Implementasi Enkripsi RSA untuk Meningkatkan Keamanan Database E-Voting Pemilu

Agnes Tamara Putri 18220010
Program Studi Sistem dan Teknologi Informasi
Sekolah Teknik Elektro dan Informatika
Institut Teknologi Bandung, Jalan Ganesha 10 Bandung
E-mail (gmail): agnestamaraptr@gmail.com

***Abstract*—E-Voting atau pemungutan suara elektronik merupakan salah satu sistem pemungutan suara yang menggunakan teknologi elektronik, seperti komputer dan internet untuk mengumpulkan dan melakukan perhitungan suara dalam proses pemilihan. Jika dibandingkan dengan pemungutan suara secara konvensional, e-voting dinilai lebih mudah dan cepat. Namun, dalam penerapannya, terdapat persoalan lain terkait keamanan informasi, yaitu data yang tidak terjaga kerahasiaannya. Dengan menerapkan kriptografi, yaitu enkripsi RSA pada pemungutan suara elektronik, persoalan ini dapat diatasi.**

Keywords—e-voting; RSA; enkripsi; data; keamanan informasi; kunci publik; kunci privat

I. PENDAHULUAN

Voting atau pemungutan suara adalah salah satu cara pengambilan keputusan atau perumusan masalah dengan cara pemungutan suara terbanyak. Voting berkaitan dengan sebuah pilihan[1].

Indonesia merupakan negara demokrasi, di mana demokrasi adalah pemerintahan yang berasal dari rakyat, oleh rakyat, dan untuk rakyat[2]. Oleh karena itu, Indonesia perlu mengadakan pemilihan umum untuk memilih dan menentukan para pemimpin yang akan menduduki posisi dalam pemerintahan. Proses ini diadakan secara berkala setiap 5 tahun sekali[3]. Dalam prosesnya, rakyat ikut berpartisipasi, salah satunya adalah memberikan suaranya.

Metode pemungutan suara yang diterapkan di Indonesia masih merupakan pemungutan suara konvensional, di mana rakyat datang ke tempat pemungutan suara dan menggunakan hak suaranya di biliki suara dengan mencoblos atau mencontreng surat suara dan memasukkannya ke dalam kotak suara[3]. Setelah itu, suara yang diberikan akan melalui proses penghitungan manual. Namun, ditemukan beberapa kekurangan yang mendorong pertimbangan pergantian metode ini dengan e-voting atau pemungutan suara elektronik yang merupakan metode pemungutan suara dengan memanfaatkan teknologi elektronik seperti komputer dan internet. Beberapa kendala yang sering terjadi, antara lain kesalahan pemilih dalam menandai surat suara, ketentuan keabsahan penandaan yang kurang jelas sehingga banyak kartu suara yang dinyatakan tidak sah, keterlambatan dalam proses pengumpulan kartu suara, proses penghitungan suara yang berlangsung cukup lama[3], kesalahan dalam perhitungan suara, serta biaya proses pemilihan yang tinggi[4].

Dengan penerapan metode e-voting ini, waktu pemrosesan pemilihan dapat dipersingkat dan mengurangi biaya, serta perhitungan suara dan pengumuman hasil dapat dilakukan dengan lebih cepat dan akurat[5].

Dalam proses penyelenggaran pemilihan umum, hal paling krusial yang perlu diperhatikan adalah keamanan dan kepercayaan publik[3]. Namun, di samping keunggulan yang dimiliki, terdapat persoalan lain terkait keamanan informasi, yaitu keutuhan data (integrity) dan kerahasiaan informasi (confidentiality). Penerapan e-voting ini memiliki celah kemungkinan manipulasi data atau hasil suara yang diberikan oleh rakyat. Untuk menghindari hal ini, diperlukannya sebuah sistem untuk melakukan pemungutan suara yang dilengkapi dengan sistem keamanan.

Salah satu langkah untuk mengembangkan sistem pemungutan suara yang terjamin keamanannya (keutuhan data dan kerahasiaan informasi) adalah dengan menggunakan teknik kriptografi, di mana kriptografi berurusan dengan pembangunan dan analisis protokol untuk mengatasi pengaruh pihak ketiga dan memastikan keamanan komunikasi[6]. Salah satu teknik kriptografi yang dapat diterapkan dalam kasus ini adalah kriptografi RSA.

