160 = 1
161 mod 160 = 1
1 = 1
maka, d = 23
Enkripsi :
PlainText = INFORMATIKA
I : 73
N : 78
F : 70
O : 79
R : 82
M : 77
A : 65
T : 84
I : 73
K : 75
A : 65
c[0] = m^emod n = 75^7 mod 187 = 114
c[1] = m^emod n = 78^7 mod 187 = 56
c[2] = m^emod n = 70^7 mod 187 = 60
c[3] = m^emod n = 79^7 mod 187 = 139
c[4] = m^emod n = 82^7 mod 187 = 91
c[5] = m^emod n = 77^7 mod 187 = 121
c[6] = m^emod n = 65^7 mod 187 = 142
c[7] = m^emod n = 84^7 mod 187 = 50
c[8] = m^emod n = 73^7 mod 187 = 61
c[9] = m^emod n = 75^7 mod 187 = 114
c[10] = m^emod n = 65^7 mod 187 = 142

Ubah dalam bentuk karekterasci
c[0] = 114 = [
c[1] = 56 = =
c[2] = 60 = r
c[3] = 139 = =
c[4] = 91 = L
c[5] = 121 =
c[6] = 142 = ¦
c[7] = 50 = Ž
c[8] = 61 =
c[9] = 141 K
c[10] = 142 = D
ChiperText = **[=r=L¦Ž KD2[Ž**

b. ChipertextElGamal
Plainteks : INFORMATIKA

Karakter	Plainteks M_i	ASCII	Kunci
I	M_1	73	31
N	M_2	78	42
F	M_3	70	21
O	M_4	79	13
R	M_5	62	17
M	M_6	77	34
A	M_7	65	48
T	M_8	84	67
I	M_9	73	87
K	M_{10}	75	71
A	M_{11}	65	53

3.2 Perhitungan Algoritma Elgamal

$y \equiv g^x \bmod p$
$M_i \equiv b_i . a_i^{p-1-x} \bmod p$
p = 257
g = 23
x = 13

$y \equiv g^x \bmod p$
$\equiv 23^{13} \bmod 257$
$\equiv 117$

Enkripsi a:
$a \equiv g^k \bmod p$
$a_1 \equiv 23^{31} \bmod 257$
$\equiv 67$
$a_2 \equiv 23^{42} \bmod 257$
$\equiv 60$
$a_3 \equiv 23^{21} \bmod 257$
$\equiv 46$
$a_4 \equiv 23^{13} \bmod 257$
$\equiv 117$
$a_5 \equiv 23^{17} \bmod 257$
$\equiv 111$
$a_6 \equiv 23^{34} \bmod 257$

$\equiv 242$
$a_7 \equiv 23^{48} \bmod 257$
$\equiv 241$
$a_8 \equiv 23^{67} \bmod 257$
$\equiv 88$
$a_9 \equiv 23^{87} \bmod 257$
$\equiv 176$
$a_{10} \equiv 23^{71} \bmod 257$
$\equiv 11$
$a_{11} \equiv 23^{53} \bmod 257$
$\equiv 211$

Enkripsi b:
$b \equiv y^k.m \bmod p$
$b_1 \equiv 117^{31}.73 \bmod 257$
$\equiv 241$
$b_2 \equiv 117^{48}.78 \bmod 257$
$\equiv 115$
$b_3 \equiv 117^{21}.70 \bmod 257$
$\equiv 60$
$b_4 \equiv 117^{13}.79 \bmod 257$
$\equiv 72$
$b_5 \equiv 117^{17}.82 \bmod 257$
$\equiv 75$
$b_6 \equiv 117^{34}.77 \bmod 257$
$\equiv 161$
$b_7 \equiv 117^{48}.65 \bmod 257$
$\equiv 245$
$b_8 \equiv 117^{67}.84 \bmod 257$
$\equiv 104$
$b_9 \equiv 117^{87}.73 \bmod 257$
$\equiv 253$
$b_{10} \equiv 117^{71}.75 \bmod 257$
$\equiv 108$
$b_{11} \equiv 117^{53}.65 \bmod 257$
$\equiv 238$
Pola selang – seling
a_1,b_1,a_2,b_2, a_3,b_3, a_4,b_4, a_5,b_5,a_6,b_6,a_7,b_7, a_8,b_8, $a_9,b_9,a_{10},b_{10},a_{11},b_{11}$,
Sehingga membentuk Cipherteks:
67,241,60,115,46,60,117,72,111,75,242,161,241,245,88,104,176,253,11,108,211,238

