SISTEM PENGAMANAN PENGIRIMAN DATA MONITORING KUALITAS UDARA DI KOTA MEDAN MENGGUNAKAN ALGORITMA KRIPTOGRAFI RSA

SKRIPSI

Oleh:

SAPRI TUA HALOMOAN SIAGIAN

178160044

PROGRAM STUDI TEKNIK INFORMATIKA

FAKULTAS TEKNIK

UNIVERSITAS MEDAN AREA

2023

SISTEM PENGAMANAN PENGIRIMAN DATA MONITORING KUALITAS UDARA DI KOTA MEDAN MENGGUNAKAN ALGORITMA KRIPTOGRAFI RSA

SKRIPSI

Diajukan sebagai Salah Satu Syarat untuk Memperoleh
Gelar Sarjana di Fakultas Teknik
Universitas Medan Area

Oleh:

SAPRI TUA HALOMOAN SIAGIAN
178160044

PROGRAM STUDI INFORMATIKA
FAKULTAS TEKNIK
UNIVERSITAS MEDAN AREA
MEDAN
2023

LEMBAR PENGESAHAN

Judul Skripsi : Sistem Pengamanan Pengiriman Data Monitoring Kualitas Udara Di Kota Medan Menggunakan Algoritma Krptografi RSA

Nama : Sapri Tua Halomoan Siagian

NPM : 178160044

Fakultas : Teknik

Disetujui Oleh
Komisi Pembimbing

Susilawati, S.Kom, M.Kom
Pembimbing I

Nurul Khairina, S.Kom, M.Kom
Pembimbing II

Dr. Rahmad Syah, S.Kom, M.Kom
Dekan Fakultas Teknik

Raski Multiono, S.Kom, M.Kom
Ka. Prodi

Tanggal lulus : 11 April 2023

HALAMAN PERNYATAAN

Saya menyatakan bahwa skripsi yang saya susun, sebagai syarat memperoleh gelar sarjana merupakan hasil karya tulissaya sendiri. Adapun bagian-bagian tertentu dalam penulisan skripsi ini yang saya kutip dari hasil karya orang lain telah dituliskan sumbernya secara jelas sesuai dengan norma, kaidah, dan etika penulis ilmiah.

Saya bersedia menerima sanksi pencabutan gelar akademnik yang saya peroleh dan sanksi-sanksi lainnya dengan peraturan yang berlaku, apabila di kemudia hari detemukan adanya plagiat dalam skripsi ini.

Medan,

Sapri Tua halomoan Siagian

178160044

HALAMAN PERNYATAAN PERSETUJUAN PUBLIKASI TUGAS AKHIR/SKRIPSI/TESIS UNTUK KEPENTINGAN AKADEMIS

Sebagai sivitas akademik Universitas Medan Area, saya yang bertanda tangan di bawah ini:

Nama	: Sapri Tua Halomoan Siagian
NPM	: 178160044
Program Studi	: Informatika
Fakultas	: Teknik
Jenis karya	: Tugas Akhir/Skripsi/Tesis

Demi pengembangan ilmu pengetahuan, menyetujui untuk memberikan kepada Universitas Medan Area **Hak Bebas Royalti Noneksklusif (*Non-exclusive Royalty-Free Right*)** atas karya ilmiah saya yang berjudul :

Sistem Pengamanan Pengiriman Data Monitoring Kualitas Udara Di Kota Medan Menggunakan Algoritma Kriptografi RSA.

Beserta perangkat yang ada (jika diperlukan). Dengan Hak Bebas Royalti Noneksklusif ini Universitas Medan Area berhak menyimpan, mengalihmedia/format-kan, mengelola dalam bentuk pangkalan data (*database*), merawat, dan memublikasikan tugas akhir/skripsi/tesis saya selama tetap mencantumkan nama saya sebagai penulis/pencipta dan sebagai pemilik Hak Cipta. Demikian pernyataan ini saya buat dengan sebenarnya.

Dibuat di : Medan
Pada tanggal : 25 Juli 2023
Yang menyatakan

(Sapri Tua Halomoan Siagian)

ABSTRAK

Kota Medan merupakan daerah di Indonesia yang memiliki kualitas udara yang buruk. Menurut indeks kualitas udara (AQI), tingkat polusi udara di Kota Medan berada dalam kategori tidak sehat sehingga diperlukannya perangkat monitoring kualitas udara yang merupakan salah satu perangkat yang bertujuan memantau tingkat polusi udara di Kota Medan. Perangkat secara berkala mengunggah dan mengirim data ke *database* pada *server* IoT dan akan dianalisa lebih lanjut untuk mendapatkan informasi yang bermanfaat mengenai kualitas udara. Untuk mengamankan data polusi udara dari tindak kejahatan melalui jaringan internet, maka penelitian ini memiliki tujuan yaitu merancang sistem pengamanan data *monitoring* kualitas udara di kota Medan dengan menerapkan algoritma kriptografi RSA agar dapat menghidari terjadinya pencurian data atau peretasan sistem dari pihak yang tidak bertanggung jawab. Penelitian ini menggunakan data primer yang diperoleh dari perangkat IoT yang berupa *dataset* polusi. Perangkat IoT diletakkan di 3 lokasi yaitu di jalan Sei Deli, Tembung, dan KIM. Analisis yang digunakan yaitu dengan menerapkan algoritma RSA, tahapan algoritma RSA yaitu proses pembentukan kunci, enkripsi dan dekripsi. Hasil penelitian menunjukkan bahwa algoritma RSA dapat diterapkan untuk pengamanan data *monitoring* kualitas udara di kota Medan pada perangkat IoT dengan jumlah *dataset* polusi udara yang diperoleh sebanyak 249.364 data. Penerapan algoritma RSA untuk proses enkripsi dan dekripsi berhasil dilakukan pada semua dataset yang tersimpan pada *database* di *server*.

Kata kunci : Kualitas udara, Kota Medan, Sistem pengamanan, Kriptografi RSA.

ABSTRACT

Medan City is an area in Indonesia that has poor air quality. According to the air quality index (AQI), the level of air pollution in the city of Medan is in the unhealthy category, so an air quality monitoring device is needed, which is one of the devices that aims to monitor the level of air pollution in the city of Medan. The device periodically uploads and sends data to a database on the IoT server which will be further analyzed to obtain useful information about air quality. To secure air pollution data from crime via the internet network, this research has the goal of designing an air quality monitoring data security system in Medan City by implementing the RSA cryptographic algorithm to avoid data theft or system hacking from irresponsible parties. This study uses primary data obtained from IoT devices in the form of pollution datasets. IoT devices are placed in 3 locations, namely at Jalan Sei Deli, Tembung, and KIM. The analysis used is by applying the RSA algorithm, the stages of the RSA algorithm are the process of forming keys, encryption, and decryption. The results showed that the RSA algorithm can be applied to secure air quality monitoring data in the city of Medan on IoT devices with a total of 249,364 air pollution datasets obtained. The application of the RSA algorithm for the encryption and decryption process was successfully carried out on all datasets stored in the database on the server.

Keywords: Air quality, Medan City, Security system, RSA Cryptography.

RIWAYAT HIDUP

Sapri Tua Halomoan Siagian lahir di Kota Batam pada tanggal 31 Mei 1999. Anak pertama (1) dari lima (5) bersaudara. Penulis merupakan putra dari bapak Parluhutan Siagian dan Ibu Lisbeth Situmeang.

Penulis menyelesaikan pendidikan Sekolah Dasar (SD) di SDK Santo Fransiskus Assisi, Kecamatan Sangatta Utara, Kabupaten Kutai Timur, pada tahun 2011. Pada tahun 2011 penulis melanjutkan pendidikan Sekolah Menengah Pertama (SMP) di SMPK Santo Fransiskus Assisi, Kecamatan Sangatta Utara, Kabupaten Kutai Timur, dan lulus pada tahun 2014. Pada tahun 2014 penulis melanjutkan pendidikan pendidikan Sekolah Menengah Kejuruan (SMK) di SMK Negeri 1 Sangatta Utara, Kecamatan Sangatta Utara, Kabupaten Kutai Timur, dengan mengambil jurusan Multimedia dan lulus pada tahun 2017.

Pada tahun 2017 penulis melanjutkan pendidikan perguruan tinggi, tepatnya pada Universitas Medan Area (UMA) dan terdaftar sebagai mahasiswa Fakultas Teknik pada Program Studi Informatika. Pada tahun 2020 penulis mengikuti kegiatan Program kreativitas Mahasiswa (PKM) dan pada tahun yang sama penulis melaksanankan Kerja Lapangan (KP) di PT. Karya Murni Perkasa dengan mengangkat judul penelitian, yaitu Sistem Informasi Penyewaan Alat-Alat Berat Pada PT. Karya Murni Perkasa.

KATA PENGANTAR

Puji dan syukur penulis panjatkan kepata Tuhan Yesus Kristus, atas berkat dan karunia-Nya. Penulis dapat menyelesaikan skripsi dengan judul sistem pengamanan pengiriman data monitoring kualitas udara di kota medan menggunakan algoritma krptografi rsa. Sebagai salah satu syarat dalam menyelesaikan program studi sarjana (S1) pada Fakultas Teknik Informatika Universitas Medan Area.

Tak lupa penulis mengucapkan banyak terima kasih kepada pihak-pihak yang telah memberikan banyak antuan dan bimbingan dalam menyelesaikan penelitian ini dengan baik, pada kesempatan yang diberikan penulis mengucapkan banyak terima kasih kepada :

1. Kedua orang tua dan adik, serta keluarga yang telah memberi saya banyak dukungan dan doa dalam menyusun skripsi ini.
2. Yayasan Pendidikan Haji Agus Salim selaku pelaksana Uniersitas Medan Area.
3. Bapak Prof. Dr. Dadan Ramdan, M.Eng, M.Sc selaku rektor Universitas Medan Area.
4. Bapak Dr. Rahmad Syah, S.kom, M.Kom selaku Dekan Fakultas Universitas Medan Area.
5. Bapak Rizki Muliono, S.Kom, M.Kom selaku Kepala Program Studi Teknik Informatika Universitas Medan Area.
6. Ibu Susilawati, S.Kom, M.Kom selaku pembimbing yang telah bersedia meluangkan waktu dan memberikan arahan selama penyusunan skripsi ini.
7. Ibu Nurul Khairina, S.Kom, M.Kom selaku pembimbing yang telah bersedia meluangkan waktu dan memberikan arahan selama penyusunan skripsi ini.
8. Seluruh Dosen serta seluruh Staff Program Studi Teknik Informatika Universitas Medan Area.
9. Sahabat yang telah membantu serta memberikan banyak motivasi sehingga penulis dapat menyelesaikan skripsi ini dengan baik.
10. Semua teman yang telah membantu serta memberikan masukkan dan motivasi sehingga penulis dapat menyelesaikan skripsi ini dengan baik.
11. Serta semua pihak yang tidak dapat disebutkan satu persatu yang telah memberi dukungan, bantuan, dan doa.

Penulis juga menyadari masih terdapat kekurangan dalam penelitian skripsi ini. Oleh karena itu, penulis menerima kritik maupun saran yang membangun, yang kiranya dapat menciptakan penelitian yang lebih baik lagi kedepannya. Penulis juga berharap semoga skripsi ini dapat bermanfaat pada penelitian lainnya.

Medan,

Penulis,

Sapri Tua Halomoan Siagian

DAFTAR ISI

DAFTAR TABEL

Halaman

DAFTAR GAMBAR

Halaman

BAB I
PENDAHULUAN

1.1 Latar Belakang

Kota Medan merupakan salah satu daerah di Indonesia yang memiliki kualitas udara yang buruk. Indeks kualitas udara (AQI) menjelaskan, tingkat polusi udara di Kota Medan berada dalam kategori tidak sehat. Penyebab pencemaran udaranya berasal dari kendaraan bermotor, gas dari asap industri, gas dari asap rumah tangga, kebakaran hutan dan lain-lain. Kurangnnya ruang terbuka hijau juga dapat mempengaruhi tingkat polusi udara di Kota Medan dalam memenuhi kebutuhan udara. (Abri Montgomery Blackstone, 2022)

Seiring dengan meningkatnya aktivitas manusia yang dapat memicu pencemaran udara, sehingga diperlukannya solusi untuk meminimalisir efek yang dapat mengganggu kesehatan. Untuk memperkirakan jika udara dilingkungan sekitar tercemar atau tidak manusia dapat menggunakan inderanya, tetapi tidak dapat dilakukan pemantauan kualiatas udara secara terus menerus. Untuk melakukan pemantauan secara *realtime* dan mendapatkan data mengenai kualitas udara dapat dilakukan dengan membangun suatu perangkat keras yang dapat terhubung dengan sistem *monitoring* kualitas udara. (Novelan, 2020)

Perangkat *monitoring* kualitas udara adalah salah satu perangkat yang bertujuan memantau tingkat polusi udara di Kota Medan. Perangkat tersebut dipasang dibeberapa titik Kota Medan. Perangkat secara berkala mengunggah dan mengirim data ke *database* pada *server* IoT dan akan dianalisa lebih lanjut untuk mendapatkan informasi yang bermanfaat mengenai kualitas udara di Kota Medan. Namun pada proses mengirim data yang dilakukan dalam sehari terdapat 1.440 data yang dikirimkan dalam tiap satu menit secara *realtime* ke *database* pada *server* IoT. Hal ini memungkinkan dapat terjadinya pencurian data atau peretasan sistem dari pihak yang tidak bertanggung jawab. Untuk mengamankan data yang dikirim ke *database* pada *server* IoT diperlukannya suatu sistem keamanan untuk menghindarkan kemungkinan terjadinya hal-hal tidak diinginkan.

