JURNAL TIMES
TECHNOLOGY INFORMATICS & COMPUTER SYSTEM

Volume XV No 1, 2026
*p*ISSN : 2337 – 3601
*e*ISSN : 2549 – 015X

Tersedia *online* di http://ejournal.stmik-time.ac.id

IMPLEMENTASI SKEMA SIGN-THEN-ENCRYPT MENGGUNAKAN KRIPTOSISTEM RSA-OAEP DAN TANDA TANGAN DIGITAL DISSANAYAKE

Rahmad Bahri1[1)], Rahman Pradipta[2)]
Program Studi Informatika
Universitas Samudra
Jl, Prof. Dr. Syarief Thayeb, Meurandeh, Langsa
e-mail: rahmadbahri@unsam.ac.id[1)] , rahman.pradipta@unsam.ac.id[2)]

Abstrak
Perkembangan teknologi informasi yang masif menuntut adanya jaminan keamanan data yang tangguh selama proses transmisi pada jaringan terbuka guna memitigasi risiko intersepsi pasif dan modifikasi aktif oleh pihak ilegal. Penelitian ini bertujuan untuk mengimplementasikan dan menganalisis performa skema keamanan *Sign-then-Encrypt* yang mengintegrasikan Kriptosistem *Optimal Asymmetric Encryption Padding* (RSA-OAEP) dengan *Dissanayake Digital Signature*. Metode penelitian dilakukan melalui pengujian eksperimental terhadap parameter waktu eksekusi (*execution time*) komponen *key generation*, enkripsi, dekripsi, serta verifikasi menggunakan variasi panjang *plaintext* dari 50 hingga 250 karakter, dilanjutkan dengan pengujian sensitivitas *Avalanche Effect*. Hasil penelitian menunjukkan fungsi penandatanganan digital (*signing*) dan verifikasi pada Algoritma Dissanayake bekerja baik, dengan rata-rata waktu *signing* stabil pada 0,02-0,024 detik dan waktu verifikasi pada skala mikro-detik (0,000048-0,000062 detik). Sementara itu, proses enkripsi RSA-OAEP memerlukan waktu di bawah 0,08 detik, dan proses dekripsinya berkisar antara 0,503–0,963 detik. Pengujian *Avalanche Effect* menghasilkan nilai rata-rata yang sangat ideal mendekati ambang batas kriptografis kokoh, yaitu sebesar 50,95% untuk algoritma Dissanayake dan 51,15% untuk RSA-OAEP. Kesimpulan dari penelitian ini membuktikan bahwa integrasi skema *Sign-then-Encrypt* tersebut sangat optimal, sensitif terhadap perubahan satu karakter data, dan andal dalam menjaga kerahasiaan serta integritas pesan.
Kata kunci : *Avalanche Effect*; Dissanayake *Digital Signature*; Kriptosistem RSA-OAEP; Skema *Sign-then-Encrypt*; *Time Execution*.

1. Pendahuluan

Perkembangan teknologi informasi yang masif dalam era digitalisasi menuntut perlindungan data yang sangat tinggi selama proses transmisi berlangsung. Keamanan dalam jaringan terbuka menghadapi tantangan besar akibat meningkatnya intensitas serangan siber, baik berupa intersepsi pasif maupun modifikasi data secara aktif [1]. Kebocoran informasi pada sektor-sektor krusial menegaskan bahwa sistem pertukaran data konvensional tidak lagi memadai tanpa adanya lapisan proteksi yang tangguh [2]. Oleh karena itu, arsitektur keamanan modern wajib menerapkan mekanisme perlindungan hibrida yang mampu memenuhi aspek kerahasiaan (*confidentiality*), autentikasi (*authentication*), dan penyangkalan (*non-repudiation*) secara bersamaan [3]. Upaya penyeimbangan antara keandalan matematis algoritma dan ketahanan terhadap berbagai teknik kriptanalisis kini menjadi fokus utama bagi para peneliti di bidang keamanan informasi [4].

Dalam mengimplementasikan layanan keamanan ganda tersebut, urutan operasi antara penyandian dan penandatanganan memegang peranan krusial terhadap integritas teks sandi (*ciphertext*). Salah satu paradigma yang secara luas diadopsi adalah skema *Sign-then-Encrypt*, di mana dokumen ditandatangani terlebih dahulu menggunakan kunci privat pengirim sebelum seluruh komponen tersebut dibungkus oleh enkripsi kunci publik penerima [5]. Dibandingkan dengan skema alternatif seperti *Encrypt-then-Sign*, skema *Sign-then-Encrypt* memiliki keunggulan filosofis yang lebih kuat dalam mempertahankan validitas hukum dari aspek *non-repudiation* [6]. Melalui skema *Sign-then-Encrypt*, penerima pesan dapat memverifikasi secara langsung bahwa entitas yang membubuhkan tanda tangan adalah pemilik sah dari kunci privat tersebut, bukan pihak ketiga yang sekadar melakukan enkapsulasi ulang terhadap dokumen rahasia milik orang lain [7]. Konstruksi ini memastikan bahwa akuntabilitas pengirim tetap terjaga secara utuh di dalam sistem komunikasi digital [8].

Meskipun memiliki keunggulan struktural yang solid, performa operasional dari skema *Sign-then-Encrypt* kerap kali terkendala oleh tingginya beban komputasi pada algoritma tanda tangan digital asimetris konvensional (seperti RSA standar atau ECDSA). Kompleksitas perhitungan matematika berbasis eksponensial modular pada kunci berukuran besar sering kali memicu terjadinya latensi transmisi yang tinggi, terutama jika diterapkan pada lingkungan dengan keterbatasan sumber daya (*resource-constrained devices*) [9]. Guna mengatasi permasalahan tersebut, Dissanayake *Digital Signature* diperkenalkan sebagai solusi alternatif yang memanfaatkan karakteristik unik dari teori bilangan ganjil, dimana penjumlahan dua bilangan ganjil yang berbeda akan selalu menghasilkan nilai kelipatan empat [10]. Penerapan relasi matematika ini terbukti mampu menyederhanakan algoritma pemrosesan secara signifikan selama fase pembangkitan kunci dan verifikasi dokumen [11]. Akselerasi waktu eksekusi yang ditawarkan oleh algoritma Dissanayake menjadikannya kandidat yang sangat potensial untuk mengoptimalkan skema hibrida [12].

Di sisi lain, parameter konfidensialitas dalam skema *Sign-then-Encrypt* juga memerlukan penguatan substansial pada lapisan enkripsinya. Eksekusi fungsi enkripsi asimetris yang bersifat deterministik murni (seperti RSA murni tanpa pra-pemrosesan) sangat rentan terhadap serangan *chosen-plaintext attack* (IND-CPA) karena pesan yang sama akan selalu menghasilkan bentuk teks terenkripsi yang identik [13]. Sejarah perkembangan protokol keamanan menunjukkan bahwa skema padding tradisional terdahulu, seperti PKCS#1 v1.5, terbukti memiliki celah fatal terhadap serangan aktif berbasis *adaptive chosen-ciphertext attack* yang memanfaatkan respon error dari padding oracle untuk merekonstruksi isi pesan [14]. Guna memitigasi celah keamanan struktural tersebut, penggunaan *Optimal Asymmetric Encryption Padding* (RSA-OAEP) menjadi standar wajib karena mampu mentransformasikan enkripsi menjadi skema probabilistik yang tangguh dari serangan teks-terenkripsi terpilih (IND-CCA2) [15]. RSA-OAEP bekerja dengan mengintegrasikan jaringan Feistel dan fungsi random oracles untuk memastikan bahwa penyerang tidak dapat mengekstrak informasi struktural apa pun dari *ciphertext* [16].

