JIPI (Jurnal Ilmiah Penelitian dan Pembelajaran Informatika)
Journal homepage: https://jurnal.stkippgritulungagung.ac.id/index.php/jipi
ISSN: 2540-8984
Vol. 11, No. 3, September 2026, Pp.2370-2382

PENERAPAN KRIPTOGRAFI HYBRID MENGGUNAKAN ALGORITMA RSA DAN HILL CIPHER DALAM ENKRIPSI DAN DEKRIPSI PESAN TEKS

Lorenza Raquel Lenak*[1)], Derel Filandy Kaunang[2)], Nicky Kurnia Tumalun[3)]
1. Jurusan Matematika, Universitas Negeri Manado, Indonesia
2. Jurusan Matematika, Universitas Negeri Manado, Indonesia
3. Jurusan Matematika, Universitas Negeri Manado, Indonesia

Article Info
Kata Kunci: Hill Cipher; Kriptografi; RSA

Keywords: Cryptography; Hill Cipher; RSA

Article history:
Received 21 February 2026
Revised 13 April 2026
Accepted 27 April 2026
Available online 1 September 2026

DOI :
https://doi.org/10.29100/jipi.v11i3.10191

* Corresponding author.
Corresponding Author
E-mail address:
lorenzalenak@gmail.com

ABSTRAK
Kemajuan teknologi informasi di masa kini membawa dampak positif bagi kehidupan. Namun, adanya kemudahan dalam mengakses media informasi juga menyebabkan informasi tersebut dapat dengan mudah diakses oleh pihak lain dan disalahgunakan. Oleh karena itu, diperlukan adanya pengamanan informasi. Pengamanan informasi dapat dilakukan dengan menggunakan kriptografi. Penelitian ini bertujuan untuk merancang dan mengembangkan sistem kriptografi *hybrid* yang mengombinasikan algoritma RSA dan dilanjutkan dengan algoritma Hill Cipher dalam enkripsi dan dekripsi pesan teks. Algoritma RSA digunakan terlebih dahulu dengan memanfaatkan kunci publik dan kunci privat, kemudian dilanjutkan dengan algoritma Hill Cipher yang menggunakan matriks kunci berukuran 3×3. Hasil penelitian ini menunjukkan bahwa kombinasi algoritma RSA dan Hill Cipher dapat menghasilkan *plaintext* hasil dekripsi yang sama dengan sebelum dienkripsi, serta *ciphertext* yang tidak dapat dibaca dan sangat berbeda dengan *plaintext* aslinya. Dengan demikian, sistem kriptografi *hybrid* yang mengombinasikan algoritma RSA dan Hill Cipher yang telah dirancang ini dapat membantu meningkatkan keamanan pesan teks.

ABSTRACT
The development of information technology today has brought positive impacts on life. However, the ease of accessing information media also allows information to be easily accessed by other parties and misused. Therefore, information security is required. Information security can be achieved through cryptography. This study aims to design and develop a hybrid cryptographic system that combines the RSA algorithm and is followed by the Hill Cipher algorithm for the encryption and decryption of text messages. The RSA algorithm is applied first by using public and private keys, followed by the Hill Cipher algorithm which uses a 3×3 key matrix. The results show that the combination of RSA and Hill Cipher algorithms produces ciphertext that is unreadable and totally different from the original plaintext, while the decryption process successfully restores the message to its original plaintext form. These findings indicate that the designed hybrid cryptographic system combining RSA and Hill Cipher can enhance text message security.

I. PENDAHULUAN

Perkembangan teknologi di era modern ini menyebabkan perubahan besar dalam tatanan kehidupan. Teknologi berkembang sangat cepat seiring dengan perkembangan zaman sehingga tidak dapat dihindari [1]. Teknologi hadir untuk mendukung dan memudahkan manusia dalam melakukan berbagai aktivitas [2]. Kemajuan teknologi informasi yang sangat pesat menyebabkan kemajuan media komunikasi sebagai media penyampaian informasi dari suatu tempat ke tempat lainnya [3]. Pada masa sekarang ini, berkomunikasi dengan orang lain menggunakan pesan teks melalui media komunikasi menjadi pilihan banyak orang karena sangat memudahkan. Akan tetapi, adanya kemudahan dalam mengakses media informasi dan komunikasi berdampak pada keamanan informasi tersebut. Informasi pada media komunikasi dapat dengan mudah diakses dan diketahui oleh orang lain, baik penyedia layanan maupun pihak lain yang ingin mendapatkan informasi untuk keperluan mereka

JIPI (Jurnal Ilmiah Penelitian dan Pembelajaran Informatika)
Journal homepage: https://jurnal.stkippgritulungagung.ac.id/index.php/jipi
ISSN: 2540-8984
Vol. 11, No. 3, September 2026, Pp.2370-2382

sendiri [4]. Masalah tersebut harus diatasi untuk menghindari penyalahgunaan informasi atau hal-hal lain yang merugikan pengguna media komunikasi.

Pengamanan informasi dapat dilakukan dengan menggunakan kriptografi. Kriptografi didefinisikan sebagai suatu ilmu atau seni untuk menciptakan pesan rahasia. Pesan asli atau *plaintext,* diubah menjadi pesan rahasia (*ciphertext*) melalui proses enkripsi, kemudian melalui proses dekripsi *ciphertext* diubah kembali menjadi *plaintext* [5]. Dalam kriptografi, ada dua jenis algoritma yang dapat diterapkan untuk mengamankan pesan teks yaitu algoritma simetris dan asimetris. Algortima asimetris merupakan algoritma yang menggunakan kunci yang berbeda untuk proses enkripsi dan dekripsinya (kunci publik dan kunci privat), contohnya algoritma RSA (Rivest-Shamir-Adleman). Algoritma simetris merupakan algoritma yang menggunakan kunci yang sama untuk proses enkripsi dan dekripsinya, contohnya algoritma Hill Cipher [6].

Menurut Rahayu, algoritma RSA merupakan salah satu jenis algoritma dalam kriptografi yang termasuk ke dalam jenis kriptografi asimetris dengan proses enkripsi yang menggunakan sebuah *public key* (kunci publik) dan dalam proses dekripsinya digunakan sebuah *private key* (kunci rahasia) [7]. Algoritma Hill Cipher adalah algoritma yang proses enkripsinya menggunakan suatu matriks persegi sebagai matriks kunci dan proses dekripsinya menggunakan invers dari matriks persegi tersebut sebagai matriks kunci [8]. Kriptografi hybrid adalah sistem kriptografi yang mengkombinasikan dua algoritma dalam kriptografi khususnya algoritma asimetri dan simetri [9]. Dengan mengombinasikan RSA sebagai algoritma asimetri dan Hill Cipher sebagai algoritma simetri, keamanan pesan teks dapat ditingkatkan.

Dalam penelitian yang dilakukan oleh Jamaludin, diterapkan kriptografi hybrid dengan menggunakan algoritma Hill Cipher yang menggunakan matriks berukuran 2×2 sebagai kunci dan dikombinasikan dengan algoritma RSA. Hasil penelitian tersebut menyatakan bahwa kombinasi algoritma Hill Cipher dan RSA mempunyai tingkat kesulitan pengamanan data yang lebih tinggi dan cepat [10]. Sementara itu, penelitian terkait juga dilakukan oleh Pangaribuan [11], dengan menerapkan kriptografi hybrid menggunakan algoritma Hill Cipher yang dilanjutkan dengan RSA dan menggunakan matriks berukuran 3×3 sebagai kunci Hill Cipher. Berdasarkan penelitian-penelitian tersebut, penggunaan kombinasi algoritma Hill Cipher dan RSA umumnya dilakukan dengan menempatkan Hill Cipher pada tahap awal enkripsi sebelum RSA. Namun, belum terdapat penelitian yang secara spesifik mengembangkan sistem kriptografi hybrid dengan menempatkan RSA pada tahap awal enkripsi dan kemudian dilanjutkan dengan Hill Cipher. Oleh karena itu, penelitian ini mengusulkan RSA ditempatkan pada tahap awal enkripsi lalu dilanjutkan dengan Hill Cipher.