Dalam perkembangan teknologi dan informasi terutama pada bidang internet yang mengakibatkan munculnya kejahatan baru melalui jaringan internet. Di

Indonesia terjadinya beberapa kasus *cyber crime*, seperti tindak manipulasi data milik orang lain, penipuan, penyadapan data pribadi, *hacking*, dan *spaming email.* Pada tahun 2003 tindak kejahatan meningkat dengan menggunakan teknologi informasi. Sebagai contoh tindak kejahatan *hacking, cracking, phising (internet banking fraud), carding (credit card fraud), ATM/EDC skimming,* dan *malware*. Selain itu terdapat juga pada bagian pengelolaan informasi dan data tepatnya pada pengelolaan data pribadi yang sangat membutuhkan keamanan. Kemajuan perkembangan teknologi dan informasi juga membuat privasi sangat lemah tepatnya berbagai data-data pribadi menjadi sangat mudah tersebar (Ririn Aswandi, 2020). Dalam menjaga keamanan data dapat menerapkan algoritma kriptografi RSA.

Kriptografi merupakan ilmu mengamankan data yang bertujuan sebagai pembingungan, dengan cara mengubah *plaintext* (teks polos) menjadi *ciphertext* (teks rahasia) dengan menggunakan algoritma tertentu. Kriptografi memiliki proses enkripsi dan dekripsi, dimana proses enkripsi dapat mengubah *plaintext* menjadi *ciphertext,* sedangkan proses dekripsi dapat mengembalikan *ciphertext* menjadi *plaintext*. Dalam proses tersebut menggunakan sebuah kunci rahasia, semakin banyak kunci rahasia yang digunakan maka akan semakin kuat tingkat keamanannya. Kriptografi dapat dibagi menjadi 2 (dua) yaitu algoritma simetris dan algoritma asimetris. Salah satu contoh dari algoritma asimetris yaitu algoritma RSA (Rivest, Shamir, Adleman) (Susanto, 2018). Algoritma RSA disebut algoritma asimetris karena pada proses enkripsi dan dekripsinya berbeda serta disebut juga dengan algoritma kunci publik karena pada proses enkripsi kunci yang digunakan dapat diketahui oleh publik.

Algoritma RSA merupakan algoritma yang paling umum digunakan sampai saat ini. Dengan mengalikan 2 (dua) bilangan prima besar, lalu kunci telah dibuat, bilangan prima asli dapat dibuang atau tidak digunakan lagi. Kunci publik dan kunci privat sangat dibutuhkan dalam proses enkripsi dan dekripsi. Kunci publik digunakan untuk mengenkripsi teks dan dapat diketahui oleh publik, sedangkan kunci privat tidak dikirim karena digunakan untuk mendekripsi teks yang telah dienkripsi. (Muhammad Ridwan Rambe, 2019)

Terdapat beberapa penelitian yang pernah dilakukan oleh peneliti terdahulu

dalam menggunakan algoritma RSA yaitu penelitian yang dilakukan oleh (Rahmat Sulaiman, 2018) peneliti menyimpulkan dengan menerapkan algoritma RSA dalam proses enkripsi untuk meningkatkan keamanan pesan berbasis *Android*. Pengirim dapat menentukan kunci yang akan digunakan dan pesan yang dikirim di dekripsi menjadi pesan asli, sehingga pesan menjadi cukup aman dan pihak yang tidak memiliki hak tidak dapat membaca pesan tersebut.

Penelitian yang dilakukan oleh (Badrul Anwar, 2019) penelitian bertujuan untuk menerapkan algoritma RSA untuk menyelesaikan permasalahan pada pengamanan data Simpan Pinjam. Menggunakan 2 (dua) kunci untuk sistem keamanan data agar tidak mudah dipecahkan pihak yang tidak memiliki kepentingan, serta prosesnya akan memakan waktu sedikit lama. Untuk mendapatkan 2 (dua) kunci, terlebih dahulu harus memfaktorkan bilangan prima.

Berdasarkan penelitian yang telah dilakukan peneliti sebelumnya maka penulis bermaksud untuk membagun sebuah sistem pengamanan pengiriman data *monitoring* kualitas udara di Kota Medan menggunakan algoritman kriptografi RSA yang bertujuan untuk mengamankan data kualitas udara pada proses pengiriman data ke *database* pada *server* IoT.

1.2 Rumusan Masalah

Adapun rumusan yang jadi masalah dalam penelitian ini adalah bagaimana menerapkan algoritma kriptografi RSA untuk pengamanan data *monitoring* kualitas udara.

1.3 Batasan Masalah

Adapun batasan masalah dalam penelitian ini adalah

1. Pengambilan data polusi dilakukan melalui perangkat IoT yang diletakkan di 3 titik di Kota Medan yaitu, Sei Deli, Tembung, dan KIM.
2. Menerapkan algoritma RSA sebagai sistem pengamanan data.
3. Pembangkitan kunci menggunakan bilangan prima acak.
4. Menggunakan panjang *n* hanya 64 bit.

1.4 Tujuan

Adapun tujuan dalam penelitian ini adalah untuk menerapkan algoritma kriptografi RSA untuk pengamanan data *monitoring* kualitas udara di kota Medan.

1.5 Manfaat

Adapun manfaat dalam penelitian ini adalah

1. Merupakan salah satu syarat untuk memperoleh gelar sarjana di Fakultas Teknik Universitas Medan Area.
2. Menambah pemahaman dan pengetahuan dalam menggunakan algoritma kriptografi RSA.
3. Membangun sistem pengamanan data *monitoring* kualitas udara di kota Medan menggunakan algoritman RSA.

BAB II
TINJAUAN PUSTAKA

2.1 Penelitian Terdahulu

Terdapat beberapa penelitian yang pernah dilakukan oleh peneliti terdahulu yang menjadi referensi dalam penelitian ini yang dapat dilihat pada tabel 2.1 berikut ini.

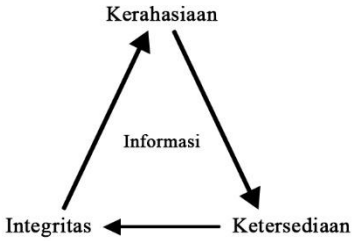
Tabel 2.1 Penelitian Terdahulu.

No	Peneliti	Judul Penelitian	Kesimpulan
1	Rahmat sulaiman, Marina Vebu, 2019.	Peningkatan Keamanan Pesan Berbasis *Android* Menggunakan Algoritma Kriptografi RSA.	Dengan menerapkan algoritma RSA dalam proses enkripsi untuk meningkatkan keamanan pesan berbasis *Android*. Pengirim dapat menentukan kunci yang akan digunakan dan pesan yang dikirim di dekripsi menjadi pesan asli, sehingga pesan menjadi cukup aman dan pihak yang tidak memiliki hak tidak dapat membaca pesan tersebut.
2	Yusuf Anshori, A. Y. Erwin Dodu, Dewa Made P. Wedananta, 2019.	Implementasi Algoritma Kriptografi Rivest Shamir Adleman (RSA) pada Tanda Tangan Digital.	Penelitian mendapatkan hasil bahwa dengan menggunakan algoritma RSA dapat menjamin keamanan dokumen dari aplikasi tanda tangan digital yang telah ditandatangani dalam 3 (tiga) aspek yaitu: *authentication*, *non-repudiation* dan *integrity*.
3	Badrul Anwar, Nurcahyo Budi	Implementasi Algoritma RSA Terhadap Keamanan Data.	Penelitian bertujuan untuk menerapkan algoritma RSA untuk menyelesaikan permasalahan pada pengamanan data Simpan Pinjam.

	Nugroho, Jaka Prayudha, Azanuddin, 2019.	Simpan Pinjam.	Menggunakan 2 (dua) kunci untuk sistem keamanan data agar tidak mudah dipecahkan pihak yang tidak memiliki kepentingan, serta prosesnya akan memakan waktu sedikit lama. Untuk mendapatkan 2 (dua) kunci, terlebih dahulu harus memfaktorkan bilangan prima.
4	Muhammad Syahputa Novelan, 2020.	Sistem *Monitoring* Kualitas Udara Dalam Ruangan Menggunakan Mikrokontroler dan Aplikasi Android.	Sistem *monitoring* kualitas udara dapat mengidentifikasikan kadar udara berbahaya (CO) dan suhu di dalam ruangan yang kemudian dapat memberikan indikasi dan informasi kepada pengguna.
5	Toni Nur Hakim, Moh. Farid Susanto, 2020.	Sistem *Monitoring* Kualitas Udara Berbasis *Internet of Things*.	Sistem monitoring kualitas udara yang dibangun terealisasikan 100% sesuai dengan trancangan yang di buat. Sensor-sensor yang dipasang yaitu MQ135, DHT22, dan MQ131 dapat mengukur parameter udara yang telah ditentukan, yaitu O3, NO, CO, kelembapan dan suhu.

2.2 Sistem Keamanan Data Informasi

Keamanan informasi merupakan suatu tindakan untuk mendeteksi atau mencegah adanya suatu tindakan penipuan pada sistem yang berbasis infromasi. Secara tidak langsung keamanan informasi tidak menjamin keberlangsungan usaha, pengembalian modal, dan mencegah risiko-risiko yang dapat terjadi. Banyaknya data infromasi perusahaan yang dikelola dan disimpan maka semakin besar juga risiko yang dapat terjadi seperti kehilangan, kerusakan atau diketahui oleh pihak lain. Keamanan informasi terbagi dari tiga aspek yaitu kerahasiaan, integritas, dan ketersediaan yang disebut CIA. (Ramadhani, 2018)



Gambar 2.1 Keamanan Informasi.

Kerahasiaan *(Confidentiality)* ialah memastikan hanya yg memiliki hak yang dapat mengakses informasi, menjaga kerahasiaan atas informasi data, dan menjaga kerahasiaan data informasi yang dikirim, diterima, dan disimpan. Integritas (*Integrity)* ialah menjamin bahwa yang tidak memiliki hak tidak dapat mengubah data, serta tetap menjaga keutuhan data dan keakuratan inforasi. Serta ketersediaan (*Availability)* ialah memastikan hanya pengguna yang meiliki hak yang dapat menggunakan perangkat atau informasi terkait, serta menjamin data akan tetap tersedia ketika dibutuhkan. (Ramadhani, 2018)

2.3 Udara

Udara merupakan sebuah lapisan gas yang mengelilingi bumi yang berfungsi melindungi bumi dari gangguan. Pada lingkungan kota udara tidak seutuhnya bersih di karenakan polutan yang diakibatkan oleh aktivitas manuasia. Untuk mengetahui parameter keadaan kualitas udara, udara di ukur untuk mengetahui keadaaan udara pada suatu wilayah. Polutan seperti limbah gas rumah tangga, asap industri, beberapa jenis gas, dan asapa kendaraan mengakibatkan penurunan kualitas udara. (Jaka Prayudha, 2018)

Menurut (Indrayani, 2018) terdapat beberapa parameter pencemaran udara yang berdampak terhadap kesehatan manusia, sebagai berikut:

1. Parameter Karbon Monoksida (CO), menyebabkan keracunan CO, mengganggu fungsi kerja otot pada orang yang memiliki penyakit jantung dan perubahan tekanan darah.
2. Paramteer Nitrogen Dioksida (NO_2), mnagkibatkan kelumpuhan pada sistem syaraf, keracunan, dan kematian.
3. Paramter Hidrokarbon (HC), apabila *Plycyclic Aromatic Hidrocarbon* terhirup ke dalam paru-paru dapat merangsang terbentuknya sel-sel kanker dan

menimbulkan luka.