Pada makalah ini, akan dibahas mengenai implementasi kriptografi RSA dalam memastikan keamanan dan integritas dalam sistem e-voting. Keunggulan metode RSA terletak pada kompleksitas dalam memfaktorkan sebuah bilangan menjadi bilangan faktor prima[7]. Dengan begitu, suara yang diberikan oleh rakyat sebagai pemilih terlindungi dan sulit untuk diakses atau dimanipulasi oleh pihak yang tidak berwenang. Hal ini membantu menjaga kerahasiaan suara dan memastikan integritas pemilihan dalam sistem e-voting.

II. METODOLOGI PENELITIAN

A. Metode Penulisan

Makalah ini ditulis metode studi literatur, di mana data yang dibutuhkan menggunakan metode pengumpulan dari berbagai sumber, seperti jurnal, web, buku dokumentasi, dan sumber lainnya yang berasal dari internet.

B. Batasan Penulis

Penelitian yang dilakukan pada makalah ini hanya akan membahas mengenai keamanan proses pemungutan suara dengan menggunakan enkripsi RSA.

C. Eksperimen

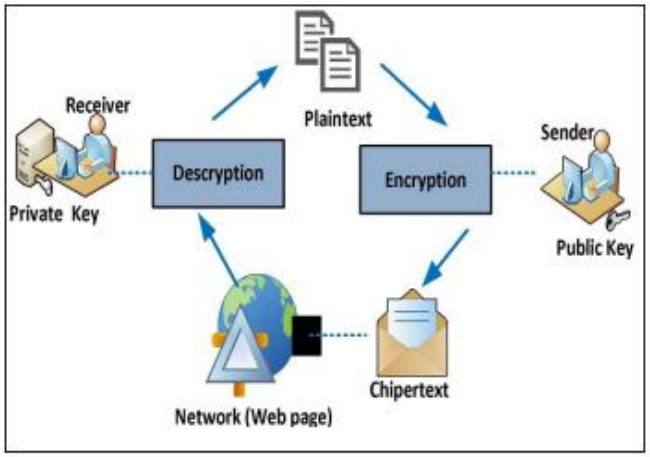
Dalam penyusunan makalah ini, penulis melakukan percobaan pembuatan sistem e-voting dengan menggunakan bahasa pemrograman Python. Program yang dibuat akan mengenkripsi suara pemilih dengan menggunakan kunci publik dan mendekripsinya kembali dengan menggunakan kunci privat.

III. Teori dan Studi Literatur

A. *Kriptografi*

Kriptografi adalah bidang ilmu yang mempelajari metode-metode matematika yang berkaitan dengan keamanan informasi, seperti kerahasiaan, integritas data, serta otentikasi(Menez, 1996). Kata *cryptography* sendiri berasal dari bahasa Yunan yang memiliki arti *"secret writing"* atau *"hidden writing"*[8]. Kriptografi memiliki empat layanan, yaitu *confidentiality* (kerahasiaan pesan), *data integrity* (keaslian pesan), *authentication* (keaslian pengirim dan penerima), dan *non-repudiation* (anti penyangkalan).

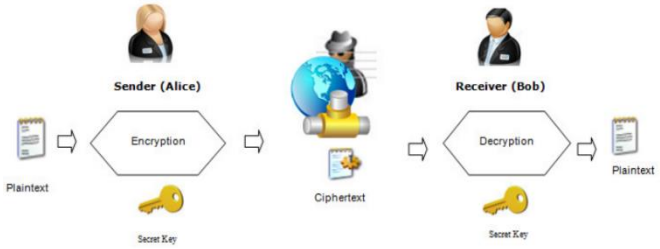
Selama 2 tahun terakhir, di Indonesia, tercatat hampir 287 juta kasud dugaan kebocoran data. Jumlah kasus tersebut di luar kasus pencurian data, pengaksesan data secara ilegal, dan lain sebagainya. Oleh karena itu, pentingnya penggunaan kriptografi menjadi semakin mendesak dalam menjaga keamanan data dan informasi[8]. Kriptografi akan mengubah *plaintext* (teks asli) menjadi *ciphertext*[9] agar pesan tidak dapat dibaca oleh pihak yang tidak berhak[8].