Ketangguhan model keamanan probabilistik yang ditawarkan oleh RSA-OAEP sangat vital untuk melindungi integritas data sensitif di dalam jaringan pertukaran data real-time [17]. Namun demikian, implementasi algoritma dengan tingkat keamanan seketat RSA-OAEP sering kali membawa dampak sampingan berupa peningkatan konsumsi daya instruksi CPU (*computational overhead*) [18]. Kompleksitas ganda yang muncul dari kombinasi padding Feistel dan enkripsi kunci publik menuntut adanya strategi penyelarasan performa di tingkat aplikasi [19]. Oleh karena itu, integrasi komponen kriptografi yang efisien dari segi waktu eksekusi seperti tanda tangan digital Dissanayake, namun didukung oleh kekuatan konfidensialitas superior dari RSA-OAEP, menjadi sebuah urgensi dan solusi arsitektural dalam pengembangan protokol komunikasi masa kini [20].

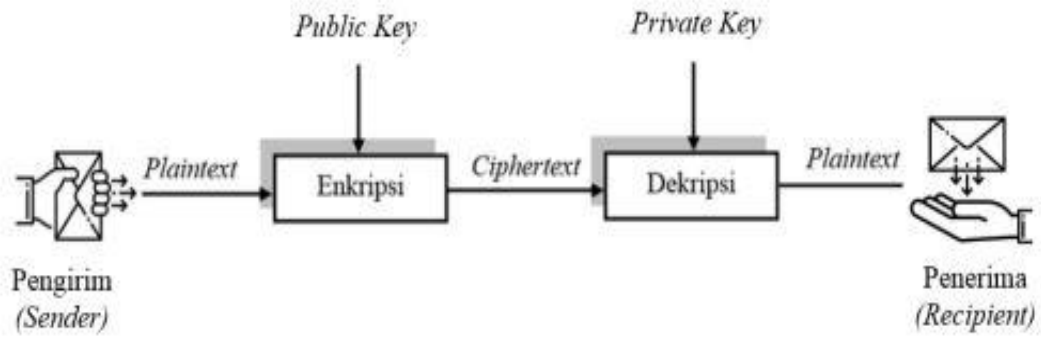
2. Landasan Teori

Kriptografi

Kriptografi merupakan cabang ilmu dan seni matematika yang digunakan untuk menjaga keamanan pesan dengan cara mentransformasikannya ke dalam bentuk sandi yang tidak dapat dipahami tanpa otoritas khusus [1]. Di era digitalisasi modern, teknik kriptografi memegang peranan krusial dalam melindungi jalur komunikasi data dari berbagai bentuk ancaman siber, baik berupa intersepsi pasif maupun modifikasi informasi secara aktif [2]. Implementasi kriptografi kontemporer dirancang untuk menyediakan layanan keamanan fundamental yang mencakup aspek kerahasiaan (*confidentiality*), integritas data (*integrity*), autentikasi entitas (*authentication*), serta jaminan anti-penyangalan (*non-repudiation*) [18].

Kriptosistem asimetris

Kriptosistem asimetris, atau dikenal secara luas sebagai kriptografi kunci publik, beroperasi dengan memanfaatkan sepasang kunci yang berbeda namun terikat secara matematis, yaitu kunci publik untuk proses penyandian (*encryption*) dan kunci privat untuk proses pembongkaran sandi (*decryption*) [3]. Tingkat keamanan skema asimetris ini bersandar penuh pada kompleksitas penyelesaian masalah matematika laten, seperti komputasi faktorisasi bilangan prima besar ataupun logaritma diskrit [13]. Untuk mencapai tingkat keamanan semantik tertinggi seperti *Indistinguishability under Adaptive Chosen-Ciphertext Attack* (IND-CCA2), kriptosistem deterministik murni seperti RSA memerlukan integrasi skema prapemrosesan probabilistik, salah satunya melalui metode *Optimal Asymmetric Encryption Padding* (RSA-OAEP) [14], [15]. Penggunaan padding berbasis Feistel ini sangat vital untuk mencegah penyerang mengeksploitasi struktur teks sandi (*ciphertext*) [16], [19].

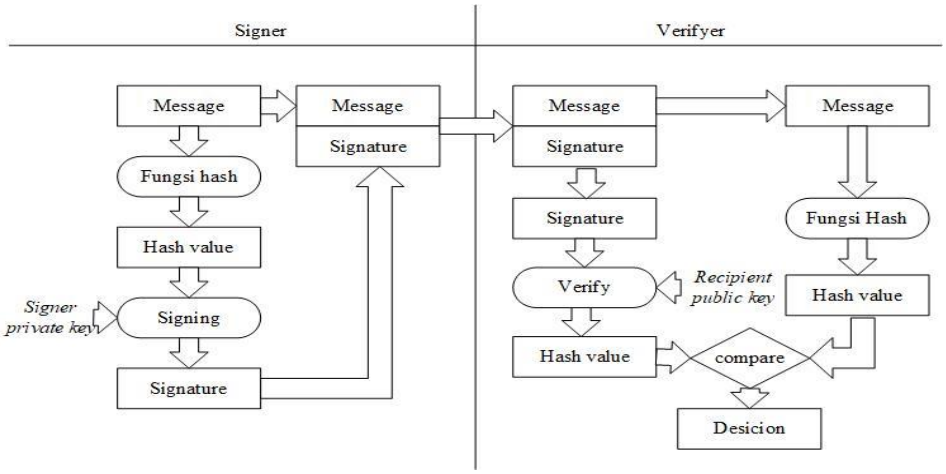


Gambar 1. Kriptosistem asimetris

Tanda Tangan Digital (*Digital Signature)*

Tanda tangan digital merupakan mekanisme kriptografi asimetris yang diterapkan untuk memverifikasi keabsahan (*authenticity*) dari sebuah dokumen elektronik sekaligus memberikan jaminan hukum *non-repudiation* bagi pihak pengirim [9]. Mekanisme ini bekerja dengan memanfaatkan kunci privat pengirim untuk menandai representasi unik dari pesan, yang kemudian dapat diverifikasi secara terbuka oleh entitas penerima menggunakan kunci publik pengirim yang

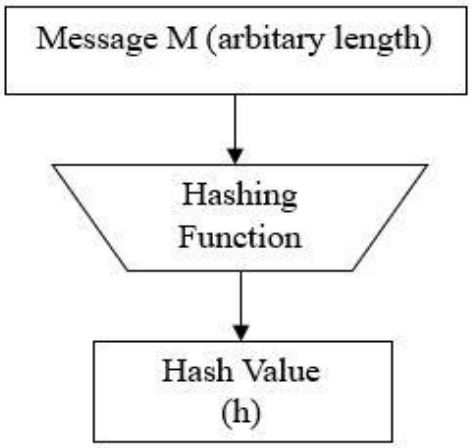
bersesuaian [10]. Dalam perkembangannya, skema tanda tangan digital inovatif seperti *Dissanayake Digital Signature* diperkenalkan untuk memangkas beban instruksi komputasi yang tinggi pada algoritma konvensional melalui pemanfaatan sifat unik dari teori bilangan ganjil [11], [12]. Reduksi beban pemrosesan ini menjadikannya sangat adaptif untuk diimplementasikan pada arsitektur sistem yang memiliki keterbatasan sumber daya (*resource-constrained devices*) [17].