4. Parameter Slufur Dioksida (SO_2), mengakibatkan iritasi pada pernapasan.
5. Prameter Partikel Debu (PM_{10} dan TSP), partikel debu yang bertebangan dapat menghalangi daya pandangan mata dan menyebabkan iritasi pada mata.
6. Parameter Timah Hitan (Pb), apabila tertelan dalam jumlah yang banyak dapat mengakibatkan muntah, diare akut atau sakit perut, bahkan dapat mengakibatkan gejala kronis yang menyebabkan kelelah berlebihan, anemia atau sakit kepala, gangguan pengelihatan, gangguan pencernaan, kelumpuhan pada anggota badan, kejang-kejang.
7. Parameter Oksidan (O_3), apabila terhirup ke dalam tubuh dapat mengakibatkan gangguan pernapasan normal dan oksidan fotokimia yang mengakibatkan iritasi pada mata.

2.4 Internet of Things

IoT (*Internet of Things*) merupakan sebuah perkembangan teknologi yang sangat memudahkan penggunanya. IoT dapat menguntungkan kehidupan penggunanya dengan menggunakan sebuah sensor pintar serta benda yang terkoneksi jaringan internet. Bermacam-macam peralatan dapat dikendalikan melalui internet dengan menggunakan sensor-sensor pintar. Melalui sensor pintar, data tangkap kemudia dirubah menjadi data digital yang kemudian data dikirim dan diproses secara *realtime*. Dengan begitu peralatan dapat dikendalikan atau dikontrol dari jarak jauh dalam arsitektur IoT.

IoT berkerja denga benda yang memiliki alamat IP (*Internet Protocol*). Alamat IP merupakan identitas sebuah benda yang membuat benda tersebut dapat diperintahkan melalui jaringan yang sama oleh benda lain. Benda tersebut akan dikoneksikan ke internet dengan menggunakan alamat IP.

Pengguna dapat memberi perintah atau memantau benda dengan menggunakan internet. Setelah telah memiliki alamat IP dan terhubung dengan internet selanjutnya benda akan dipasangkan sensor. Sensor akan mengumpulkan informasi, setelah informasi telah dikumpulkan, benda dapat mengelolah informasi dengan sendirinya, benda dapat saling komunikasi dengan benda lain yang terhubung koneksi internet dan memiliki alamat IP. Benda-benda tersebut akan melakukan

proses pertukaran informasi. Benda tersebut dapat menyuruh benda lain untuk ikut bekerja. (Wilianto, 2018).

2.5 Kriptografi

Kriptografi menurut (Sebastian Suhandinata, 2019) berasal dari kata *crypto* yaitu rahasia dan *graphia* yaitu tulisan, kedua kata bersebut berasal dari bahasa Yunani. Kriptografi merupakan seni atau ilmu dalam menjaga kerahasiaan pengamanan pesan yang akan dikirim ke suatu tempat.

Kriptografi merupakan langkah atau urutan dalam menjaga kerahasiaan informasi. Menurut Amita Pandey, dasar-dasar dalam konsep kriptografi terdiri dari:

1. *Plaintext*, merupakan pesan murni.
2. *Ciphertext*, merupakan pesan acak yang tidak dapat dimengerti oleh siapapun yang awalnya merupakan pesan asli (*plaintext)*.
3. *Encryption*, mengubah *plaintext* menjadi *ciphertext*, dan memerlukan kunci proses enkripsi.
4. *Decryption*, mengubah *ciphertext* menjadi *plaintext*, dan memerlukan kunci dan proses dekripsi.
5. *Key*, gabungan dari simbol spesial, huruf, atau angka yang digunakan pada proses enkripsi dan dekripsi. Kriptografi sangat bergantung terhdapat kunci sehingga *Key* memiliki peran yang sangat penting.

Kriptografi dibagi 3 berdasarkan kunci yang digunakan, yaitu simetris, asimetris dan *hybrid*.

2.5.1 Kriptografi Simetris

Kriptografi simetris menggunakan kunci yang sama pada proses enkripsi dan dekripsi, sehingga kerahasiaan kunci dapat terjamin dan tersembunyi. Kelebihan algortma ini yaitu bekerja secara cepat dalam mengenkripsi dan sumber daya komputer yang sangat kecil. Dalam kalgoritma simetris terdapat 2 yaitu sebagai *stream cipher* dan *block cipher*. Mode *stream cipher* data dipotong menjadi bits-bits kecil yang diacak lalu dilakukan proses enkripsi, sedangkan mode *block cipher* kunci tergantung dari panjang block yang sebelumnya data dipotong menjadi

beberapa blok. Contoh kriptografi simetris yaitu, algoritma RC4, algoritma *Blowfish*, algoritma AES, DES, dan *Triple* DES. (Sebastian Suhandinata, 2019)

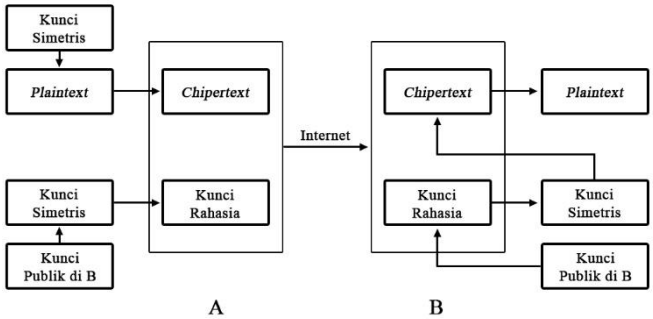
2.5.2 Kriptografi Asimetris

Kriptografi asimetris pada proses emkripsi dan dekirpsi memiliki kunci yang berbeda atau disebut dengan enkripsi kumci publick. Kunci disebarkan merupakan kunci publik dan kunci yang dirahasiakan merupakan kunci privat.

Kriptografi asimetris digunakan untuk memberikan kunci emkripsi secara aman meski kedua pihak tidak mempunyai kesempatan untuk menyetujui kunci privat. Umumnya kumci kriptografi asimetris memiliki kunci yang panjang untuk meningkatkan keamanan data, panjang kunci kurang lebih berukuran 3000bit agar mendapat keamanana yang kuat. Contoh dari algoritma asimetris adalah algoritma *Diffie-Hellman* dan RSA. (Sebastian Suhandinata, 2019)

2.5.3 Kriptografi *Hybrid*

Kriptografi *hybrid* menggunakan keunggulan dari tiap algoritma dengan memanfaatkan beberapa sandi dari algoritma yang berbeda secara bersamaan. Kriptografi *hybrid* digunakan dalam membangkitkan kunnci simetris dan enkripsi kunci menggunakan kunci asimetris dari kunci publik si penerima. Data dienkripsi menggunakan kunci simetris dikirim kepada penerima berserta kunci rahasia. Penerima menggunakan kunci privat miliknya akan mendekripsi kuncii rahasia terlebih dahulu, lalu nendekripsi menggunakan kuncii yang telah didekripsi tersebut.



Gabmar 2.2 Kriptografi *Hybrid*.

Pada gambra 2.2, menjelaskan skema sistem kriptografi *hybrid* dengan menggunakan keuntungan algoritma kriptografi simetris dalam kecepatan enkripsi

dan mengamankan proses pertukaran kunci dengan kemampuan algoritma kriptografi asimetris. (Sebastian Suhandinata, 2019)

2.6 Algoritma RSA

Algoritma RSA pada proses enkripsi dan dekripsi menggunakan kunci yang berbeda. Proses enkripsi kunci yang digunakan disebut kunci publik, untuk proses dekripsi kunci yang digunakan disebut kunci privat. Algoritma RSA disebut juga sebagai algoritma asimetris (Lutfi Pratama, 2018). Pada tahun 1978 algoritma RSA diperkenalkan oleh 3 profesor yang bernama Ron Rivest, Adi Shamir, dan Leonard Adleman yang berasal dari MIT (*Massachussets Institute of Technology*). (Jonson Manurung, 2018)

Algorima RSA memiliki 3 (tiga) langkah, yaitu proses pembangkitan kunci, enkripsi, dan dekripsi. Bilangan prima acak yang digunakan menentukan parameter kuat tidaknya suatu kunci. Pesan akan sulit untuk di *cracking* jika bilangan prima yang dibangkitkan kuat. Proses enkripsi dan dekripsi merupakan proses yang hampir sama. (Lutfi Pratama, 2018)

Menurut (Susilawati, 2018) apabila kunci yang digunakan sangat panjang pada algoritma RSA dapat dikatakan aman (dikatakan tidak aman jika hanya 512 bit, dikatakan cukup aman jika hanya 768 bit, dan 1024-2048 bit atau lebih dapat dikatakan aman). Semakin panjang kunci publik yang digunakana maka tingkat keamanannya semakin tinggi. Algoritma RSA dapat dijelaskan sebagia berikut :

1. $\phi(n) = (p - 1)(q - 1)$ merupakan rahasia.
2. Kunci publik (*e*) merupakan tidak rahasia.
3. Kunci privat (*d*) merupakan rahasia.
4. *Plainteks (m)* merupakan rahasia.
5. *Cipherteks* (*c*) merupakan tidak rahasia.

2.6.1 Pembangkit Kunci

1. Memiliki 2 bilangan prima *p* dan *q* dengan nilai yang berbeda.
2. Hitung nilai $n = p \times q$ ..... (2.1)
3. Hitung nilai $\phi(n) = (p - 1) * (q - 1)$ ..... (2.2)
4. Kunci publik, ***e*** yang relatif prima terhadap $\phi(n)$. Relatif prima terhadap $\phi(n)$

dapat di artikan faktor pembagi terbesar keduanya = 1, dapat dirumuskan sebagai $gcd(e, \phi(n)) = 1$ ..... (2.3)

5. Membangkitkan kunci privat (d) dengan menggunakan persamaan $e * d = 1$ mod n atau $(1 + m . n)/e$, sehingga secara sederhana d dapat dihitung dengan $d = \frac{1+k\phi(n)}{e}$ ..... (2.4)

2.6.2 Enkripsi Dan Dekripsi

Enkripsi :

1. Mengambil kunci publik penerima e dan modulus n
2. Menjelaskan plainteks m dibagi menjadi bebrapa blok $m_1, m_2, ...,$ sehingga setiap blok mendekripsikan nilai [0, n -1].
3. Setiap blok-blok M_i di enkripsi menjadi blok C_i :

   $C_i = m_i^e \bmod n$ ..... (2.5)

   Dekripsi :

   pada blok *cipherteks* C_i di dekripsi menjadi blok M_i :

   $M_i = C_i^d \bmod n$ ..... (2.6)

2.7 PHP

PHP (*Hypertext Preprocessor*) merupakan bahasa program digunakan untuk menjalankan baris program yang hanya dimngerti oleh komputer ke dalam HTML (*HyperText Markup Language*) berbasisi *server-side*. PHP digunakan oleh pengembang *web* yang merupakan salah satu bahasa pemrograman. (Sudaria, 2021)

PHP adalah bahasa program dalam bentuk skrpi yang ditaruh ke dalam *web server*. PHP dirancang untuk membangun sebuah *web* yang dinamis maksudnya, dapat membangun tampilan berdasarkan suatu permintaan. Misalnya halaman *web* dapat menampilkan *database.*

2.8 *Website*

Website merupakan kumpulan halaman *web* yang memiliki URL (*Uniform Resource Locator*) atau domain serta dapat diakses oleh pengguna internet. *Website* biasanya ditulis dalam format HTML (*HyperText Markup Language*) atau berupa dokumen yang dapat diakses melalui protokol HTTP (*HyperText Transfer*

Protocol). Dalam menyampaikan berbagai informasi dari *website* kepada pengguna menggunakan *web browser* merupakan tugas dari suatu protokol HTTP. (Yudin Wahyudin, 2020).

Web server adalah perangkat lunak yang memliki fungsi dalam menerima *request* melalui protokol HTTP atau HTTPS (*HyperText Transfer Protocol Secure*) dari pelanggan kemudian mengirim kembali dalam halaman *web*. Contoh PHP dan MySQL (Sudaria, 2021).