Gambar 1. Diagram Implementasi Kriptografi

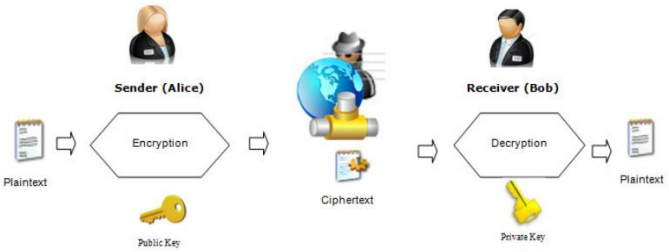
(sumber:https://www.e3s-conferences.org/articles/e3sconf/pdf/2021/104/e3sconf_icstunkhair2021_03005.pdf)

Kriptografi memiliki tiga jenis algoritma, yaitu kriptografi simetris, asimetris, dan hibrida. Perbedaan ketiganya terletak pada kunci yang digunakan dalam proses enkripsi dan dekripsi. Kriptografi simetris hanya menggunakan satu kunci untuk enkripsi dan dekripsinya, kriptografi asimetris menggunakan pasangan kunci publik dan privat di mana kunci publik digunakan untuk mengenkripsi pesan dan kunci privat digunakan untuk mendekripsi pesan, sedangkan kriptografi hibrida memanfaatkan dua tingkatan kunci[10]. Salah satu contoh algoritma yang menggunakan kriptografi asimetris adalah RSA (Rivest, Shamir dan Adleman)[14].



Gambar 2. Skema Kriptografi Kunci Privat

(sumber: https://www.zuj.edu.jo/wp-content/uploads/2014/05/PA_05.pdf)



Gambar 3. Skema Kriptografi Kunci Publik

(sumber: https://www.zuj.edu.jo/wp-content/uploads/2014/05/PA_05.pdf)

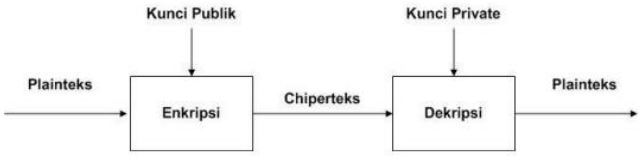
B. *E-Voting*

E-Voting merupakan sebuah sistem pemungutan suara yang berbasis teknologi[12]. Sistem ini mencatat, menyimpan, dan memproses data dalam bentuk informasi digital. [11]. Metode ini dinilai dapat menggantikan metode konvensional jika dilihat dari aspek efisiensi dan efektivitas. Dengan menggunakan metode ini, proses pemungutan dan penghitungan suara dapat berlangsung lebih cepat dan risiko kesalahan dapat dikurangi, serta biaya yang dikeluarkan akan lebih sedikit[13].

C. *Algoritma RSA*

RSA adalah sebuah algoritma yang dibuat oleh tiga peneliti dari MIT, yaitu Ronald Rivest, Adi Shamir, dan Leonard Adleman pada tahun 1976. Algoritma ini sering digunakan untuk membangun sebuah sistem keamanan karena sulitnya memfaktorkan bilangan bulat yang besar manjadi faktor-faktor prima sehingga semakin besar bilangan prima, maka tingkat keamanannya akan semakin tinggi dan kualitas keamanannya akan semakin baik[15]. Seperti yang telah disebutkan sebelumnya, algoritma ini termasuk dalam kriptografi simetri, yang berarti terdapat pasangan kunci, yaitu kunci publik dan kunci privat. Kunci publik yang didapatkan akan digunakan untuk melakukan enkripsi terhadap suatu pesan, sedangkan

kunci privat akan digunakan untuk melakukan dekripsi terhadap suatu pesan.



Gambar 3. Skema Enkripsi dan Dekripsi RSA

(sumber: https://nero.trunojoyo.ac.id/index.php/nero/article/view/113/114)

Berikut merupakan beberapa properti dari algoritma RSA.

1. p dan q bilangan prima (rahasia)
2. n = p*q (tidak rahasia)
3. Φ(n) = (p-1)*(q-1) (rahasia)
4. e (kunci enkripsi) (tidak rahasia)

   Syarat: PBB(e, ϕ(n)) = 1 atau gcd(e, ϕ(n)) = 1
5. d (kunci dekripsi) (rahasia)
6. m (plaintext) (rahasia)
7. c (ciphertext) (tidak rahasia)

Dalam implementasinya, RSA menggunakan 3 tahapan: pembangkitan kunci, enkripsi, dan dekripsi[6]. Dari komponen-komponen di atas dapat dilakukan prosedur pembangkitan sepasang kunci dan akan didapatkan pasangan kunci publik dan privat sebagai berikut.