Gambar 2. Skema Tanda Tangan Digital

Fungsi Hash (Hash Function)

Fungsi hash adalah algoritma matematika searah yang memetakan data digital dengan panjang bervariasi menjadi sebuah nilai string berukuran tetap yang disebut sebagai intisari pesan (*message digest*) [1]. Dalam aplikasi kriptografi hibrida dan penandatanganan digital, fungsi hash seperti SHA-256 bertindak sebagai komponen krusial untuk menjamin integritas data sebelum proses matematis asimetris dijalankan [11], [12]. Karakteristik utama dari fungsi hash yang aman wajib meliputi sifat *pre-image resistance*, *second pre-image resistance*, dan *collision resistance*, yang memastikan bahwa rekonstruksi balik dari nilai hash menjadi pesan asli secara komputasi tidak mungkin dilakukan oleh pihak luar [12].



Gambar 3. Skema *Hash Function*

Signcryption

Signcryption atau paradigma *authenticated encryption* merupakan pendekatan kriptografi hibrida yang secara simultan mengeksekusi fungsi tanda tangan digital dan enkripsi dalam satu kesatuan langkah logis untuk menghemat waktu pemrosesan [4]. Pendekatan tradisional untuk mencapai fungsi perlindungan ganda ini melibatkan pengurutan operasi terstruktur, seperti skema *Encrypt-then-Sign* (EtS) dan *Sign-then-Encrypt* (StE) [5], [6]. Skema StE dipilih karena memiliki keunggulan filosofis yang lebih kuat, di mana identitas hukum pengirim dilekatkan secara langsung pada konten pesan asli di dalam lapisan pelindung enkripsi, sehingga memberikan proteksi penuh terhadap serangan manipulasi teks sandi oleh pihak ketiga [7], [8], [20].

Avalanche Effect

Avalanche effect merupakan salah satu parameter evaluasi utama yang digunakan untuk mengukur tingkat kekuatan, keacakan (*randomness*), dan ketahanan dari suatu algoritma kriptografi, baik pada fungsi hash maupun enkripsi blok [3].

Fenomena matematika ini menyatakan bahwa perubahan sekecil apa pun pada masukan data asli, seperti modifikasi satu bit pada plaintext atau komponen kunci, harus menghasilkan perubahan yang radikal dan tidak terprediksi pada hampir setengah dari total bit teks sandi atau nilai hash keluaran [12], [15]. Semakin tinggi persentase nilai *avalanche effect* yang mendekati nilai ideal 50%, maka algoritma tersebut dinilai semakin tangguh dan aman dalam menangkal serangan kriptanalisis berbasis statistika maupun perbedaan linier [15].

$$avalanche\ effect = \frac{jumlah\ bit-bit\ yang\ berbeda}{jumalah\ total\ bit} \times\ 100\ \% \quad (1)$$

3. Metode Penelitian

Algoritma *Dissanayake Digital Signature*

Algoritma *Dissanayake Digital Signature* bersandar pada manipulasi aritmatika teori bilangan ganjil dan faktorisasi bilangan prima besar. Dissanayake *digital signature* diusulkan berdasarkan pada faktorisasi bilangan prima dan properti matematika yang sederhana. Properti matematika pada algoritma ini merupakan jumlah dari 2 bilangan ganjil tambahan yaitu kelipatan dari 4. Algoritma *digital signature* ini menggunakan *public key* (e, n), e merupakan bilangan prima besar yang kurang dari n, dan r merupakan variabel yang dipilih oleh penandatangan.

a. Pembangkitan Kunci
   1. Memilih dua bilangan prima yang berbeda untuk nilai p dan q.
   2. Hitung nilai $n = p \times q$.
   3. Hitung $\phi(n) = (p-1) \times (q-1)$.
   4. Memilih bilangan prima d, sehingga $\gcd(d, \phi(n) = 1$, digunakan sebagai kunci private pengirim.
   5. Hitung kunci publik e, sehingga $e.d\ mod\ \phi(n)\ \equiv 1$.
   6. Pilih bilangan bulat r, sehingga $(m + r) mod\ 4\ \equiv 0$.
   7. Temukan bilangan ganjil (a), sehingga $(a) = \frac{m+r-2}{2}$
      (α) adalah bilangan ganjil.
   8. Publish (e, n)
   9. Simpan $(p, q, \phi(n), d)$
   10. Kirim (m, r)

b. Sign (*Signer*)
   Hitung $S\ \equiv\ \alpha^d \bmod n$

c. Verifikasi (Recipients)
   1. Hitung V, sehingga $S^e\ mod\ n\ \equiv\ \alpha'$
   2. Temukan bilangan ganjil (a), sehingga $(a) = \frac{m+r-2}{2}$
      (α) adalah bilangan ganjil.
      Jika $a' = a$, maka *signature* valid, jika $a' \neq a$ maka *signature* invalid.

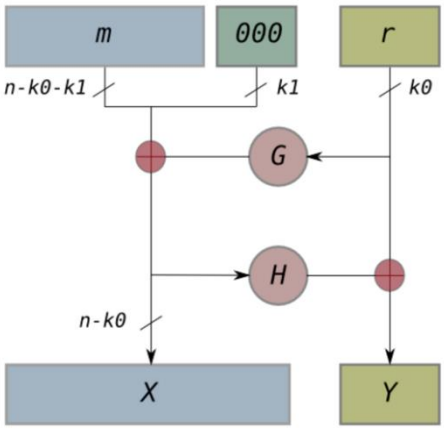
Kriptosistem RSA-OAEP

Optimal Asymmetric Encryption Padding (RSA-OAEP) bertindak sebagai skema prapemrosesan (*padding*) sebelum data dieksekusi oleh fungsi RSA standar. OAEP menggunakan struktur jaringan Feistel dua tingkat dengan bantuan dua fungsi penyandi masker (*Mask Generation Function*), yaitu G dan H.

Ada dua tujuan dari Kriptosistem OAEP:

a. Menambahkan padding acak ke plaintext dapat mengubah RSA dari skema deterministik menjadi skema probabilistik.
b. Mencegah kebocoran informasi struktur enkripsi yang disebabkan oleh serangan plaintext terpilih.

Proses padding OAEP ditunjukkan seperti di bawah ini:



Gambar 4. Skema Kriptosistem OAEP

Dimana,

- n: panjang bit modulus RSA
- k_0 dan k_1: angka yang ditentukan oleh protokol OAEP
- m: teks biasa dengan panjang $n - k_0 - k_1 bit$
- G dan H adalah dua fungsi hash kriptografi
- $\oplus$: operasi xor
- r: string acak yang dihasilkan dengan panjang k_0 bit

Enkripsi OAEP:

a. Teks biasa m padding dengan k_1 nol yang ditambahkan m ke m' dengan panjang $n - k_0$ bit.
b. r diubah menjadi string $n - k_0$ bit oleh fungsi hash kriptografi G.
c. $X = m' \oplus G(r)$.
d. X direduksi menjadi k_0 bit oleh H.
e. $Y = r \oplus H(X)$.
f. Hasil pengisian adalah X dan Y.