Web Service merupakan logika aplikasi yang diakses dan dipublikasi melaluii standar Internet (*web*, HTTP, IP/TCp). *Web serivce* dapat diimplementasikan pada dau lingkungan internal dan eksternal. Lingkungan internal sebagai kebutuhan integritas antar sistem aplikasi EAI (*Enterprise Application Integration*) dan pada lingkungan eksternal sebagai mendukung aplikasi *business-to-business (e-business).* (Rachamat Adi Purnama, 2018)

Web Hosting merupakan tempat yang dapat menyimpan *file*, data dan lainya yang dibutuhkan oleh suatu *website* dan dapat diakses melalui jaringan internet. Tiap paket pada *hosting* memiliki layanan *hosting* yang berbeda. Paket-paket ini dapat dibedakan berdasarkan *Bandwith*, ukuran kapasitas penyimpanan, harga, jumlah *domain* yang dimiliki, dan jenis *hosting*. (Febyana Nur Yahya, 2020)

2.9 MySQL

MySQL menggunakan bahasa SQL (*Structured Query Language*) dan sistem dalam memanajemen *database* yang paling populer serta bersifat *open source*. MySQL menmiliki fitur seperti DBMS (*Database Manajemen Sistem*), *multi-user,* dan *multithreaded*. MySQL dibuat berdasarkan keperluaan sistem *database* yang mudah digunakan, cepat, dan handal (Sudaria, 2021). Terdapat beberapa instruksi dasar dalam menggunakan MySQL, yaitu:

1. Untuk menampilkan data menggunakan *Select.*
2. Untuk menambahkan atau mengimput data menggunakan *Insert.*
3. Untuk mengubah data menggunakan *Update*.
4. Untuk menghapus data pada *database* menggunakan *Delete.*

MySQL dapat menyimpan data dalam bentuk tabel yang sangat membantu pengguna. Pada tabel untuk mengelompokkan data berdasarkan kategori tertentu

disebut kolom (*field*) dan untuk yang mengimputkan data adalah baris (*record)*. (Haslinda, 2019)

2.10 ASCII

ASCII (*American Standart Code for Infromation Interchange*) adalah simbol, dan huruf yang hanya berjumlah 255 kode. Kode untuk manipulasi teks menggunakan ANSI-ASCII 0-127. Kode untuk manipulasi grafik atau gambar menggunakan ANSI-ASCII ASCII 128-225. ANSI kepanjangan dari *American National Standards Institute*. Dalam meningkatkan keamanan informasi banyak menggunakan kode ASCII. Contohnya seperti kemanan informasi pada *e-voting*, yang tidak mudah untuk ditebak dalam menghasilkan suatu baris karakter dan kemungkinan luas dapat memberikan lebih banyak karakter yang tidak hanya pada alfabet tetapi juga dapat mencakup simbol seperti ‘, @, =, *, # dan lainnya. (Deni Hamdani, 2020)

Tabel 2.2 Karakter ASCII (Desimal).

Desimal	Karakter	ASCII (desimal)	Keterangan
0.	!	33	Simbol tanda seru
1.	"	34	Simbol kutip dua
2.	#	35	Simbol pagar
3.	$	36	Simbol mata uang dolar
4.	%	37	Simbol persen
5.	&	38	Simbol ampersand
6.	‘	39	Simbol *Apostrof*
7..	(	40	Tanda buka kurung
8.	)	41	Tanda tutup kurung
9.	*	42	Simbol bintang
10.	+	43	Simbol tanda tambah
11.	’	44	Simbol tanda koma
12.	-	45	Simbol strip

13.	.	46	Simbol tanda titik
14.	/	47	Simbol garis miring
15.	0	48	Simbol angka nol
16.	1	49	Simbol angka satu
17.	2	50	Simbol angka dua
18.	3	51	Simbol angka tiga
19.	4	52	Simbol angka empat
20.	5	53	Simbol angka lima
21.	6	54	Simbol angka enam
22.	7	55	Simbol angka tujuh
23.	8	56	Simbol angka delapan
24.	9	57	Simbol angka sembilan
25.	:	58	Simbol titik dua
26.	;	59	Simbol titik koma
27.	<	60	Simbol lebih kecil
28.	=	61	Simbol sama dengan
29.	>	62	Simbol lebih besar
30.	?	63	Simbol Tanda tanya
31.	@	64	Simbol a keong (@)
32.	A	65	Alfabet huruf A
33.	B	66	Alfabet huruf B
34..	C	67	Alfabet huruf C
35	D	68	Alfabet huruf D
36.	E	69	Alfabet huruf E
37.	F	70	Alfabet huruf F
38.	G	71	Alfabet huruf G
39.	H	72	Alfabet huruf H
40.	I	73	Alfabet huruf I
41.	J	74	Alfabet huruf J
42.	K	75	Alfabet huruf K
43.	L	76	Alfabet huruf L

44.	M	77	Alfabet huruf M
45.	N	78	Alfabet huruf N
46.	O	79	Alfabet huruf O
47.	P	80	Alfabet huruf P
48.	Q	81	Alfabet huruf Q
49.	R	82	Alfabet huruf R
50.	S	83	Alfabet huruf S
51.	T	84	Alfabet huruf T
52.	U	85	Alfabet huruf U
53.	V	86	Alfabet huruf V
54.	W	87	Alfabet huruf W
55.	X	88	Alfabet huruf X
56.	Y	89	Alfabet huruf Y
57.	Z	90	Alfabet huruf Z
58.	[	91	Buka kurung siku
59.	\	92	Simbol Garis miring terbalik
60.	]	93	Tutup kurung siku
61.	^	94	Simbol pangkat
62.	_	95	Simbol garis bawah
63.	`	96	Tanda petik satu
64.	a	97	Alfabet huruf a
65.	b	98	Alfabet huruf b
66.	c	99	Alfabet huruf c
67.	d	100	Alfabet huruf d
68.	e	101	Alfabet huruf e
69.	f	102	Alfabet huruf f
70.	g	103	Alfabet huruf g
71.	h	104	Alfabet huruf h
72.	i	105	Alfabet huruf i
73.	j	106	Alfabet huruf j
74.	k	107	Alfabet huruf k

75.	l	108	Alfabet huruf l
76.	m	109	Alfabet huruf m
77.	n	110	Alfabet huruf n
78.	o	111	Alfabet huruf o
79.	p	112	Alfabet huruf p
80.	q	113	Alfabet huruf q
81.	r	114	Alfabet huruf r
82.	s	115	Alfabet huruf s
83.	t	116	Alfabet huruf t
84.	u	117	Alfabet huruf u
85.	v	118	Alfabet huruf v
86.	w	119	Alfabet huruf w
87.	x	120	Alfabet huruf x
88.	y	121	Alfabet huruf y
89.	z	122	Alfabet huruf z
90.	{	123	Buka kurung kurawal
91.	¦	124	Dua garis vertikal
92.	}	125	Tutup kurung kurawal
93.	~	126	Simbol gelombang

2.11 *Unifield Modeling Language*

Unifield Modeling Language (UML) merupakan suatu metode yang digunakan untuk merancang sebuah sistem yang diorientasikan dalam bentuk pemodelan visual pada sebuah objek. UML adalah standar dalam penulisan dimana termasuk menjelaskan sebuah proses dan penulisan kelas-kelas menggunakan bahasa yang spesifik (Prihandoyo, 2018). UML dibagi dalam berbeberapa pemodelan yaitu *sequence diagram, class diagram, activity diagram,* dan *use case diagram*.

2.12 *Use Case Diagram*

Use case diagram merupakan suatu fungsionalitas dalam merepresentasikan suatu gambaran interkasi antar sistem dan aktor atau menjelaskan gambaran yang diharapkan dari sebuah sistem. Aktor merupakan entitas manusia atau yang

melakukan pekerjaan dia sistem. (Prihandoyo, 2018)

Use case diagram mendeskripsikan suatu fungsi dari sistem melalui sudut pandang pengguna. *Use case diagram* menjelaskan apa yang akan diproses oleh sistem serta komponen–komponen yang ada di dalam sistem. *Use case* diagram dapat menjelaskan skenario atau urutan-urutan dari langkah-langkah yang akan dilakukan oleh pengguna terhdapat sistem maupun sebaknya. (Setiyani, 2021)

2.13 *Flowchart*

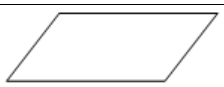
Flowchart menurut (Khesya, 2021) dapat diartikan sebagai langkah-langkah yang dituliskan atau gambarakan dalam simbol-simbol tertendu dalam penyelesaian masalah. *Flowchart* akan menjelaskan alur-alur yang berjalan pada sistem secara jelas.

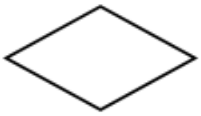
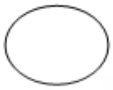
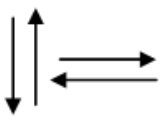
Flowchart digunakana sebagai pedoman tidak hanya digunakan sebagai alat komunikasi pada sistem. Sebelum menggunakan simbol-simbol pada *flowchart* terlebih dahulu dapat memahami aturan dalam menggunakan *flowchart*, berikut merupakan aturan dalam menggunakan *flowchart*, yaitu :

1. *Flowchat* digambarkan sebagai awal dari atas ke bawah atau dari kiri ke kanan.
2. Setiap proses atau aktivitas harus dinyatakan dengan jelas.
3. Diagram alur dimulai dari posisi awal dan diakhiri dengan satu atau lebih.
4. Untuk menunjukkan koneksi antar algoritma terputus, perpindahan atau perubahan halaman dapat menggunakan konektor halaman atau keluar halaman dengan menggunakan tanda yang sama.

Berikut ini simbol dan kegunaan dari *flowchart* yang sering digunakan untuk menggambarkan suatu algoritma, yaitu:

Tabel 2.3 Simbol Pada *Flowchart*.

No	Simbol	Nama	Fungsi simbol
1		*Terminal*	Merupakan awal/akhir suatu program (prosedur).
2		*Output/Input*	Input/output terlepas dari jenis perangkat.

3		*Process*	Untuk menunjukkan proses operasional.
4		*Decision*	Untuk menunjukkan bahwa suatu kondisi tertentu mengarah pada 2 kemungkinan, yaitu iya dan tidak.
5		*Connector*	Koneksi penghubung proses ke proses lain di halaman yang sama.
6		*Offline Connector*	Koneksi penghubung dari satu proses ke proses lain di halaman lain.
7		*Predifined Process*	Mewakili ketentuan penyimpan untuk diproses untuk memberikan awal harga.
8		*Punched Card*	Output ditulis ke dalam kartu atau input yang berasal dari kartu.
9		*Punch Tape*	-
10		*Document*	Mencetak output ke format dokumen.
11		*Flow*	Menunjukkan arah suatu alur arus atau proses.

BAB III
METODOLOGI PENELITIAN

3.1 Data Yang Digunakan

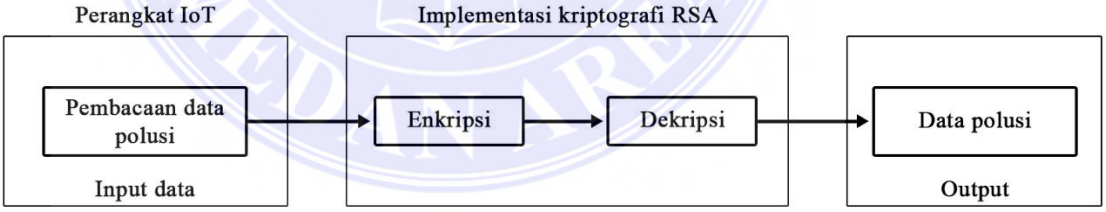
Dalam penelitian data yang digunakan dapat dijelaskan pada tahapan yang membahas mengenai jenis dan sumber data serta metode pengumpulan data sebagai berikut.

3.2 Jenis Dan Sumber Data

Dalam penelitian ini jenis dan sumber data diperoleh dari perangkat IoT, pada perangkat IoT terdapat sensor MQ-7 sebagai alat sensor pendeteksi gas karbon monoksida (CO) denagn menggunakan mikrokontroler arduino nano yang kemudian data polusi akan melakukan proses pengiriman data menggunakan modul *wifi* wemos ISP 6288 secara *realtime* setiap satu menit ke *database* pada *server*. Data polusi akan disimpan pada *database* menggunakan MySQL.

3.2.1 Metode Pengumpulan Data

Adapun metode pengumpulan data pada penelitian ini dapat dijelaskan pada gambar 3.1 berikut.



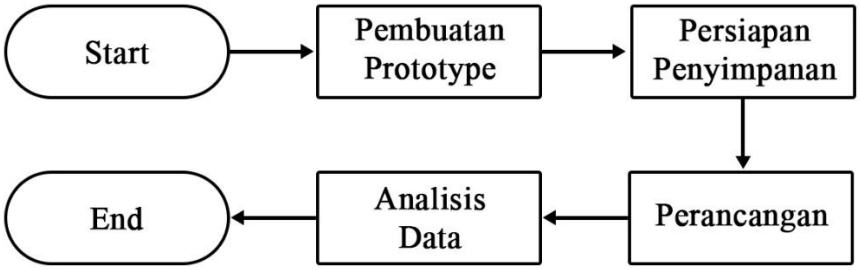
Gambar 3.1 Pengumpulan Data.

Pada gmbar 3.1, data polusi dari perangkat IoT akan dikirim ke *database* pada *server* dan data polusi akan dienkripsi dengan menerapkan algoritma RSA. Data yang telah dienkripsi akan didekripsi untuk mengembalikan nilai pesan asli dari data polusi.

