Implementasi Kriptografi Dengan Metode RSA Untuk Keamanan Data Pada Email Berbasis PHP

Novanto Prio Utomo[1], Nuniek Fahriani[2], M. Amirul[3]
[1,2,3]Program Studi Teknik Informatika Fakultas Teknik Universitas Muhammadiyah Surabaya
Jl. Raya Sutorejo No.59, Dukuh Sutorejo, Kec. Mulyorejo, Surabaya, Jawa Timur, telp. 031 381 1966
e-mail: [1]novantopu@gmail.com, [2]nuniekfahriani@ft.um-surabaya.ac.id, [3]amirulhaq@ft.um-surabaya.ac.id

Abstrak

Email merupakan salah satu platform yang digunakan untuk melakukan pertukaran data atau informasi yang masih tetap digunakan sampai sekarang. Email lebih sering digunakan untuk pertukaran informasi dengan pihak-pihak tertentu seperti penulis jurnal ataupu buku. Dalam sebuah pertukaran informasi data atau informasi yang ada dapat dimanipulasi oleh pihak ketiga sehingga data dengan sis yang berbeda akan diterima oleh penerima. Oleh karena itu dibutuhkan sebuah mekanisme untuk mengamankan data yang disimpan didalamnya, sehingga data tersebut tidak dapat dibaca ataupun dimanipulasi oleh pihak yang tidak berwenang. Dalam penelitian ini menggunakan algoritma kriptografi RSA untuk mengamankan data yang ada. RSA sendiri merupakan algoritma kriptografi asimetris yang menggunakan sepasang kunci, yaitu kunci public dan kunci pribadi. Keamanan algoritma RSA terletak pada sulitnya memfaktorkan bilangan prima. Dalam penelitian ini pengujian dilakukan dengan memasukkan data atau informasi yang akan dikirim melalui email ataupun platform lainnya. Data yang akan dikirimkan kemudian dienkripsi menggunakan algoritma kriptografi RSA. Sehingga data atau informasi yang disimpan ke dalam email berupa data chipertext yang tidak bisa dibaca oleh pihak yang tidak berwenang.

Kata Kunci*: Email, Kriptografi RSA, Keamanan data*

Abstract

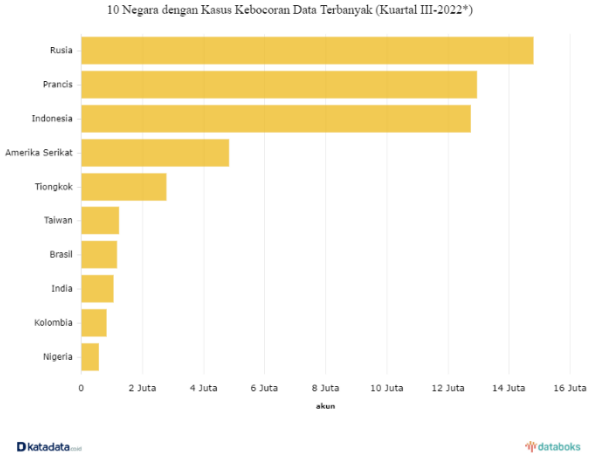
Email is a platform used to exchange data or information which is still used today. Email is more often used to exchange information with certain parties such as journal or book authors. In an information exchange, existing data or information can be manipulated by a third party so that data with a different system will be received by the recipient. Therefore, a mechanism is needed to secure the data stored therein, so that the data cannot be read or manipulated by unauthorized parties. In this research, the RSA cryptographic algorithm is used to secure existing data. RSA itself is an asymmetric cryptographic algorithm that uses a pair of keys, namely a public key and a private key. The security of the RSA algorithm lies in the difficulty of factoring prime numbers. In this research, testing is carried out by entering data or information that will be sent via email or other platforms. The data to be sent is then encrypted using the RSA cryptographic algorithm. So the data or information stored in email is in the form of ciphertext data which cannot be read by unauthorized parties.