Dekripsi OAEP:

a. r dipulihkan dengan $r = Y \oplus H(X)$.
b. m^r dipulihkan dengan $m' = X \oplus G(r)$.

4. Hasil Penelitian

Hasil implementasi dan pengujian dari skema *Sign-then-Encrypt* menggunakan kombinasi kriptosistem RSA-OAEP dan *Dissanayake Digital Signature*. Evaluasi sistem difokuskan pada tiga parameter utama, yaitu uji fungsionalitas, analisis performa waktu komputasi, dan analisis efek longsoran (*avalanche effect*).

Pengujian dari Algoritma *Dissanayake Digital Signature*

Hasil dari proses pembangkitan kunci oleh pengirim menggunakan algoritma tanda tangan digital Dissanayake menghasilkan kunci publik dan kunci privat.

Pembangkitan Kunci dari *Dissanayake Digital Signature*

Proses pembangkitan kunci publik dan private *Dissanayake Digital Signature*

```
p: 172711972172564492098744666937173617483003964653402306918203388422875130982274 28...
q: 156661697317580915932504736412461011241686388001843441064865595821981276759971 70...
n: 270573507076207564892047324753605658191500458809111773159912131380633365426376 08...
d (Private): 109417189851338800807963199784586324613885910395478657371722405082857557825541 78...
e (Public): 65537
```

Gambar 5. Hasil Pembangkitan Kunci *Dissanayake Digital Signature*

Pembangkitan Tanda Tangan (*signature*) dari *Dissanayake Digital Signature*

Setelah proses pembangkitan kunci, Langkah selanjutnya yaitu melakukan *sign* atau pembangkitan tanda tangan (*signature*)

```
Formula      : a = (M + r - 2) / 2
Hash Int (M) : 996512224332899541499372192276610688069241546150970727782211189597648829933 60
Nilai r      : 0 (agar M+r habis dibagi 4)
Cek Mod 4    : (99651222433289954149... + 0) % 4 = 0
----------------------------------------
TRANSFORMASI GANJIL:
Numerator    : (M+r-2)/2 -> 996512224332899541499372192276610688069241546150970727782211189597648829933 58
Nilai a      : 498256112166449770749686096138305344034620773075485363891105594798824414966 79
Cek Ganjil?  : YA
----------------------------------------
Sign S       : S = a^d mod n
Signature S  : 130869776089735747558718106481673169704404195323136038879329028631604148591623 52...
```

Gambar 6. Hasil Pembangkitan *Signature* mengunakan *Dissanayake Digital Signature*

Verifikasi Tanda Tangan (*signature*) dari *Dissanayake Digital Signature*

Langkah selanjutnya melakukan *unsign* atau verifikasi tanda tangan (*signature*)

```
Proses: Hash(M) -> Hitung r -> Rumus Ganjil
Hash Int (M)  : 996512224332899541499372192276610688069241546150970727782211189597648829933 60
Hitung r      : 0
Rumus         : a = (M + r - 2) / 2
Hash value a (Message) : 498256112166449770749686096138305344034620773075485363891105594798824414966 79
```

Gambar 7. Hasil Verifikasi *Signature* mengunakan *Dissanayake Digital Signature*

Bandingkan (*compare*) Tanda Tangan (*signature*) dan pesan asli (*Plaintext*)

Hasil membandingkan nilai *hash plaintext* dan nilai *hash* yang dibangkitkan dari nilai tanda tangan.

```
a' (Signature) : 498256112166449770749686096138305344034620773075485363891105594798824414966 79
a  (Message)   : 498256112166449770749686096138305344034620773075485363891105594798824414966 79
MATCH: True
```

Gambar 8. Hasil *Compare Hash Signature* dan *hash plaintext*

Pengujian dari Kriptosistem RSA-OAEP

Hasil dari pengujian menggunakan Kriptosistem RSA-OAEP dengan proses pembangkitan kunci, enkripsi dan proses deskripsi.

Pembangkitan Kunci dari Kriptosistem RSA-OAEP

Proses pembangkitan kunci public dan private Kriptosistem RSA-OAEP.

```
n (Public) : 19700738730745354454804677066692865578409457303251335505848636023509328283613794...
e (Public) : 65537
d (Private): 21843950965624951153025108465645587968594136096702580935324079797798869675795388...
p          : 14797355912324847145744993268733827222040250413999682338618436905556414853600891...
q          : 13313688504536433349121040079709973005517254908652347904170328692479262893674436...
```

Gambar 9. Hasil pembangkitan kunci public dan private Kriptosistem RSA-OAEP.

Pengujian Enkripsi Menggunakan Kriptosistem RSA-OAEP

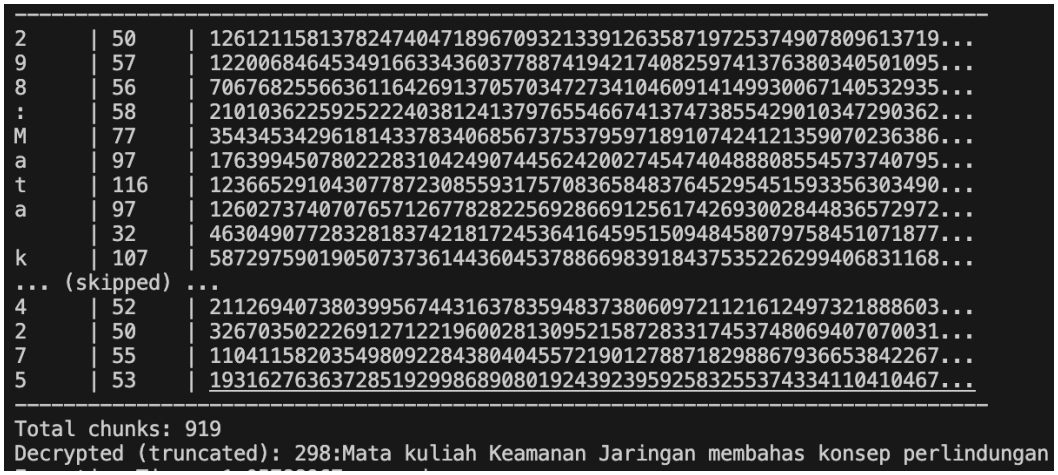
Proses pengujian enkripsi menggunakan kriptosistem RSA-OAEP.

```
------------------------------------------------------------------------------------------
2     | 50    | 126121158137824740471896709321339126358719725374907809613719...
9     | 57    | 122006846453491663343603778874194217408259741376380340501095...
8     | 56    | 706768255663611642691370570347273410460914149930067140532935...
:     | 58    | 210103622592522240381241379765546674137473855429010347290362...
M     | 77    | 354345342961814337834068567375379597189107424121359070236386...
a     | 97    | 176399450780222831042490744562420027454740488808554573740795...
t     | 116   | 123665291043077872308559317570836584837645295451593356303490...
a     | 97    | 126027374070765712677828225692866912561742693002844836572972...
      | 32    | 463049077283281837421817245364164595150948458079758451071877...
k     | 107   | 587297590190507373614436045378866983918437535226299406831168...
... (skipped) ...
4     | 52    | 211269407380399567443163783594837380609721121612497321888603...
2     | 50    | 326703502226912712219600281309521587283317453748069407070031...
7     | 55    | 110411582035498092284380404557219012788718298867936653842267...
5     | 53    | 193162763637285192998689080192439239592583255374334110410467...
------------------------------------------------------------------------------------------
Total chunks: 919
```

Gambar 10. Hasil pengujian enkripsi kriptosistem RSA-OAEP.