3.3 Kerangka Kerja Penelitian

Dalam kerangka kerja penelitian merupakan kerangka kerja yang berupa

tahapan-tahapan pada sistem yang dirancang yang dapat dijelaskan pada gambar berikut.

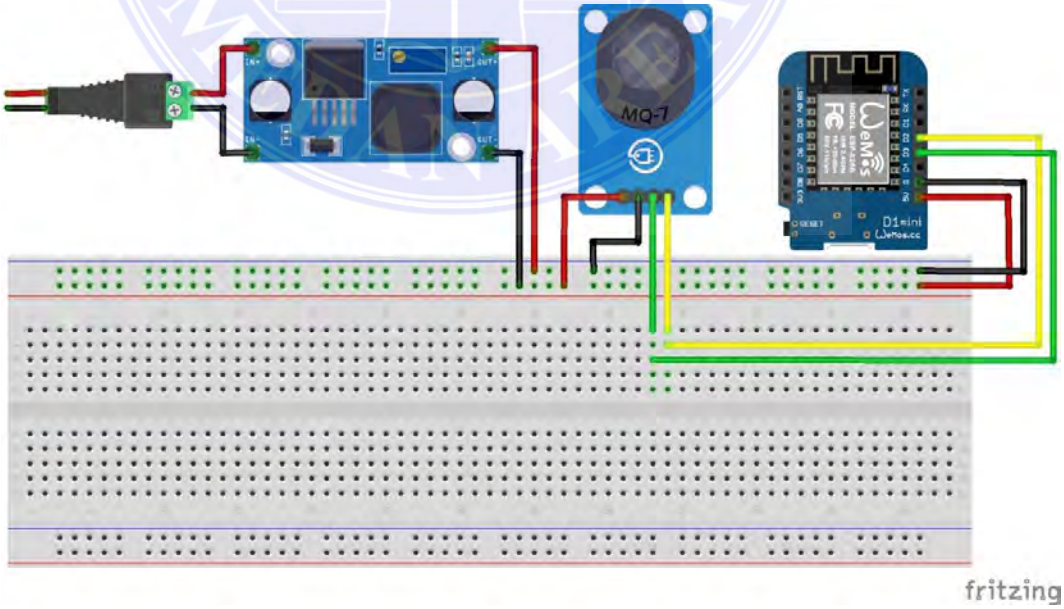


Gambar 3.2 Kerangka Kerja Penelitian.

Gambar 3.2, berikut proses kerangka kerja penelitian akan dimulai dari pembuatan *prototype*, melakukan persiapan penyimpanan, perancangan, dan analisis data. Tahapan-tahapan tersebut akan dijelaskan sebagai berikut.

3.3.1 Pembuatan *Prototype*

Perangkat dibuat menggunakan mikrokontroler arduino nano sebagai alat pengendali, sensor MQ-7 sebagai detektor gas karbon monoksida (CO) dan modul *Wifi* wemos ISP 6288 yang berfungsi untuk sebagai pengirim data gas CO ke *server*. Sumber daya utama pada perangkat IoT ini berasal adaptop yang disambungkan ke listrik.



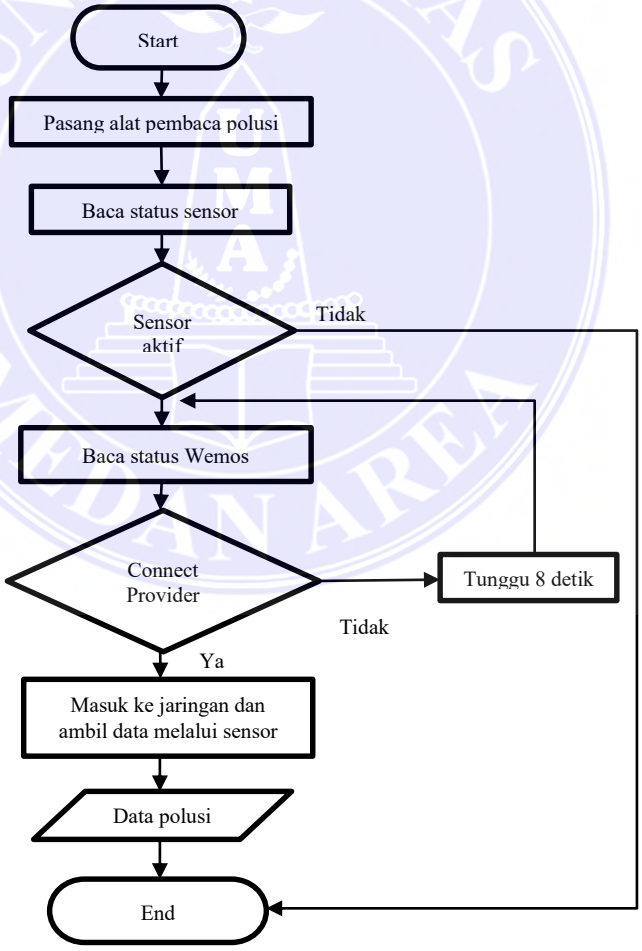
Gambar 3.3 *Prototype* Perangkat IoT.

Gambar 3.3, perangkat IoT dirancang dengan menggunakan beberapa

komponen perangkat yaitu :

1. Mikrokontroler arduino nano, digunakan sebagai alat pengendali perangkat IoT.
2. Sensor MQ-7, digunakan sebagai pendeteksi atau penangkap gas karbon monoksida (CO).
3. Modul *Wifi* Wemos ISP 6288, digunakan sebagai pengirim data gas CO ke *server* dengan menggunakan koneksi internet *Wifi*.
4. Stepdown modul, untuk mengatur tengan dari adaptor ke mikrokontroler arduino nano dan sensor MQ-7.
5. Adaptor sebagai sumber daya.

Tahapan dalam merancang pembuatan *prototype* dapat dijelaskan melalui *flowchart* berikut ini :



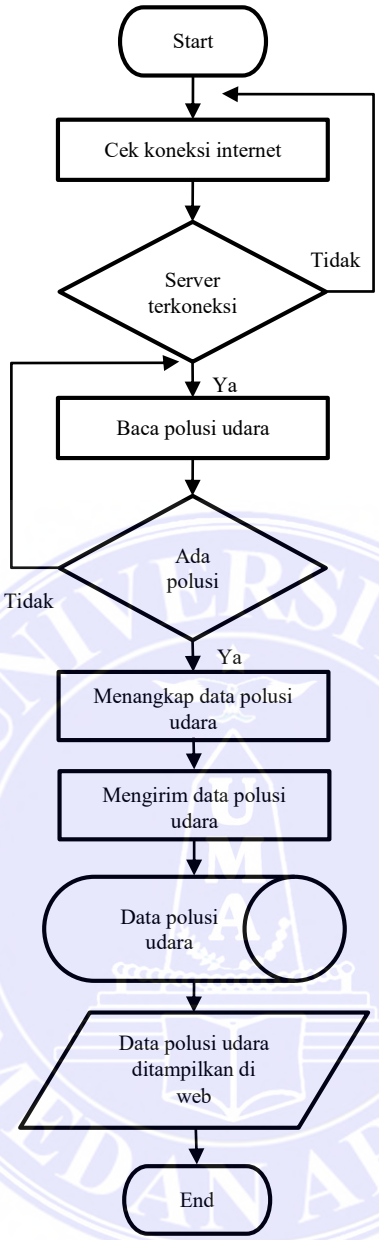
Gambar 3.4 *Flowchart Prototype* Perangkat IoT.

Gambar 3.4, menjelaskan pertama melakukan pemasangan perangkat IoT yang

menggunakan mikrokontroler arduino nano yang dilengkapi dengan sensor pembaca polusi yaitu sensor MQ-7, kemudian dilakukan pengecekan status sensor apakah aktif atau tidak, apabila sensor tidak aktif maka alat akan berhenti, apabila sensor aktif maka akan melakukan koneksi ke modul *Wifi* wemos ISP 6288 kemudian modul *Wifi* akan melakukan koneksi ke *provider*. Jika koneksi gagal makan modeul *Wifi* akan melakukan koneksi ulang dengan waktu *delay* selama 8 detik, apabila berhasil melakukan koneksi maka data polusi yang diperoleh oleh sensor akan dikirimkan ke *server*.

3.3.2 Persiapan Penyimpanan

Adapun persiapan penyimpanan yang pertama dilakukan adalah dengan mempersiapkan *hosting* dengan menyewa *hosting* pada halaman *web* https://www.rumahweb.com yang menyediakan jasa *hosting* dan *domain*, kemudian peneliti membuat nama *domain* yaitu https://www.getudara.com setelah membuat nama *domain* dan *hosting*, tahap selanjutnya adalah membuat *database* dengan menggunakan MySQL.



Gambar 3.5 *Flowchart* Proses Penyimpanan Data.

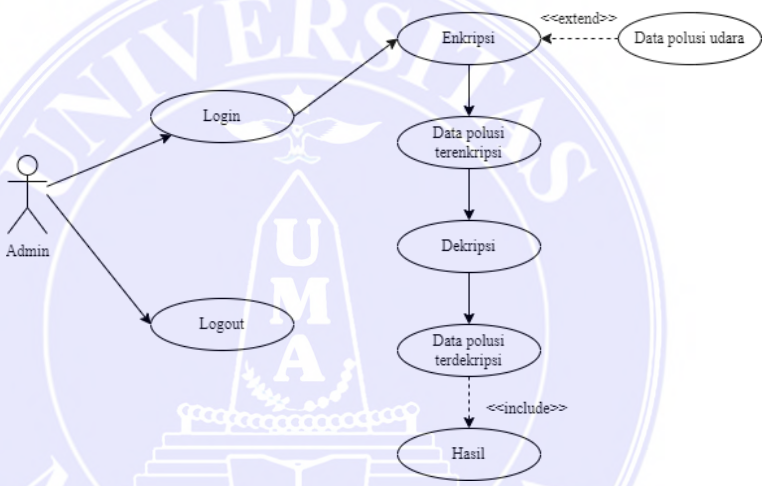
Gambar 3.5, merupakan alur pengiriman data dari *server* ke *web* yang dimulai dari pengecekan koneksi internet, jika *server* tidak terkoneksi internet akan melakukan pengecekan koneksi internet ulang dan jika *server* terkoneksi dengan internet maka akan melakukan proses pembacaan data polusi udara. Jika tidak ada data polusi makan akan melakukan pembacaan data polusi udata ulang dan jika terdapat polusi udara maka akan melakukan proses pemisahan data berdasarkan id_perangkat, lalu data polusi akan disimpan ke dalam *database.* Setelah disimpan data tersebut akan dipanggil dan ditampilkan pada halaman *web*.

3.3.3 Perancangan

Adapun perancangan sistem yang akan dibangun pada penelitian ini menggunakan alur *Use Case Diagram,* perancangan *interface,* perancangan *database* yang dapat dijelaskan sebagai berikut ini.

3.3.3.1 Use Case Diagram

Perancangan sistem pengukur kualitas udara menggunakan *Use Case Diagram* dapat dijelaskan pada gambar 3.8 berikut.



Gambar 3.6 *Use Case Diagram* Penerapan Algoritma RSA Untuk Pengamanan Data.

Pada gambar 3.6, dimulai admin yang dapat melakukan *login* ke sistem atau *logout*. Setelah *login* Admin dapat melakukan proses enkripsi data polusi udara yang berasal dari *database*, enkripsi yang dilakukan menerepkan metode algoritma kriptografi RSA. Data polusi yang terenksipsi (*cipherteks*) akan melalui proses dekripsi algoritma kriptografi RSA. Data polusi yang terdekripsi (*plainteks*) akan menghasilkan pesan atau data polusi udara yang asli.