Keywords*: Email, RSA Cryptography, Data security*

1. PENDAHULUAN

Perkembangan teknologi yang semakin pesat tidak dapat dipungkiri telah mengubah cara kerja berbagai kegiatan dalam bidang kehidupan manusia mulai dari perusahaan sampai pemerintah. Dengan perkembangan teknologi saat ini pertukaran informasi antar pihak sangat diperlukan. Jika keamanan pertukaran informasi tidak bisa di jaga, maka pihak lain dapat memanfaatkan informasi tersebut sehingga akan merugikan pihak-pihak yang berhak atas informasi tersebut.

Menurut data perusahaan keamanan *siber Surfshark*. Indonesia menempati urutan ke-3 negara dengan jumlah kasus kebocoran data terbanyak di dunia. tercatat, ada 12,74 juta akun yang menglami kebocoran data di Indonesia selama *kuartal III-2022* yang tercatat hingga 13 september 2022 [1].



Gambar 1. *Chart* kasus kebocoran data terbanyak selama *Kuartal III* 2022.

Dari data diatas diketahui bahwa di Indonesia masih banyak terjadi kasus kebocoran data yang merugikan banyak pengguna internet di Indonesia. Hal ini dapat menyebabkan kerusakan bagi individu ataupun organisasi tergantung dari data yang dicuri akan digunakan untuk apa oleh sipelaku.

Ada beberapa bentuk ancaman terhadap pertukaran informasi seperti penyadapan, pencurian dan pemalsuan informasi. Untuk itu keamanan dari pertukaran informasi tersebut sangatlah diperlukan. *Kriptografi* adalah salah satu solusi yang tepat untuk menjaga kerahasiaan dan keaslian data serta dapat meningkatkan keamanan suatu data [2].

Pada masa kini pertukaran informasi menjadi lebih cepat dan mudah sebagaimana percakapan yang seharusnya tidak bisa dilakukan karena jarak yang jauh menjadi mungkin dengan *email* dan aplikasi *messenger* yang lain, akan tetapi dengan mudahnya pertukaran informasi ini membuat banyak penggunanya lalai dalam keamanan data atau informasi yang dilakukan waktu pertukaran informasi yang memungkinkan terjadinya resiko pencurian data [3].

Untuk itu perlu adanya sistem keamanan data yang mana salah satu caranya adalah dengan menggunakan algoritma kriptografi, dengan salah satu metode yang digunakan untuk mengamankan datanya yaitu algoritma *Rivest Shamir Adleman* (RSA).

Dalam penelitian ini menggunakan kombinasi algoritma RSA karena algortima RSA mempunyai kemampuan yang cukup baik karena mempunyai kunci autentikasi 2 arah yaitu *public key* dan *private key* jadi lebih aman. Berdasarkan dari latar belakang tersebut, diperlukan sebuah keamanan data untuk menjaga kerahasiaan, keaslian data dan meningkatkan keamanan pada data.

2. METODE PENELITIAN

Metode Pengumpulan Data

Metode pengumpulan data yang dugunakan adalah menggunakan studi literatur. Studi literatur merupakan studi yang menggunakan bahan sebagai referensi tertulis untuk mengumpulkan data dengan membaca seperti buku, skripsi, jurnal dan berbagai sumber

sumber internet manapun yang berkaitan dengan Algoritma kriptografi RSA dan Perancangan Kriptografi [4].