Dalam bentuk karakter ASCII:
Cñ<s.<uHoKò¡ñõXh°ýlÓî

c. Nilai Entropy RSA dan ElGamal
Entropy RSA
Chipertext : **[=r=L¦Ž KD2[Ž**

chiper	frekuensi	probabilitas	entropi
[	2	0.153846154	0.415452264
=	2	0.153846154	0.415452264
r	1	0.076923077	0.284649209
L	1	0.076923077	0.284649209
¦	1	0.076923077	0.284649209
Ž	2	0.153846154	0.415452264
K	1	0.076923077	0.284649209
D	1	0.076923077	0.284649209
2	1	0.076923077	0.284649209
			2.954252048

d. EntropyElGamal
Chipertext : **Cñ<s.<uHoKò¡ñõXh°ýlÓî**

chiper	frekuensi	probabilitas	entropi
C	1	0.047619048	0.209157973
ñ	2	0.095238095	0.32307785
<	2	0.095238095	0.32307785
s	1	0.047619048	0.209157973
.	1	0.047619048	0.209157973
<	2	0.095238095	0.32307785
u	1	0.047619048	0.209157973
H	1	0.047619048	0.209157973
o	1	0.047619048	0.209157973
K	1	0.047619048	0.209157973
ò	1	0.047619048	0.209157973
¡	1	0.047619048	0.209157973
ñ	2	0.095238095	0.32307785
õ	1	0.047619048	0.209157973

Dari hasil pengujian di atas, didapatkan nilai entropy hasil chipertext algoritma RSA lebih tinggi dibandingkan hasil entropychipertext algoritma ElGamal.

4. KESIMPULAN

Berdasarkan hasil pengujian, nilai entropi cipherteks yang dihasilkan oleh algoritma RSA lebih tinggi dibandingkan dengan algoritma ElGamal. Hal ini menunjukkan bahwa tingkat kekacauan dan ketidakpastian data hasil enkripsi RSA lebih besar dibandingkan ElGamal, sehingga RSA memiliki potensi keamanan yang lebih baik dalam menjaga kerahasiaan data dari perspektif analisis entropi. Namun, perbedaan ini tidak hanya bergantung pada nilai entropi, tetapi juga dipengaruhi oleh faktor lain seperti efisiensi komputasi, ukuran kunci, serta kebutuhan aplikasi yang digunakan. Oleh karena itu, pemilihan algoritma enkripsi harus mempertimbangkan kebutuhan

spesifik aplikasi, seperti tingkat keamanan, kecepatan, dan efisiensi sistem.

DAFTAR PUSTAKA

[1] R. I. H. Nasution, Achmad Fauzi, and Husnul Khair, "Hybrid Cryptosystem Algorithm Vigenere Cipher and Base64 for Text Message Security Utilizing Least Significant Bit (LSB) Steganography as Insert into Image," *J. Artif. Intell. Eng. Appl.*, vol. 2, no. 3, pp. 89–98, 2023, doi: 10.59934/jaiea.v2i3.201.

[2] A. Fauzi, "Analisis Hybrid Cryptosystem Algoritma Elgamal dan Algoritma Triple Des," 2014.

[3] T. B. Surbakti, A. Fauzi, and H. Khair, "Rivest Shamir Adleman (RSA) Hybrid Algorithm System and the deep Blum Blum Shub (BBS) Algorithm Securing E-Absence Database Files," *Indones. J. Educ. Comput. Sci.*, vol. 1, no. 2, pp. 53–61, 2023, doi: 10.60076/indotech.v1i2.59.

[4] H. K. Rani Rianda Br Ginting, Achmad Fauzi, "Penerapan Algoritma RSA Dan AES Dalam Pengamanan Data Tunggakan Tagihan PDAM Kota Binjai | Bulletin of Multi-Disciplinary Science and Applied Technology." Accessed: Mar. 27, 2025. [Online]. Available: https://ejurnal.seminar-id.com/index.php/bimasati/article/view/2476

[5] Listiyono, "Implementasi Algoritma Kunci Public Pada Algoritma Rsa," *J. Din. Inform.*, vol. 1, no. 2, pp. 95–99, 2009.

[6] A. H. Hasugian, R. A. Putri, and A. S. Zuhri, "Penerapan Metode Elgamal Untuk Mengamankan Teks Pada File Dokumen Word," *KLIK Kaji. Ilm. Inform. dan Komput.*, vol. 4, no. 2, pp. 1143–1153, 2023, doi: 10.30865/klik.v4i2.1277.

[7] R. Solin and P. Ramadhani, "Modifikasi Pembangkit Kunci Algoritma Elgamal Dengan Menerapkan Algoritma Freivalds," *KOMIK (Konferensi Nas. ...*, vol. 4, pp. 351–356, 2020, doi: 10.30865/komik.v4i1.2719.

[8] M. S. Dairi, M. Setiani Asih, and corespondent author, "Implementasi Algoritma Kriptografi RSA Dalam Aplikasi Sistem Informasi Perpustakaaan Implementation Of RSA Cryptographic Algorithms in Library Information System Applications," *Januari*, vol. 2023, no. 2, pp. 214–223, 2022, [Online]. Available: https://jurnal.unity-academy.sch.id/index.php/jirsi/index%0Ahttp://creativecommons.org/licenses/by-sa/4.0/

[9] A. Khumaidi, "Simulasi Entropi Shannon, Entropi Renyi, dan informasi pada kasus Spin Wheel," *AKSIOMA J. Mat. dan Pendidik. Mat.*, vol. 12, no. 1, pp. 120–128, 2021, doi: 10.26877/aks.v12i1.6893.