RSA merupakan algoritma kriptografi asimetris yang melibatkan kunci publik dan kunci privat serta memiliki kompleksitas matematis yang lebih tinggi dibandingkan algoritma simetris seperti Hill Cipher yang hanya melibatkan satu kunci. Hal tersebut didukung oleh penelitian sebelumnya yang menunjukkan bahwa algoritma simetris seperti AES dan DES memiliki keunggulan dalam efisiensi dan kecepatan, namun memiliki kelemahan pada aspek distribusi kunci. Sementara itu, algoritma asimetris seperti RSA memiliki tingkat keamanan yang lebih baik dalam proses pertukaran kunci meskipun membutuhkan sumber daya komputasi yang lebih besar. Sehingga, pendekatan kriptografi hybrid digunakan untuk mengombinasikan keunggulan kedua jenis algoritma tersebut [12]. Dengan demikian, penelitian ini bertujuan untuk merancang dan mengimplementasikan sistem kriptografi hybrid dengan menempatkan RSA pada tahap awal enkripsi yang dilanjutkan dengan Hill Cipher

II. METODE PENELITIAN

Penelitian ini menggunakan metode penelitian terapan (*applied research*) yang berfokus pada perancangan dan implementasi sistem kriptografi hybrid dengan mengombinasikan algoritma RSA dan Hill Cipher. Tahapan penelitiannya: (1) melakukan studi literatur, (2) perancangan sistem kriptografi, (3) implementasi algoritma, serta (4) pengujian dan validasi sistem.

Dalam penelitian ini, dilakukan pengujian menggunakan beberapa variasi data teks untuk mengevaluasi kinerja algoritma secara lebih baik. Data uji yang digunakan meliputi teks pendek, teks sedang, teks panjang, serta teks dengan kombinasi karakter huruf dan angka. Variasi data ini bertujuan untuk menguji konsistensi dan keandalan algoritma dalam berbagai kondisi input. Selain itu, skenario pengujian yang dilakukan meliputi:

1. Pengujian enkripsi dan dekripsi untuk memastikan bahwa sistem dapat mengubah *plaintext* menjadi *ciphertext* dan mengembalikannya kembali ke bentuk semula secara akurat.
2. Pengujian menggunakan variasi plaintext dengan panjang dan karakter yang berbeda. Pengujian ini dilakukan untuk mengevaluasi kinerja algoritma dalam berbagai kondisi input.
3. Pengujian *Avalanche Effect*. Dalam kriptografi, *avalanche effect* digunakan sebagai indikator untuk menilai kualitas suatu algoritma dengan cara mengamati perubahan bit pada *plaintext* atau kunci yang menyebabkan perubahan pada sejumlah bit *ciphertext*. Perubahan kecil pada input seharusnya

JIPI (Jurnal Ilmiah Penelitian dan Pembelajaran Informatika)
Journal homepage: https://jurnal.stkippgritulungagung.ac.id/index.php/jipi
ISSN: 2540-8984
Vol. 11, No. 3, September 2026, Pp.2370-2382

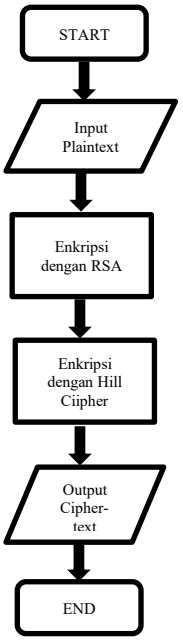
menghasilkan perubahan yang signifikan pada output [13]

$$Avalanche\ effect = \frac{Jumlah\ bit\ berbeda}{Total\ bit} \times 100\%$$

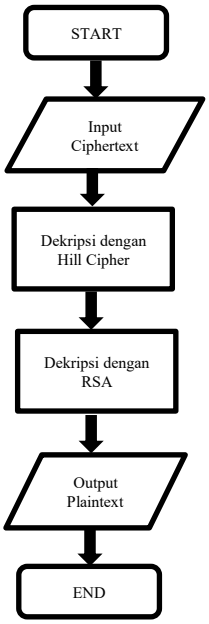
4. Pengujian waktu proses enkripsi dan dekripsi.
   Seluruh proses pengujian dilakukan menggunakan bantuan perangkat lunak MATLAB untuk memperoleh hasil yang akurat dan efisien.

Pada penelitian ini, karakter yang digunakan dibatasi sebanyak 37 karakter yang terdiri dari huruf (A–Z), angka (0–9), serta satu karakter tambahan yaitu "@". Setiap karakter dipetakan ke dalam bentuk numerik. Karakter "@" digunakan sebagai *dummy character* untuk melengkapi panjang blok pada algoritma Hill Cipher. Pemilihan 37 karakter tersebut didasarkan pada kebutuhan representasi teks yang umum digunakan, yaitu huruf dan angka, sehingga sistem mampu menangani pesan-pesan sederhana. Pembatasan jumlah karakter dilakukan untuk menyederhanakan proses pemetaan karakter ke bentuk numerik serta perhitungan dalam algoritma kriptografi, sehingga sistem menjadi lebih mudah diimplementasikan.

Untuk memperjelas alur proses pada sistem, tahapan enkripsi dan dekripsi divisualisasikan dalam bentuk diagram alur (*flowchart*) sebagai berikut.



Gambar. 1. Flowchart proses enkripsi



Gambar. 2. Flowchart proses dekripsi

JIPI (Jurnal Ilmiah Penelitian dan Pembelajaran Informatika)
Journal homepage: https://jurnal.stkippgritulungagung.ac.id/index.php/jipi
ISSN: 2540-8984
Vol. 11, No. 3, September 2026, Pp.2370-2382

Berikut ini adalah teori-teori yang menjadi acuan dalam penelitian ini.

A. *Kriptografi*

Kriptografi (cryptography) berasal dari bahasa Yunani, yaitu *kryptos* yang berarti tersembunyi atau rahasia, serta *graphein* yang berarti menulis [14]. Kriptografi merupakan ilmu yang mempelajari tentang teknik untuk menjaga kemananan komunikasi antara dua pihak. Umumnya, terdapat dua pihak yang ingin saling mengirimkan pesan, akan tetapi kedua pihak tersebut tidak ingin ada pihak ketiga yang mengetahui isi atau makna pesan tersebut jika pesan tersebut jatuh ke tangan pihak yang tidak berwenang [15]. Menurut Vaudenay, kriptografi merupakan ilmu perlindungan informasi dari pihak yang tidak berwenang dengan mencegah perubahan atau penggunaan yang tidak sah. Tujuan utama kriptografi ialah untuk menjaga keamanan informasi [16]. Algoritma kriptografi adalah algoritma matematika yang menegakkan perlindungan tersebut [17]. Informasi atau data sebelum dilakukan enkripsi dikenal sebagai *plaintext*, sementara hasil dari proses enkripsi tersebut disebut *ciphertext* [18].

Kriptografi hybrid merupakan gabungan antara algoritma kriptografi yang menggunakan kriptografi asimetris dan kriptografi simetris. Kombinasi tersebut dibuat untuk memaksimalkan keamanan sekaligus efisiensi komputasi dalam proses pertukaran data [19]. Kriptografi hybrid juga didefinisikan sebagai sebuah teknik yang menggunakan beberapa cipher yang berbeda untuk memanfaatkan masing-masing keunggulannya [20]. Kriptografi hybrid sering dipakai karena memanfaatkan keunggulannya yaitu peningkatan keamanan dan tingkat kesulitan yang lebih tinggi. Dengan kata lain, penggunaan kriptografi hybrid lebih aman dari serangan kriptanalis dibandingkan dengan hanya menggunakan satu jenis algoritma kriptografi [10].