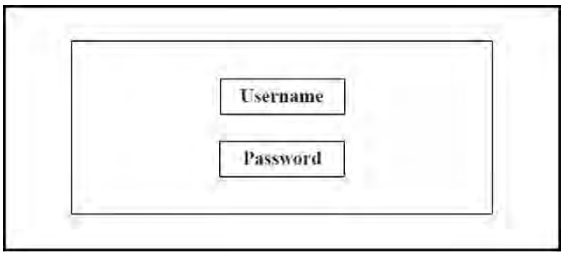
3.3.3.2 Perancangan *Interface*

Perancangan *interface* dapat sistem dapat dijelaskan pada gambar berikut :

1. Menu *Login*

   Pada menu *login* terdapat kolom untuk mengimput username dan password

untuk admin yang dapat dilihat pada gambar 3.7. Setelah admin *login* akan diantarkan ke halaman *home.*



Gambar 3.7 Perancangan Halaman *Login.*

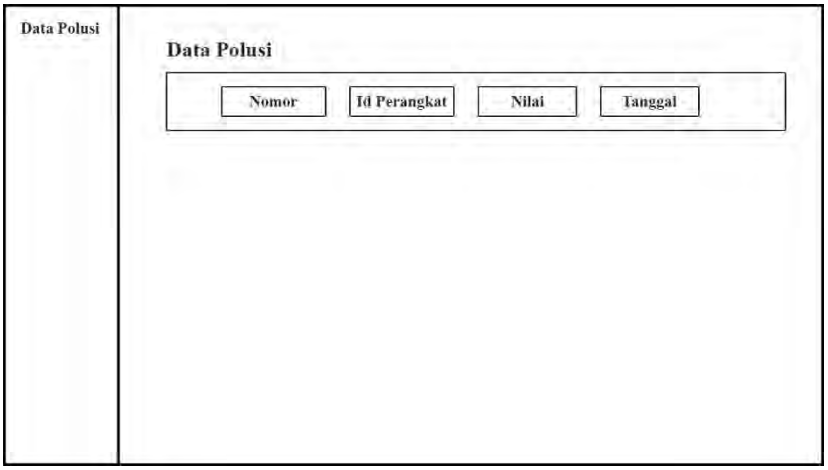
2. Halaman *Home*

Pada halaman *home* akan menampilkan kalimat selamat datang dan gambar serta di sebelah kiri terdapat menu *home*, RSA, data polusi, Fuzzy, dan Bayes yang dapat dilihat pada gambar 3.8 berikut.

Gambar 3.8 Perancangan Halaman *Home.*

3. Menu Data Polusi

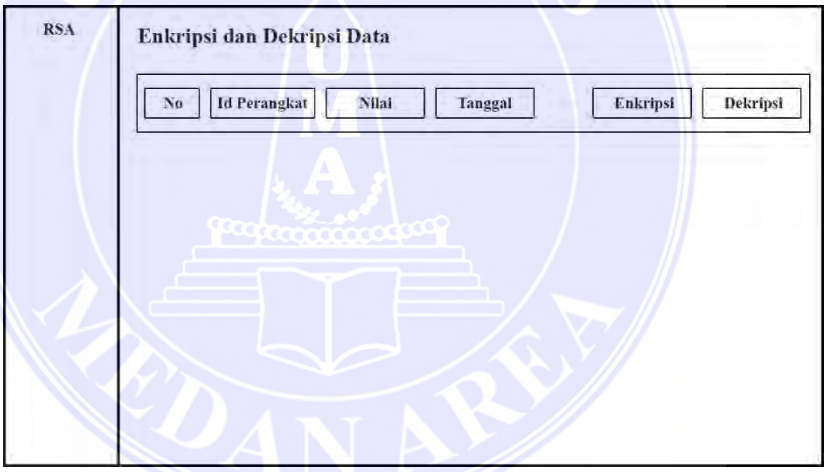
Pada data polusi tedapat tabel yang terdiri dari nomor, Id_perangkat, nilai dan tanggal. Data tersebut diperoleh dari perangkat IoT yang disimpan pada *database* yang dapat dilihat pada gambar 3.9 berikut.



Gambar 3.9 Perancangan Halaman Data Polusi.

4. Menu RSA

Pada menu RSA terdapat tabel no, id_perangkat, nilai, dan tanggal dari *database*. Disebelah kanan tabel terdapat tombol enkripsi dan dekripsi untuk melakukan proses penerapan algoritma RSA yang dapat dilihat pada gambar 3.10.



Gambar 3.10 Perancangan Halaman RSA.

3.3.3.3 Perancangan *database*

Struktur *database* pada alat monitoring kualitas udara yang akan dirancang dapat dilihat pada tabel berikut.

Tabel 3.1 Struktur Tabel *Login*.

No	Nama Field	Tipe	Panjang	Keterangan
1	id_user	int	11	Primery key
2	username	varchar	40	

3	password	varchar	40	
4	ket	varchar	50	

Pada Tabel 3.1 terdapat 4 atribut yaitu *primary key* adalah id_user dengan tipe data *integer* 11 karakter, username dengan tipe data *varchar* 40 karakter, *password* dengan tipe data *varchar* 40 karakter, dan ket dengan tipe data *varchar* 50 karakter.

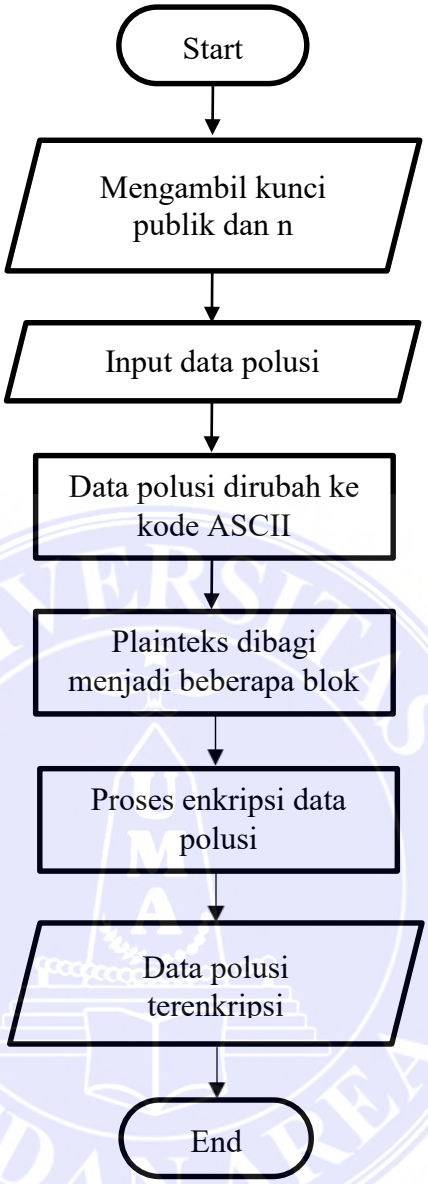
Tabel 3.2 Struktur Tabel Data Polusi.

No	Nama Field	Tipe	Panjang	Keterangan
1	id	int	11	Primery key
2	id_perangkat	varchar	5	
3	nilai	int	11	
4	tanggal	timestamp	-	

Pada tabel 3.2 terdapat 4 atribut yaitu *primery key* id dengan tipe data *integer* 11 karakter, id_perangkat dengan tipe data *varchar* 5 karakter, nilai dengan tipe data *integer* 11 karakter, dan tanggal dengan tipe data *timestamp*.

3.3.3.4 Analisis Data

Adapun analisi data yang dilakukan dengan menggunakan alur *flowchart* diagram berikut.



Gambar 3.11 *Flowchart* Proses Enkripsi.

Pada gambar 3.11, pertama dengan mengambil kunci publik dan *n* dengan melakukan proses pembangkitan kunci, lalu mengimput data polusi udara dari perangkat IoT kemudian data polusi dirubah ke dalam kode ASCII. Setelah dirubah ke dalam kode ASCII data polusi dibagi menjadi beberapa blok untuk melakukan proses enkripsi data polusi dan akan menghasilkan data polusi terenkripsi (*cpiherteks*).

Gambar 3.12 *Flowchart* Proses Dekripsi.

Pada gambar 3.12, mengimput kembali data polusi yang sudah dienkripsi (*cpiherteks*) kemudian data polusi tersebut dibagi kembali menjadi beberapa blok, setelah itu dilakukan proses dekripsi data polusi yang menghasilkan *plainteks* data polusi. *plainteks* data polusi akan dirubah kembali ke dalam kode ASCII. Setelah dirubah ke dalam kode ASCII data polusi udara akan menghasilkan pesan atau data polusi udara yang asli.

Adapun analisis data yang dilakukan dengan menerapkan algoritma RSA yang dimulai dari tahapan-tahapan pembangkitan kunci, enkripsi, dan dekripsi yang dapat dijelaskan dengan contoh studi kasus berikut.

A. Proses pembangkitan kunci

1. Memilih dua bilangan prima besar secara acak :

   p : 37, (bilangan prima)

q : 61, (bilangan prima)

2. Menghitung $n = p \times q$
   $n = 37 \times 61$
   $n = 2257$
3. Menghitung $\phi(n) = (p - 1) \times (q - 1)$
   $\phi(n) = (37-1) \times (61-1)$
   $\phi(n) = 36 \times 60$
   $\phi(n) = 2160$
4. Menghitung *e* yang relatif prima terhadap $\phi(n)$. Nilai $gcd(e, \phi(n)) = 1$, *e* harus bernilai 1. Untuk menemukan nilai kunci publik (*e*) dapat ditunjukkan pada tabel perhitungan dibawah.

Tabel 3.3 Perhitungan Nilai Kunci Publik.

Nilai bilangan prima	gcd(*e*, 2160) = 1
2	2160 mod 2 = 0 gcd(2, 2160) = 0
3	2160 mod 3 = 0 gcd(3, 2160) = 0
5	2160 mod 5 = 0 gcd(5, 2160) = 0
7	2160 mod 7 = 4 gcd(7, 2160) = 4
11	2160 mod 11 = 4 gcd(11, 2160) = 4
13	2160 mod 13 = 2 gcd(13, 2160) = 2
17	2160 mod 17 = 1 gcd(17, 2160) = 1

Jadi nilai kunci publik (*e*) yang diperoleh adalah 17.

5. Menghitung kunci privat (*d*), dengan menggunakan persamaan $d = \frac{1+k\phi(n)}{e}$. Nilai *k* dapat dihitung dengan mencoba nilai-nilai = 1,2,3,4,... sehingga diperoleh nilai *d* bilangan bulat. Untuk menemukan nilai kunci privat (*d*) dapat ditunjukkan pada tabel perhitungan dibawah.

Tabel. 3.4 Perhitungan Nilai Kunci Privat.

Nilai	$d = \frac{1 + k\phi(n)}{e}$	Hasil
1	$d = \frac{1 + 1.2160}{17}$	127.117647055882
2	$d = \frac{1 + 2.2160}{17}$	254.17647058823
3	$d = \frac{1 + 3.2160}{17}$	381.23529411764
4	$d = \frac{1 + 4.2160}{17}$	508.23529411764
5	$d = \frac{1 + 5.2160}{17}$	635.35294117647
6	$d = \frac{1 + 6.2160}{17}$	762.41176470588
7	$d = \frac{1 + 7.2160}{17}$	889.47058823529
8	$d = \frac{1 + 8.2160}{17}$	1016.5294117647
9	$d = \frac{1 + 9.2160}{17}$	1143.588235241
10	$d = \frac{1 + 10.2160}{17}$	1270.6470588235
11	$d = \frac{1 + 11.2160}{17}$	1396.7058823529
12	$d = \frac{1 + 12.2160}{17}$	1524.7647058823
13	$d = \frac{1 + 13.2160}{17}$	1651.8235294117
14	$d = \frac{1 + 14.2160}{17}$	1778.8823529411
15	$d = \frac{1 + 15.2160}{17}$	1905.9411764705
16	$d = \frac{1 + 16.2160}{17}$	2033

Jadi nilai kunci privat (d) yang diperoleh adalah 2033

Dari perhitungan tersebut diperoleh kunci publik (17, 2257) dan kunci privat

(2033, 2257). Kunci publik dan kunci privat akan digunakan untuk proses enkripsi dan dekripsi pada algoritma RSA .

B. Proses Enkripsi

Setelah melakukan proses pembangkitan kunci selanjutnya melakukan proses enkripsi pesan, misal menggunakan pesan : "KAMIS"

Table 3.5 Proses Enkripsi Pesan.

Pesan	K	A	M	I	S
ASCII	75	65	77	73	83

Plaintext : 7565777383

Kemudian dipecah menjadi 4 blok yang berisi 3 digit :

Tabel 3.6 *Plaintext* Pesan.

Plainteks	756	577	738	003

$C1 = 756^{17} \bmod 2257 = 2005$
$C2 = 577^{17} \bmod 2257 = 1929$
$C3 = 738^{17} \bmod 2257 = 1129$
$C4 = 003^{17} \bmod 2257 = 1394$
Jadi *ciphertext* yang dihasilkan adalah :

Tabel 3.7 *Ciphertext* Pesan.

Cipherteks	2005	1929	1129	1394

C. Proses Dekripsi

Selanjutnya *ciphertext* tersebut didekripsi agar kembali ke pesan aslinya dengan menggunakan kunci privat sebagai berikut :

$P1 = 2005^{2033} \bmod 2257 = 756$
$P2 = 1929^{2033} \bmod 2257 = 577$
$P3 = 1129^{2033} \bmod 2257 = 738$
$P4 = 1394^{2033} \bmod 2257 = 3$

Plaintext : 7565777383

Blok *plaintext* yang lain dikembalikan dengan cara serupa. Akhirnya diperoleh kembali *plaintext* semula.