Pengujian Dekripsi Menggunakan Kriptosistem RSA-OAEP

Hasil dekripsi Kriptosistem RSA-OAEP menggunakan kunci privat untuk membalikan *plaintext*.



Gambar 11. Hasil pengujian dekripsi kriptosistem RSA-OAEP.

Hasil simulasi waktu eksekusi untuk melakukan analisi terhadap proses *Sign* dan *unsign* (verifikasi) serta proses enkripsi dan dekripsi didasarkan pada eksperimen dengan panjang *plaintext* yang berbeda. Satuan waktu eksekusi menggunakan detik (*seconds*).

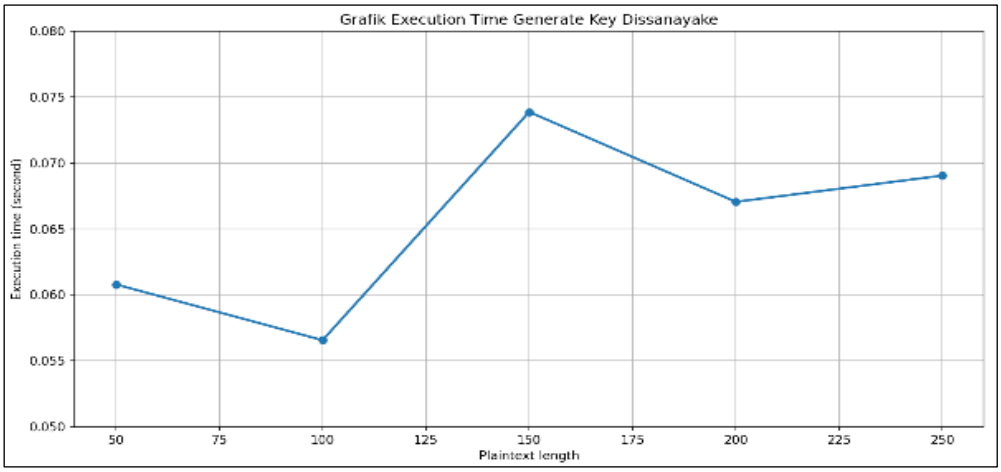
Time Execution Algoritma *Dissanayake Digital Signature*

Waktu Proses pembangkitan kunci (*key generate*), penandatanganan dan verifikasi menggunakan algoritma tanda tangan digital Dissanayake menghitung waktu pemrosesan berdasarkan panjang teks biasa, yaitu 50 karakter, 100 karakter, 150 karakter, 200 karakter, dan 250 karakter.

Time Execution *Key Generate* Algoritma *Dissanayake Digital Signature*

Tabel 1. Hasil *Time Execution Key Generate* Algoritma Dissanayake *Digital Signature*

Plaintext length	Execution Time (second)			
	ke-1	ke-2	ke-3	Average
50	0.0589797	0.0724169	0.0509781	0.0607916
100	0.0658214	0.0388329	0.0650320	0.0565621
150	0.0445652	0.0929491	0.0841020	0.0738721
200	0.0783637	0.0610376	0.0617612	0.0670542
250	0.0813942	0.0318334	0.0939099	0.0690458



Gambar 12. Grafik Hasil *Time Execution Key Generate* Algoritma Dissanayake *Digital Signature*

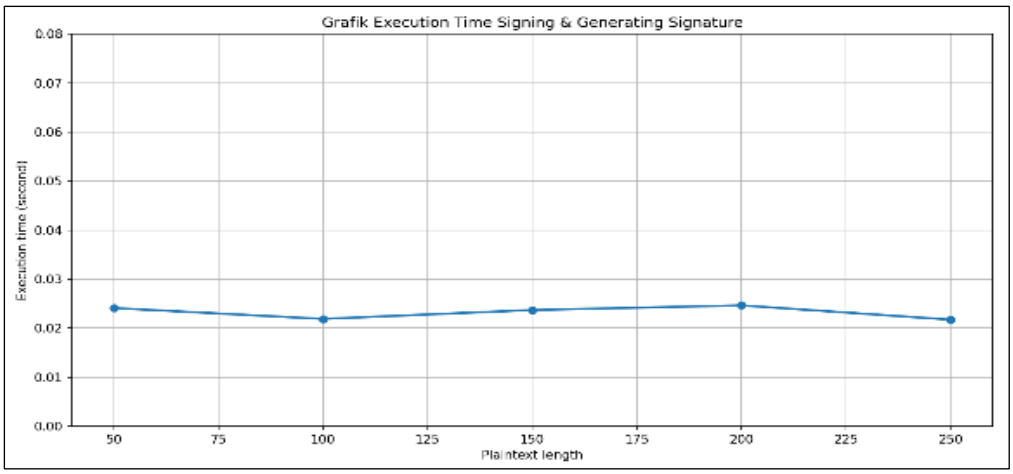
Berdasarkan Tabel.1 dan Grafik Hasil Pengujian, proses key generation pada Algoritma Dissanayake *Digital Signature* terbukti memiliki efisiensi komputasi yang tinggi dengan rata-rata waktu eksekusi yang sangat cepat di bawah

0,08 detik (berkisar antara 0,056 hingga 0,073 detik). Pergerakan garis pada grafik menunjukkan tren fluktuasi yang non-linear dan acak dimana titik terendah dicapai pada *plaintext* length 100 (0,056 detik) dan lonjakan tertinggi terjadi pada panjang 150 (0,073 detik) yang mengindikasikan bahwa panjang plaintext tidak memiliki pengaruh linear atau hubungan sebab-akibat langsung terhadap beban kerja pembangkitan kunci.

Time Execution *Generate Signature (sign)* Algoritma *Dissanayake Digital Signature*

Tabel 2. Hasil *Time Execution Generate Signature* Algoritma Dissanayake *Digital Signature*

Plaintext length	Execution Time (second)			
	ke-1	ke-2	ke-3	Average
50	0.0226751	0.0284092	0.0212128	0.0240990
100	0.0223389	0.0235313	0.0197716	0.0218806
150	0.0215941	0.0228197	0.0266608	0.0236915
200	0.0223230	0.0250946	0.0265103	0.0246426
250	0.0218795	0.0216925	0.0216058	0.0217259