B. *Algoritma RSA*

Algoritma RSA dikembangkan pada tahun 1978 oleh Ron Rivest, Adi Shamir dan Leonard Adleman [21]. RSA merupakan sistem kriptografi asimetris yang menggunakan dua jenis kunci, yaitu kunci publik untuk proses enkripsi dan kunci privat untuk proses dekripsi [22]. Kunci publik dapat diakses oleh siapa saja, sedangkan kunci privat hanya dimiliki dan diketahui oleh pemilik data [23].

Langkah-langkah pengimplementasian algoritma RSA sebagaimana dijelaskan dalam [11] adalah sebagai berikut. Pertama, tentukan kunci publik (*public key*) E dengan cara memilih dua buah bilangan sembarang yaitu p dan q, lalu tentukan nilai $r = pq$ dan $\phi(r) = (p-1)(q-1)$. Kemudian tentukan nilai E sebagai kunci publik yang memenuhi syarat $gcd\,(E, \phi(r))$ dan $1 < E < r$. Kedua, tentukan kunci privat (*private key*) D dimana D adalah invers modulo dari E atau dapat ditulis $ED \equiv 1\ mod\ \phi(r)$. Ketiga, tentukan *plaintext* yang akan dienkripsi dan ubah menjadi bentuk numerik. Keempat, *plaintext* dalam bentuk numerik tersebut dienkripsi dengan menggunakan rumus

$$c_i = p_i^E\ mod\ r \tag{1}$$

untuk memperoleh ciphertext. Kelima, untuk mengubah kembali *ciphertext* menjadi *plaintext*, dilakukan proses dekripsi menggunakan rumus

$$p_i = c_i^D\ mod\ r \tag{2}$$

dengan p dan c adalah *plaintext* dan *ciphertext* dalam bentuk numerik, E adalah kunci publik, D adalah kunci privat dan r adalah hasil perkalian dua bilangan prima yang telah diperoleh sebelumnya.

C. *Algoritma Hill Cipher*

Algoritma Hill Cipher dikembangkan oleh Lester S. Hill pada tahun 1929 dengan menggunakan sebuah matriks persegi sebagai kunci yang dapat digunakan untuk melakukan enkripsi dan dekripsi [24]. Algoritma ini melibatkan operasi perkalian matriks dalan proses enkripsi dan dekripsinya [25]. Algoritma Hill Cipher yang menggunakan kunci matriks berukuran 2×2 disebut *Hill 2-cipher*, berlaku juga untuk penggunaan kunci matriks 3×3 disebut *Hill 3-cipher*. Secara umum, disebut *Hill n-cipher* untuk proses enkripsi dan dekripsi yang menggunakan matriks $n \times n$ dengan entri bilangan bulat [26].

Langkah-langkah pengimplementasian algoritma RSA sebagaimana dijelaskan dalam [11] adalah sebagai berikut. Pertama, tentukan matriks kunci A untuk digunakan dalam proses enkripsi. Kedua, tentukan matriks invers dari A modulo m yaitu A^{-1} untuk digunakan dalam proses dekripsi, dengan m adalah jumlah karakter yang digunakan. Ketiga, tentukan plaintext yang akan digunakan dan ubah menjadi bentuk numerik, lalu bagi menjadi beberapa blok sesuai dengan ukuran matriks kunci. Jika matriks kunci berukuran 3×3, maka setiap blok terdiri dari tiga elemen *plaintext* dalam bentuk numerik yang direpresentasikan dalam matriks kolom berukuran 3×1. Keempat, *plaintext* dalam bentuk numerik tersebut dienkripsi dengan menggunakan rumus

$$c = Ap\ (mod\ m) \tag{3}$$

untuk memperoleh *ciphertext*. Kelima, untuk mengubah kembali *ciphertext* menjadi *plaintext*, dilakukan proses dekripsi menggunakan rumus

$$p = A^{-1}c\ (mod\ m) \tag{4}$$

JIPI (Jurnal Ilmiah Penelitian dan Pembelajaran Informatika)
Journal homepage: https://jurnal.stkippgritulungagung.ac.id/index.php/jipi
ISSN: 2540-8984
Vol. 11, No. 3, September 2026, Pp.2370-2382

dengan p dan c adalah *plaintext* dan *ciphertext* dalam bentuk numerik. A adalah matriks kunci dan A^{-1}adalah inversnya.

III. HASIL DAN PEMBAHASAN

Berikut ini adalah tabel karakter yang digunakan dalam penelitian ini.

TABEL I
KONVERSI KARAKTER KE NUMERIK

A	B	C	D	E	F	G	H	I	J
1	2	3	4	5	6	7	8	9	10
K	L	M	N	O	P	Q	R	S	T
11	12	13	14	15	16	17	18	19	20
U	V	W	X	Y	Z	0	1	2	3
21	22	23	24	25	26	27	28	29	30
4	5	6	7	8	9	@			
31	32	33	34	35	36	0			

A. Pembentukan Kunci

1) Pembentukan Kunci RSA

Misalkan digunakan $p = 3$ dan $q = 11$, maka diperoleh $r = p \times q = 3 \times 11 = 33$ dan $\phi(r) = (p-1)(q-1) = 2 \times 10 = 20$.

Selanjutnya akan ditentukan nilai E (kunci publik) yang memenuhi syarat $gcd(E, \phi(r)) = 1$ dan $1 < E < r$. Misalkan digunakan $E = 7$, akan dicari nilai D (kunci rahasia).

$ED \equiv 1 \; mod \; \phi(r)$
$7 \cdot D \equiv 1 \; mod \; 20$
$7 \cdot 3 \equiv 1 \; mod \; 20$
$21 \equiv 1 \; mod \; 20$

Diperoleh $D = 3$. Jadi untuk kunci publik $E = 7$, diperoleh kunci privat $D = 3$.

2) Pembentukan Kunci Hill Cipher

Misalkan digunakan matriks kunci sebagai berikut.

$$A = \begin{bmatrix} 4 & -3 & 2 \\ 1 & 5 & -4 \\ -2 & 1 & 0 \end{bmatrix}$$

Selanjutnya akan dicari invers dari A. Namun, sebelum itu akan ditentukan nilai $det(A)$, invers modulo dari $det(A)$ dan $Adj(A)$ yang akan digunakan untuk mencari invers dari A terhadap modulo m. Jumlah karakter yang digunakan adalah 37, maka $m = 37$. Diperoleh $det(A) = 14$. Karena $gcd(14,37) = 1$, maka $det(A)$ memiliki invers mod 37.

$$14 \cdot x \equiv 1 \; mod \; 37$$
$$14 \cdot 8 \equiv 1 \; mod \; 37$$
$$112 \equiv 1 \; mod \; 37$$

Diperoleh $x = 8$. Jadi, invers dari $14 \; mod \; 37$ adalah 8.

Kemudian, diperoleh juga $Adj(A) = \begin{bmatrix} 4 & 2 & 2 \\ 8 & 4 & 18 \\ 11 & 2 & 23 \end{bmatrix}$. Sehingga, didapatkan invers dari A:

$$A^{-1} = \frac{1}{det\,(A)} Adj(A) \; (mod \; m)$$
$$= det\,(A^{-1}) \; Adj(A) \; (mod \; m)$$
$$= 8 \begin{bmatrix} 4 & 2 & 2 \\ 8 & 4 & 18 \\ 11 & 2 & 23 \end{bmatrix} (mod \; 37)$$
$$= \begin{bmatrix} 32 & 16 & 16 \\ 64 & 32 & 144 \\ 88 & 16 & 184 \end{bmatrix} (mod \; 37)$$
$$= \begin{bmatrix} 32 & 16 & 16 \\ 27 & 32 & 33 \\ 14 & 16 & 36 \end{bmatrix}.$$

JIPI (Jurnal Ilmiah Penelitian dan Pembelajaran Informatika)
Journal homepage: https://jurnal.stkippgritulungagung.ac.id/index.php/jipi
ISSN: 2540-8984
Vol. 11, No. 3, September 2026, Pp.2370-2382

Jadi, untuk matriks kunci $A = \begin{bmatrix} 4 & -3 & 2 \\ 1 & 5 & -4 \\ -2 & 1 & 0 \end{bmatrix}$, diperoleh $A^{-1} = \begin{bmatrix} 32 & 16 & 16 \\ 27 & 32 & 33 \\ 14 & 16 & 36 \end{bmatrix}$.