- Kunci publik: (e, n)
- Kunci privat: (d, n)

Untuk melakukan enkripsi, apabila terdapat pesan dengan ukuran yang besar, pesan tersebut dapat dipecah menjadi blok-blok plainteks yang lebih kecil $(m_1, m_2, m_3, \ldots)$ dengan syarat (syarat: $0 \leq m_i < n - 1$), lalu lakukan perhitungan cipherteks c_i untuk plainteks m_i menggunakan kunci publik e dengan persamaan $c_i = m_i^e \ mod \ n$.

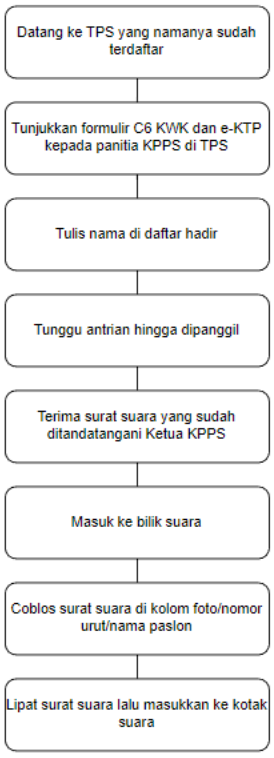
Untuk melakukan dekripsi, apabila terdapat cipherteks $(c_1, c_2, c_3, \ldots)$, lakukan perhitungan kembali blok plainteks mi dari blok cipherteks c_i menggunakan kunci privat d dengan persamaan $m_i = c_i^d \ mod \ n$.

D. *Kelebihan dan Kekurangan Kriptografi RSA*

1. Kelebihan RSA
   - Semakin tingginya tingkat keamanan karena menggunakan dua kunci yang berbeda dalam proses enkripsi dan dekripsinya
   - Dapat berfungsi sebagai tanda tangan digital sehingga dapat mencegah penyangkalan terhadap suatu tindakan atau aksi
   - Pembangkitan kunci menjadi lebih mudah karena tidak lagi diperlukan jalur aman untuk mendistribusikan kunci
   - Manajemen kunci menjadi lebih sederhana karena setiap entitas dalam sistem informasi memiliki sepasang kunci sehingga untuk n entitas hanya diperlukan total 2n kunci
   - Sulit dalam memfaktorkan bilangan non prima menjadi faktor-faktor primanya
2. Kekurangan
   - Kecepetan operasi yang dimiliki oleh RSA lebih lambat dibandingkan dengan kriptografi simetrik
   - Ukuran cipher yang meningkat sekitar dua kali lipat dari ukuran awalnya

IV. Implementasi

Alur proses pemungutan suara konvensional dapat dilihat pada gambar berikut.



Gambar 4. Alur Proses Pemungutan Suara[16]

Jika masih tetap mempertahankan metode pemungutan suara konvensional, maka akan memakan waktu yang cukup lama melihat banyaknya tahapan yang harus dilakukan saat pemilih akan memberikan suaranya, serta metode ini juga tidak dapat menjamin kerahasiaan dan keutuhan data suara pemilih. Namun, dengan menggunakan metode e-voting yang dilengkapi dengan algoritma RSA untuk sistem keamanannya, proses akan menjadi lebih singkat dan lebih aman.

Untuk menjawab permasalahan dan untuk menanggapi gagasan baru mengenai pergantian metode konvensional dengan elektronik, penulis merancang sebuah sistem yang dapat mengenkripsi pesan berupa suara yang diberikan oleh pemilih sehingga terjaga kerahasiannya serta tidak dapat diketahui atau dimanipulasi oleh pihak yang tidak memiliki kewenangan. Pesan yang berupa suara pemilih yang telah dienkripsi hanya dapat didekripsi oleh panitia yang memiliki kunci privatnya.

Dalam implementasinya, terdapat beberapa fungsi utama yang digunakan, yaitu fungsi untuk membangkitkan kunci sehingga akan dihasilkan pasangan kunci publik dan privat, enkripsi (dengan menggunakan kunci publik), dan juga dekripsi (dengan menggunakan kunci privat).