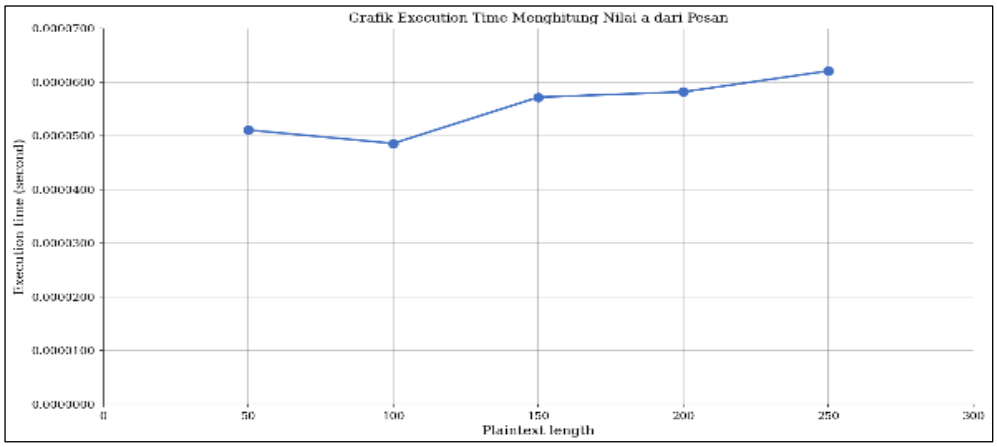
Gambar 13. Grafik Hasil *Time Execution Generate Signature* Algoritma Dissanayake *Digital Signature*

Berdasarkan data pada Tabel 2 dan Gambar 13, proses penandatanganan digital (*signing*) menggunakan Algoritma *Dissanayake Digital Signature* menunjukkan performa komputasi yang sangat konsisten, efisien, dan stabil dengan rata-rata waktu eksekusi berkisar antara 0,021 hingga 0,024 detik untuk seluruh variasi panjang *plaintext*. Berbeda dengan grafik pembangkitan kunci sebelumnya, visualisasi data pada Gambar 2 memperlihatkan pergerakan garis rata-rata (*Average*) yang cenderung konstan dan melandai mendekati garis horizontal tanpa adanya lonjakan drastis, dengan titik waktu terendah pada panjang data 250 (0,0217259 detik) dan titik tertinggi yang relatif kecil pada panjang data 200 (0,0246426 detik). Karakteristik grafik yang stabil ini membuktikan bahwa beban algoritma dalam melakukan fungsi penandatanganan digital (*signing*) terhadap pesan atau pembuatan *hash signature* berjalan sangat optimal serta tidak terpengaruh secara signifikan oleh penambahan beban panjang karakter teks input (dari 50 hingga 250).

Time Execution verifikasi Algoritma Dissanayake Digital Signature

Tabel 3. Hasil *Time Execution* verifikasi Algoritma Dissanayake *Digital Signature*

Plaintext length	Execution Time (second)			
	ke-1	ke-2	ke-3	Average
50	0.0000401	0.0000393	0.0000739	0.0000511
100	0.0000496	0.0000474	0.0000488	0.0000486
150	0.0000713	0.0000476	0.0000526	0.0000572
200	0.0000614	0.0000543	0.0000588	0.0000582
250	0.0000540	0.0000588	0.0000734	0.0000621



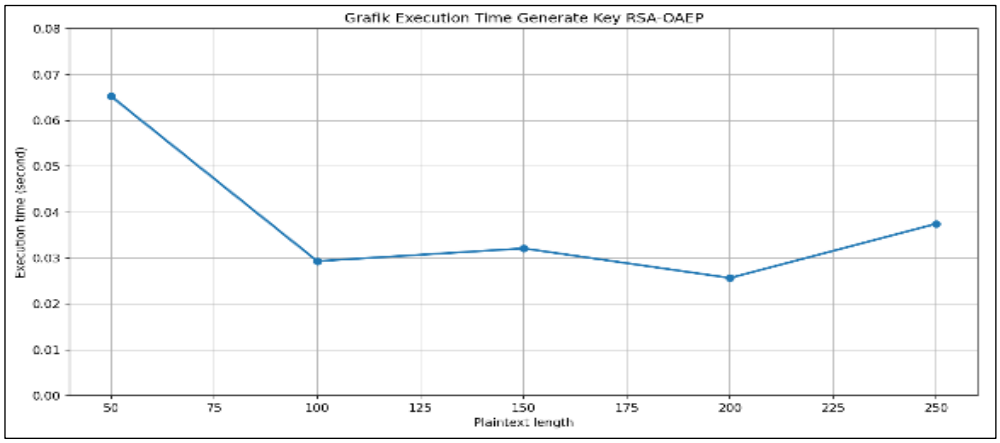
Gambar 13. Grafik Hasil *Time Execution* verifikasi Algoritma Dissanayake *Digital Signature*

Berdasarkan data pada Tabel 3 dan Gambar 13, proses verifikasi menggunakan Algoritma Dissanayake Digital Signature menunjukkan performa komputasi yang baik dengan rata-rata waktu eksekusi yang berada di skala berkisar antara 0,0000486 hingga 0,0000621 detik saja. Pergerakan garis rata-rata (Average) pada grafik memperlihatkan tren peningkatan yang sangat landai seiring bertambahnya panjang data dimulai dari waktu eksekusi terendah pada plaintext length 100 sebesar 0,0000486 detik hingga mencapai titik tertinggi pada panjang data 250 sebesar 0,0000621 detik yang membuktikan adanya korelasi positif minor namun stabil antara penambahan ukuran karakter teks input dengan durasi kalkulasi matematis fungsi verifikasi.

Time Execution Pembangkitan Kunci dari Kriptosistem RSA-OAEP

Tabel 4. Hasil *Time Execution* Pembangkitan Kunci dari Kriptosistem RSA-OAEP

Plaintext length	Execution Time (second)			
	ke-1	ke-2	ke-3	Average
50	0.0927440	0.0581580	0.0450279	0.0653100
100	0.0327416	0.0340118	0.0212715	0.0293416
150	0.0366218	0.0267657	0.0329818	0.0321231
200	0.0305563	0.0147584	0.0317084	0.0256744
250	0.0134580	0.0627216	0.0363170	0.0374989



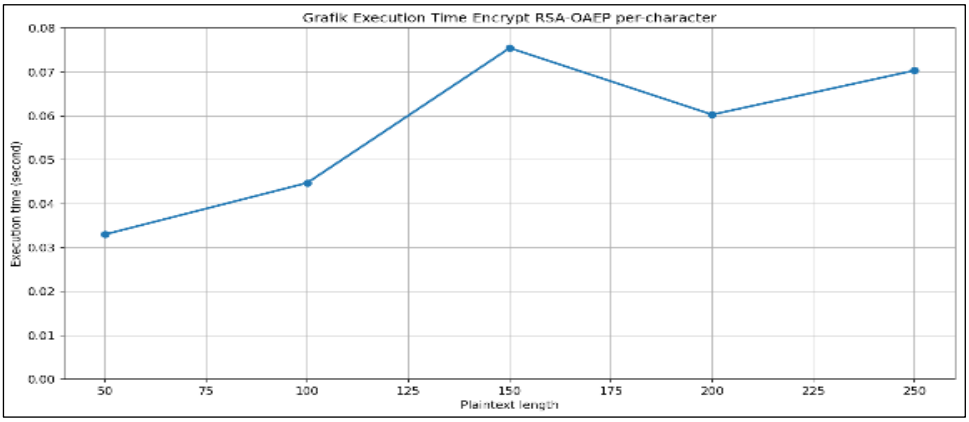
Gambar 14. Grafik Hasil *Time Execution* Pembangkitan Kunci dari Kriptosistem RSA-OAEP

Berdasarkan data pada Tabel 4 dan Gambar 14, proses pembangkitan kunci (*key generation*) pada Kriptosistem RSA-OAEP menunjukkan performa yang sangat efisien dan cepat dengan rata-rata waktu eksekusi keseluruhan berada di bawah angka 0,07 detik (berkisar antara 0,025 hingga 0,065 detik). Kurva rata-rata (*Average*) pada grafik memperlihatkan tren fluktuasi non-linear yang diawali dengan durasi tertinggi pada *plaintext length* 50 sebesar 0,0653100 detik, lalu menurun tajam dan bergerak landai secara stabil pada rentang panjang data 100 hingga 200 (berada di kisaran 0,025–0,032 detik), sebelum akhirnya mengalami sedikit kenaikan pada panjang data 250 menjadi 0,0374989 detik.