B. Proses Enkripsi

Misalkan digunakan *plaintext* sebagai berikut.
LORENZARAQUELLENAK22504045
Berikut ini adalah konversi *plaintext* ke numerik berdasarkan Tabel I.

TABEL II
KONVERSI PLAINTEXT KE NUMERIK

L	O	R	E	N	Z	A	R	A	Q
12	15	18	5	14	26	1	18	1	17
U	E	L	L	E	N	A	K	2	2
21	5	12	12	5	14	1	11	29	29
5	0	4	0	4	5	5			
32	27	31	27	31	32	32			

1) Enkripsi RSA

Misalkan $p_1 = 12;\ p_2 = 15;\ p_3 = 18;\ p_4 = 5;\ p_5 = 14;\ p_6 = 26;\ p_7 = 1;\ p_8 = 18;\ p_9 = 1;\ p_{10} = 17;\ p_{11} = 21;\ p_{12} = 5;\ p_{13} = 12;\ p_{14} = 12;\ p_{15} = 5;\ p_{16} = 14;\ p_{17} = 1;\ p_{18} = 11;\ p_{19} = 29;\ p_{20} = 29;\ p_{21} = 32;\ p_{22} = 27;\ p_{23} = 31;\ p_{24} = 27;\ p_{25} = 31;\ p_{26} = 32$ dan telah diperoleh sebelumnya $E = 7$ dan $r = 33$. Menurut rumus (1), berikut ini proses enkripsinya.

$c_i = {p_i}^7 mod\ 33$
$c_1 = {p_1}^7 mod\ 33 = 12^7 mod\ 33 = 12$
$c_2 = {p_2}^7 mod\ 33 = 15^7 mod\ 33 = 27$
$c_3 = {p_3}^7 mod\ 33 = 18^7 mod\ 33 = 6$
$c_4 = {p_4}^7 mod\ 33 = 5^7 mod\ 33 = 14$
$c_5 = {p_5}^7 mod\ 33 = 14^7 mod\ 33 = 20$
$c_6 = {p_6}^7 mod\ 33 = 26^7 mod\ 33 = 5$
$c_7 = {p_7}^7 mod\ 33 = 1^7 mod\ 33 = 1$
$c_8 = {p_8}^7 mod\ 33 = 18^7 mod\ 33 = 6$
$c_9 = {p_9}^7 mod\ 33 = 1^7 mod\ 33 = 1$
$c_{10} = {p_{10}}^7 mod\ 33 = 17^7 mod\ 33 = 8$
$c_{11} = {p_{11}}^7 mod\ 33 = 21^7 mod\ 33 = 21$
$c_{12} = {p_{12}}^7 mod\ 33 = 5^7 mod\ 33 = 14$
$c_{13} = {p_{13}}^7 mod\ 33 = 12^7 mod\ 33 = 12$
$c_{14} = {p_{14}}^7 mod\ 33 = 12^7 mod\ 33 = 12$
$c_{15} = {p_{15}}^7 mod\ 33 = 5^7 mod\ 33 = 14$
$c_{16} = {p_{16}}^7 mod\ 33 = 14^7 mod\ 33 = 20$
$c_{17} = {p_{17}}^7 mod\ 33 = 1^7 mod\ 33 = 1$
$c_{18} = {p_{18}}^7 mod\ 33 = 11^7 mod\ 33 = 11$
$c_{19} = {p_{19}}^7 mod\ 33 = 29^7 mod\ 33 = 17$
$c_{20} = {p_{20}}^7 mod\ 33 = 29^7 mod\ 33 = 17$
$c_{21} = {p_{21}}^7 mod\ 33 = 32^7 mod\ 33 = 32$
$c_{22} = {p_{22}}^7 mod\ 33 = 27^7 mod\ 33 = 3$
$c_{23} = {p_{23}}^7 mod\ 33 = 31^7 mod\ 33 = 4$
$c_{24} = {p_{24}}^7 mod\ 33 = 27^7 mod\ 33 = 3$
$c_{25} = {p_{25}}^7 mod\ 33 = 31^7 mod\ 33 = 4$
$c_{26} = {p_{26}}^7 mod\ 33 = 32^7 mod\ 33 = 32$

Dengan demikian telah diperoleh nilai c_1 hingga c_{26} yang akan digunakan untuk tahap selanjutnya yaitu proses enkripsi menggunakan algoritma Hill Cipher.

2) Enkripsi Hill Cipher

Berdasarkan nilai c_1 hingga c_{26} yang telah diperoleh sebelumnya, nilai-nilai tersebut kemudian dibentuk menjadi matriks-matriks yang akan dienkripsi menggunakan matriks kunci yang telah diperoleh sebelumnya, yaitu sebagai berikut.

JIPI (Jurnal Ilmiah Penelitian dan Pembelajaran Informatika)
Journal homepage: https://jurnal.stkippgritulungagung.ac.id/index.php/jipi
ISSN: 2540-8984
Vol. 11, No. 3, September 2026, Pp.2370-2382

$p_1 = \begin{bmatrix}12\\27\\6\end{bmatrix}; p_2 = \begin{bmatrix}14\\20\\5\end{bmatrix}; p_3 = \begin{bmatrix}1\\6\\1\end{bmatrix}; p_4 = \begin{bmatrix}8\\21\\14\end{bmatrix}; p_5 = \begin{bmatrix}12\\12\\14\end{bmatrix}; p_6 = \begin{bmatrix}20\\1\\11\end{bmatrix}; p_7 = \begin{bmatrix}17\\17\\32\end{bmatrix}; p_8 = \begin{bmatrix}3\\4\\3\end{bmatrix}$ dan $p_9 = \begin{bmatrix}4\\32\\0\end{bmatrix}$. Untuk melengkapi entri dari matriks p_9, digunakan angka 0 sebagai tambahan yang jika diubah ke dalam bentuk karakter akan menjadi @ atau *dummy character*. Selanjutnya, menggunakan rumus (3), dilakukan proses enkripsi sebagai berikut.

$$c_1 = Ap_1 (mod\ 37)$$
$$= \begin{bmatrix}4 & -3 & 2\\1 & 5 & -4\\-2 & 1 & 0\end{bmatrix}\begin{bmatrix}12\\27\\6\end{bmatrix}(mod\ 37)$$
$$= \begin{bmatrix}-21\\123\\3\end{bmatrix}(mod\ 37) = \begin{bmatrix}16\\12\\3\end{bmatrix}$$

$$c_2 = Ap_2 (mod\ 37)$$
$$= \begin{bmatrix}4 & -3 & 2\\1 & 5 & -4\\-2 & 1 & 0\end{bmatrix}\begin{bmatrix}14\\20\\5\end{bmatrix}(mod\ 37)$$
$$= \begin{bmatrix}6\\94\\-8\end{bmatrix}(mod\ 37) = \begin{bmatrix}6\\20\\29\end{bmatrix}$$

$$c_3 = Ap_3 (mod\ 37)$$
$$= \begin{bmatrix}4 & -3 & 2\\1 & 5 & -4\\-2 & 1 & 0\end{bmatrix}\begin{bmatrix}1\\6\\1\end{bmatrix}(mod\ 37)$$
$$= \begin{bmatrix}-12\\27\\4\end{bmatrix}(mod\ 37) = \begin{bmatrix}25\\27\\4\end{bmatrix}$$

$$c_4 = Ap_4 (mod\ 37)$$
$$= \begin{bmatrix}4 & -3 & 2\\1 & 5 & -4\\-2 & 1 & 0\end{bmatrix}\begin{bmatrix}8\\21\\14\end{bmatrix}(mod\ 37)$$
$$= \begin{bmatrix}-3\\57\\5\end{bmatrix}(mod\ 37) = \begin{bmatrix}34\\20\\5\end{bmatrix}$$