A. *Fungsi Pembangkitan Kunci*

Prosedur pembangkitan kunci membutuhkan dua bilangan prima, p dan q, serta sebuah bilangan bulat e sebagai kunci publik. Oleh karena itu, program ini akan menggunakan modul random dengan cara *import random* untuk mendapatkan bilangan prima p dan q, serta bilangan bulat e. Setelah ketiga bilangan tersebut didapatkan, maka pasangan kunci dapat di-*generate* dan akan menghasilkan pasangan kunci publik dan privat yang nantinya akan digunakan untuk mengenkripsi dan mendekripsi pesan suara pemilih.

```
# Generate key
def GenerateKey(self):
    key = self.genPubPrivKey()
    priv = key[0]
    pub = key[1]
    namafile = self.name.get()
    if namafile == '':
        messagebox.showerror("Error",f"Masukkan nama pemilih")
    else:
        try:
            with open(f"key/{namafile}.pri", "w") as myfile:
                myfile.write(f"{priv}")
            with open(f"key/{namafile}.pub", "w") as myfile:
                myfile.write(f"{pub}")
            messagebox.showinfo("info", f"Kunci berhasil disimpan di key/{namafile}.pri dan key/{namafile}.pub")
            self.button_2.config(state="normal")
        except Exception as E:
            messagebox.showerror("Error",f"Kunci tidak dapat disimpan, {E}")
```

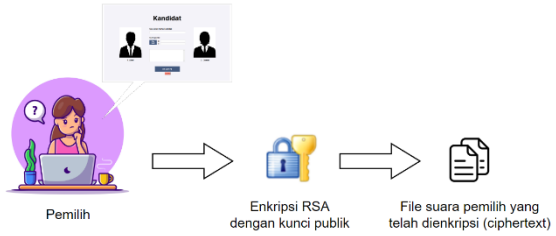
Gambar 5. Kode Program Fungsi GenerateKey

(sumber: dokumentasi pribadi)

B. *Fungsi Enkripsi*

Setelah didapatkan pasangan kunci yang dibutuhkan, pemilih akan masuk ke halaman pemilihan kandidat untuk memilih kandidat yang diinginkan. Setelah pemilih masuk ke halaman pemilihan kandidat, pemilih tidak dapat kembali ke halaman utama karena kunci yang di-*generate* menandakan bahwa pemilih sudah melakukan "*login*" ke *web* pemilihan umum.

Pada halaman pemilihan kandidat, pemilih dapat langsung memilih satu di antara beberapa kandidat yang ada dan meng-*upload file* kunci publik yang telah didapatkan saat pemilih memasukkan nama pada halaman utama pemilih sehingga data pemilih dapat terenkripsi.



Gambar 6. Proses Pemilihan Kandidat

(sumber: dokumen pribadi)

Proses enkripsi yang dilakukan pada implementasi oleh makalah ini akan menggunakan algoritma asimetris, yaitu algoritma RSA.

```
# Enkripsi
def enkrip(self, message, e, n):
    cipher = [(ord(char) ** e) % n for char in message]
    self.input.insert(Tk.END, cipher)
    messagebox.showinfo("Encryption Successful",f"Message encrypted successfully.")
```

Gambar 7. Kode Program Fungsi Enkripsi

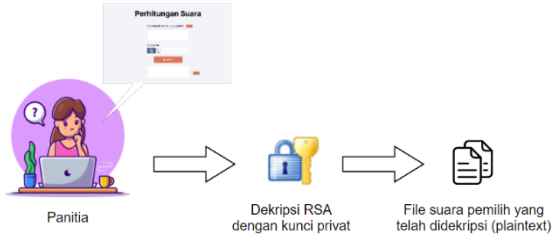
(sumber: dokumentasi pribadi)

Setelah data dienkripsi, pemilih harus menekan tombol "Save File" agar *ciphertext* (pesan yang telah terenskripsi) tersimpan.

C. *Fungsi Dekripsi*

Langkah terakhir dalam proses pemungutan suara adalah penghitungan suara pemilih oleh panitia. Untuk melakukan perhitungan suara, panitia harus terlebih dahulu mendekripsi *file* suara pemilih yang telah dienkripsi sebelumnya.

Pada halaman perhitungan suara, panitia dapat langsung memasukkan *file* suara pemilih beserta kunci privatnya.