Time Execution Enkripsi Menggunakan Kriptosistem RSA-OAEP

Tabel 5. Hasil *Time Execution* Enkripsi Menggunakan Kriptosistem RSA-OAEP

Plaintext length	Execution Time (second)			
	ke-1	ke-2	ke-3	Average
50	0.0322276	0.0357086	0.0310815	0.0330059
100	0.0418049	0.0463661	0.0461014	0.0447575
150	0.1232304	0.0495537	0.0536953	0.0754931
200	0.0705315	0.0581344	0.0522731	0.0603130
250	0.0791691	0.0736394	0.0583204	0.0703763



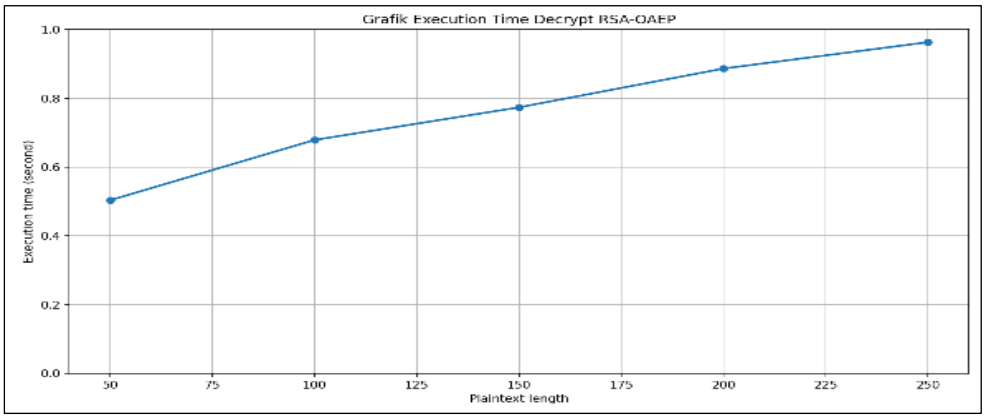
Gambar 15. Grafik Hasil *Time Execution* Enkripsi Menggunakan Kriptosistem RSA-OAEP

Berdasarkan data pada tabel 5 dan gambar 15, proses enkripsi menggunakan Kriptosistem RSA-OAEP menunjukkan performa yang efisien dengan rata-rata waktu eksekusi yang konsisten berada di bawah 0,08 detik (berkisar antara 0,033 hingga 0,075 detik). Tren pergerakan kurva rata-rata (*Average*) pada grafik memperlihatkan kenaikan yang progresif dari *plaintext length* 50 (0,0330059 detik) hingga mencapai titik puncak tertinggi pada panjang data 150 (0,0754931 detik), sebelum akhirnya mengalami sedikit penurunan pada panjang data 200 (0,0603130 detik) dan kembali meningkat pada panjang data 250 (0,0703763 detik).

Time Execution Dekripsi Menggunakan Kriptosistem RSA-OAEP

Tabel 6. Hasil *Time Execution* Dekripsi Menggunakan Kriptosistem RSA-OAEP

Plaintext length	Execution Time (second)			
	ke-1	ke-2	ke-3	Average
50	0.5012855	0.5081220	0.5013551	0.5035875
100	0.6912233	0.6697773	0.6758596	0.6789534
150	0.7724033	0.7865429	0.7624596	0.7738019
200	0.8831501	0.8830705	0.8935482	0.8865896
250	0.9427616	0.9815254	0.9656954	0.9633275



Gambar 16. Grafik Hasil *Time Execution* Dekripsi Menggunakan Kriptosistem RSA-OAEP

Berdasarkan data pada Tabel 6 dan Gambar 16, proses dekripsi menggunakan Kriptosistem RSA-OAEP menunjukkan karakteristik komputasi yang stabil namun membutuhkan durasi yang lebih tinggi dibandingkan proses enkripsinya, dengan rata-rata waktu eksekusi berkisar antara 0,503 hingga 0,963 detik. Kurva rata-rata (*Average*) pada grafik memperlihatkan tren peningkatan yang sangat linear dan konsisten seiring bertambahnya panjang *plaintext* dimulai dari waktu tercepat pada panjang data 50 sebesar 0,5035875 detik hingga mencapai titik tertinggi pada panjang data 250 sebesar 0,9633275 detik yang membuktikan adanya hubungan sebab-akibat langsung di mana ekspansi ukuran karakter input secara signifikan memperberat beban kalkulasi matematis fungsi eksponensial modular menggunakan kunci privat (*private key*) serta proses *unpadding* OAEP.

Pengujian Avalanche Effect

Pengujian dalam penelitian ini mengenai hasil tanda tangan (*digital signature*) dari proses penandatanganan menggunakan algoritma digital Dissanayake *digital signature* dan ciphertext dari proses enkripsi algoritma Kriptosistem RSA-OAEP untuk mendapatkan nilai *Avalanche Effect*. Pengujian yang dilakukan untuk mendapatkan nilai rata-rata hasil *Avalanche Effect*.

Pengujian Avalanche Effect Terhadap Algoritma Digital Dissanayake *Digital Signature*

```
================================================================================
Simulation Results of Avalanche Effect Dissanayake Digital Signature
================================================================================
Metric                  | Case 1               | Case 2               | Case 3
--------------------------------------------------------------------------------
Plaintext               | INFORMATIKA          | KEAMANAN             | JARINGAN
Signature (Int)         | 775242894418864143.. | 131869664442111178.. | 525162378989619482..
Plaintext mods          | 16FORMATIK4          | K3AMANAN             | JARINGA
Signature mods          | 542080035514251487.. | 592181368530597885.. | 110009083873713160..
Avalanche effect (%)    | 51.27                | 51.03                | 50.54
--------------------------------------------------------------------------------
AVERAGE                 | 50.95 %
```

Gambar 17. Hasil Pengujian Avalanche Effect Terhadap Algoritma Digital Dissanayake *Digital Signature*

Berdasarkan data pada Gambar 17, hasil pengujian nilai *Avalanche Effect* terhadap Algoritma *Digital Dissanayake Digital Signature* menunjukkan tingkat keamanan kriptografis yang sangat ideal dan kokoh dengan pencapaian nilai rata-rata (*Average*) sebesar 50,95%. Pengujian yang dilakukan melalui tiga skenario simulasi (*Case 1, Case 2, dan Case 3*) ini memperlihatkan konsistensi performa yang sangat stabil di ambang batas ketat 50%.