$$c_5 = Ap_5 (mod\ 37)$$
$$= \begin{bmatrix}4 & -3 & 2\\1 & 5 & -4\\-2 & 1 & 0\end{bmatrix}\begin{bmatrix}12\\12\\14\end{bmatrix}(mod\ 37)$$
$$= \begin{bmatrix}40\\16\\-12\end{bmatrix}(mod\ 37) = \begin{bmatrix}3\\16\\25\end{bmatrix}$$

$$c_6 = Ap_6 (mod\ 37)$$
$$= \begin{bmatrix}4 & -3 & 2\\1 & 5 & -4\\-2 & 1 & 0\end{bmatrix}\begin{bmatrix}20\\1\\11\end{bmatrix}(mod\ 37)$$
$$= \begin{bmatrix}99\\-19\\-39\end{bmatrix}(mod\ 37) = \begin{bmatrix}25\\18\\35\end{bmatrix}$$

$$c_7 = Ap_7 (mod\ 37)$$
$$= \begin{bmatrix}4 & -3 & 2\\1 & 5 & -4\\-2 & 1 & 0\end{bmatrix}\begin{bmatrix}17\\17\\32\end{bmatrix}(mod\ 37)$$
$$= \begin{bmatrix}81\\-26\\-17\end{bmatrix}(mod\ 37) = \begin{bmatrix}7\\11\\20\end{bmatrix}$$

$$c_8 = Ap_8 (mod\ 37)$$
$$= \begin{bmatrix}4 & -3 & 2\\1 & 5 & -4\\-2 & 1 & 0\end{bmatrix}\begin{bmatrix}3\\4\\3\end{bmatrix}(mod\ 37)$$

$$= \begin{bmatrix} 6 \\ 11 \\ -2 \end{bmatrix} (mod\ 37) = \begin{bmatrix} 6 \\ 11 \\ 35 \end{bmatrix}$$

$$c_9 = Ap_9 (mod\ 37)$$

$$= \begin{bmatrix} 4 & -3 & 2 \\ 1 & 5 & -4 \\ -2 & 1 & 0 \end{bmatrix} \begin{bmatrix} 4 \\ 32 \\ 0 \end{bmatrix} (mod\ 37)$$

$$= \begin{bmatrix} -80 \\ 164 \\ 24 \end{bmatrix} (mod\ 37) = \begin{bmatrix} 31 \\ 16 \\ 24 \end{bmatrix}$$

Berdasarkan hasil enkripsi tersebut, hasil dalam bentuk numerik yaitu entri-entri matriks c_1 hingga c_9 yang telah diperoleh diubah kembali menjadi karakter.

TABEL III
KONVERSI NUMERIK KE CIPHERTEXT

Num	Char	Num	Char
16	P	25	Y
12	L	25	Y
3	C	18	R
6	F	35	8
20	T	7	G
29	2	11	K
25	Y	20	T
27	0	6	F
4	D	11	K
34	7	35	8
20	T	31	4
5	E	16	P
3	C	24	X
16	P		

Maka diperoleh *ciphertext* yaitu: PLCFT2Y0D7TECPYYR8GKTFK84PX.

C. *Proses Dekripsi*

1) *Dekripsi Hill Cipher*

Berikut ini proses dekripsi menggunakan rumus (4).

$$p_1 = A^{-1} c_1 (mod\ 37)$$

$$= \begin{bmatrix} 32 & 16 & 16 \\ 27 & 32 & 33 \\ 14 & 16 & 36 \end{bmatrix} \begin{bmatrix} 16 \\ 12 \\ 3 \end{bmatrix} (mod\ 37)$$

$$= \begin{bmatrix} 752 \\ 915 \\ 524 \end{bmatrix} (mod\ 37) = \begin{bmatrix} 12 \\ 27 \\ 6 \end{bmatrix}$$

$$p_2 = A^{-1} c_2 (mod\ 37)$$

$$= \begin{bmatrix} 32 & 16 & 16 \\ 27 & 32 & 33 \\ 14 & 16 & 36 \end{bmatrix} \begin{bmatrix} 6 \\ 20 \\ 29 \end{bmatrix} (mod\ 37)$$

$$= \begin{bmatrix} 976 \\ 1759 \\ 1448 \end{bmatrix} (mod\ 37) = \begin{bmatrix} 14 \\ 20 \\ 5 \end{bmatrix}$$

$$p_3 = A^{-1} c_3 (mod\ 37)$$

$$= \begin{bmatrix} 32 & 16 & 16 \\ 27 & 32 & 33 \\ 14 & 16 & 36 \end{bmatrix} \begin{bmatrix} 25 \\ 27 \\ 4 \end{bmatrix} (mod\ 37)$$

$$= \begin{bmatrix} 1296 \\ 1671 \\ 926 \end{bmatrix} (mod\ 37) = \begin{bmatrix} 1 \\ 6 \\ 1 \end{bmatrix}$$

$$p_4 = A^{-1} c_4 (mod\ 37)$$

$$= \begin{bmatrix} 32 & 16 & 16 \\ 27 & 32 & 33 \\ 14 & 16 & 36 \end{bmatrix} \begin{bmatrix} 34 \\ 20 \\ 5 \end{bmatrix} (mod\ 37)$$

$$= \begin{bmatrix} 1488 \\ 1723 \\ 976 \end{bmatrix} (mod\ 37) = \begin{bmatrix} 8 \\ 21 \\ 14 \end{bmatrix}$$

JIPI (Jurnal Ilmiah Penelitian dan Pembelajaran Informatika)
Journal homepage: https://jurnal.stkippgritulungagung.ac.id/index.php/jipi
ISSN: 2540-8984
Vol. 11, No. 3, September 2026, Pp.2370-2382

$$p_5 = A^{-1}c_5(mod\ 37)$$
$$= \begin{bmatrix}32 & 16 & 16\\ 27 & 32 & 33\\ 14 & 16 & 36\end{bmatrix}\begin{bmatrix}3\\16\\25\end{bmatrix}(mod\ 37)$$
$$= \begin{bmatrix}752\\1418\\1198\end{bmatrix}(mod\ 37) = \begin{bmatrix}12\\12\\14\end{bmatrix}$$
$$p_6 = A^{-1}c_6(mod\ 37)$$
$$= \begin{bmatrix}32 & 16 & 16\\ 27 & 32 & 33\\ 14 & 16 & 36\end{bmatrix}\begin{bmatrix}25\\18\\35\end{bmatrix}(mod\ 37)$$
$$= \begin{bmatrix}1648\\2406\\1898\end{bmatrix}(mod\ 37) = \begin{bmatrix}20\\1\\11\end{bmatrix}$$
$$p_7 = A^{-1}c_7(mod\ 37)$$
$$= \begin{bmatrix}32 & 16 & 16\\ 27 & 32 & 33\\ 14 & 16 & 36\end{bmatrix}\begin{bmatrix}7\\11\\20\end{bmatrix}(mod\ 37)$$
$$= \begin{bmatrix}720\\1201\\994\end{bmatrix}(mod\ 37) = \begin{bmatrix}17\\17\\32\end{bmatrix}$$
$$p_8 = A^{-1}c_8(mod\ 37)$$
$$= \begin{bmatrix}32 & 16 & 16\\ 27 & 32 & 33\\ 14 & 16 & 36\end{bmatrix}\begin{bmatrix}6\\11\\35\end{bmatrix}(mod\ 37)$$
$$= \begin{bmatrix}928\\1669\\1520\end{bmatrix}(mod\ 37) = \begin{bmatrix}3\\4\\3\end{bmatrix}$$
$$p_9 = A^{-1}c_9(mod\ 37)$$
$$= \begin{bmatrix}32 & 16 & 16\\ 27 & 32 & 33\\ 14 & 16 & 36\end{bmatrix}\begin{bmatrix}31\\16\\24\end{bmatrix}(mod\ 37)$$
$$= \begin{bmatrix}1632\\2141\\1554\end{bmatrix}(mod\ 37) = \begin{bmatrix}4\\32\\0\end{bmatrix}$$