Tabel 3.8 *Plaintext* Pesan Semula.

ASCII	75	65	77	73	83
PESAN	K	A	M	I	S

Jadi pesan awal yang telah melalui proses enkripsi dan dekripsi akan menghasilkan pesan semula yaitu "KAMIS".

BAB V
KESIMPULAN DAN SARAN

5.1 Kesimpulan

Berdasarkan hasil dan pembahasan dalam penelitian ini dapat diambil kesimpulkan bahwa :

1. Penerapan algoritma RSA untuk proses enkripsi dan dekripsi berhasil dilakukan pada semua *dataset* yang tersimpan pada *database* di *server*, namun proses enkripsi dan dekripsi dilakukan belum secara *realtime* melainkan melalui tombol proses yang disediakan pada antar muka sistem monitoring polusi udara.
2. Pada proses algoritma RSA hanya dapat menggunakan panjang *n* hanya 64 bit.
3. Pada proses enkripsi dan dekripsi sistem akan memakan waktu 3 menit dikarenakan banyaknya data polusi yang diproses.

5.2 Saran

Adapun saran yang diusulkan untuk pengembangan sistem ini adalah sebagai berikut :

1. Perlunya proses enkripsi dan dekripsi yang dapat dilakukan secara *realtime*.
2. Panjang *n* lebih besar dari 1024 bit agar pengamanan lebih kuat dan aman.

DAFTAR PUSTAKA

Abri Montgomery Blackstone, R. K. (2022). Implementasi Projek Uji Berkala Kendaraan Angkutan Umum Dalam Meningkatkan Kualitas Udara Di Kota Medan. *Jurnal Professional*, 277-284.

Badrul Anwar, N. B. (2019). Implementasi Algortima RSA Terhadap Keamanan Data Simpan Pinjam. *Sains dan Komputer*, 30-34.

Deni Hamdani, J. (2020). Modifikasi Karakter Kode Pada Cipher Hill Menggunakan Kode ASCII. *Eigen Mathematics Journal*, 23-28.

Febyana Nur Yahya, A. A. (2020). Pengembangan Sistem Manajemen Proyek dan Akun Hosting di Software House Berbasis Web (Studi Kasus Elecomp Software House). *Jurnal Pengembangan Teknologi Informasi dan Ilmu Komputer*, 4291-4299.

Haslinda, H. B. (2019). Perancangan Sistem Informasi Penyewaan Alat Berat Pada CV. Tri Daya Jaya Makassar. *MediaTIK*, 1-7.

Indrayani, S. A. (2018). Pencemaran Udara Akibat Kinerja Lalu-Lintas Kendaraan Bermotor Di Kota Medan. *Jurnal Permukiman*, 13-20.

Jaka Prayudha, A. P. (2018). Implementasi Metode Fuzzy Logic Untuk Sistem Pengukuran Kualitas Udara Di Kota Medan Berbasis Internet Of Things (IOT). *Jurnal Teknologi dan Sistem Informasi*, 141-148.

Jonson Manurung, K. S. (2018). Penerapan Algoritma RSA Untuk Pengamanan File. *Jurnal Mantik Penusa*, 112-116.

Khesya, N. (2021). Mengenal Flowchart Dan Pseudcode Dalam Algoritma Dan Pemrograman. *PMM FITK UINSU*, 1-15.

Lutfi Pratama, S. (2018). Pengamanan Tabel Database Menggunakan Kriptografi Algoritma RSA. *SKANIKA*, 925-930.

Muhammad Ridwan Rambe, E. V. (2019). Aplikasi Pengamanan Data dan Disisipkan Pada Gambar Dengan Algoritma RSA dan Modified LSB Berbasis Android. *IT Jurnal*, 51-62.

Novelan, M. S. (2020). Sistem Monitoring Kualitas Udara Dalam Ruangan Menggunakan Mikrokontroler dan Aplikasi Android. *InfoTekJar :Jurnal Nasional Informatika dan Teknologi Jaringan*, 50-54.

Prihandoyo, M. T. (2018). Unified Modeling Language (UML) Model Untuk Pengembangan Sistem Informasi Akademik Berbasis Web. *Jurnal Informatika: Jurnal Pengembangan IT*, 126-129.

Rachamat Adi Purnama, A. T. (2018). Aplikasi Web Server Berbasis Bahasa C SHARP. *Jurnal Teknologi Komputer*, 21-29.

Rahmat Sulaiman, M. V. (2018). Peningkatan keamana Pesan Berbasis Android Menggunakan Algoritma kriptografi RSA. *Jurnal SISFOKOM*, 116-120.

Ramadhani, A. (2018). Keamanan Informasi. *Journal of Information and Library Studies*, 39-51.

Ririn Aswandi, P. R. (2020). Perlindungan Data Dan Informasi Pribada Melalui

Indonesian Data Protection System (IDPS). *LEGISLATIF*, 167-190.

Sebastian Suhandinata, R. A. (2019). Analisis Performa Kriptografi Hybrid Algoritma Blowfish dan Algoritma RSA. *Jurnal Teknologi dan Sistem Informasi*, 1-10.

Setiyani, L. (2021). Desain Sistem : Use Case Diagram. *Seminar Nasional : Inovasi & Adopsi Teknologi*, 246-260.

Sudaria, A. S. (2021). Sistem Manajemen Pelayanan Pelanggan Menggunakan PHP Dan MySLQ (Studi Kasus pada Toko Surya). *TEKINFO*, 100-117.

Susanto. (2018). Penerapan Algoritma Asimetris RSA Untuk Keamanan Data Pada Aplikasi Penjualan CV. Sinergi Komputer Lubuklinggau Berbasis Web. *Jurnal SIMETRIS*, 1043-1052.

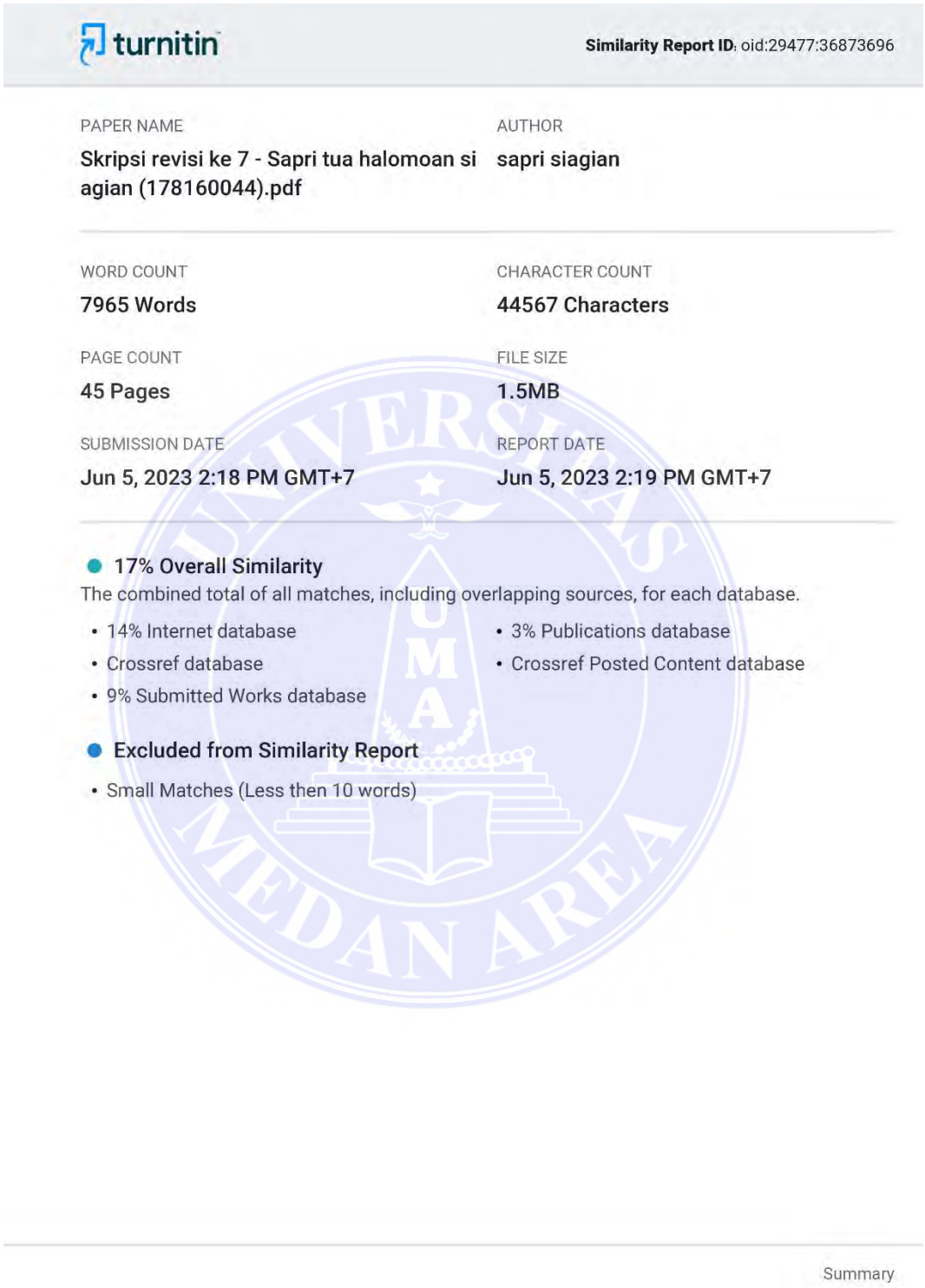
Susilawati. (2018). Perancangan Kunci Public RSA dan ElGamal pada Kriptografi untuk Kemananan Informasi. *Journa Of Imformatics Ana Telecommunication Engineering*, 82-89.

Toni Nur Hakim, M. F. (2020). Sistem Monitoring Kualitas Udara Berbasis Internet of Things. *Industrial Research Workshop and National Seminar*, 496-502.

Wilianto, A. K. (2018). Sejarah, Cara Kerja Dan Manfaat Internet Of Things. *Matrix : Jurnal Manajemen Teknologi dan Informatika*, 36-41.

Yudin Wahyudin, D. N. (2020). Analisis Metode Pengembangan Sistem Informasi Berbasis Website: A Literatur Review. *Jurnal Interkom: Jurnal Publikasi Ilmiah Bidang Teknologi Informasi dan Komunikasi*, 119-133.

LAMPIRAN



turnitin

Similarity Report ID: oid:29477:36873696

PAPER NAME
Skripsi revisi ke 7 - Sapri tua halomoan si agian (178160044).pdf

AUTHOR
sapri siagian

WORD COUNT
7965 Words

CHARACTER COUNT
44567 Characters

PAGE COUNT
45 Pages

FILE SIZE
1.5MB

SUBMISSION DATE
Jun 5, 2023 2:18 PM GMT+7

REPORT DATE
Jun 5, 2023 2:19 PM GMT+7

17% Overall Similarity
The combined total of all matches, including overlapping sources, for each database.