TABEL 1. Tabel Studi Literatur

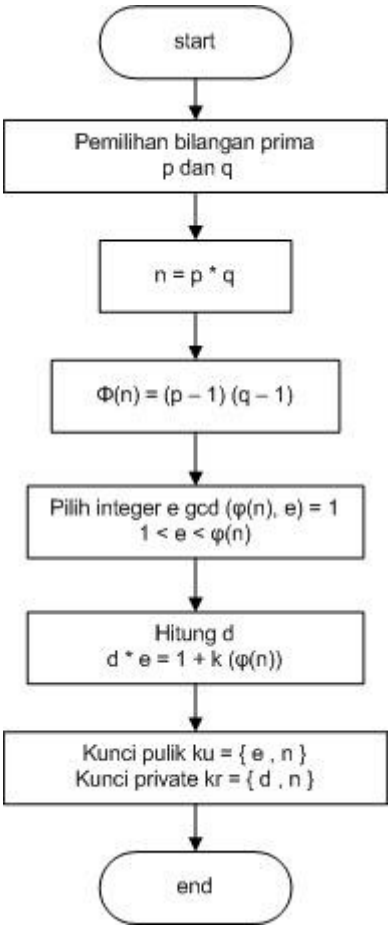
No	Nama Jurnal	Persamaan	Perbeadaan
1	Triorizka, Adrianus. 2010. *Penerapan Algoritma RSA untuk Pengamanan Data dan Digital Signature dengan .Net.* Sekolah Tinngi Manajemen Informatika dan Komputer AMIKOM, Yogyakarta.	Persamaan antara hasil studi Pustaka dengan tugas akhir ini andalah penerapan algoritma RSA untuk keamanan data.	Perbedaan antara hasil studi Pustaka dengan tugas akhir ini adalah penggunaan framework yang digunakan untuk membuat algoritma RSA yang digunakan untuk mengamankan data.
2	Rahajoeningroem, Tri dkk. 2008. *Studi dan Implementasi Algoritma RSA untuk Pengamanan Data Transkrip Akademik Mahasiswa*. Jurusan Teknik Elektro Universitas Komputer Indonesia.	Persamaan antara hasil studi Pustaka dengan tugas akhir ini andalah penerapan algoritma RSA untuk keamanan data.	Perbedaan antara hasil studi Pustaka dengan tugas akhir ini adalah ruang lingkup penelitian yang dilakukan dari data transkrip akademik mahasiswa menjadi data pribadi.
3	Nizatsary, R. N., Seta, H. B., & Wahyono, B. T. (2022). PENERAPAN KEAMANAN DATA SISWA MENGGUNAKAN INTERNATIONAL DATA ENCRYPTION ALGORITHM (IDEA) DAN RIVEST SHAMIR ADLEMAN (RSA) [5].	Persamaan antara hasil studi Pustaka dengan tugas akhir ini andalah penerapan algoritma RSA untuk keamanan data.	Perbedaan antara hasil studi Pustaka dengan tugas akhir ini adalah Pada penggunaan metode yang digunakan dalam penelitian ini yang digunakan hanya algoritma RSA, sedangkan dalam tinjaun studi adalah menggunakan IDEA dan RSA
4	Irawan, C., & Rachmawanto, E. H. (2021). Keamanan Data Menggunakan Gabungan Kriptografi AES dan RSA [6].	Persamaan antara hasil studi Pustaka dengan tugas akhir ini andalah penerapan algoritma RSA untuk keamanan data.	Perbedaan antara hasil studi Pustaka dengan tugas akhir ini adalah dalam penelitian ini yang digunakan hanya algoritma RSA, sedangkan dalam tinjaun studi adalah gabungan kriptografi AES dan RSA