2) Dekripsi RSA

Hasil dekripsi berupa entri entri matriks p_1 hingga p_9 kemudian digunakan untuk tahap selanjutnya yaitu dekripsi menggunakan algoritma RSA untuk memperoleh kembali *plaintext*. Misalkan $c_1 = 12;\ c_2 = 17;\ c_3 = 6;\ c_4 = 14;\ c_5 = 20;\ c_6 = 5;\ c_7 = 1; c_8 = 6;\ c_9 = 1;\ c_{10} = 8;\ c_{11} = 21;\ c_{12} = 14;\ c_{13} = 12;\ c_{14} = 12;\ c_{15} = 14;\ c_{16} = 20;\ c_{17} = 1;\ c_{18} = 11;\ c_{19} = 13;\ c_{20} = 13;\ c_{21} = 32;\ c_{22} = 3;\ c_{23} = 4;\ c_{24} = 3;\ c_{25} = 4;\ c_{26} = 32;\ c_{27} = 0$ dan telah diperoleh sebelumnya $D = 3$. Berikut ini proses dekripsi menggunakan rumus (2).

$$p_i = {c_i}^3 mod\ 33$$
$$p_1 = {c_1}^3 mod\ 33 = 12^3 mod\ 33 = 12$$
$$p_2 = {c_2}^3 mod\ 33 = 27^3 mod\ 33 = 15$$
$$p_3 = {c_3}^3 mod\ 33 = 6^3 mod\ 33 = 18$$
$$p_4 = {c_4}^3 mod\ 33 = 14^3 mod\ 33 = 5$$
$$p_5 = {c_5}^3 mod\ 33 = 20^3 mod\ 33 = 14$$
$$p_6 = {c_6}^3 mod\ 33 = 5^3 mod\ 33 = 26$$
$$p_7 = {c_7}^3 mod\ 33 = 1^3 mod\ 33 = 1$$
$$p_8 = {c_8}^3 mod\ 33 = 6^3 mod\ 33 = 18$$
$$p_9 = {c_9}^3 mod\ 33 = 1^3 mod\ 33 = 1$$
$$p_{10} = {c_{10}}^3 mod\ 33 = 8^3 mod\ 33 = 17$$
$$p_{11} = {c_{11}}^3 mod\ 33 = 21^3 mod\ 33 = 21$$
$$p_{12} = {c_{12}}^3 mod\ 33 = 14^3 mod\ 33 = 5$$
$$p_{13} = {c_{13}}^3 mod\ 33 = 12^3 mod\ 33 = 12$$
$$p_{14} = {c_{14}}^3 mod\ 33 = 12^3 mod\ 33 = 12$$

JIPI (Jurnal Ilmiah Penelitian dan Pembelajaran Informatika)
Journal homepage: https://jurnal.stkippgritulungagung.ac.id/index.php/jipi
ISSN: 2540-8984
Vol. 11, No. 3, September 2026, Pp.2370-2382

$p_{15} = {c_{15}}^3 mod\ 33 = 14^3 mod\ 33 = 5$
$p_{16} = {c_{16}}^3 mod\ 33 = 20^3 mod\ 33 = 14$
$p_{17} = {c_{17}}^3 mod\ 33 = 1^3 mod\ 33 = 1$
$p_{18} = {c_{18}}^3 mod\ 33 = 11^3 mod\ 33 = 11$
$p_{19} = {c_{19}}^3 mod\ 33 = 17^3 mod\ 33 = 29$
$p_{20} = {c_{20}}^3 mod\ 33 = 17^3 mod\ 33 = 29$
$p_{21} = {c_{21}}^3 mod\ 33 = 32^3 mod\ 33 = 32$
$p_{22} = {c_{22}}^3 mod\ 33 = 3^3 mod\ 33 = 27$
$p_{23} = {c_{23}}^3 mod\ 33 = 4^3 mod\ 33 = 31$
$p_{24} = {c_{24}}^3 mod\ 33 = 3^3 mod\ 33 = 27$
$p_{25} = {c_{25}}^3 mod\ 33 = 4^3 mod\ 33 = 31$
$p_{26} = {c_{26}}^3 mod\ 33 = 32^3 mod\ 33 = 32$
$p_{27} = {c_{27}}^3 mod\ 33 = 0^3 mod\ 33 = 0$

Nilai p_{21} hingga p_{27} yang telah diperoleh diubah kembali menjadi karakter sehingga diperoleh LORENZARAQUELLENAK22504045@. Sehingga jika *dummy character* dihilangkan, diperoleh kembali plaintext yaitu LORENZARAQUELLENAK22504045.

D. *Uji Coba Hasil Enkripsi dan Dekripsi Menggunakan MATLAB*

Berikut ini adalah proses enkripsi dan dekripsi teks menggunakan algoritma RSA dan Hill Cipher melalui *software* MATLAB online yang dapat diakses melalui laman https://matlab.mathworks.com/. MATLAB digunakan sebagai alat bantu untuk memvalidasi hasil perhitungan enkripsi dan dekripsi yang dilakukan secara manual. Parameter yang digunakan dalam pengujian meliputi *plaintext*, kunci publik dan privat RSA, serta matriks kunci Hill Cipher. Hasil yang diperoleh dari MATLAB kemudian dibandingkan dengan hasil perhitungan manual, dan menunjukkan kesesuaian. Dalam proses enkripsi dihasilkan *ciphertext* yang sama dengan yang telah diperoleh, serta dihasilkan *plaintext* yang sama dalam proses dekripsi, sehingga membuktikan bahwa algoritma yang diimplementasikan berjalan dengan benar.

```
=== PROGRAM KRIPTOGRAFI HYBRID RSA & HILL CIPHER ===
Masukkan plaintext:

LORENZARAQUELLENAK22504045

Masukkan modulo RSA (r):

33

Masukkan kunci publik RSA (e):

7

Masukkan kunci privat RSA (d):

3

Masukkan modulo Hill Cipher:

37

Masukkan matriks kunci Hill Cipher A (contoh [4 3; 5 7])
A =

[4,-3,2;1,5,-4;-2,1,0]

Plaintext numerik:
  Columns 1 through 10

    12    15    18     5    14    26     1    18     1    17

  Columns 11 through 20

    21     5    12    12     5    14     1    11    29    29

  Columns 21 through 26

    32    27    31    27    31    32

Hasil Enkripsi RSA:
  Columns 1 through 10

    12    27     6    14    20     5     1     6     1     8

  Columns 11 through 20

    21    14    12    12    14    20     1    11    17    17

  Columns 21 through 26

    32     3     4     3     4    32

Hasil Enkripsi Hill Cipher:
    16     6    25    34     3    25     7     6    31
    12    20    27    20    16    18    11    11    16
     3    29     4     5    25    35    20    35    24

Ciphertext dalam bentuk karakter:
PLCFT2Y0D7TECPYYR8GKTFK84PX
```

Gambar. 3. Enkripsi *plaintext* menggunakan MATLAB

JIPI (Jurnal Ilmiah Penelitian dan Pembelajaran Informatika)
Journal homepage: https://jurnal.stkippgritulungagung.ac.id/index.php/jipi
ISSN: 2540-8984
Vol. 11, No. 3, September 2026, Pp.2370-2382



Gambar. 4. Dekripsi *ciphertext* menggunakan MATLAB

Hasil enkripsi menunjukkan bahwa *plaintext* berhasil diubah menjadi *ciphertext* yang tidak memiliki pola yang mudah dikenali dan hasil dekripsi berhasil mengembalikan *ciphertext* ke bentuk *plaintext* semula secara akurat.

E. *Uji Variasi Karakter Plaintext*

Pada pengujian ini dilakukan variasi karakter pada plaintext yang digunakan sebagai input, digunakan beberapa plaintext dengan panjang karakter yang berbeda.