Pengujian Avalanche Effect Terhadap Algoritma Kriptosistem RSA-OAEP

```
================================================================================
Simulation Results of Avalanche Effect RSA-OAEP Algorithm
================================================================================
Metric                  | Case 1               | Case 2               | Case 3
--------------------------------------------------------------------------------
Plaintext               | INFORMATIKA          | KEAMANAN             | JARINGAN
Ciphertext (Int)        | 295231055906675603.. | 776453789418411881.. | 999159875488392510..
Plaintext mods          | 16FORMATIK4          | K3AMANAN             | JARINGA
Ciphertext mods         | 115682821485280509.. | 102783080656463027.. | 130166273366549849..
Avalanche effect (%)    | 50.51                | 51.34                | 51.59
--------------------------------------------------------------------------------
AVERAGE (%)             | 51.15 %
```

Gambar 18. Hasil Pengujian Avalanche Effect Terhadap Algoritma Kriptosistem RSA-OAEP

Berdasarkan data pada Gambar 18, hasil pengujian nilai *Avalanche Effect* terhadap Algoritma Kriptosistem RSA-OAEP membuktikan tingkat keamanan yang baik dengan pencapaian nilai rata-rata (*Average*) sebesar 51,15%. Pengujian melalui tiga skenario simulasi ini memperlihatkan sifat sensitivitas algoritma yang stabil di ambang batas ketat standar keamanan kriptografi (lebih dari 50%).

5. Kesimpulan

Berdasarkan hasil implementasi, pengujian, dan analisis yang telah dilakukan, skema keamanan Sign-then-Encrypt yang mengintegrasikan Kriptosistem RSA-OAEP dengan Dissanayake Digital Signature berhasil memberikan lapisan perlindungan data yang sangat baik. Hasil pengujian performa menunjukkan bahwa fungsi penandatanganan digital (signing) dan verifikasi pada Algoritma Dissanayake bekerja dengan tingkat efisiensi yang baik, di mana rata-rata waktu signing stabil pada kisaran 0,021- 0,024 detik dan waktu verifikasi berada pada skala second berkisar (0,000048-0,000062 detik). Di sisi lain, Kriptosistem RSA-OAEP terbukti andal dalam menjaga kerahasiaan data dengan rata-rata

waktu enkripsi di bawah 0,08 detik, meskipun proses dekripsinya membutuhkan durasi komputasi yang lebih tinggi, yakni berkisar antara 0,053 hingga 0,963 detik karena kompleksitas fungsi eksponensial modular kunci privat. Dari aspek ketahanan kriptografis, pengujian Avalanche Effect membuktikan tingkat acakan biner yang sangat ideal mendekati nilai sempurna, dengan capaian rata-rata sebesar 50,95% untuk algoritma Dissanayake dan 51,15% untuk RSA-OAEP ketika data input dimodifikasi satu karakter. Angka ini mengonfirmasi bahwa skema hibrida yang dibangun memiliki sifat confusion dan diffusion yang sangat optimal, sehingga sangat sensitif terhadap perubahan sekecil apa pun dan mampu memitigasi risiko analisis pola teks (*cryptanalysis*) secara mutlak.

Daftar Pustaka

[1] S. Sharma and R. Kumar, "Review on modern cryptographic techniques and cyber security challenges," IEEE Access, vol. 10, pp. 21045-21060, 2022.
[2] A. Kumar and N. Singh, "Hybrid cryptography for secure data transmission in cloud environments," Journal of King Saud University - Computer and Information Sciences, vol. 34, no. 5, pp. 1845-1856, 2022.
[3] M. Ramadhan, A. S. Ahmad, and T. Wahyuni, "Analisis perbandingan performa algoritma kriptografi kunci publik pada pengamanan data teks," Jurnal Nasional Teknik Elektro dan Teknologi Informasi, vol. 12, no. 2, pp. 145-152, 2023.
[4] S. Al-Riyami, "An overview of signcryption and authenticated encryption paradigms," Journal of Information Security and Applications, vol. 72, Art. no. 103412, 2024.
[5] J. An, "A Note on Relation between Encryption and Signature Schemes in the Public-Key Model," Cryptology ePrint Archive, Report 2001/018, 2001.
[6] X. Boyen and G. Waters, "Signcryption vs. sign-then-encrypt: Paradigm analysis in public-key cryptography," Designs, Codes and Cryptography, vol. 91, no. 4, pp. 1125-1148, 2023.
[7] H. Siregar, "Implementasi protokol kemanan jaringan berbasis sign-then-encrypt untuk pengamanan dokumen elektronik," Jurnal Ilmiah Teknologi Informasi, vol. 22, no. 1, pp. 34-43, 2024.
[8] L. Zhang, "Security analysis of sign-then-encrypt paradigm in public-key settings," Journal of Computer Security, vol. 32, no. 1, pp. 45-67, 2024.
[9] K. Prasad, "Performance evaluation of lightweight digital signatures in asymmetric environments," International Journal of Information Security, vol. 23, no. 3, pp. 189-201, 2023.
[10] M. W. D. M. G. Dissanayake, "A Novel Scheme for Digital Signatures," International Journal of Electronics and Information Engineering, vol. 11, no. 2, pp. 61-72, Dec. 2019.
[11] R. Bahri, M. A. Budiman, and B. B. Nasution, "Sign-Then-Encrypt Scheme with Cramer-Shoup Cryptosystem and Dissanayake Digital Signature," Journal of Computing and Applied Informatics, vol. 7, no. 2, pp. 114-123, 2023.
[12] M. A. Budiman, R. Bahri, and H. Wijaya, "Optimasi waktu komputasi tanda tangan digital berbasis teori bilangan ganjil," Jurnal Teknologi dan Sistem Komputer, vol. 12, no. 1, pp. 55-62, 2024.
[13] J. Gomez, "Mathematical reduction of modular exponentiation overhead in asymmetric schemes," IEEE Transactions on Information Forensics and Security, vol. 20, pp. 889-902, 2025.
[14] T. Shindo and H. Tanaka, "Provable security of RSA-OAEP under adaptive chosen ciphertext attacks in the standard model," IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences, vol. E106-A, no. 9, pp. 1201-1215, 2023.
[15] A. Pratama, "Kajian komparatif keamanan skema padding rsa-oaep terhadap serangan oracle aktif," Jurnal Cyberku, vol. 8, no. 2, pp. 89-98, 2022.
[16] J. Manger, "A chosen ciphertext attack on RSA optimal asymmetric encryption padding (OAEP) as defined in PKCS #1 v2.0," Journal of Cryptographic Engineering, vol. 14, no. 1, pp. 85-99, 2021.
[17] Y. Lu, "Resource-constrained cryptographic protocols: A comparative analysis," IEEE Internet of Things Journal, vol. 11, no. 2, pp. 3120-3135, 2024.
[18] P. Gupta, "Cryptographic overhead reduction in real-time communication systems," Computer Networks, vol. 258, Art. no. 110432, 2025.
[19] I. K. Wijaya and R. Kusuma, "Analisis penggunaan resource memori pada algoritma enkripsi asimetris probabilistik," Jurnal Infotel, vol. 15, no. 3, pp. 201-209, 2023.
[20] L. Tan, M. Watson, and H. Kim, "Authenticated encryption and hybrid envelope paradigms in modern cloud architectures," International Journal of Communication Systems, vol. 39, no. 2, pp. 1412-1430, 2026.