5	Tampubolon, A. (2021). Implementasi Kombinasi Algoritma RSA dan Algoritma DES Pada Aplikasi Pengaman Pesan Teks [7].	Persamaan antara hasil studi Pustaka dengan tugas akhir ini andalah penerapan algoritma RSA untuk keamanan data.	Perbedaan antara hasil studi Pustaka dengan tugas akhir ini adalah Pada algoritma yang akan digunakan dalam melakukan pengamanan data
6	Reychan Davia Al Huday, & Sejati Waluyo. (2022). Pengamanan File Rekam Medis Pada Puskesmas Larangan Utara Menggunakan Algoritma Kriptografi RSA Berbasis Web [8].	Persamaan antara hasil studi Pustaka dengan tugas akhir ini andalah penerapan algoritma RSA untuk keamanan data.	Perbedaan antara hasil studi Pustaka dengan tugas akhir ini adalah Objek yang akan digunakan dalam pengamanan data
7	Irma Listiani, Maimanah Salsabila Nasution, Wini Istya Sari, & Adnan Buyung Nasution. (2022). PERANCANGAN KEAMANAN DATA PASIEN DI KLINIK KECANTIKAN RATU BEAUTY STUDIO MENGGUNAKAN METODE KRIPTOGRAFI RSA [9].	Persamaan antara hasil studi Pustaka dengan tugas akhir ini andalah penerapan algoritma RSA untuk keamanan data.	Perbedaan antara hasil studi Pustaka dengan tugas akhir ini adalah Objek yang akan digunakan dalam pengamanan data
8	Fatonah, & Dadang Iskandar Mulyana. (2022). Implementasi Metode Rivest Shamir Adleman untuk Enkripsi dan Dekripsi Text [10].	Persamaan antara hasil studi Pustaka dengan tugas akhir ini andalah penerapan algoritma RSA untuk melkukan enkripsi dan dekripsi.	Perbedaan antara hasil studi Pustaka dengan tugas akhir ini adalah Objek yang ada pada studi Pustaka tidak dibatasi
9	Putra, Y. P., Mufizar, T., & Alfiyani, E. (2022). IMPLEMENTASI SUPER ENKRIPSI AES DAN RSA PADA PENGAMANAN DATA REKAM MEDIS PASIEN [11].	Persamaan antara hasil studi Pustaka dengan tugas akhir ini andalah penerapan algoritma RSA untuk keamanan data.	Perbedaan antara hasil studi Pustaka dengan tugas akhir ini adalah Objek yang akan digunakan dalam pengamanan data
10	Mahfud, I., & Hadi Utomo, P. (2022). Implementasi Sistem Kriptografi RSA Signature dengan SHA-256 pada Mekanisme Autentikasi REST API [12].	Persamaan antara hasil studi Pustaka dengan tugas akhir ini andalah penerapan algoritma RSA untuk keamanan data.	Perbedaan antara hasil studi Pustaka dengan tugas akhir ini adalah Objek yang akan digunakan dalam pengamanan data

Dari tinjauan studi tersebut didapatkan banyak keamanan data yang menggunakan algoritma RSA dikarenakan dalam algoritma RSA memiliki dua kunci yaitu kunci privat dan kunci public yang mana membuat data kita menjadi lebih aman dari kasus pencurian data oleh pihak ketiga.

Rancangan Sistem

Dalam penelitian ini penulis merancang sebuah aplikasi proses enkripsi dan dekripsi berbasis web menggunakan bahasa pemrograman PHP. Proses enkripsi dan dekripsi dilakukan dengan mengambil file yang akan/telah dikirim, dari file tersebut akan dilakukan proses enkripsi dan dekripsi pada sistem yang telah dirancang. Proses enkripsi dan dekripsi dapat dilihat dari flowchart berikut:



Gambar 2. Flowchart Pembagkitan algoritma RSA

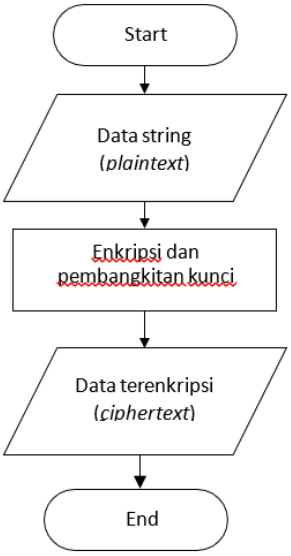
Flowchart Pembangitan algoritma RSA pada gambar 2 diatas dapat dijelaskan sebagai berikut:

1. Dipilih dua bilangan prima p ≠ q secara acak dan terpisah untuk tiap-tiap p dan q.
2. Hitung N dengan persamaan: N = p q.
3. Hitung φ dengan persamaan: φ = (p-1)(q-1).
4. dipilih bilangan bulat (integer) antara satu dan φ (1 < e < φ) yang juga merupakan coprime dari φ.