Gambar 8. Kode Program Fungsi Enkripsi

(sumber: dokumentasi pribadi)

```
# Dekripsi
def dekrip(self):
    encrypted_message = self.masukan_file.get()
    d = int(self.d.get("1.0",'end-1c'))
    n2 = int(self.n2.get("1.0",'end-1c'))
    encrypted_list = [int(char) for char in encrypted_message.split()]
    # plain = [chr((char ** d) % n2) for char in encrypted_message]
    plain = [chr(pow(char, d, n2)) for char in encrypted_list]
    decrypted_message = ''.join(plain)
    self.output.insert(Tk.END, decrypted_message)
    messagebox.showinfo("Decryption Successful", "Message decrypted successfully.")
```

Gambar 9. Kode Program Fungsi Dekripsi

(sumber: dokumentasi pribadi)

Setelah data didekripsi, panitia harus menekan tombol “Save File” agar *plaintext* (pesan yang telah terdekripsi) tersimpan dan dapat digunakan untuk perhitungan suara.

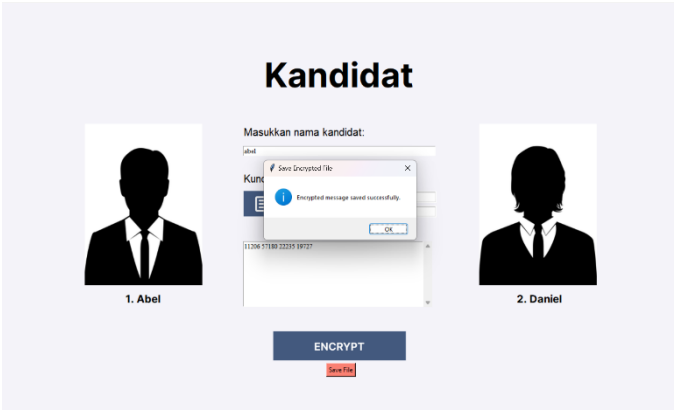
V. Testing

Untuk mempermudah dilakukannya pengujian sistem pemungutan suara yang telah dirancang, penulis telah membuat tampilan *web* pemungutan suara.

Pada halaman utama, jika pengguna merupakan pemilih dapat menekan tombol “PEMILIH”, tetapi jika pengguna merupakan panitia, dapat menekan tombol “PANITIA”.

Jika menekan tombol sebagai pemilih, maka akan sampai ke halaman utama pemilih, di mana pada halaman ini pemilih harus memasukkan nama dan menekan tombol “Generate Key” sehingga pasangan kunci dapat ter-*generate*.

Setelah itu, pemilih akan menemui halaman pemilihan kandidat, di mana pemilih dapat menentukan kandidat yang diinginkan dan memasukkan kunci publik yang telah didapatkan sehingga suara pemilih dapat terenkripsi dan tersimpan.



Jika menekan tombol sebagai panitia, maka akan sampai ke halaman utama panitia, di mana pada halaman ini panitia harus memasukkan *file encrypted text* beserta kunci privatnya sehingga *encrypted text* dapat terdekripsi dan tersimpan.

VI. Kesimpulan

Berdasarkan percobaan dan analisis penulis, dapat disimpulkan bahwa metode e-voting yang disertai dengan sistem keamanan oleh algoritma RSA dapat dijadikan alternatif untuk menggantikan metode pemungutan suara konvensional yang masih digunakan sampai saat ini. Penggunaan metode ini sangat efektif dan efisien, serta terjaga keamanan dan keutuhan data/informasinya.

Video Link at Youtube

https://bit.ly/TugasAkhirKriptoAgnes

Github

https://github.com/agnestamaraa/Tugas-Akhir-Kriptografi.git

Referensi

[1] Ikhsan Darmawan, Nurul Nurhandjati, and Evida Kartini. (2014). *Memahami E-Voting: Berkata dari Pengalaman Negara-Negara Lain dan Jembrana (Bali)*. Jakarta: Fakultas Ilmu Sosial dan Ilmu Politik UI.

[2] Fornieri, Joseph R. (2014). *The Gettysburg Address: A Commentary*. Rowman & Littlefield.