TABEL IV
VARIASI KARAKTER PLAINTEXT

Plaintext	Panjang karakter	Ciphertext
HALO	4	26770T
KRIPTO	6	SRUBJM
M4T3M4T1K4	10	470IF65CDPD2
MATEMATIKAUNIMA2022	19	SX@HPGT@RZSDINSAF4QC

Dengan demikian, sistem yang dirancang dapat digunakan untuk *plaintext* yang bervariasi yaitu memiliki panjang karakter berbeda-beda (teks panjang dan pendek) serta dapat digunakan kombinasi huruf dan angka yang terdapat pada Tabel I.

F. *Uji Avalanche Effect*

Hasil pengujian *Avalance Effect* dilakukan dengan menggunakan sistem yang telah dirancang yaitu algoritma kriptografi hybrid RSA dan Hill Cipher serta algoritma RSA saja sebagai pembanding. Dibawah ini adalah hasil pengujian tersebut yang telah diperoleh dengan bantuan MATLAB.

TABEL V
HASIL UJI AVALANCHE EFFECT

Plaintext Awal	Plaintext Uji	Avalanche Effect (%)	
		Hybrid (RSA & Hill Cipher)	Hanya RSA
HELLO	HXLLO	16,67	7,5
KRIPTOGRAFI	KRIPTVGRAFI	7,29	3,41
M4T3M4T1K4	M4T3M4X1K4	5,21	1,25
MATHUNIMA2022	M4THUNIMA2022	6,67	1,92

Berdasarkan hasil pengujian *avalanche effect* pada Tabel V, dapat dilihat bahwa perubahan kecil pada *plaintext* menghasilkan perubahan pada *ciphertext*. Pada seluruh sampel pengujian, nilai avalanche effect pada metode hybrid (RSA dan Hill Cipher) selalu lebih tinggi dibandingkan dengan RSA tunggal. Hal ini menunjukkan bahwa kombinasi kedua algoritma memberikan tingkat penyebaran perubahan yang lebih baik dibandingkan penggunaan satu algoritma saja yaitu misalnya algoritma RSA saja.. Nilai *avalanche effect* pada metode hybrid menunjukkan fluktuasi pada setiap sampel pengujian, yang dipengaruhi oleh karakteristik *plaintext*. Meskipun demikian, secara keseluruhan metode hybrid tetap menunjukkan kecenderungan menghasilkan *avalanche effect* yang lebih tinggi dibandingkan RSA tunggal.

G. *Uji Waktu Enkripsi dan Dekripsi*

Selanjutnya juga dilakukan uji waktu proses enkripsi dan dekripsi untuk mengetahui berapa lama dilakukannya proses enkripsi dan dekripsi. Dibawah ini adalah hasil pengujian tersebut.

TABEL VI

HASIL UJI WAKTU ENKRIPSI DAN DEKRIPSI

Plaintext	Ciphertext	Waktu Enkripsi (detik)	Waktu Dekripsi (derik)
HALO	26770T	0,000179	0,000023
KRIPTO	SRUBJM	0,000197	0,000024
MATEMATIKA	CSX@HPGT@DA8	0,000215	0,000026
UNIVERSITASNEGERIM4N4D0	QXOU4GVUZEWK@X@3PCANLR4H	0,000315	0,000045

Berdasarkan hasil pengujian waktu enkripsi dan dekripsi yang ditunjukkan pada Tabel VI, dapat diketahui bahwa setiap proses enkripsi dan dekripsi membutuhkan waktu komputasi yang sangat kecil, yaitu berada pada rentang milidetik hingga mikrodetik. Dari hasil pengujian, terlihat bahwa semakin panjang *plaintext* yang digunakan, maka waktu enkripsi dan dekripsi yang dibutuhkan juga cenderung meningkat. Berdasarkan hasil pengujian, dapat disimpulkan bahwa sistem kriptografi yang diusulkan memiliki waktu komputasi yang efisien karena seluruh proses enkripsi dan dekripsi masih berada pada skala waktu yang sangat kecil, sehingga sistem dapat dikatakan layak untuk digunakan dari sisi performa waktu.

H. Pembahasan

Dari sisi keamanan, sistem ini memiliki ketahanan terhadap serangan brute force yang lebih tinggi dibandingkan penggunaan satu algoritma saja. Hal ini disebabkan oleh penggunaan dua tahap enkripsi yang mengombinasikan RSA dan Hill Cipher. Pada sistem ini, penyerang harus terlebih dahulu memecahkan algoritma RSA untuk memperoleh hasil dekripsi awal, sebelum melanjutkan proses analisis terhadap Hill Cipher. Brute force attack merupakan metode penyerangan dengan mencoba seluruh kemungkinan kunci hingga ditemukan kunci yang benar. Pada algoritma Hill Cipher yang digunakan dengan matriks kunci berukuran 3×3 dan modulo 37, jumlah kemungkinan kunci yang dapat dibentuk adalah sebesar 37^9 atau sekitar $1{,}3 \times 10^{14}$ kemungkinan. Jika diasumsikan bahwa sistem mampu menguji 10^6 kemungkinan per detik, maka waktu yang dibutuhkan untuk melakukan brute force attack adalah sekitar $1{,}3 \times 10^8$ detik. Hal ini menunjukkan bahwa proses pencarian kunci secara brute force membutuhkan waktu yang sangat lama, sehingga meningkatkan tingkat kesulitan dalam melakukan serangan terhadap sistem. Selain itu, algoritma RSA memiliki tingkat keamanan yang bergantung pada kesulitan faktorisasi bilangan menjadi dua bilangan prima. Semakin besar ukuran kunci, maka akan semakin lama juga prosesnya. Dengan demikian, kombinasi kedua algoritma tersebut meningkatkan resistansi sistem terhadap brute force attack.

Pada sistem ini, yang menjadi perbedaan utama dengan penelitian sebelumnya adalah urutan penggunaan algoritma, di mana sebelumnya Hill Cipher digunakan terlebih dahulu sebelum RSA, sedangkan pada penelitian ini RSA digunakan pada tahap awal enkripsi yang kemudian dilanjutkan dengan Hill Cipher. Perbedaan urutan tersebut menunjukkan adanya pendekatan yang berbeda dalam proses pengamanannya. Pada penelitian ini, penggunaan RSA pada tahap awal memungkinkan *plaintext* terlebih dahulu diproses menggunakan algoritma asimetris yang memiliki kompleksitas matematis tinggi, sebelum memasuki tahap selanjutnya menggunakan Hill Cipher. Dengan demikian, pendekatan pada sistem ini memberikan alternatif dalam perancangan sistem kriptografi hybrid.

Sistem ini memiliki beberapa keunggulan yaitu, penggunaan dua algoritma yang berbeda, yaitu RSA dan Hill Cipher yang menyebabkan proses enkripsi dilakukan dalam dua tahap sehingga menghasilkan perlindungan yang lebih kompleks. Selain itu, kombinasi antara algoritma asimetris dan simetris memungkinkan setiap algoritma dimanfaatkan sesuai dengan kelebihannya masing-masing. Namun, sistem ini juga memiliki beberapa keterbatasan, yaitu keterbatasan jumlah karakter yang digunakan serta sistem ini juga belum diuji terhadap berbagai jenis serangan secara langsung, sehingga analisis keamanan yang dilakukan masih berdasarkan konsep dan teori.

IV. KESIMPULAN

Berdasarkan hasil penelitian yang telah dilakukan, dapat disimpulkan bahwa sistem kriptografi hybrid RSA dan Hill Cipher berhasil diimplementasikan dengan baik dalam proses enkripsi dan dekripsi pesan teks. Proses enkripsi dilakukan melalui dua tahap, yaitu RSA dan Hill Cipher, sehingga menghasilkan *ciphertext* yang sangat berbeda dengan *plaintext*, sedangkan proses dekripsi berhasil mengembalikan *ciphertext* menjadi *plaintext* semula. Berdasarkan pengujian variasi karakter plaintext, sistem ini juga tetap mampu memproses berbagai jenis input *plaintext* dengan panjang dan kombinasi karakter berbeda sesuai dengan tabel karakter yang digunakan.