5. Hitung d dengan persamaan : de ≡ 1 (mod φ).
6. Hasil dari algoritma ini:

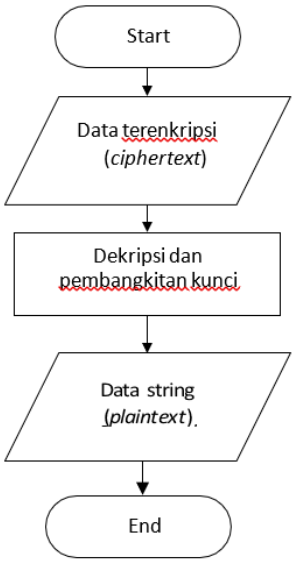
   Kunci public : pasangan (N,e)

   Kunci privat : pasangan (N,d)



Gambar 3. Flowchart Enkripsi

Pada flowchart enkripsi seperti Gambar 3 di atas langkah yang dilakukan pertama menentukan file yang akan dienkripsi, selanjutnya sistem akan melakukan enkripsi dan pembangkitan kunci untuk file yang dienkripsi. Hasil dari proses tersebut akan memberikan kunci privat dan public yang nantinya akan digunakan untuk melakukan dekripsi file tersebut.



Gambar 4. Flowchart Dekripsi

Pada flowchart enkripsi seperti Gambar 4 di atas langkah yang dilakukan pertama mengambil file yang sudah dienkripsi, kemudian menginputkan public dan private key yang didapatkan dari proses enkripsi. Hasil dari proses tersebut akan mengembalikan file yang telah dienkripsi tersebut kembali menjadi file yang belum terenkripsi(Kembali menjadi file aslinya).

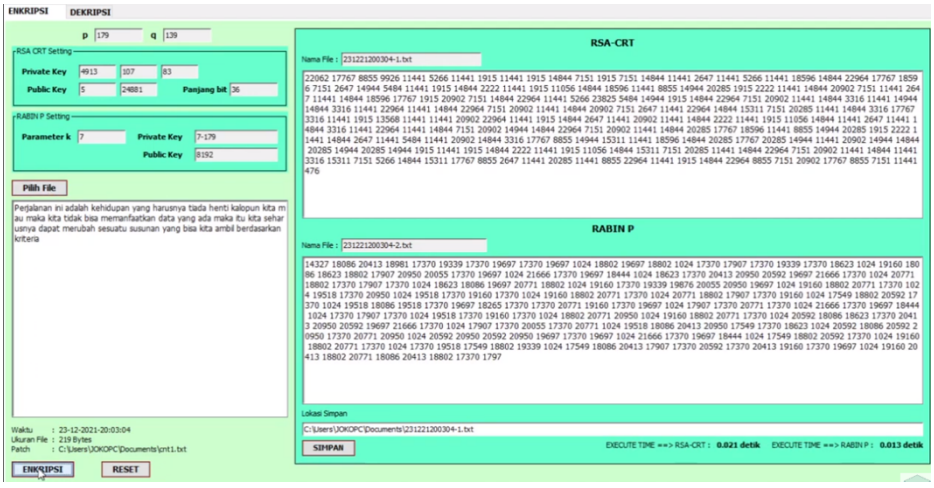
3. HASIL DAN PEMBAHASAN

Aplikasi Kriptografi ini berjalan pada sistem berbasis web yang mana aplikasi ini dibangun menggunakan bahasa pemrograman PHP. Hasil yang diperoleh dari tahap implementasi ini akan menjaga informasi yang dimiliki sehingga tidak akan dimanipulasi oleh pihak yang tidak bertanggung jawab. pada gambar 5 dibawah ini adalah tampilan awal dari sistem yang dibuat:

Gambar 5. Tampilan awal aplikasi

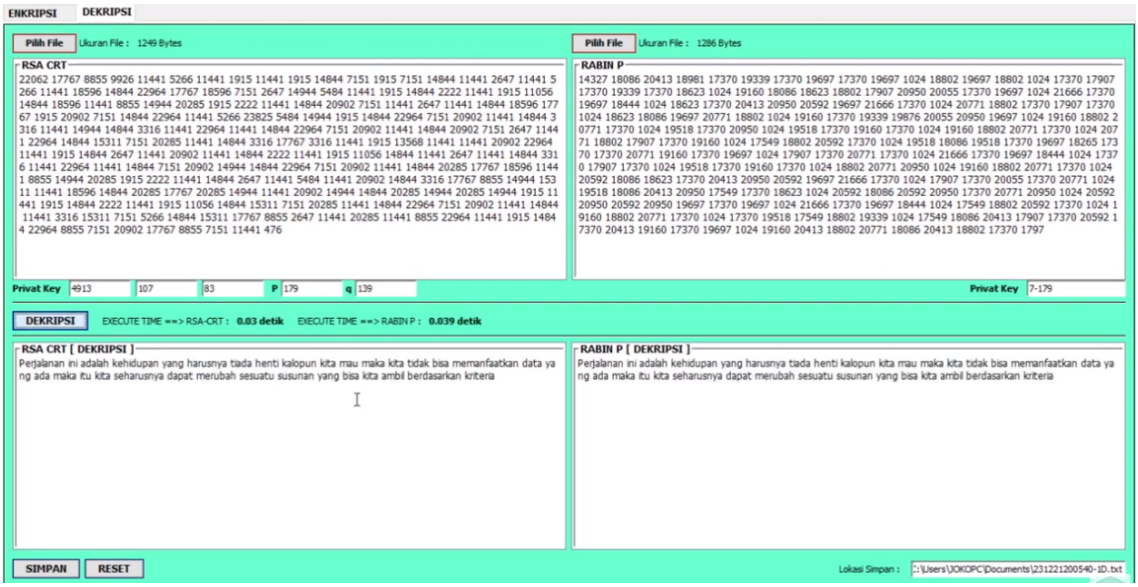
Pada gambar 5 diatas pertama user akan diminta untuk memilih file yang ingin di enkripsi, kemudian setelah file dimasukkan kedalam aplikasi user dapat mengklik tombol enkripsi untuk memulai proses enkripsi.

Hasil Enkripsi



Gambar 6. Hasil Enkripsi

Hasil enkripsi pada gambar 6 di atas menunjukkan bahwa file telah berhasil dienkripsi dengan didapatkannya kunci privat dan publik yang nantinya akan digunakan untuk melakukan proses dekripsi.



Gambar 7. Hasil Dekripsi

Hasil dari dekripsi pada gambar 7 diatas mengharuskan user untuk memasukkan kunci privat dan public yang telah didapatkan dalam proses enkripsi. Setelah user memasukkan kunci privat dan public yang sesuai dengan yang diperoleh dari proses enkripsi user tinggal mengklik tombol dekripsi, setah itu sistem akan secara otomatis melakukan proses dekripsi.