[3] Sulistyo, Andri. (2016). *Model Sistem Electronic Voting (E-Voting) Berbasis Web dengan Menerapkan Quick Response Code (QR-Code) sebagai Sistem Keamanan dalam Pemilihan Legislatif*. Universitas Negeri Semarang, Semarang. Accessed from http://lib.unnes.ac.id/28056/1/5302411195.pdf

[4] AmboSamra, et al. (2017). *A Practical, Secure, and Auditable E-Voting System*. *Journal of Information Security and Applications, 36*. 69-89. Retrieved May 20, 2023, from https://daneshyari.com/article/preview/4955738.pdf

[5] Kersting, Norbert, & Baldersheim, Harald. (2004). *Electronic Voting and Democracy*. New York: Palgrave Macmillan.

[6] Fashoto, et al. (2016). *Securing a Scalable E-Voting System Using the RSA Algorithm: The Case of a Group Voting Process in a Tertiary School*. *Computer Technology and Application, 7*. 11-27. Retrieved May 21, 2023, from http://www.davidpublisher.com/Public/uploads/Contribute/568f286b72291.pdf

[7] Indrawanti, et al. (2018). *Secure E-Voting Menggunakan Metode RSA dan Autentikasi RFID*. *Jurnal Ilmiah NERO, 4(1)*. 67-75. Retrieved May 21,

2023, from https://nero.trunojoyo.ac.id/index.php/nero/article/view/113/114

[8] Munir, Rinaldi. (2023). *01-Pengantar Kriptografi*[Presentation slides]. Accessed from https://informatika.stei.itb.ac.id/~rinaldi.munir/Kriptografi-dan-Koding/2022-2023/01-Pengantar-Kriptografi-(2023).pdf

[9] Putra, et al. (2021). *Implementasi Kriptografi dalam Pengamanan Database E-Voting Menggunakan RSA dan Base64 Berbasis Progresive Web Apps*. *Jurnal Sistem Informasi dan Teknologi Informasi, 10(1)*. 30-40. Retrieved May 21, 2023, from https://media.neliti.com/media/publications/496210-none-acdce8aa.pdf

[10] Ariyus, Dony. (2008). *Pengantar Ilmu Kriptografi: Teori, Analisis, dan Implementasi*. Yogyakarta: ANDI OFFSET.

[11] Rumaf, Edy Waly. (2019). *Implementasi Algoritma Blowfish untuk Privacy Data E-Voting*. *Jurnal Sistem Informasi & Komputer, 1(1)*. 1-7. Retrieved May 21, 2023, from http://ejournal.stmik-tm.ac.id/index.php/jurasik/article/view/2

[12] Suwarjono, et al. (2021). *Cryptography Implementation for Electronic Votivng Security*. *E3S Web of Conferences, 328*. Retrieved May 21, 2023, from https://www.e3s-conferences.org/articles/e3sconf/pdf/2021/104/e3sconf_icstunkhair2021_03005.pdf

[13] Ridwan, et al. (2016). *Rancang Bangun E-Voting dengan Menggunakan Keamanan Algoritma Rivest Shamir Adleman Berbasis Web*. *Jurnal Informatika Mulawarman, 11(2)*. 22-28. Retrieved May 21, 2023, from https://e-journals.unmul.ac.id/index.php/JIM/article/view/210/pdf

[14] Basri. (2016). *Kriptografi Simetris dan Asimetris dalam Perspektif Keamanan Data dan Kompleksitas Komputasi*. *Jurnal Ilmiah Komputer, 2(2)*. 16-23. Retrieved May 21, 2023, from https://media.neliti.com/media/publications/458062-none-8d4775d7.pdf

[15] Munir, Rinaldi. (2023). *10-Algoritma RSA*[Presentation slides]. Accessed from https://informatika.stei.itb.ac.id/~rinaldi.munir/Kriptografi-dan-Koding/2022-2023/10-Algoritma-RSA-2023.pdf

[16] Nurhanisah, Yuli. (2020). *Kenali Lebih Dekat Tata Cara Mencoblos di TPS*. Retrieved May 21, 2023, from https://indonesiabaik.id/infografis/kenali-lebih-dekat-tata-cara-mencoblos-di-tps

PERNYATAAN

Dengan ini saya menyatakan bahwa makalah yang saya tulis ini adalah tulisan saya sendiri, bukan saduran, atau terjemahan dari makalah orang lain, dan bukan plagiasi.

Bandung, 21 Mei 2023

Agnes Tamara
18220010