Hasil pengujian Avalanche Effect menunjukkan bahwa sistem hybrid menghasilkan perubahan bit yang lebih besar dibandingkan dengan hanya menggunakan satu algoritma yaitu RSA saja, meskipun nilai yang diperoleh

masih bervariasi. Hal ini menunjukkan bahwa sistem memiliki kemampuan dalam menyebarkan perubahan pada *ciphertext*. Sementara itu, hasil uji waktu menunjukkan bahwa proses enkripsi dan dekripsi berjalan dengan waktu komputasi yang sangat kecil. Selain itu, waktu komputasi meningkat seiring bertambahnya panjang *plaintext*. Dengan demikian, sistem kriptografi hybrid yang dirancang mampu meningkatkan aspek keamanan melalui Avalanche Effect dengan tetap mempertahankan efisiensi waktu proses.

DAFTAR PUSTAKA

[1] Y. F. Tammu, A. L. F. Tilaar, dan D. F. Kaunang, "Asesmen Pembelajaran Matematika di SMP Negeri 2 Tondano pada Masa Pandemi Covid-19," 2023.
[2] I. P. Damopolii, A. L. F. Tilaar, dan S. J. A. Sumarauw, "Analisis penggunaan aplikasi Alef Education pada pembelajaran matematika di MTs Al-Mujahidin Tomohon," *Dharmas Education Journal (DE_Journal)*, vol. 5, no. 1, hlm. 211–218, 2024.
[3] D. A. Meko, "Perbandingan algoritma DES, AES, IDEA dan Blowfish dalam enkripsi dan dekripsi data," *Jurnal Teknologi Terpadu*, vol. 4, no. 1, hlm. 8–15, 2018.
[4] A. A. Permana, "Penerapan kriptografi pada teks pesan dengan menggunakan metode Vigenere Cipher berbasis Android," *Jurnal Al-Azhar Indonesia Seri Sains Dan Teknologi*, vol. 4, no. 3, hlm. 110–115, 2018.
[5] M. Z. Siambaton, "Pengamanan data teks menggunakan algoritma kriptografi Elgamal dan XOR dari serangan hacker," *sudo Jurnal Teknik Informatika*, vol. 2, no. 4, hlm. 176–187, 2023.
[6] N. A. Nanda, M. Sari, dan I. Gunawan, "Kriptografi dan penerapannya dalam sistem keamanan data," *Jurnal Media Informatika*, vol. 4, no. 2, hlm. 90–93, 2023.
[7] A. Rahayu, A. P. Ardana, C. Pramudhita, D. Syafitri, dan R. Z. Sirega, "Perbandingan algoritma RSA dengan algoritma Blowfish pada perancangan aplikasi keamanan data," *Jurnal Ilmu Komputer dan Sistem Informasi (JIKOMSI)*, vol. 7, no. 1, hlm. 203–207, 2024.
[8] A. Serdano, M. Zarlis, S. Sawaluddin, dan D. Hartama, "Pengamanan pesan menggunakan algoritma Hill Cipher dalam keamanan komputer," *Jurnal Mahajana Informasi*, vol. 4, no. 2, hlm. 5–9, 2019.
[9] F. D. Yonathan, H. Nasution, dan H. Priyanto, "Aplikasi pengaman dokumen digital menggunakan algoritma Kriptografi Hybrid dan algoritma Kompresi Huffman," *JEPIN (Jurnal Edukasi dan Penelitian Informatika)*, vol. 7, no. 2, hlm. 181–195, 2021.
[10] J. Jamaludin, "Rancang bangun kombinasi Hill Cipher dan RSA menggunakan metode Hybrid Cryptosystem," *Sinkron: jurnal dan penelitian teknik informatika*, vol. 2, no. 2, hlm. 86–93, 2018.
[11] L. J. Pangaribuan, "Kriptografi hybrida algoritma Hill Cipher dan RSA sebagai pengembangan kriptografi kunci simetris (studi kasus: nilai mahasiswa AMIK MBP)," *Jurnal Teknologi Informasi dan komunikasi*, vol. 7, no. 1, hlm. 11–26, 2018.
[12] M. Zuna, A. Wulansari, dan A. B. Putra, "PERBANDINGAN ALGORITMA KRIPTOGRAFI SIMETRIS DAN ASIMETRIS DALAM KEAMANAN DATA DIGITAL," *JATI (Jurnal Mahasiswa Teknik Informatika)*, vol. 10, no. 1, hlm. 249–253, 2026.
[13] W. S. Tyas, M. F. Ardiansyah, dan G. J. O. P. Soares, "Analisis Keamanan Algoritma Beaufort Cipher Berdasarkan Panjang dan Tingkat Keacakan Kunci," *Jurnal Aplikasi Teknologi dan Komputasi*, vol. 1, no. 1, hlm. 41–51, 2025.
[14] N. A. Nanda, M. Sari, dan I. Gunawan, "Kriptografi dan penerapannya dalam sistem keamanan data," *Jurnal Media Informatika*, vol. 4, no. 2, hlm. 90–93, 2023.
[15] S. Rubinstein-Salzedo, *Cryptography*, 1st ed., vol. 260. Cham: Springer, 2018.
[16] H. Putri, L. Virna, T. Febrianti, dan T. Sutabri, "Pengamanan Data Transmisi Aplikasi Web Menggunakan Algoritma Kriptografi RSA: Studi Kasus dan Analisis," *Jurnal Manajemen Informatika & Teknologi*, vol. 5, no. 1, hlm. 153–170, 2025.
[17] S. Vaudenay, *A classical introduction to cryptography: Applications for communications security*. New York: Springer, 2006.
[18] S. Oktaviani, F. Rizky, dan I. Gunawan, "Analisis Keamanan Data Dengan Menggunakan Kriptografi Modern Algoritma Advance Encryption Standar (AES)," *Jurnal Media Informatika*, vol. 4, no. 2, hlm. 97–101, 2023.
[19] A. Andri, R. Prasetya, dan S. Sepniyanti, "Rancang Bangun Sistem Pengamanan E-Mail Berbasis Android Menggunakan Pendekatan Hybrid Cryptosystem," *MARAS: Jurnal Penelitian Multidisiplin*, vol. 4, no. 1, hlm. 159–173, 2026.
[20] H. Maulana, M. Tahir, N. Farrohah, F. Maulana, dan R. R. Aprilianyani, "Perancangan Sistem Keamanan File Menggunakan Hybrid Encryption Untuk Perlindungan Data," *Jurnal RESTIKOM: Riset Teknik Informatika dan Komputer*, vol. 7, no. 1, hlm. 87–96, 2025.
[21] R. L. Rivest, A. Shamir, dan L. Adleman, "A method for obtaining digital signatures and public-key cryptosystems," *Commun. ACM*, vol. 21, no. 2, hlm. 120–126, 1978.
[22] M. S. A. Mohamad, R. Din, dan J. I. Ahmad, "Research trends review on RSA scheme of asymmetric cryptography techniques," *Bulletin of Electrical Engineering and Informatics*, vol. 10, no. 1, hlm. 487–492, 2021.
[23] M. S. D. Dairi dan M. S. Asih, "Implementasi Algoritma Kriptografi RSA Dalam Aplikasi Sistem Informasi Perpustakaaan," *Jurnal Ilmu Komputer dan Sistem Informasi*, vol. 2, no. 1, hlm. 98–107, 2023.
[24] L. S. Hill, "Cryptography in an algebraic alphabet," *The American Mathematical Monthly*, vol. 36, no. 6, hlm. 306–312, 1929.
[25] A. Azanuddin, R. Kartadie, F. Erwis, A. F. Boy, dan A. H. Nasyuha, "A combination of Hill Cipher and RC4 methods for text security," *TELKOMNIKA (Telecommunication Computing Electronics and Control)*, vol. 22, no. 2, hlm. 351–361, 2024.
[26] H. Anton dan C. Rorres, *Elementary linear algebra: Applications version*, 11th ed. New York: John Wiley & Sons, 2013.