4. KESIMPULAN

Keamanan informasi yang dihasilkan dengan menggunakan aplikasi kriptografi ini membuat file menjadi terenkrpsi. Enkripsi file dengan 2 kuci yaitu privat dan public yang membuat file lebih sulit untuk dimanipulasi oleh pihak yang tidak bertanggung jawab. Enkripsi yang dihasilkan untuk membatasi hak akses dalam menerima suatu infromasi sehingga keamanan informasi didalam file dapat terjaga dengan baik. Pada proses dekripsi dari aplikasi ini membuat pihak yang diijinkan dapat membaca informasi yang ingin disampaikan. Enkripsi dan dekripsi dalam sistem kriptografi ini menggunakan metode RSA, keuntungan dalam metode RSA sendiri terdapat 2kunci yaitu kunci publik dan privat, dan kesulitannya dalam memecahkan pemfaktorannya.

UCAPAN TERIMAKASIH

Ucapan terimakasih penulis berikan kepada semua pihak yang sudah memberikan dukungan selama proses penelitian berlangsung.

DAFTAR PUSTAKA

[1] C. M. Annur, "Indonesia Masuk 3 Besar Negara dengan Kasus Kebocoran Data Terbanyak Dunia," 13 09 2022. [Online]. Available: https://databoks.katadata.co.id.

[2] F. R. I. G. Selli Oktaviani, "Analisis Keamanan Data Dengan Menggunakan Kriptografi Modern Algoritma Advance Encryption Standar (AES)," *Jurnal Media Informatika,* 2023.

[3] F. F. P. F. A. S. S. Agus Setiawan, "SISTEM KEAMANAN PESAN TEKS WEB-BASED MENGGUNAKAN RSA PADA UNIT PELAYANAN PEMUNGUTAN PAJAK TAMBORA," *Prosiding Seminar Nasional Mahasiswa Fakultas Teknologi Informasi (SENAFTI),* 2023.

[4] D. I. M. Fatonah, "Implementasi Metode Rivest Shamir Adleman untuk Enkripsi dan Dekripsi Text," *Jurnal Informatika dan Teknologi Komputer (JICOM),* 2022.

[5] H. B. S. B. T. W. Raina Nabila Nizatsary, "PENERAPAN KEAMANAN DATA SISWA MENGGUNAKAN INTERNATIONAL DATA ENCRYPTION ALGORITHM (IDEA) DAN RIVEST SHAMIR ADLEMAN (RSA)," *Informatik : Jurnal Ilmu Komputer,* 2022.

[6] I. C. E, "KEAMANAN DATA MENGGUNAKAN GABUNGAN KRIPTOGRAFI AES DAN RSA," *SENDIU ,* 2021.

[7] A. Tampubolon, "Implementasi Kombinasi Algoritma RSA dan Algoritma DES Pada Aplikasi Pengaman Pesan Teks," *Jurnal SAINTIKOM,* 2021.

[8] S. W. Reychan Davia Al Huday, "Pengamanan File Rekam Medis Pada Puskesmas Larangan Utara Menggunakan Algoritma Kriptografi RSA Berbasis Web," *Prosiding Seminar Nasional Mahasiswa Fakultas Teknologi Informasi (SENAFTI),* 2022.

[9] M. S. N. W. I. S. A. B. N. Irma Listiani, "PERANCANGAN KEAMANAN DATA PASIEN DI KLINIK KECANTIKAN RATU BEAUTY STUDIO MENGGUNAKAN METODE KRIPTOGRAFI RSA," *JINTEKS,* 2022.

[10] D. I. M. Fatonah, "Implementasi Metode Rivest Shamir Adleman untuk Enkripsi dan Dekripsi Text," *Jurnal Informatika Dan Teknologi Komputer (J-ICOM),* 2022.

[11] T. M. E. A. Yuda Purnama Putra, "IMPLEMENTASI SUPER ENKRIPSI AES DAN RSA PADA PENGAMANAN DATA REKAM MEDIS PASIEN," *JURNAL VOI (VOICE OF INFORMATICS),* 2022.

[12] P. H. U. Ilyas Mahfud, "Implementasi Sistem Kriptografi RSA Signature dengan SHA-256 pada Mekanisme Autentikasi REST API," *Prosiding Seminar Nasional Teknoka,* 2022.