- 14% Internet database
- Crossref database
- 9% Submitted Works database
- 3% Publications database
- Crossref Posted Content database

Excluded from Similarity Report

- Small Matches (Less then 10 words)

Summary

Source Code

Proses Enkripsi

```php
<?php

if(isset($_POST['enkrip']))
{
//Proses RSA (Encript)
$pp=$_POST["p"];
$qq=$_POST["q"];
$nn=$pp*$qq;
$mm=($pp-1)*($qq-1);

echo "p = ".$pp."<br>";
echo "q = ".$qq."<br>";
echo "n = ".$nn."<br>";
echo "m = ".$mm."<br>";

$p=3;
$q=11;
$n=$p*$q;
$m=($p-1)*($q-1);

$e=0;
$d=0;
for($i=1;$i<=$n;$i++){
    $a=0;
    for($j=1;$j<=$i;$j++){
        if($i%$j==0){
            $a++;
    }
    }
    if($a==2){
        $gcd=$m%$i;
        if($gcd==1){
            $e=$i;
        }
    }
    }
    $e=7;
    $aa=0;
    for($ii=1;$ii<=2000;$ii++){
        $a++;
        $key_d=(1+($ii*$m))/$e;
        $key_d_len=strlen($key_d);
        $key_d_integer=substr($key_d,0,$key_d_len);
```

```
        $ket="";
        for($jj=0;$jj<=$key_d_len;$jj++){
            $kata=substr($key_d,$jj,1);
            if($kata=="."){
                $ket="decimal";
            break;
            }else{
                $ket="bulat";
            }
            }
            if($ket=="bulat"){
            $d=$key_d;
            break;
            }
            }
            echo "e = ".$e."<br>";
            echo "d = ".$d."<br><br>";

            $query_data=mysqli_query($koneksi,"SELECT * FROM data_rsa where status='Buka'
order by id asc");
            while($data=mysqli_fetch_array($query_data)){
            echo "ID PERANGKAT<br>";
            $ci_text_id_perangkat="";
            $id_perangkat=$data["id_perangkat"];
            echo "Plaintext = ". $id_perangkat."<br>";
            $pjg_id_perangkat=strlen($id_perangkat);
            for ($nm=0;$nm<=$pjg_id_perangkat-1;$nm++){
                $id_p=substr($id_perangkat,$nm,1);
                $id_per=$id_p*1;
                $c_id_perangkat=pow($id_per,$e)%$n;

                if($ci_text_id_perangkat==""){
                    $ci_text_id_perangkat=$ci_text_id_perangkat.$c_id_perangkat;
                }else{
                    $ci_text_id_perangkat=$ci_text_id_perangkat."9909".$c_id_perangkat;
                    }
                }
                echo "Cippertext = ". $ci_text_id_perangkat."<br>";

            echo "<br>NILAI<br>";
            $ci_text_nilai="";
            $nilai=$data["nilai"];
            echo "Plaintext = ". $nilai."<br>";
            $pjg_nilai=strlen($nilai);
                for ($nn=0;$nn<=$pjg_nilai-1;$nn++){
                    $nil=substr($nilai,$nn,1);
                    $nila=$nil*1;
```

```
                    $c_nilai=pow($nila,$e)%$n;
                    echo "C=".$nila ." = ". $nila."^".$e." mod ".$n." = ".$c_nilai."<br>";

                    if($ci_text_nilai==""){
                        $ci_text_nilai=$ci_text_nilai.$c_nilai;
                    }else{
                        $ci_text_nilai=$ci_text_nilai."9909".$c_nilai;
                    }

                    }
                    echo "Cippertext = ". $ci_text_nilai."<br>";

                    echo "<br>";

                    mysqli_query($koneksi,"UPDATE data_rsa SET
id_perangkat='".$ci_text_id_perangkat."', nilai='".$ci_text_nilai."',
                    status='Kunci', p='".$pp."', q='".$qq."', n='".$n."', e='".$e."',
d='".$d."' WHERE id='".$data["id"]."'");
                }
            echo "<script>document.location='?halaman=rsa';</script>";
            }
?>
```

Proses Dekripsi

```
<?php
if (isset($_POST['dekrip']))
{
$query_cek=mysqli_query($koneksi,"SELECT * FROM data_rsa where status='Kunci' and
p='".$_POST["p"]."' and q='".$_POST["q"]."'");
if(mysqli_num_rows($query_cek)>0){
    //Proses RSA (Decript)
    $pp=$_POST["p"];
    $qq=$_POST["q"];
    $nn=$pp*$qq;
    $mm=($pp-1)*($qq-1);

    echo "p = ".$pp."<br>";
    echo "q = ".$qq."<br>";
    echo "n = ".$nn."<br>";
    echo "m = ".$mm."<br>";

    $p=3;
    $q=11;
    $n=$p*$q;
    $m=($p-1)*($q-1);
```

```
    $e=0;
    $d=0;
    for($i=1;$i<=$n;$i++){
        $a=0;
    for($j=1;$j<=$i;$j++){
        if($i%$j==0){
            $a++;
        }
    }
        if($a==2){
            $gcd=$m%$i;
        if($gcd==1){
            \$e=$i;
        }
    }
    }
    $e=7;
    $aa=0;
        for($ii=1;$ii<=2000;$ii++){
            $a++;
            $key_d=(1+($ii*$m))/$e;
            $key_d_len=strlen($key_d);
            $key_d_integer=substr($key_d,0,$key_d_len);
            $ket="";
        for($jj=0;$jj<=$key_d_len;$jj++){
            $kata=substr($key_d,$jj,1);
            if($kata=="."){
                $ket="decimal";
            break;
            }else{
                $ket="bulat";
            }
            }
            if($ket=="bulat"){
                $d=$key_d;
            break;
            }
            }
            echo "e = ".$e."<br>";

            echo "d = ".$d."<br><br>";

            $query_data=mysqli_query($koneksi,"SELECT * FROM data_rsa where status='Kunci'
and p='".$_POST["p"]."' and q='".$_POST["q"]."' order by id asc");
            while($data=mysqli_fetch_array($query_data)){
            echo "<br>ID PERANGKAT<br>";
```


Document Accepted 3/8/23

Access From (repository.uma.ac.id)3/8/23

```
                $pl_text_id_perangkat="";
                $id_perangkat=$data["id_perangkat"];
                $id_perangkat=str_replace("9909",",",$id_perangkat);
                echo "Chippertext = ". $id_perangkat."<br>";
                $id_perangkat9=explode(",",$id_perangkat);
                $pjg_id_perangkat=count($id_perangkat9);
                for ($nn=0;$nn<=$pjg_id_perangkat-1;$nn++){
                    $per=$id_perangkat9[$nn];
                    $perang=$per*1;
                    echo $perang."<br>";
                    $pl_id_perangkat=pow($perang,$d)%$n;
                    echo "PL=".$perang ." = ". $perang."^".$e." mod ".$n." =
".$pl_id_perangkat."<br>";
                    $pl_text_id_perangkat=$pl_text_id_perangkat.$pl_id_perangkat;

                    }
                    echo "Plaintext = ". $pl_text_id_perangkat."<br>";

                    echo "<br>NILAI<br>";
                    $pl_text_nilai="";
                    $nilai=$data["nilai"];
                    echo "Chippertext = ". $nilai."<br>";
                    $nilai=str_replace("9909",",",$nilai);
                    echo "Chippertext = ". $nilai."<br>";
                    $nilai9=explode(",",$nilai);
                    $pjg_nilai=count($nilai9);
                    for ($nn=0;$nn<=$pjg_nilai-1;$nn++){
                        $nil=$nilai9[$nn];
                        $nila=$nil*1;
                        echo $nila."<br>";
                        $pl_nilai=pow($nila,$d)%$n;
                        echo "PL=".$nila ." = ". $nila."^".$e." mod ".$n." =
".$pl_nilai."<br>";
                            $pl_text_nilai=$pl_text_nilai.$pl_nilai;
                        }
                        echo "Plaintext = ". $pl_text_nilai."<br>";

                        echo "<br>";

                        mysqli_query($koneksi,"UPDATE data_rsa SET
id_perangkat='".$pl_text_id_perangkat."', nilai='".$pl_text_nilai."', status='Buka',
p='0', q='0', n='0', e='0', d='0' WHERE id='".$data["id"]."'");
                    }
                echo "<script>document.location='?halaman=rsa';</script>";
            }else{
                echo "<script>alert('nilai p dan q
salah');document.location='?halaman=rsa';</script>";
```

```
            }
        }
?>
```

UNIVERSITAS MEDAN AREA
FAKULTAS TEKNIK
Kampus I : Jalan Kolam Nomor 1 Medan Estate/Jalan PBSI Nomor 1 ☎(061) 7366878, 7360168, 7364348, 7366781, Fax.(061) 7366998 Medan 20223
Kampus II : Jalan Setiabudi Nomor 79 / Jalan Sei Serayu Nomor 70 A, ☎ (061) 8225602, Fax. (061) 8226331 Medan 20122
Website: www.teknik.uma.ac.id E-mail: univ_medanarea@uma.ac.id

Nomor : 204/FT.6/01.10/VII/2022 **23 Juli 2022**
Lamp : -
H a l : **Perpanjang SK Pembimbing Tugas Akhir**

Yth. Pembimbing Tugas Akhir
Susilawati, S.Kom, M.Kom
Nurul Khairina, S. Kom, M. Kom
di
Tempat

Dengan hormat,
Sehubungan telah berakhirnya waktu masa berlaku SK pembimbing nomor 44/FT.6/01.10/V/2021 tertanggal 7 Mei 2021 maka perlu diterbitkan kembali SK Pembimbing Skripsi baru atas nama mahasiswa berikut :

N a m a : Sapri Tua Halomoan Siagian
N P M : 178160044
Jurusan : Informatika

Oleh karena itu kami mengharapkan kesediaan saudara :

1. Susilawati, S.Kom, M.Kom (Sebagai Pembimbing I)
2. Nurul Khairina, S. Kom, M. Kom (Sebagai Pembimbing II)

Adapun Tugas Akhir Skripsi berjudul :

"Sistem Pengamanan Pengiriman Data Monitoring Kualitas Udara di Kota Medan Menggunakan Algoritma Kriptografi RSA"

SK Pembimbing ini berlaku selama enam bulan terhitung sejak SK ini diterbitkan. Jika proses pembimbing melebihi batas waktu yang telah ditetapkan, SK ini dapat ditinjau ulang.

Demikian kami sampaikan, atas kesediaan saudara diucapkan terima kasih.

Dekan,

Dr. Rahmad Syah, S. Kom, M. Kom

UNIVERSITAS MEDAN AREA
FAKULTAS TEKNIK

Kampus I : Jalan Kolam Nomor 1 Medan Estate/Jalan PBSI Nomor 1☎(061) 7366878, 7360168, 7364348, 7366781, Fax.(061) 7366998 Medan 20223
Kampus II : Jalan Setiabudi Nomor 79 / Jalan Sei Serayu Nomor 70 A, ☎ (061) 8225602, Fax. (061) 8226331 Medan 20122
Website: www.teknik.uma.ac.id E-mail: univ_medanarea@uma.ac.id

Nomor : 178/FT.6/01.10/X/2021 25 Oktober 2021
Lamp : -
H a l : **Penelitian Dan Pengambilan Data Tugas Akhir**

Yth. Pimpinan PT. Kolibri Indonesia
Jl. Yos Sudarso Lorong 14C
Di
Medan

Dengan hormat,
Kami mohon kesediaan Bapak/Ibu berkenan untuk memberikan izin dan kesempatan kepada mahasiswa kami tersebut dibawah ini :

NO	N A M A	N P M	PRODI
1	Sapri Tua Halomoan Siagian	178160044	Informatika

Untuk melaksanakan Penelitian dan Pengambilan Data Tugas Akhir pada perusahaan/Instansi yang Bapak/Ibu Pimpin.

Perlu kami jelaskan bahwa Pengambilan Data tersebut adalah semata-mata untuk tujuan ilmiah dan Skripsi yang merupakan salah satu syarat bagi mahasiswa tersebut untuk mengikuti ujian sarjana lengkap pada Fakultas Teknik Universitas Medan Area dan tidak untuk dipublikasikan, dengan judul penelitian :

Sitem Pengamanan Pengiriman Data Monitoring Kualitas Udara di Kota Medan Menggunakan Algoritma Kriptografi RSA

Atas perhatian dan kerja sama yang baik diucapkan terima kasih.

Dekan,

Dr. Ir. Dina Maizana, MT

Tembusan :
1. Ka. BAMAI
2. Mahasiswa
3. File

PT. Kolibri Indonesia
Jl. Yos Sudaso Lr XIV C.
Glugur Darat, Medan Barat, Sumatera Utara 20116

Online your Effort
http://www.kolibriindonesia.com
e-mail : marketing@kolibriindonesia.com

Medan, 25 Januari 2022

Nomor : 073 / KLBR.02/I/2022
Lamp. : -
Perihal : Surat selesai penelitian

Kepada Yth.
Dekan Fakultas Teknik
Universitas Medan Area
Di
Tempat.

Dengan hormat, Bersama ini kami sampaikan bahwa mahasiswa yang tersebut di bawah ini :

NO	Mahasiswa	NPM	Judul Penelitian
1	Johannes K Siahaan	178160092	Penerapan Metode Naive Bayes Untuk Menentukan Tingkat Polusi Udara di Kota Medan
2	Prayogi Permana	178160008	Penerapan Algoritma Fuzzy Mamdani untuk Menentukan Kualitas Udara di Kota Medan
3	Sapri Tua Halomoan Siagian	178160044	Penerapan Kriptografi RSA Untuk Pengamanan Data Monitoring Kuliatas Udara di Kota Medan
4	Theofil Tri Saputra Sibarani	178160076	Pemodelan dan Analisis Perangkat Keras Untuk Monitoring Kualitas Udara di Kota Medan berbasis Internet of Things (IoT)

Adalah benar telah menyelesaikan penelitian untuk memenuhi syarat dalam menyelesaikan studinya di laboratorium teknis PT. Kolibri Indonesia. Penelitian tersebut telah dilaksanakan mulai bulan Novemver 2021 sampai dengan Januari 2022

Demikian surat ini disampaikan untuk dapat diketahui dan dipergunakan seperlunya.

Direktur
PT Kolibri Indonesia

Stephanus Priyowidodo, M. Kom

Tembusan :
- File